servicenow

Gestão de Segurança de Washington DC

Última atualização: 17/12/2025

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A tradução automática pode proporcionar uma ideia básica do conteúdo em um idioma que você entende. Ela é totalmente automatizada e não envolve intervenção humana. A qualidade e a precisão da tradução automática podem variar significativamente de um texto para outro e entre diferentes pares de idiomas. A ServiceNow não garante a precisão e não se responsabiliza por possíveis erros. Alguns conteúdos (como imagens, vídeos, arquivos etc.) podem não ser traduzidos devido a limitações técnicas do sistema.

Alguns exemplos e gráficos aqui representados são fornecidos somente para fins de ilustração. Nenhuma associação ou conexão real com produtos ou serviços ServiceNow é intencional ou deve ser inferida.

ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow
são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas e
de produtos podem ser marcas comerciais das respectivas empresas
às quais estão associados.

Leia os Termos de Uso do Site do ServiceNow em www.servicenow.com/terms-of-use.html

Tradução automática

Sede da empresa
2225 Lawson Lane
Santa Clara, CA 95054
Estados Unidos
(408) 501-8550

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Índice

Security Operations **6**

Noções básicas do Security Operations 12

O pacote Security Operations de aplicações 14

Security Operations cenários e exemplos 21
[store-future: BEGIN review]

Reduza o tempo de análise de ameaças usando automação 21
[store-future: BEGIN review]
[End]

Priorizar vulnerabilidades de alto perfil 27
[store-future: BEGIN review]
[End]

[End]

Security Operations e o ServiceNow Store 30

Baixe uma aplicação de ServiceNow Store pela primeira vez 30

Instalar uma integração Security Operations 36

Atualizar uma aplicação baixada anteriormente do ServiceNow Store 40

Atualize sua instância para a próxima versão da família 41

Painel executivo de segurança cibernética 41

Aceitação de pontuações de parâmetro de comparação 56

Definir metas 57

Security Simulation and Training Integration for Security Operations 57

Security Incident Response 60

Noções básicas do Security Incident Response 61

Configuração do Security Incident Response 69

Espaço de resposta a incidentes de segurança 154

Criação de incidente de segurança 263

Gerenciar Predictive Intelligence para phishing relatado pelo usuário 303

Configurar Predictive Intelligence for User Reported Phishing 307

Atribuição de analistas de segurança 310

Gerenciamento de incidentes de segurança e solicitações de entrada 314

Gerenciar ameaças à segurança usando o Espaço do analista de segurança 381

Recursos do Playbook 408

Relatório do Security Incident Response 533

Gestão de incidentes graves de segurança 543

Integrações do Security Incident Response 671

Experiência Móvel para Security Incident Response 1346

Orquestração de resposta de incidente de segurança 1384

Modelos de fluxo do Security Incident Response 1418
[store-future: BEGIN review]
[End]

Controle de posturas de segurança 1435

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorar o Controle de posturas de segurança....1436
Vulnerability Response....1486
Explorando a aplicação Vulnerability Response 1487
Implementação de Vulnerability Response....1557
Integrações do Vulnerability Response....1705
Vulnerability Response Espaços....1968
Vulnerability Response visão geral da correção....2098
Soluções de análise e relatório para Vulnerability Response....2202
Vulnerability Response informações de referência....2251
Experiência de dispositivos móveis Vulnerability Response....2293
Orquestração do Vulnerability Response....2315
Application Vulnerability Response....2320
Explorar o Application Vulnerability Response....2321
Configuração do Application Vulnerability Response....2326
Integração do Application Vulnerability Response a outras aplicações....2359
Corrigindo Application Vulnerability Response vulnerabilidades....2400
Soluções Análise da plataforma para Application Vulnerability Response 2445
referências de Application Vulnerability Response 2457
Exibição de produto do Application Vulnerability Response....2482
Vulnerability Response contêiner....2484
Explorar o Vulnerability Response contêiner....2494
Configuração do Vulnerability Response contêiner....2496
Integração do Vulnerability Response contêiner a outras aplicações....2502
Correção de vulnerabilidades de contêiner....2508
Soluções de análise e relatório para Vulnerability Response contêiner 2528
Referência do Vulnerability Response contêiner....2537
Configuration Compliance....2545
Explorar o Configuration Compliance....2547
Instalando, instalando e configurando a aplicação Configuration Compliance 2575
Integrações do Configuration Compliance....2628
Configuration Compliance correção....2720
Análise e relatório para Configuration Compliance....2752
Configuration Compliance informações de referência....2765
Comum do Vulnerability Response....2793
Estrutura de relatórios agregados....2794
Inteligência contra ameaças....2800
Noções básicas do Inteligência contra ameaças....2801
Configurar Inteligência contra ameaças....2806
Repositório LOC....2822
MITRE-ATT&CK™ visão geral da estrutura do....2866
Administração do Inteligência contra ameaças....2934
Integrações do Inteligência contra ameaças....2936

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Orquestração de inteligência contra ameaças....3001
Security Case Management....3006
Security Operations funcionalidade comum....3037
Criar e definir grupos de filtros no Security Operations....3040
Transformação de dados compartilhados....3042
Security Operations processamento de e-mail....3045
Security Operations mapeamento de campo....3056
Security Operations transformações de valor de campo....3060
Security Operations mapeamento de dados de aprimoramento....3061
Security Operations escalação definida pelo usuário....3064
Criar substituições de propriedade separadas por domínio....3065
Criar um grupo de sistemas operacionais....3066
Configurar grupos de marcadores de segurança e marcadores....3068
Anotações de segurança....3072
Componentes instalados com Security Support Common....3074
Acesso ao módulo por função para aplicações Security Operations....3075
[store-future: BEGIN review]
[End]
Pesquisar Security Operations....3730
Referência do Security Operations Integrations....3730
Security Operations gatilhos de fluxo de trabalho....3867
Orquestração do Security Operations....3869
Data Loss Prevention Incident Response....3882
Explorar o Data Loss Prevention Incident Response....3883
Instalando e configurando o DLP IR Incident Response....3885
DLP Incident Response Administration....3886
Data Loss Prevention Incident Response Gestão de incidentes....3938
Integração de entrada para Data Loss Prevention Incident Response....3955
Integrações do DLP....3958
Lista de materiais de software....3999
Explorar o Lista de materiais de software....4000

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Security Operations

ServiceNow® Security Operations O traz dados de incidentes de suas ferramentas de segurança para um mecanismo de resposta estruturado que usa fluxos de trabalho inteligentes, automação e uma conexão profunda com a TI para priorizar e resolver ameaças com base no impacto que elas representam para a organização.

Automatize todas as suas ferramentas de segurança e trabalhe perfeitamente com a TI

Com Security Operations, aproveite todo o valor da sua solução Now Platform®. Muitas organizações têm dificuldade em identificar ameaças e vulnerabilidades à segurança, priorizá-las e coordenar com a TI para corrigi-las. Usando Security Operations, os analistas de segurança e os gerentes de vulnerabilidade podem automatizar perfeitamente suas ferramentas de segurança e se comunicar com a TI trabalhando em uma plataforma unificada.

Exiba e baixe o cartão de informações completo para um destaque dos recursos de Security Operations .

	Identificar, priorizar e corrigir vulnerabilidades em software, sistemas operacionais e ativos A aplicação ServiceNow® Vulnerability Response ajuda as organizações a identificar e responder de forma rápida e eficiente a vulnerabilidades. Verifique os dados dos principais fornecedores para fornecer às suas equipes uma plataforma única de resposta que possa ser compartilhada entre a segurança e a TI para resolver vulnerabilidades.
	Identificar, priorizar e corrigir incidentes de segurança críticos A aplicação ServiceNow® Security Incident Response simplifica o processo de identificação de incidentes críticos aplicando fluxo de trabalho avançado e ferramentas de automação que aceleram a correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Identificar, priorizar e corrigir ativos configurados incorretamente

A aplicação ServiceNow® Configuration Compliance prioriza e corrige ativos configurados incorretamente usando dados coletados de verificações de avaliação de configuração de segurança de terceiros.

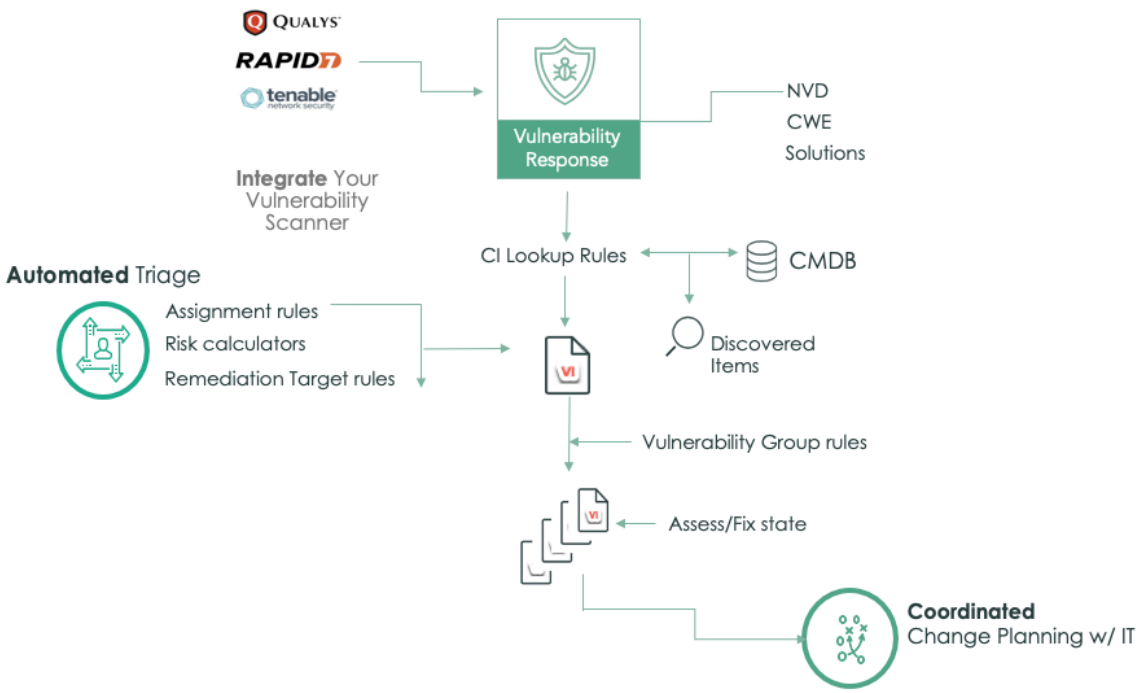
Acesse os dados da Expressão de informações de ameaças estruturadas (STIX) da sua empresa

A aplicação ServiceNow® Inteligência contra ameaças ajuda os respondentes do incidente a encontrar Indicadores de compromisso (IoC) e a procurar ataques e ameaças de baixa visibilidade. Os resultados são relatados diretamente para os incidentes de segurança.

Acesse o Security Operations com seu dispositivo móvel

Acesse as aplicações Vulnerability Response e Security Incident Response na sua instância Now Platform com seu dispositivo móvel Android ou iOS. Como proprietário de correção ou analista de segurança, gerencie incidentes de segurança e grupos de vulnerabilidades para que você possa iniciar a correção sem estar vinculado à sua área de trabalho.

Identificar, priorizar e corrigir vulnerabilidades em software, sistemas operacionais e ativos



A aplicação Vulnerability Response importa e agrupa automaticamente itens vulneráveis de acordo com regras de grupo, permitindo que você corrija vulnerabilidades rapidamente. Os dados de vulnerabilidade são extraídos de fontes internas e externas, como o National Vulnerability Database (NVD) ou integrações de terceiros. Compare os dados de vulnerabilidade extraídos de fontes internas e externas. Para todos os itens vulneráveis, crie solicitações de mudança e incidentes de segurança usando grupos de vulnerabilidades para corrigir problemas e reduzir riscos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

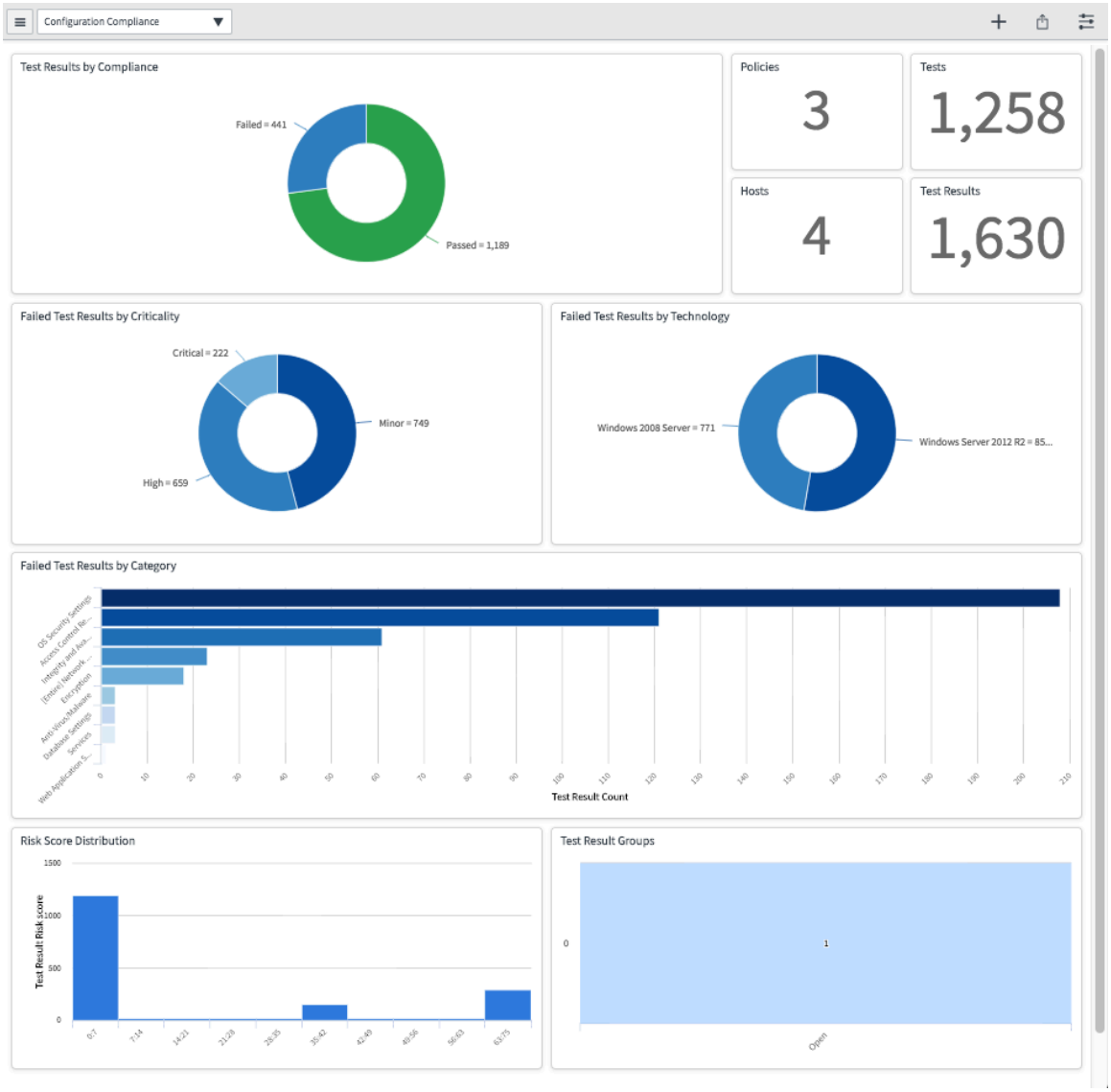
Identificar, priorizar e corrigir incidentes de segurança críticos

Com a aplicação Security Incident Response (SIR), integre suas ferramentas existentes do Security Information and Event Manager (SIEM) com aplicações Security Operations para importar dados de ameaça (por meio de APIs ou alertas de e-mail) e criar automaticamente incidentes de segurança priorizados. Gerencie o ciclo de vida de seus incidentes de segurança, desde a análise inicial até a contenção, erradicação e recuperação. A aplicação Security Incident Response permite que você obtenha uma compreensão abrangente dos procedimentos de resposta do incidente realizados por seus analistas e entenda as tendências e os gargalos nesses procedimentos com painéis orientados por análise e relatórios.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Identificar, priorizar e corrigir ativos configurados incorretamente

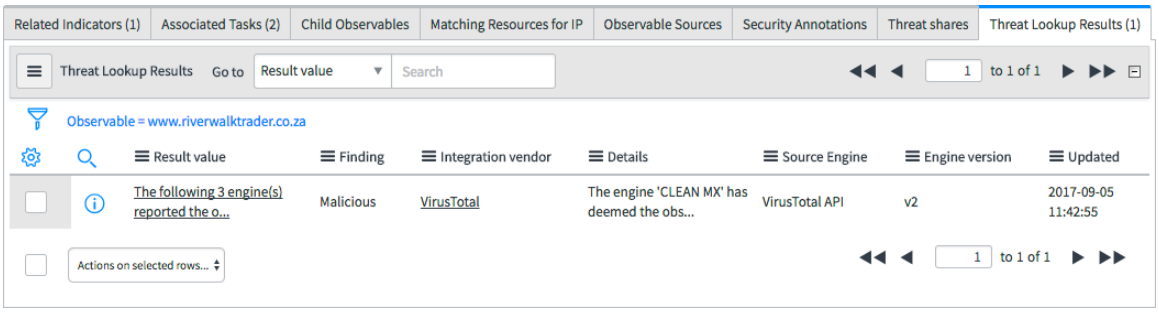


Com a aplicação Configuration Compliance, use os resultados de testes obtidos de integrações de avaliação de configuração de segurança (SCA) de terceiros para verificar a conformidade com as políticas corporativas ou de segurança. Esta aplicação usa os ativos listados no ServiceNow® Configuration Management Database (CMDB) para determinar quais itens são mais críticos. Fluxos de trabalho e automação permitem uma ação rápida em relação a ativos individuais ou grupos para mudanças em massa. Identifique e corrija itens de configuração fora de conformidade. Importe automaticamente políticas, testes, fontes autorizadas e tecnologias e atribua resultados de testes a grupos ou indivíduos para correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesse os dados da Expressão de informações de ameaças estruturadas (STIX) da sua empresa

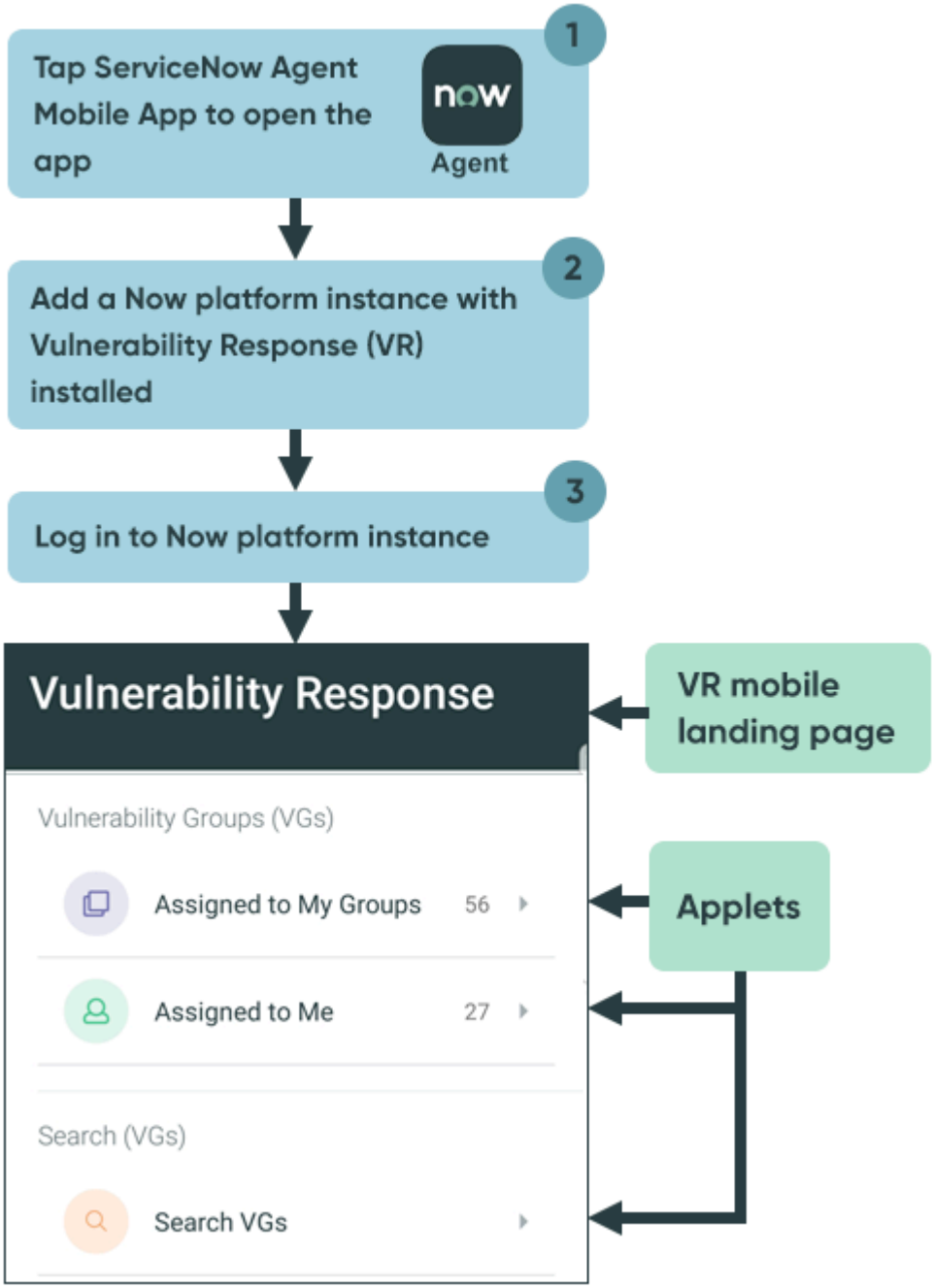


Use a aplicação Inteligência contra ameaças para pesquisar automaticamente informações relevantes em feeds de ameaças quando um IoC estiver conectado a um incidente de segurança e puder enviar IoCs para fontes de terceiros para análise adicional. A aplicação Inteligência contra ameaças usa a Expressão de informações de ameaça estruturada (STIX) como uma linguagem para descrever informações de ameaça cibernética de maneira padronizada e estruturada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Experiência de dispositivos móveis Security Operations



Acesse as aplicações Vulnerability Response e Security Incident Response na sua instância Now Platform com seu dispositivo móvel Android ou iOS.

Iniciar

- Para obter uma visão geral sobre Security Operations na sua instância Now Platform, consulte Noções básicas sobre Security Operations.
- Para obter informações sobre todas as aplicações Security Operations disponíveis para download na ServiceNow Store, consulte Security Operations e ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aprenda

- O que é IA para segurança?
- O que é Gestão de patches?
- O que é SOAR?
- O que é o CAIQ?
- O que é a estrutura do Mitre Att&ck?
- O que é gestão de vulnerabilidades?
- O que é segurança na nuvem?
- O que é DevSecOps?
- O que são operações de segurança (SecOps)?
- O que é um centro de operações de segurança (SOC)?

Aplicações e recursos

- Vulnerability Response
- Security Incident Response
- Controle de posturas de segurança
- Major Security Incident Management
- Configuration Compliance
- Inteligência contra ameaças
- Prevenção de perda de dados
- Operational Technology Vulnerability Response
- Lista de materiais de software

Noções básicas do Security Operations

Security Operations O traz dados de incidentes de suas ferramentas de segurança para um mecanismo de resposta estruturado que usa fluxos de trabalho inteligentes, automação e uma conexão profunda com a TI para priorizar e resolver ameaças com base no impacto que elas representam para a organização.

Security Operations em resumo

O ecossistema Security Operations pode ser configurado de várias maneiras, dependendo das necessidades da sua empresa e dos produtos Security Operations que você licencia. O diagrama a seguir fornece o fluxo de um sistema Security Operations básico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. A primeira etapa é usar a aplicação ServiceNow Discovery para encontrar aplicações e dispositivos em sua rede e, em seguida, atualizar o ServiceNow Configuration Management Database (CMDB).
2. Integre suas ferramentas existentes do Gerenciador de informações e eventos (SIEM) com aplicações Security Operations para importar dados de ameaça (por meio de APIs ou alertas de e-mail) e criar automaticamente incidentes de segurança priorizados.
3. Use fluxos de trabalho e a aplicação Vulnerability Response para priorizar instantaneamente eventos, incidentes de segurança e vulnerabilidades.
4. Aprimore os dados usando a aplicação Inteligência contra ameaças, bem como outros recursos de operações de inteligência artificial ou aprendizado de máquina.
5. Use Gestão de riscos e outras aplicações Governança, risco e conformidade para identificar, avaliar, responder e monitorar continuamente os riscos empresariais e de TI que podem afetar negativamente as operações de negócios.
6. Os fluxos de trabalho integrados a todas as aplicações Security Operations eliminam as suposições e o trabalho árduo da correção.
7. Veja instantaneamente informações detalhadas sobre sua postura de segurança usando painéis.

Tradução automática

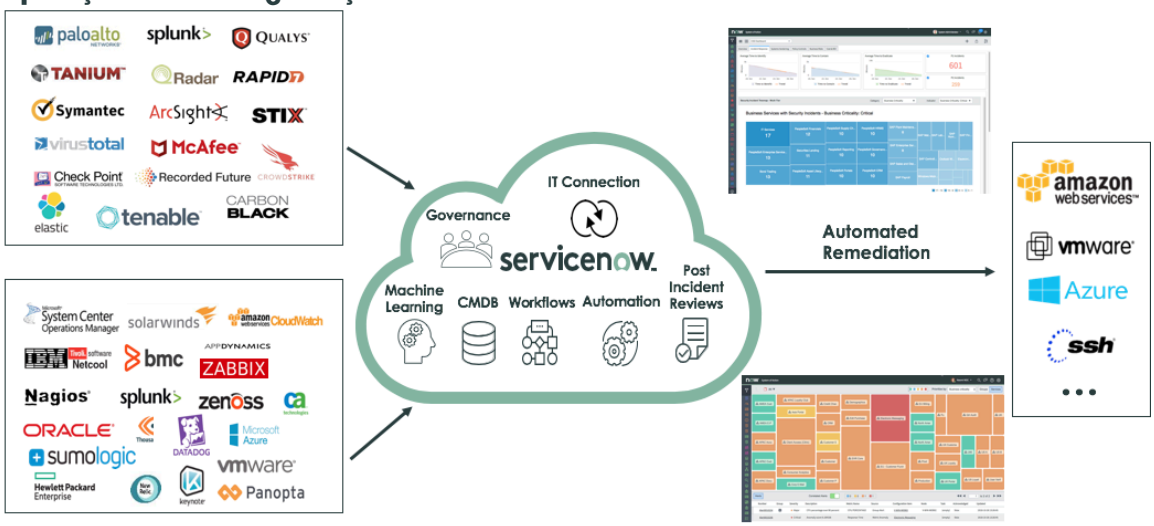
Conectar segurança com TI

Usando Security Operations, os analistas de segurança e os gerentes de vulnerabilidade podem se comunicar perfeitamente com a TI trabalhando em uma plataforma unificada. Você pode entregar patches e outras tarefas para a TI enquanto ainda mantém a visibilidade das tarefas. O roteamento baseado em habilidades atribui tarefas aos respondentes corretos e os acordos de nível de serviço garantem que o trabalho seja realizado a tempo.

O Now Platform facilita uma colaboração mais rápida entre a equipe de segurança e de TI; no entanto, os dados de segurança confidenciais ainda são protegidos por funções de usuário. Isso significa que o acesso aos dados de segurança pode ser restrito a usuários com a função de administrador, a menos que eles também tenham uma função de segurança.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

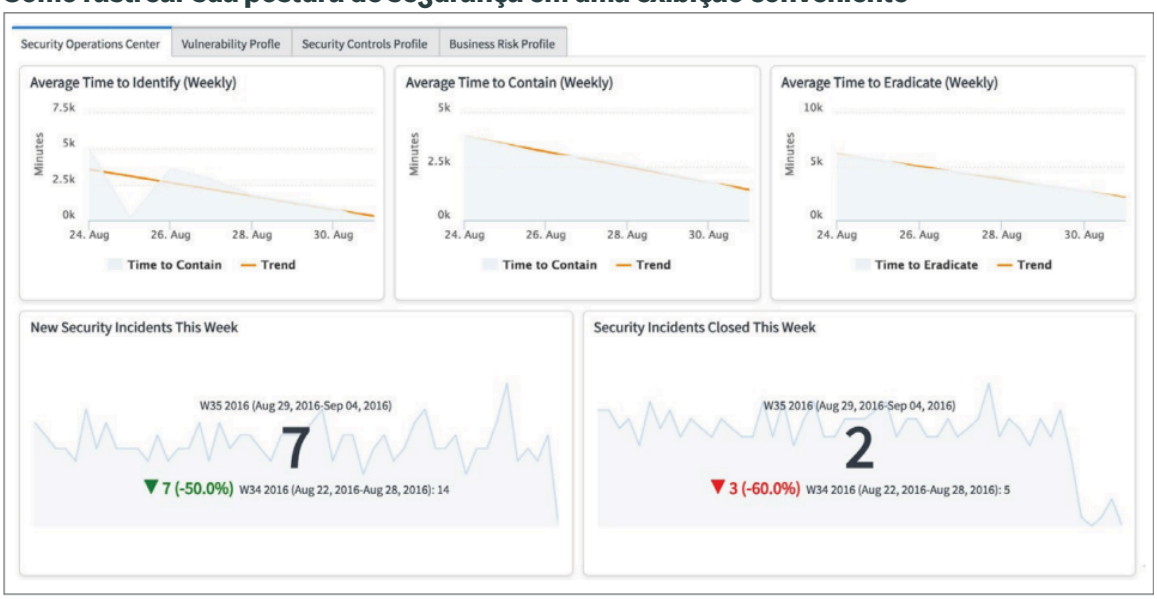
Operações de TI e segurança trabalhando na Now Platform



Acompanhamento visual da sua segurança

Security Operations O oferece painéis e relatórios baseados em função que você pode personalizar para mostrar o status da sua segurança. Todos os incidentes e vulnerabilidades de segurança, com contexto aprimorado, mostram visualmente como seus serviços de negócios críticos estão sendo afetados pelas ameaças. Painéis aprimorados com o produto ServiceNow Performance Analytics mostram o status do seu desempenho de segurança ao longo do tempo, para que você possa acompanhar como sua postura de segurança está melhorando.

Como rastrear sua postura de segurança em uma exibição conveniente



O pacote Security Operations de aplicações

Usando o poder das aplicações Now Platform, Security Operations, você pode escalonar sua solução de segurança de acordo com as necessidades do seu negócio e os tipos de ameaças cibernéticas que você enfrenta.

Tradução automática

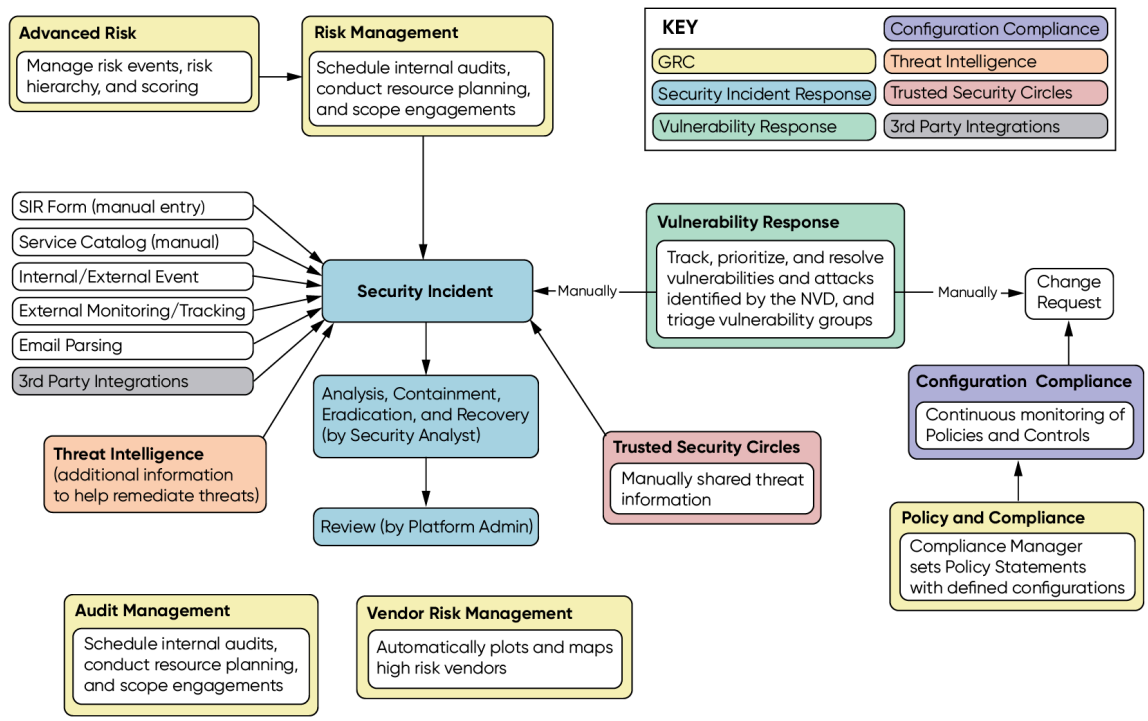
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como as peças Security Operations se encaixam

Conforme mostrado, Security Operations parece ser um quebra-cabeça. Mas quando as peças são encaixadas e você revela a imagem, o poder e a flexibilidade do Now Platform se tornam aparentes. Cada aplicação e a outra aplicação em que cada uma toca são descritas nas seções subsequentes.

Nota:
As aplicações Governance, Risk, and Compliance (GRC) não estão incluídas no pacote de aplicações Security Operations. No entanto, eles se integram e compartilham dados com Security Operationse, portanto, estão incluídos nas descrições e nos diagramas a seguir.

O pacote Security Operations (clique na imagem para ampliar)



A aplicação Security Incident Response

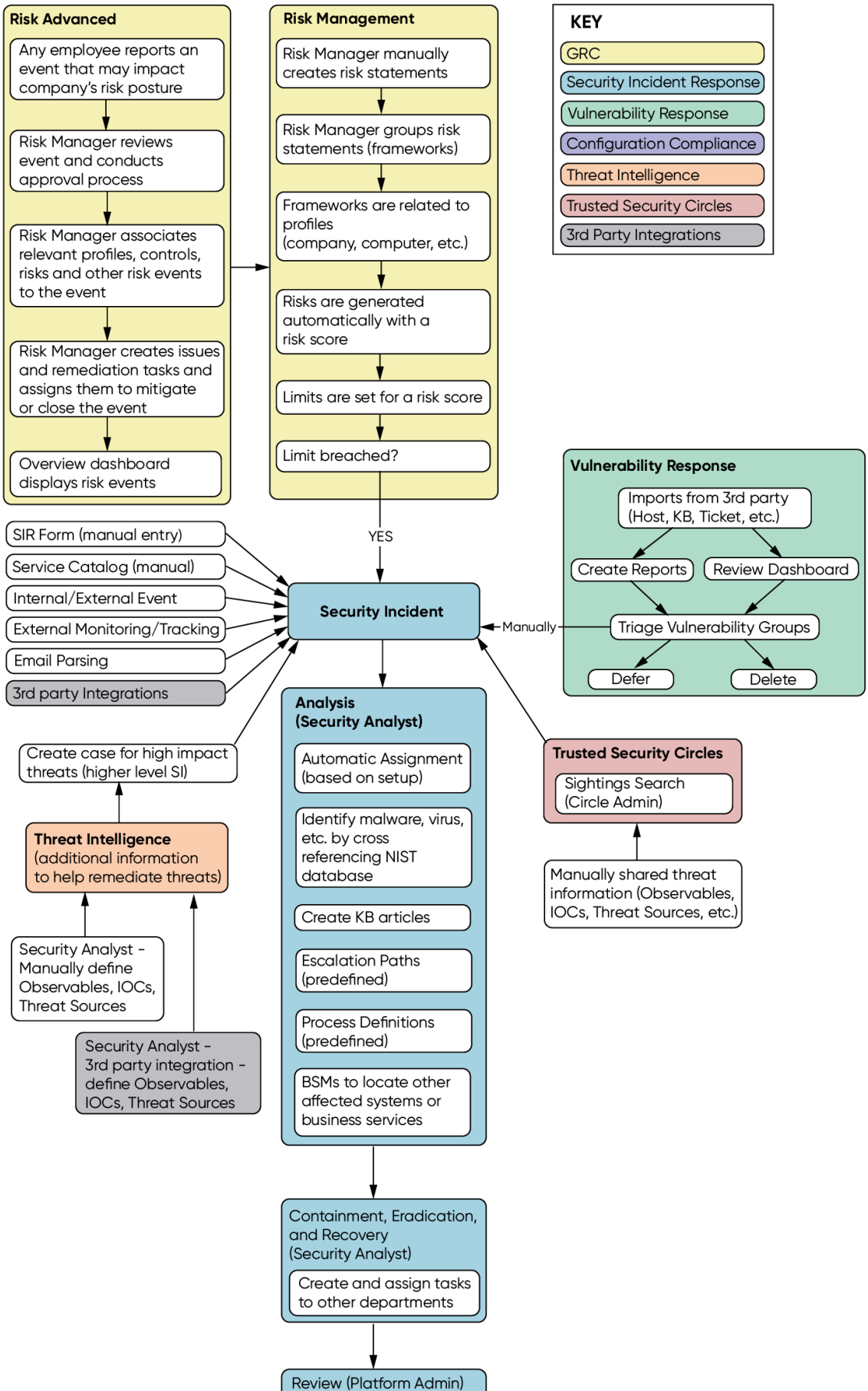
No centro do ecossistema Security Operations está a aplicação Security Incident Response (SIR). Security Incident Response simplifica o processo de identificação de incidentes críticos aplicando fluxo de trabalho avançado e ferramentas de automação que aceleram a correção. Integre suas ferramentas existentes do Gerenciador de informações e eventos (SIEM) com aplicações Security Operations para importar dados de ameaça (por meio de APIs ou alertas de e-mail) e criar automaticamente incidentes de segurança priorizados.

Existem muitos caminhos no ecossistema Security Operations para a criação automática e manual de incidentes de segurança, conforme ilustrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como Security Incident Response funciona com outras aplicações Security Operations (clique na imagem para ampliar)



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode exibir e rastrear facilmente as tarefas de resposta. Usando limites de ANS, Security Incident Response notifica os analistas atribuídos a tarefas se elas não forem concluídas a tempo ou se as tarefas forem escalonadas automaticamente, dependendo de como o sistema está configurado. Portanto, nenhuma tarefa é ignorada e nenhuma decisão é ignorada. Além disso, os analistas podem manter proativamente as partes interessadas informadas de dentro do Now Platform por meio de chamadas em conferência ou usando o recurso de bate-papo do Connect.

O Security Incident Response automatiza tarefas básicas, como solicitações de aprovação, verificações de malware ou aprimoramento de dados de ameaça quando o SIR está integrado à aplicação ServiceNow Inteligência contra ameaças. Esse tipo de automação acelera a resposta do incidente e permite que a equipe de segurança passe mais tempo na busca de ameaças complexas e críticas. Os pacotes de orquestração para produtos de segurança integrados automatizam ações repetidas com frequência, como solicitações de bloqueio de firewall, de dentro de Security Operations. Os Playbooks permitem resolver determinados tipos de ameaças à segurança passo a passo. Por exemplo, você pode resolver ataques de phishing e ameaças causados por atividade de código mal-intencionado usando playbooks.

Todas as atividades de incidente, desde análise e investigação, até contenção e correção, são rastreadas na plataforma. Quando um incidente é encerrado, uma revisão pós-incidente é distribuída a todos os membros da equipe para criar um registro de auditoria histórico para referência futura.

Nota:
Para obter mais informações, consulte Noções básicas do Security Incident Response.

A aplicação Vulnerability Response

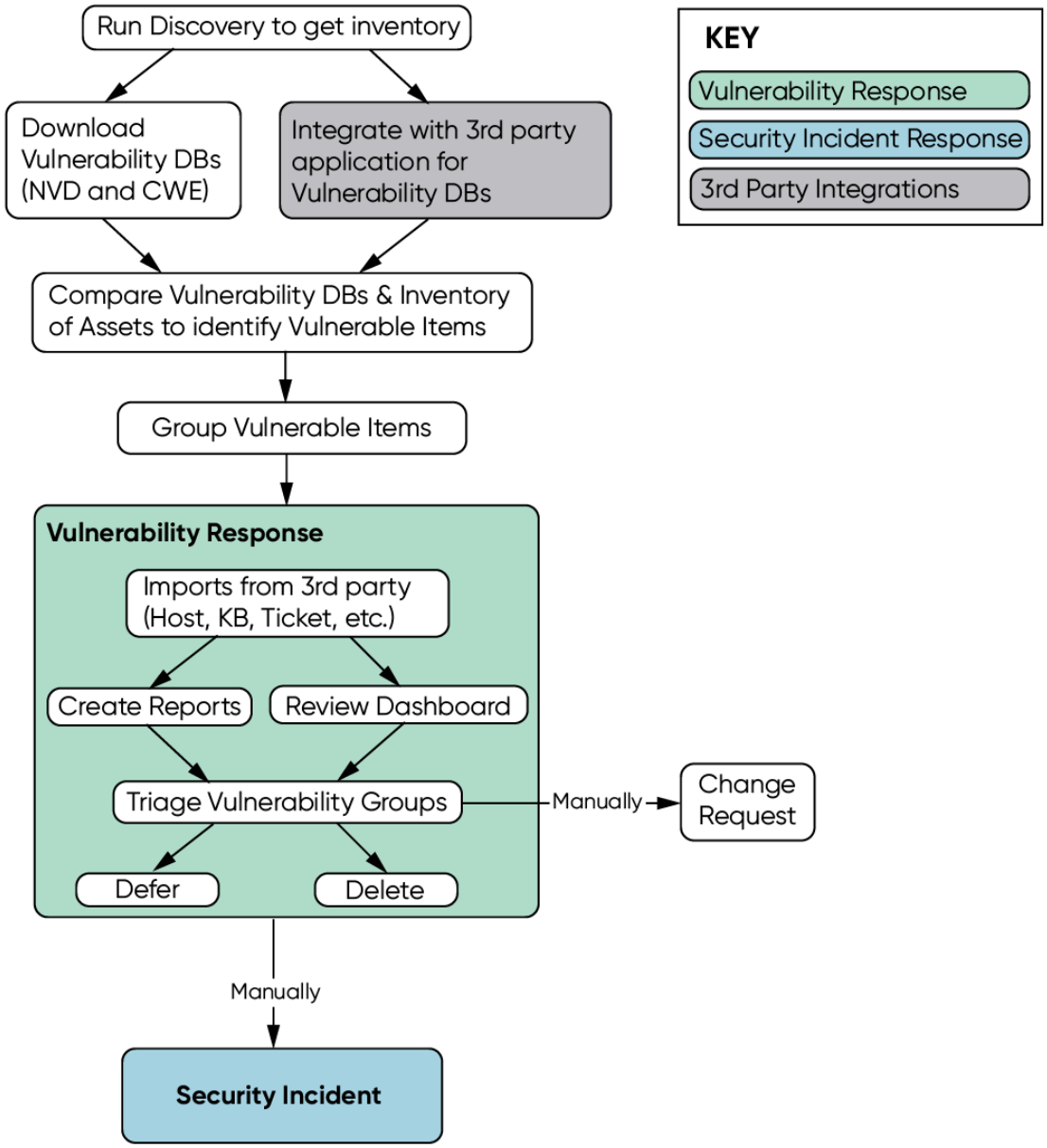
A aplicação Vulnerability Response ajuda a priorizar seus ativos vulneráveis e adiciona contexto para ajudá-lo a determinar quando sistemas críticos para os negócios estão ameaçadas. Usando o CMDB, Vulnerability Response também pode identificar facilmente dependências entre sistemas e avaliar rapidamente o impacto nos negócios de mudanças ou tempos de inatividade. Você pode exibir todas as vulnerabilidades que afetam um determinado serviço, bem como o estado atual de todas as vulnerabilidades que afetam sua organização.

As equipes de resposta também podem aproveitar o fluxo de trabalho e as ferramentas de automação no Now Platform para corrigir vulnerabilidades mais rapidamente. Quando vulnerabilidades críticas são encontradas, um fluxo de trabalho pode iniciar automaticamente uma solicitação de aprovação de patch de emergência. Depois de aprovadas, as ferramentas de orquestração podem aplicar o patch e acionar uma verificação de vulnerabilidade adicional para garantir que o problema seja resolvido.

Para patches não urgentes, basta clicar em um botão para criar uma solicitação de mudança e enviar as informações relevantes para a TI. Isso resulta em uma estratégia de correção coordenada para vulnerabilidades em serviços e ativos que podem lidar com os itens mais críticos rapidamente.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como Vulnerability Response funciona com outras aplicações Security Operations



Tradução automática

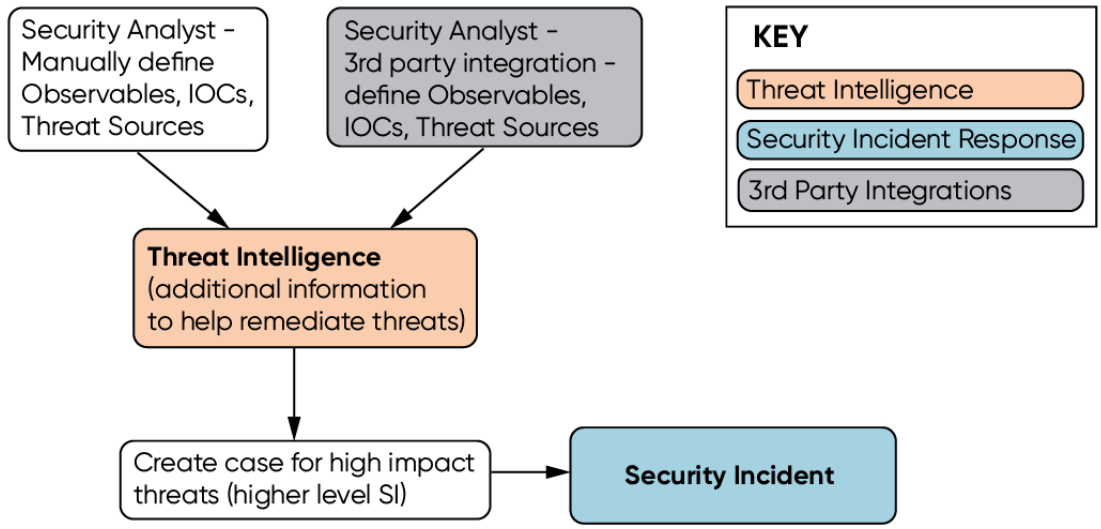
Nota:
Para obter mais informações, consulte Explorando a aplicação Vulnerability Response.

A aplicação Inteligência contra ameaças

O Security Operations inclui uma aplicação de inteligência contra ameaças para ajudar os respondentes do incidente a encontrar Indicadores de compromisso (IoC) e a buscar ataques e ameaças de baixa visibilidade. Ele pesquisa automaticamente os feeds de ameaças em busca de informações relevantes quando um IoC está conectado a um incidente de segurança e pode enviar IoCs para fontes de terceiros para análise adicional. Os resultados são relatados diretamente no registro de incidente de segurança para o analista revisar, economizando um tempo valioso. ServiceNow oferece suporte a vários feeds de ameaças, bem como STIX e TAXII, para incorporar dados de inteligência contra ameaças de várias fontes.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como Inteligência contra ameaças funciona com outras aplicações Security Operations



Nota:
Para obter mais informações, consulte.Noções básicas do Inteligência contra ameaças.

A aplicação Configuration Compliance

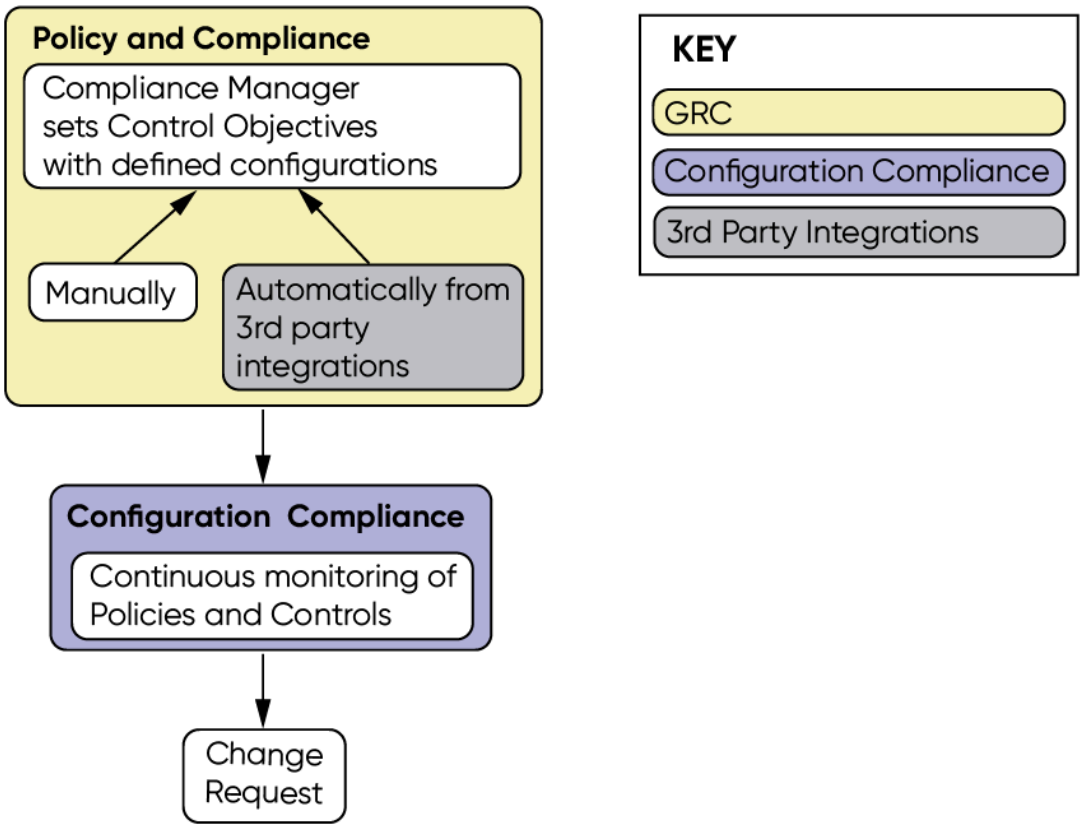
O software configurado incorretamente coloca as organizações em risco de comprometimento. Configuration Compliance prioriza e corrige ativos configurados incorretamente usando dados coletados de verificações de avaliação de configuração de segurança de terceiros. Ele aproveita o CMDB para determinar quais itens são mais críticos. Fluxos de trabalho e automação permitem uma ação rápida em relação a ativos individuais ou grupos para mudanças em massa.

Coordene facilmente com a TI em uma única plataforma para lidar com mudanças e atualizações. Além disso, os dados de Configuration Compliance podem ser alimentados no recurso de monitoramento contínuo de ServiceNow Governança, risco e conformidade para reduzir ainda mais o risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como Configuration Compliance funciona com outras aplicações Security Operations



Nota:
Para obter mais informações, consulte Explorar o Configuration Compliance.

As aplicações Governança, risco e conformidade

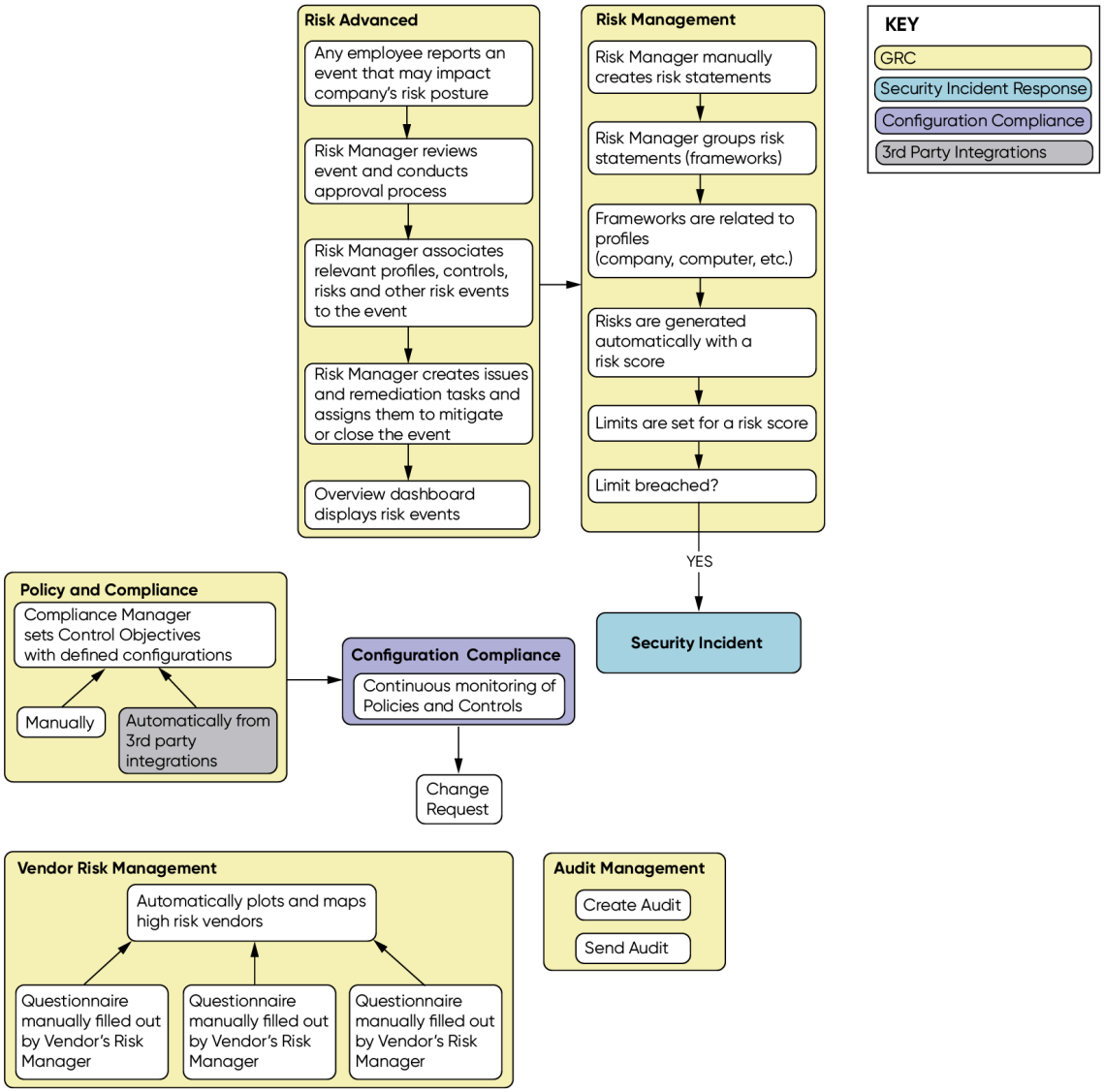
As aplicações ServiceNow Governança, risco e conformidade (GRC) ajudam a transformar processos ineficientes em sua empresa estendida em um programa de risco integrado. Por meio de monitoramento e automação contínuos, ServiceNow oferece uma exibição em tempo real de conformidade e risco, melhora a tomada de decisão e aumenta o desempenho em sua organização e com fornecedores. Somente ServiceNow pode conectar negócios, segurança e TI com uma estrutura de risco integrada que transforma processos manuais, isolados e ineficientes em um programa unificado criado em uma única plataforma.

- Gestão de riscos – Detecte e avalie a probabilidade e o impacto nos negócios de um evento com base em dados agregados em sua empresa estendida e responda a mudanças críticas na postura de risco.
- Policy and Compliance Management – Automatize os ciclos de vida das práticas recomendadas, unifique os processos de conformidade e forneça garantias sobre sua eficácia.
- Audit Management –Defina o escopo e priorize compromissos de auditoria usando dados de risco e informações de perfil para eliminar descobertas de auditoria recorrentes, aprimorar a garantia de auditoria e otimizar recursos em torno de auditorias internas.
- Gestão de riscos do fornecedor –Institua um processo padronizado e transparente para gerenciar o ciclo de vida das avaliações de riscos, due diligence e resposta a riscos com parceiros de negócios e fornecedores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como as aplicações Governança, risco e conformidade funcionam com aplicações Security Operations (clique na imagem para ampliar)



Nota:
Para obter mais informações, consulte Governance, Risk, and Compliance .

[store-future: BEGIN review]

Security Operations cenários e exemplos

Os produtos ServiceNow® Security Operations podem ser facilmente compreendidos pelo estudo de alguns cenários. Esses cenários representam recursos que você pode empregar ao usar os produtos. Eles têm o objetivo de instruí-lo sobre a potência e a flexibilidade desses produtos.

[End]
[store-future: BEGIN review]

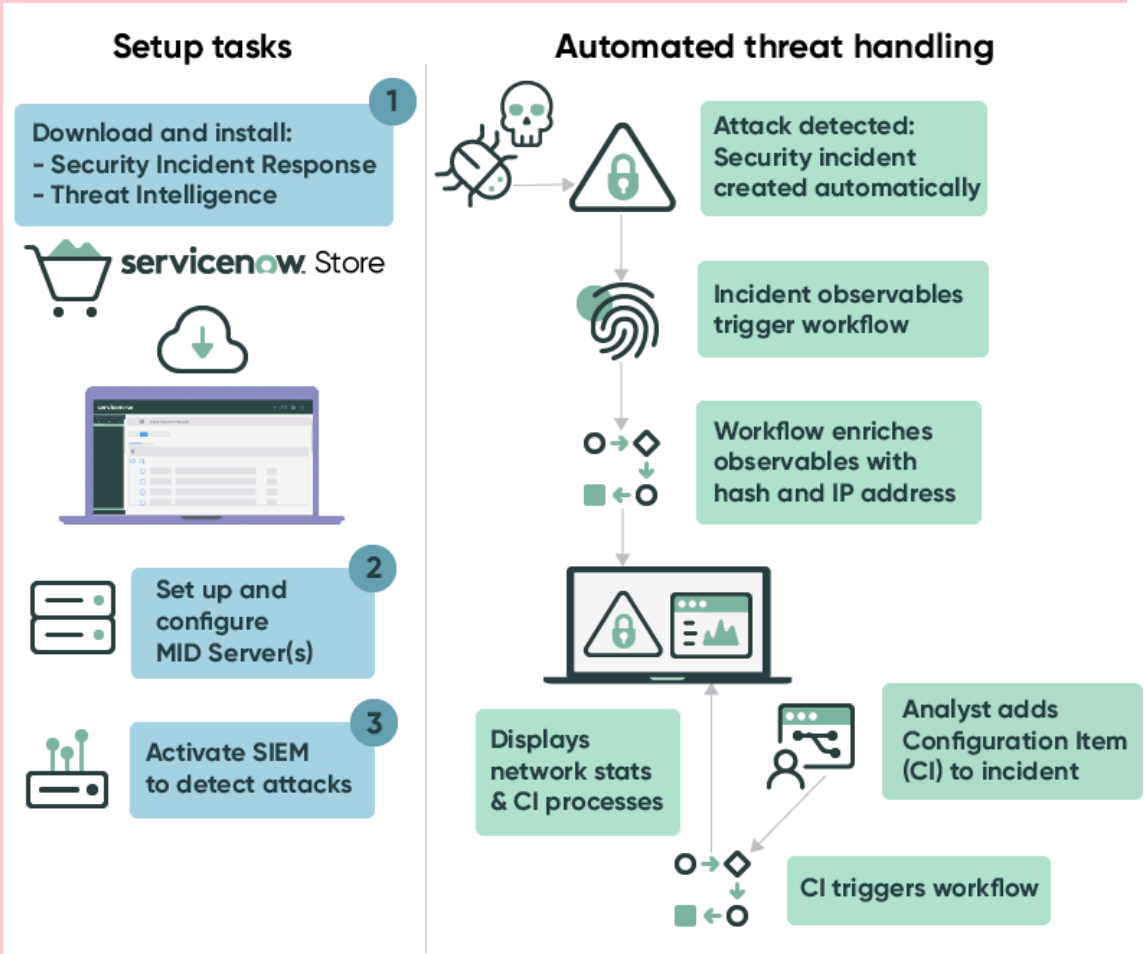
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Reduza o tempo de análise de ameaças usando automação

A triagem e a análise de incidentes de segurança são etapas necessárias para eliminar falsos positivos durante o processo de resposta a ameaças e para determinar a melhor forma de identificar, conter e eliminar as ameaças à segurança.

A triagem pode incluir etapas manuais para descobrir as causas e os impactos das ameaças. Ao automatizar muitas das etapas, você pode reduzir muito o tempo e o esforço necessários para analisar e conter ameaças. Depois de configurar a automação no software ServiceNow® Security Operations, você pode executar diferentes tipos de automação. Por exemplo, você pode aprimorar automaticamente os dados de observáveis quando um observável é adicionado a um incidente de segurança. Ou você pode exibir processos em execução ou obter estatísticas de rede quando um IC em seu CMDB for adicionado a um incidente de segurança. Esses processos, ilustrados abaixo, podem economizar um tempo valioso durante a análise de ameaças.



Neste cenário, um arquivo mal-intencionado foi detectado pela ferramenta SIEM (Security Information and Event Management) que sua empresa usa para detecção de ameaças. A integração Security Operations com o SIEM faz com que um incidente de segurança seja criado automaticamente com base no tipo de ameaça encontrada. Se o arquivo mal-intencionado já contiver observáveis ou se o analista de segurança tiver adicionado novos observáveis não expirados após o fato, um fluxo de trabalho que aprimora os registros de observáveis será acionado automaticamente. O fluxo de trabalho faz com que os observáveis sejam verificados e o hash e o endereço IP da parte que enviou o arquivo sejam adicionados ao incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Durante a triagem, o analista pode observar que os itens de configuração (IC) contidos no CMDB da empresa podem ter sido afetados pela invasão. O analista, portanto, adiciona os ICs ao incidente de segurança. Quando o incidente de segurança é salvo, dois outros fluxos de trabalho são executados e as estatísticas de rede e os processos em execução relacionados aos ICs são adicionados instantaneamente ao incidente de segurança.

[End]

Preparar para Inteligência contra ameaças automação

Antes que a automação Inteligência contra ameaças possa ser usada no processo de resposta a ameaças, você deve concluir algumas etapas de configuração preliminares. Quando a configuração estiver concluída, os fluxos de trabalho serão executados automaticamente com pouca ou nenhuma assistência do usuário.

Antes de Iniciar

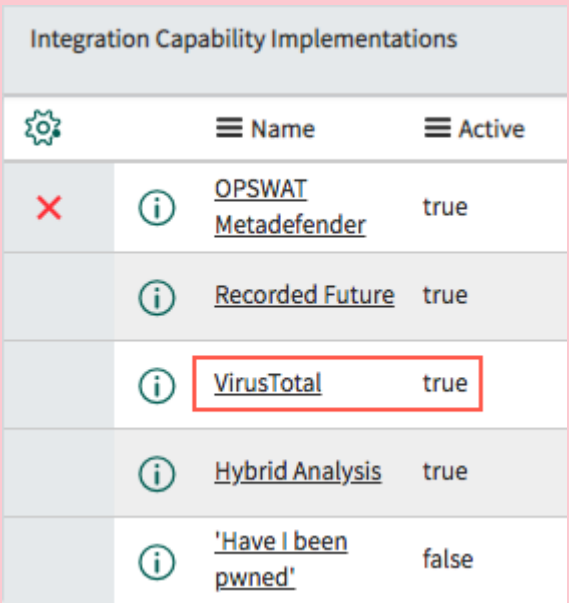
Função necessária: administrador

Procedimento

1. Baixar o Security Incident Response e Inteligência contra ameaças aplicações do ServiceNow Store.
2. Instale um ou mais MID Servers e configure as credenciais de serviço para cada um deles .
3. Quando os MID Servers estiverem instalados, certifique-se de que a implementação do recurso de integração que você está usando (VirusTotal, por exemplo) esteja ativa para o recurso Pesquisa de ameaças.
   O recurso Pesquisa de ameaças executa pesquisas para determinar se um ou mais observáveis estão associados a ameaças de segurança conhecidas.

   a. Navegar até **Security Operations** > **Integrações** > **Capacidades de integração**.

   b. Clique em **Pesquisa de ameaças** e role para baixo até a lista relacionada Implementação da capacidade de integração.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Localize a implementação que você deseja usar e verifique se a coluna **Ativa** mostra **verdadeiro**.

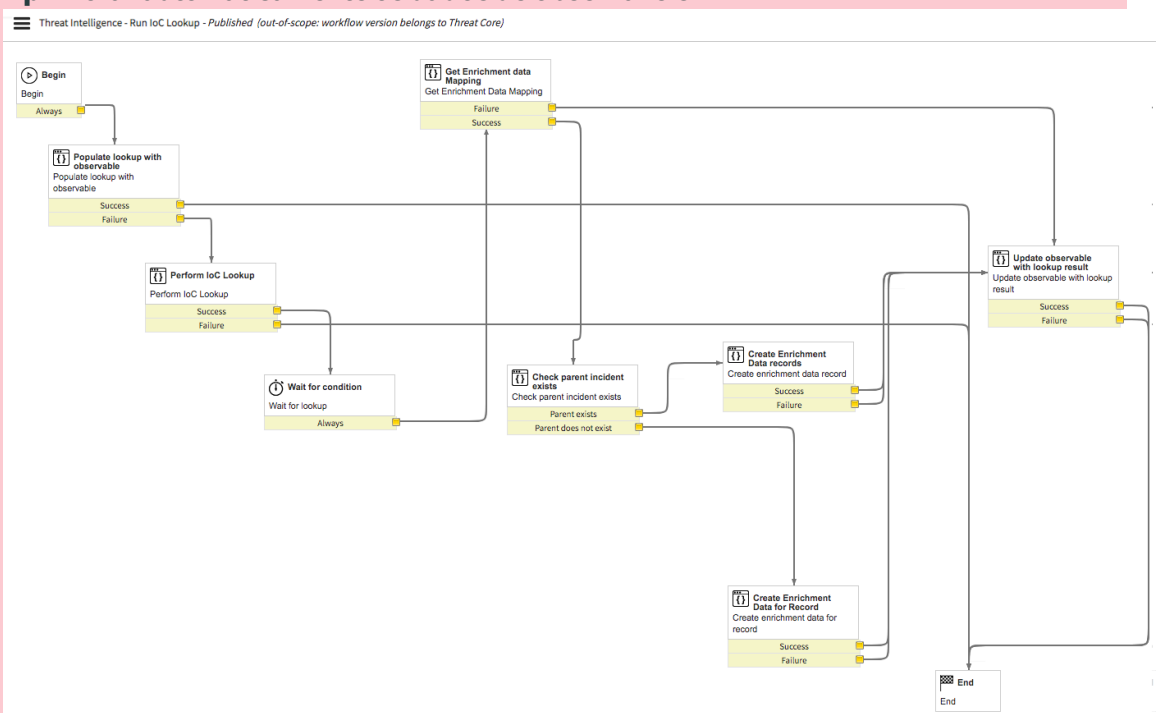
d. Se a implementação não estiver ativa, clique no **Nome**da implementação, clique para marcar a caixa de seleção **Ativa** e clique em **Atualizar**.

Aprimorar automaticamente os dados de observáveis

Depois de se preparar para a automação Inteligência contra ameaças e adicionar indicadores de comprometimento (IoC) novos ou não expirados a um incidente de segurança, o fluxo de trabalho Inteligência contra ameaças - Executar pesquisa de IoC é executado automaticamente.

As atividades de fluxo de trabalho extraem informações dos IoCs, incluindo o hash do arquivo suspeito e o endereço IP de origem sem intervenção do usuário.

Aprimorar automaticamente os dados de observáveis



Nota:
Você também pode executar a pesquisa manualmente selecionando um ou mais observáveis já anexados ao incidente de segurança e selecionando **Executar pesquisa de ameaças** na lista de seleção **Ações nas linhas selecionadas**.

O fluxo de trabalho executa as seguintes atividades:

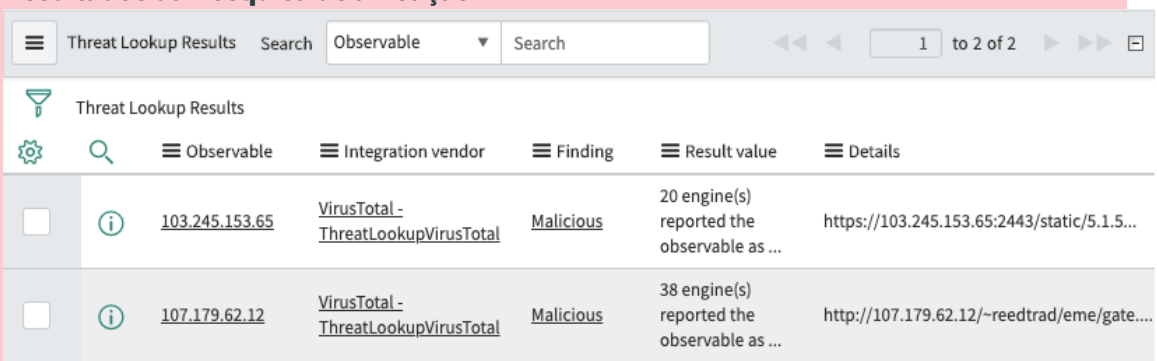
1. A atividade **Preencher pesquisa com observável** tenta encontrar um observável existente para uma pesquisa que corresponda ao valor e ao tipo da pesquisa fornecida para a atividade como entrada.
   a. Se um observável que corresponde às entradas for encontrado, a atividade **Realizar pesquisa de IoC fará** com que uma pesquisa seja realizada no ScanID do registro.
   b. Se um observável for encontrado e não estiver expirado, a pesquisa não será realizada e os resultados da pesquisa no incidente de segurança serão atualizados com as informações do observável. Para obter mais informações, consulte Preencher pesquisa com atividade observável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Quando uma pesquisa de IoC é realizada, as quatro atividades a seguir recuperam informações do mapa de dados de aprimoramento. O Mapeamento de dados de aprimoramento transforma dados de arquivos XML, JSON ou de propriedades em registros da ServiceNow. Em seguida, eles verificam se existe um incidente de segurança primário. Em caso afirmativo, um observável será criado e aprimorado. Caso contrário, o observável existente será aprimorado. Para obter mais informações, consulte Atualizar observável com atividade de resultado de pesquisa.
   - **Obter mapeamento de dados de aprimoramento**
   - **Verificar se o incidente primário existe**
   - **Criar registros de Dados de Aprimoramento**
   - **Criar dados de aprimoramento para registro**
3. Depois que o aprimoramento de dados for concluído, a atividade **Atualizar observável com resultados de pesquisa** atualiza os observáveis no incidente de segurança e grava os resultados na lista relacionada **Resultados de pesquisa de ameaças**.

Resultados da Pesquisa de ameaças



Obter automaticamente estatísticas de rede e processos em execução

Se você adicionar um item de configuração (IC) com um nome de domínio do Windows totalmente qualificado (FQDM) encontrado no CMDB a um incidente de segurança, fluxos de trabalho adicionais serão executados para fornecer estatísticas de rede e processos em execução.

Antes de Iniciar

Função necessária: administrador

Procedimento

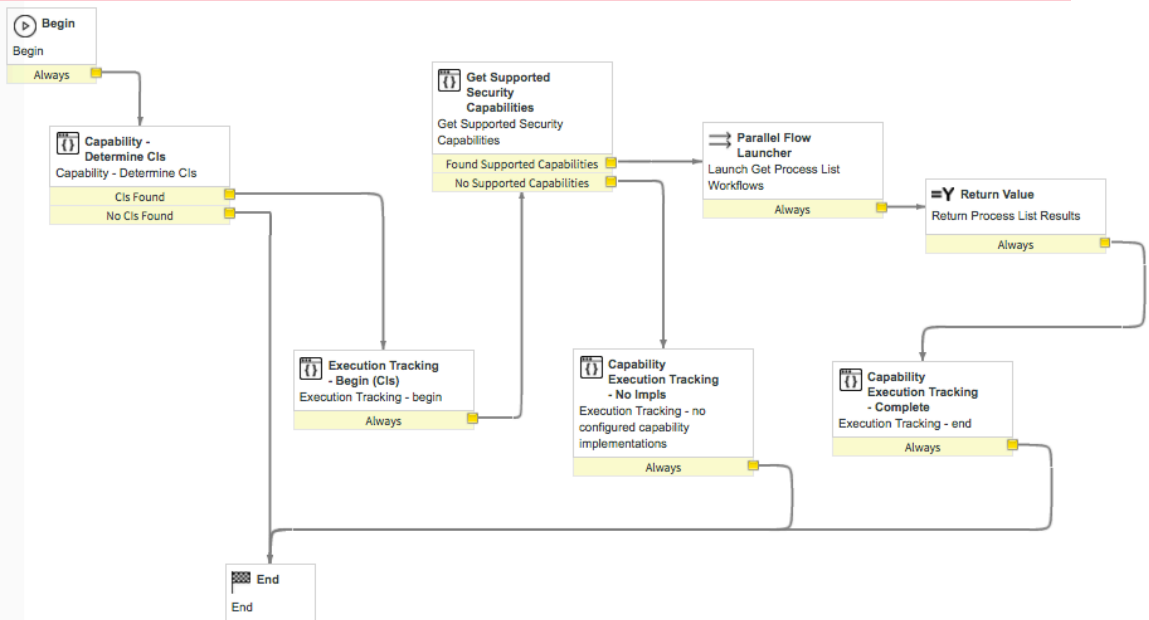
1. Usando o módulo Discovery, preencha o CMDB com nomes de domínio do Windows.

> **Nota:**
> Se você não assinar o módulo ServiceNow Discovery, deverá preencher seu CMDB manualmente ou usar um produto do tipo Discovery de terceiros.

2. Adicione um IC ao incidente de segurança.
   Os dois fluxos de trabalho a seguir são executados em paralelo.
   - Security Operations - Obter fluxo de trabalho de processos em execução: Este fluxo de trabalho recupera uma lista de processos em execução em um item de configuração (IC) de um host. Use-o para realizar uma integração, como Carbon Black, ou para um incidente de segurança baseado no Windows.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Quando o fluxo de trabalho é concluído, os processos em execução são mostrados na lista relacionada **Processos em execução** no incidente de segurança.

Processos em execução

Running Processes

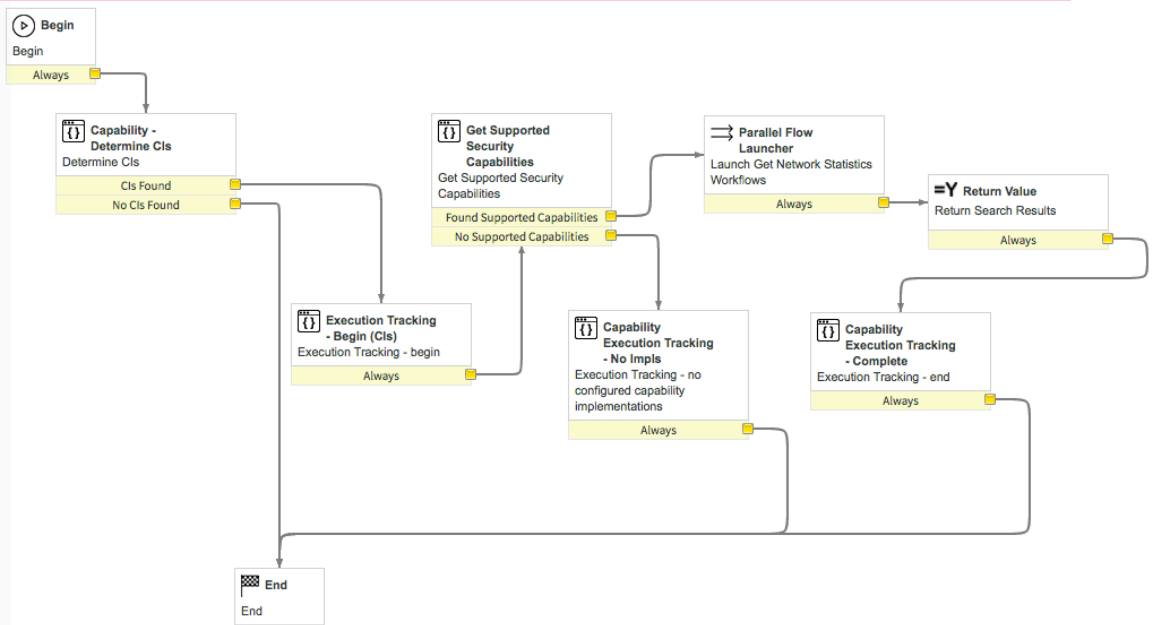
Path	Command ...	Owner	PID	Parent PID	Security Tags
C:\Windows\syste...	C:\Windows\syste...	SYSTEM	456	368	UNKNOWN
C:\Windows\syste...	C:\Windows\syste...	LOCAL SERVICE	856	456	UNKNOWN
C:\Windows\syste...	\??\C:\Windows\sy...	SYSTEM	1748	320	UNKNOWN
C:\Windows\Syste...	C:\Windows\Syste...	NETWORK SERVICE	3676	456	UNKNOWN
C:\Windows\syste...	\	Administrator	2400	1056	UNKNOWN
C:\demo\agent\jre\...	\	SYSTEM	6932	2540	UNKNOWN
C:\Windows\syste...	\	SYSTEM	6720	2968	UNKNOWN
		SYSTEM	4	0	UNKNOWN
C:\Windows\syste...	C:\Windows\syste...	SYSTEM	472	368	UNKNOWN
C:\Windows\syste...	C:\Windows\syste...	NETWORK SERVICE	964	456	UNKNOWN

1 to 10 of 50

- Security Operations Integrations - Obter fluxo de trabalho de estatísticas de rede: Este fluxo de trabalho recupera uma lista de conexões de rede ativas de um host ou endpoint. Quando

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Quando o fluxo de trabalho é concluído, as estatísticas da rede são mostradas na lista relacionada **Estatísticas de rede** no incidente de segurança.

Estatísticas de Rede

Workflow Activity History | Search | Started | Search | 1 to 8 of 8

Context = Security Operations Integration - Get Network Statistics

Started	Activity	State	Ended	Result	Fault Description
2019-05-13 13:28:38	Execution Tracking - begin	Finished	2019-05-13 13:28:38		
2019-05-13 13:28:38	Get Supported Security Capabilities	Finished	2019-05-13 13:28:38		
2019-05-13 13:28:39	Execution Tracking - end	Finished	2019-05-13 13:28:39		
2019-05-13 13:28:39	End	Finished	2019-05-13 13:28:39		
2019-05-13 13:28:39	Return Search Results	Finished	2019-05-13 13:28:39		
2019-05-13 13:28:38	Determine CIs	Finished	2019-05-13 13:28:38		
2019-05-13 13:28:38	Launch Get Network Statistics Workflows	Finished	2019-05-13 13:28:39	success	
2019-05-13 13:28:38	Begin	Finished	2019-05-13 13:28:38		

Tradução automática

Priorizar vulnerabilidades de alto perfil

Quando sua rede é afetada, as perguntas típicas feitas incluem: "como determinamos nossa exposição a riscos?" e, mais importante, "como determinamos quais sistemas abordar primeiro?"

No início de 2018, duas vulnerabilidades críticas foram liberadas: **Colapso** e **Espectro**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Priorizar vulnerabilidades de alto perfil

Meltdown exposes cached data in personal computers, mobile devices, and cloud servers to attack.

Spectre allows an attacker to trick error-free apps, which follow best practices, into leaking their secrets. The safety checks inherent in those best practices actually make the apps more susceptible to Spectre.

Programas maliciosos podem explorar o Colapso e o Espectro para obter acesso a segredos armazenados na memória de outros programas em execução. Quase três bilhões de sistemas em todo o mundo foram potencialmente afetados pelas vulnerabilidades, já que os fornecedores de hardware e software se esforçaram para colocar patches nas mãos de seus clientes.

Classificação de ameaças usando dados verificados no Vulnerability Response

Usando a aplicação Security Operations Vulnerability Response, vários métodos estão disponíveis para executar verificações de vulnerabilidade. Se a aplicação Security Incident Response estiver ativada, você também poderá iniciar verificações a partir do catálogo de incidentes de segurança, de um registro de incidente de segurança ou de uma solicitação de verificação de segurança.

Dependendo da integração de terceiros usada, os dados de vulnerabilidade são verificados e importados para a aplicação Vulnerability Response usando APIs. Em seguida, ele é comparado aos seus ativos no ServiceNow Configuration Management Database (CMDB). Os itens vulneráveis resultantes são atribuídos a uma pontuação de risco com base em vários fatores, incluindo a severidade da vulnerabilidade e a importância do ativo afetado.

Pontuação de risco

All Open Incidents

Search all incident columns

Create Incident

Number	Risk Score	Short Description	Category	Source
SIR0001774	89	DNS attack: zone transfer	Unauthorized access	Phone
SIR0001756	89	online gambling (policy breach)	Policy violation	Phone
SIR0001736	89	Email Malware in HQ	Malicious code act…	Alert
SIR0001742	82	USB drive found in server port	Criminal activity/i…	Email
SIR0001784	82	DNS redirect	Unauthorized access	Phone
SIR0001770	72	Database moved	Unauthorized access	Phone
SIR0001776	69	Sensitive data exposure (breach)	Unauthorized access	Phone
SIR0001761	65	email open relay	Unauthorized access	Phone

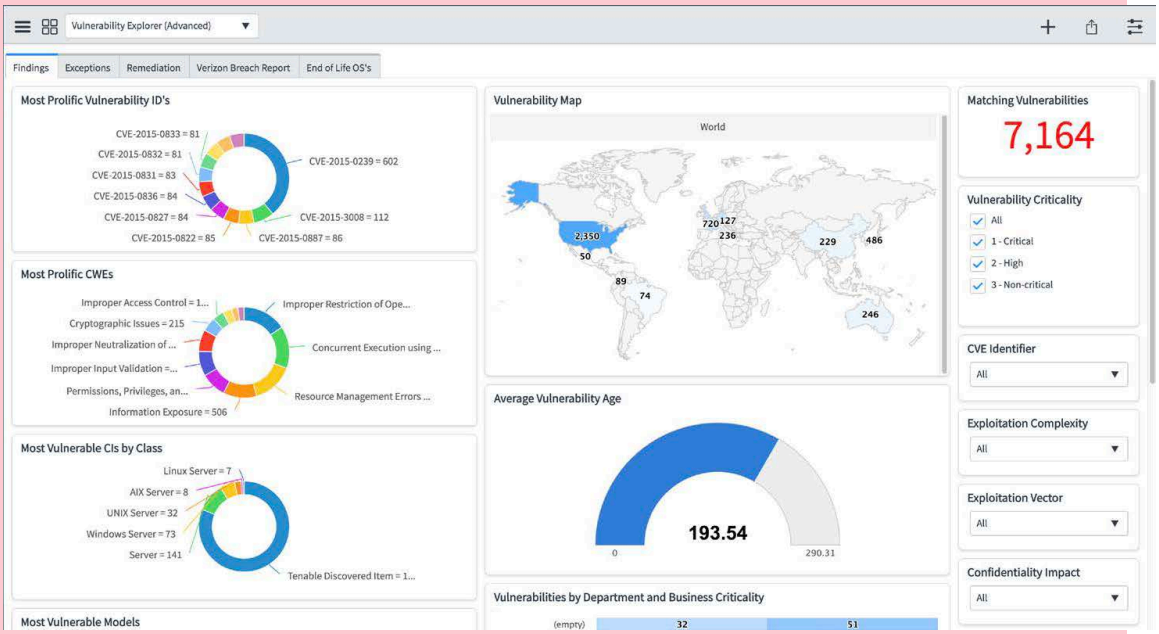
A pontuação de risco é configurável e fornece priorização rápida. Todas as informações sobre a vulnerabilidade (por exemplo, o que é, como foi explorada e como corrigir a

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ameaça) são extraídas automaticamente do Vulnerability Response do National Vulnerability Database (NVD), eliminando a necessidade de pesquisa manual. Os painéis configuráveis da solução mostram instantaneamente a exposição geral à vulnerabilidade da sua organização.

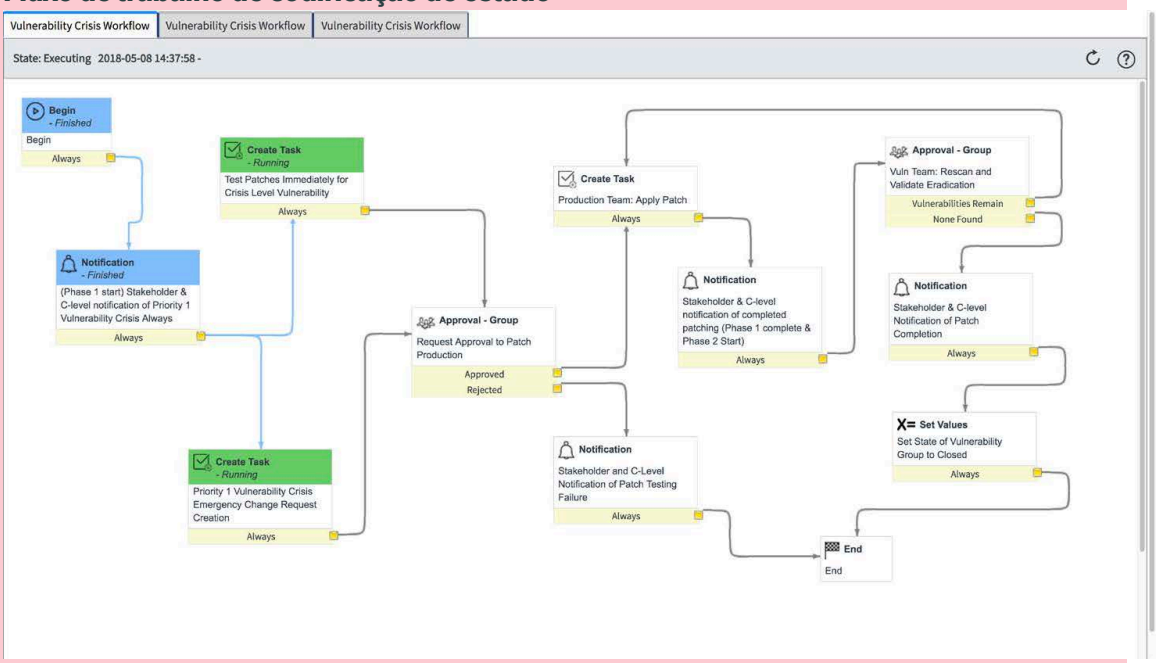
Painel de VR



Automatizando as próximas etapas

Depois de identificar e priorizar os itens vulneráveis mais críticos, os fluxos de trabalho Security Operations automatizam várias das próximas etapas.

Fluxo de trabalho de codificação de estado



Para itens vulneráveis críticos para os negócios, as solicitações para aprovar o patch automático são enviadas e os proprietários apropriados são notificados. Isso elimina a necessidade de procurar o analista de plantão ou decidir manualmente quais itens contam como "críticos".

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Após a aprovação e a conclusão do patch, uma segunda verificação será executada automaticamente para verificar a correção. Usando priorização, fluxos de trabalho e automação, os itens mais críticos são resolvidos primeiro.

Security Operations e o ServiceNow Store

Começando com Madrid, todas as aplicações Security Operations e integrações compatíveis estão disponíveis para download em ServiceNow Store. Isso permite que você obtenha recursos novos e atualizados com mais rapidez. Antes de usar qualquer aplicação Security Operations, você deve verificar se tem direito a eles (ou seja, você tem licenças válidas para usá-los), baixá-los do ServiceNow Storee ativá-los.

A lista cada vez maior de Security Operations aplicações disponíveis para download inclui:

- Security Incident Response (e integrações compatíveis)
- Vulnerability Response (e integrações compatíveis)
- Inteligência contra ameaças (e integrações compatíveis)
- Configuration Compliance
- Trusted Security Circle
- Data Loss Prevention Incident Response

Assista a este vídeo de cinco minutos para saber mais sobre como baixar as aplicações Security Operations e GRC do ServiceNow Store. Este vídeo de 5 minutos descreve como baixar aplicações Security Operations e GRC da ServiceNow Store

O processo usado para obter Security Operations aplicações e integrações depende se você está baixando uma aplicação pela primeira vez, atualizando uma aplicação que você baixou anteriormente do ServiceNow Storeou atualizando de uma versão da família para a próxima.

Baixe uma aplicação de ServiceNow Store pela primeira vez

O download de uma aplicação do ServiceNow Store pela primeira vez envolve várias etapas fáceis. Algumas das etapas são realizadas no ServiceNow Store e algumas na sua instância.

O ServiceNow Store permite que você baixe os principais produtos e aplicações. Um produto contém uma ou mais aplicações que são licenciadas como um grupo. Por exemplo, Security Incident Response é um produto. O processo envolve estas etapas:

Função necessária: administrador

- No ServiceNow Store, você deve garantir que tem direitos (ou licenças) para a aplicação e suas aplicações dependentes.

  Nota:
  Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

- Por fim, você pode ativar a aplicação e executá-la em sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Começando com as versões anteriores de Rome e versões posteriores, os plug-ins de dependência são ativados automaticamente quando você ativa uma aplicação principal. Por exemplo, quando você ativa a aplicação Vulnerability Response, o plug-in Vulnerability Response Dependências também é ativado. Para obter mais informações, consulte Ativar uma aplicação ServiceNow Store.

Obter direito para um produto ou aplicação Security Operations

A primeira etapa na instalação de uma aplicação Security Operations é verificar se a aplicação ou o produto e suas aplicações associadas têm direitos ServiceNow válidos.

Antes de Iniciar

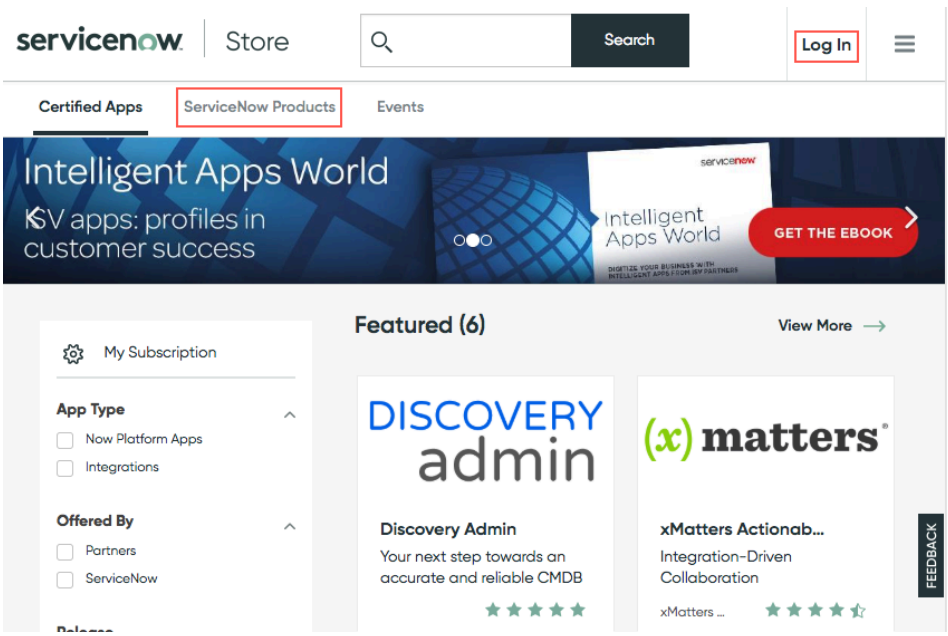
Função necessária: administrador

Os indivíduos que executam o direito devem ter uma conta Now Support e ter permissão para solicitar aplicações para as instâncias em consideração.

Nota:
Este processo se aplica somente a aplicações baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Procedimento

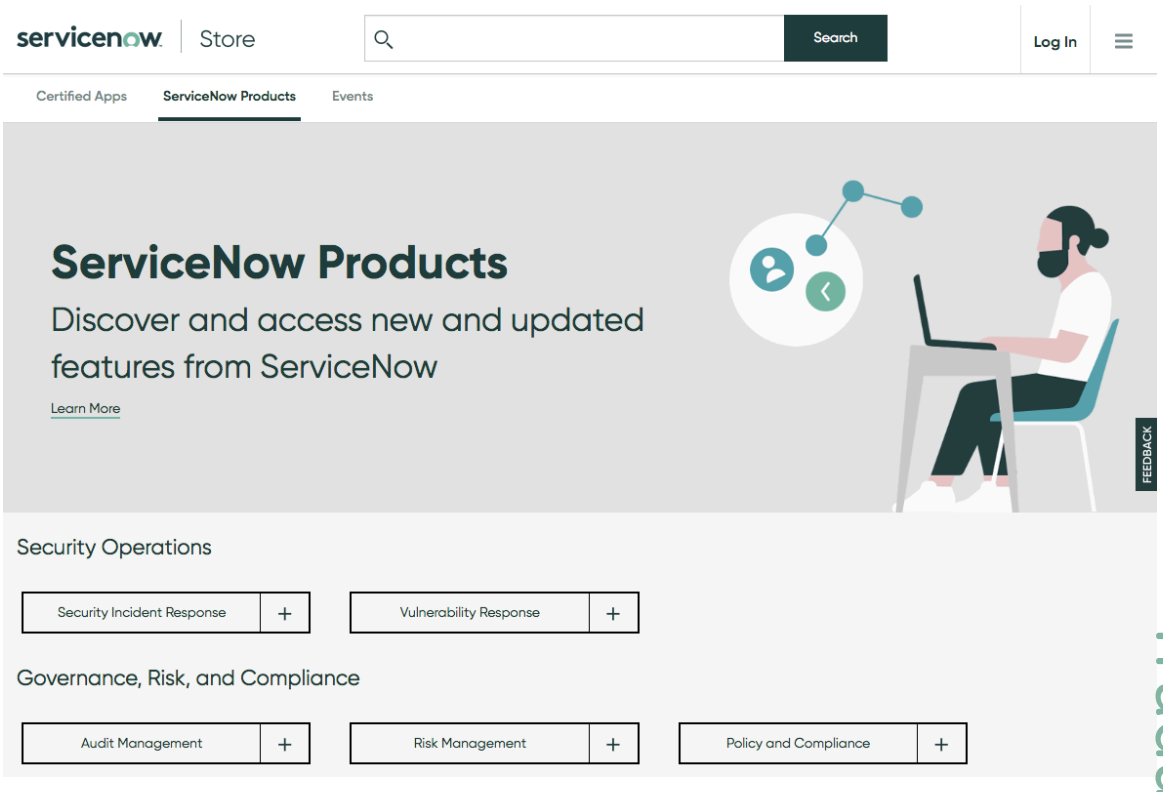
1. Navegue até o ServiceNow Store .



2. Clique em **Login** e faça login usando suas credenciais HI.
3. Clique na guia **Produtos da ServiceNow** para exibir todos os produtos ServiceNow disponíveis. Integrações e outros tipos de conteúdo são mostrados na guia **Aplicativos certificados**.

Tradução automática

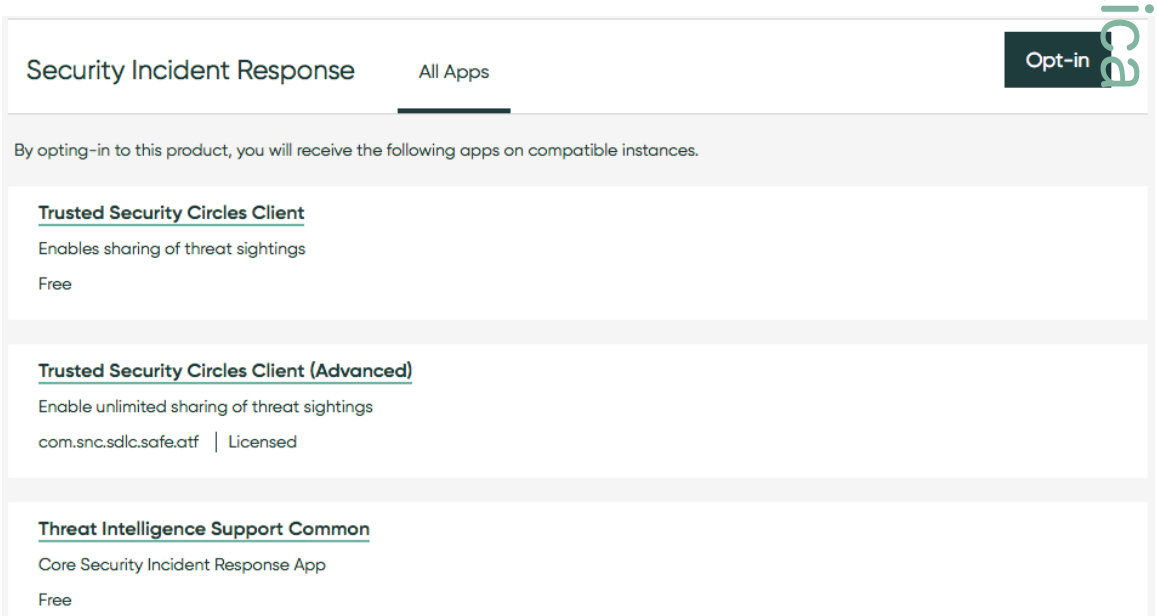
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:
Para este exemplo, suponha que você esteja adquirindo o direito do produto Security Incident Response.

4. Clique no sinal de mais (+) ao lado do nome do produto para o qual você está obtendo o direito.
Todas as aplicações associadas ao produto que você está atribuindo serão listadas. Quando você tiver obtido o direito ao produto principal, as aplicações listadas nele também serão atribuídas.

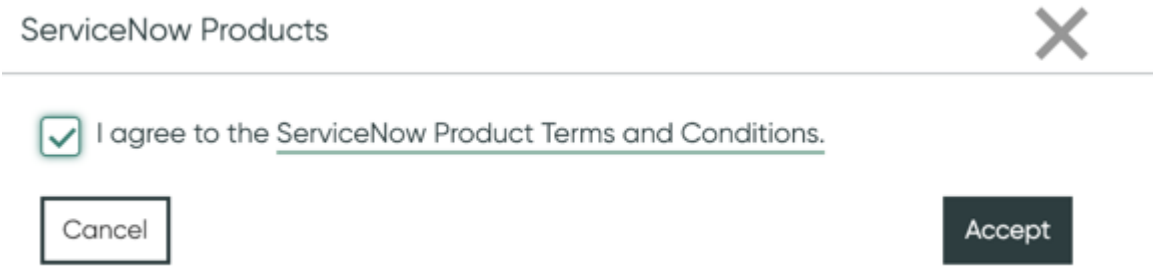
Nota:
Você também pode clicar no nome do produto para exibir mais informações sobre o produto e suas aplicações associadas.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique **em Aceitar** para verificar se você tem direito ao produto e às aplicações listadas. Você será solicitado a ler e aceitar os ServiceNow termos e

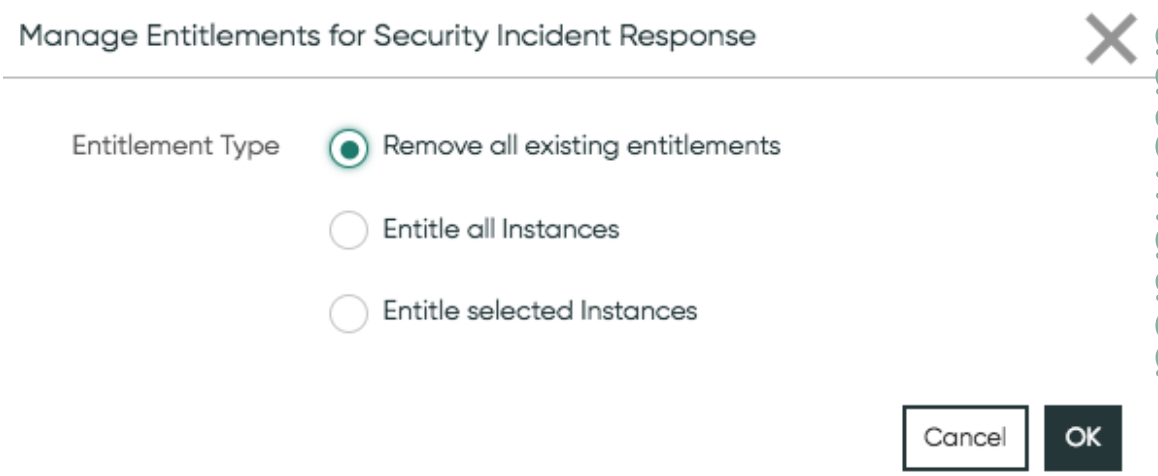


condições.

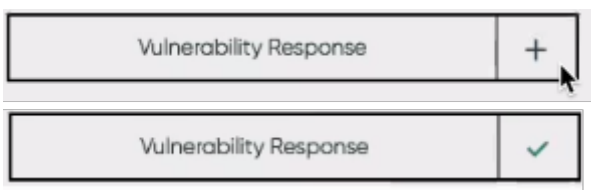
6. Marque a caixa de seleção e clique em **Aceitar**.
7. Observe que uma marca de seleção aparece ao lado do nome do produto e o botão Gerenciar direitos é exibido.

A marca de seleção indica que você assinou o produto e seus aplicativos associados. É hora de gerenciar seus direitos. Este é um processo único para este produto e quaisquer outros produtos que você queira instalar no futuro.

8. **Opcional:** Você pode clicar em **Gerenciar direitos** para mudar as instâncias afetadas pelas aplicações às quais você tem direito.



9. Depois de concordar com os ServiceNow Termos e condições e com os direitos gerenciados, você pode atribuir outros produtos com um único clique.



Nota:
Você está pronto para ativar o produto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ativar uma aplicação ServiceNow Store

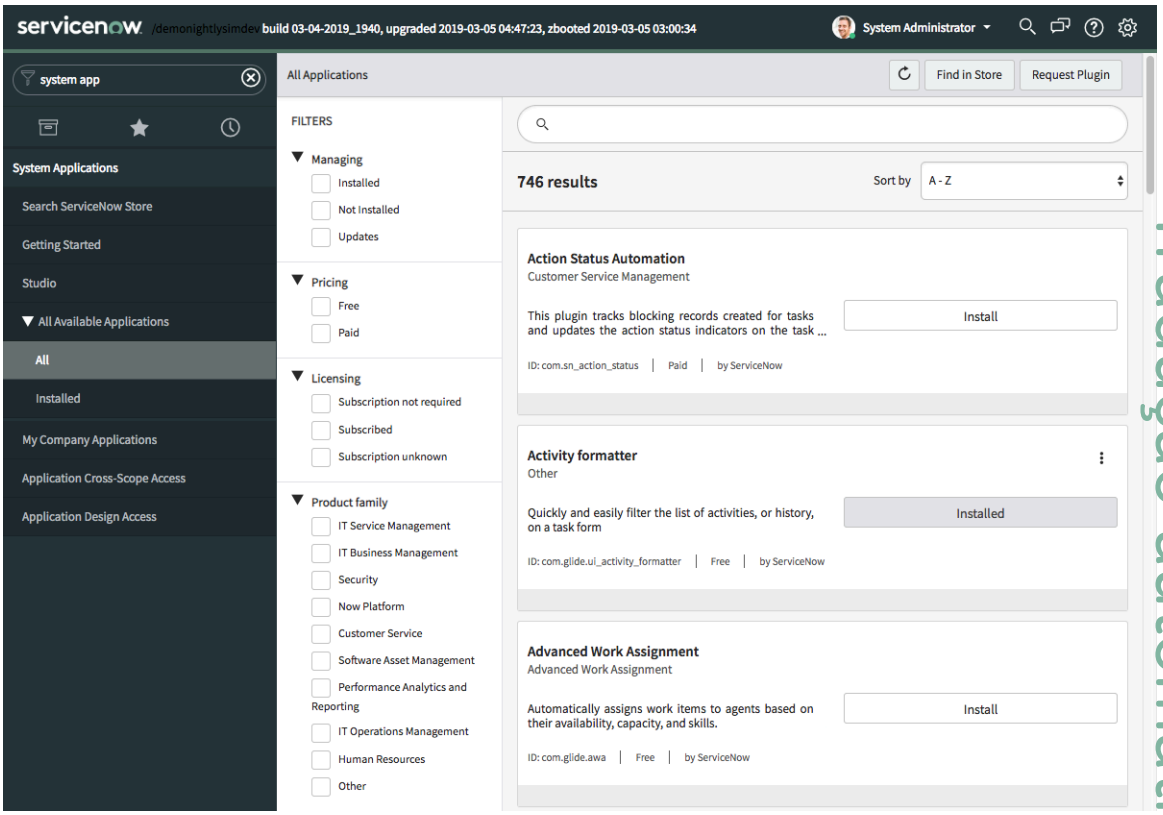
Depois que uma aplicação recebe um direito, você deve ativar o plug-in de dependências e ativar a aplicação. Este processo também se aplica a aplicações baixadas para instâncias de produto em fase de desenvolvimento.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.



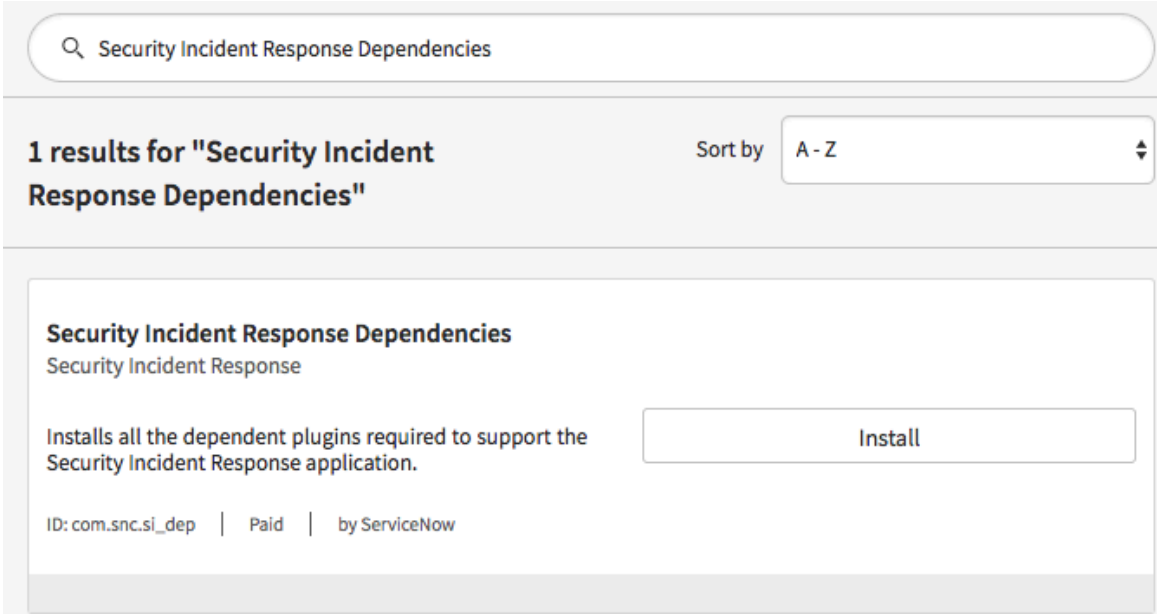
Nota:

Começando com o Orlando, os plug-ins de dependência são ativados automaticamente quando você ativa uma aplicação principal. Por exemplo, quando você ativa a aplicação Vulnerability Response, o plug-in Vulnerability Response Dependências também é ativado. Portanto, as etapas 2 a 5 são opcionais.

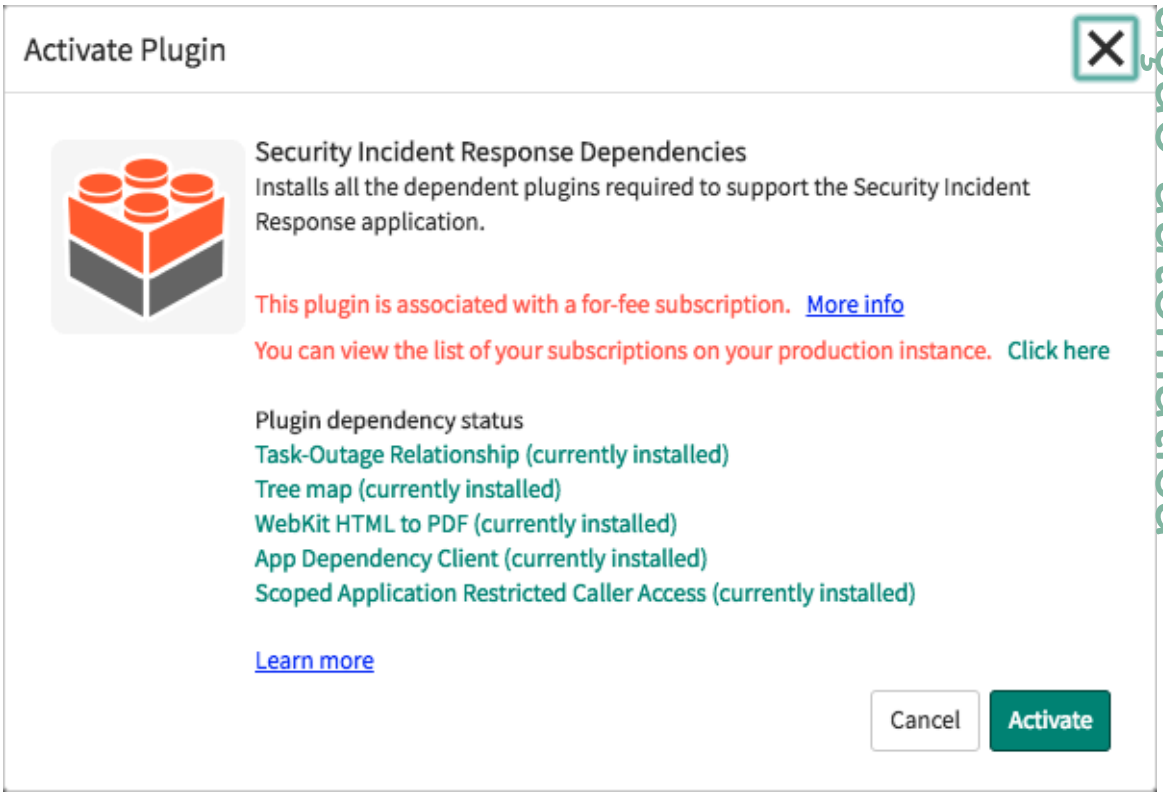
2. Pesquise o plug-in de dependências da aplicação que você deseja ativar.
Por exemplo, se você estiver ativando Security Incident Response, localize o plug-in Security Incident Response Dependências.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em **Instalar**.
   A caixa de diálogo Ativar plug-in é exibida.



4. Na caixa de diálogo **Ativar plug** -in, clique em **Ativar**.
5. Quando a ativação estiver concluída, clique em **Fechar e recarregar formulário**.
6. Agora, localize o produto principal que você está ativando, clique na caixa de seleção **Instalar com dados de demonstração** se quiser carregar dados de demonstração e clique em **Instalar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sua aplicação é instalada automaticamente na sua instância.

Nota:
Se você não marcar a caixa de seleção **Instalar com dados** de demonstração, os dados de demonstração não estarão disponíveis para instalação posterior no **Gerenciador de aplicações**. Para obter informações sobre como instalar ou reinstalar os dados de demonstração após a instalação inicial, consulte o artigo Solução alternativa para instalar dados de demonstração se a aplicação já estiver instalada [KB0722909] na Base de conhecimento HI.

Instalar uma integração Security Operations

Todas as ServiceNow integrações estão disponíveis no ServiceNow Store. As aplicações principais, como o Security Incident Response, estão visíveis na guia **Produtos da ServiceNow** na Store. Os complementos de integração estão visíveis na guia **Aplicativos certificados**.

Antes de Iniciar

Função necessária: administrador

As instalações da Store exigem uma conta Now Support e permissão para solicitar aplicações para as instâncias em consideração.

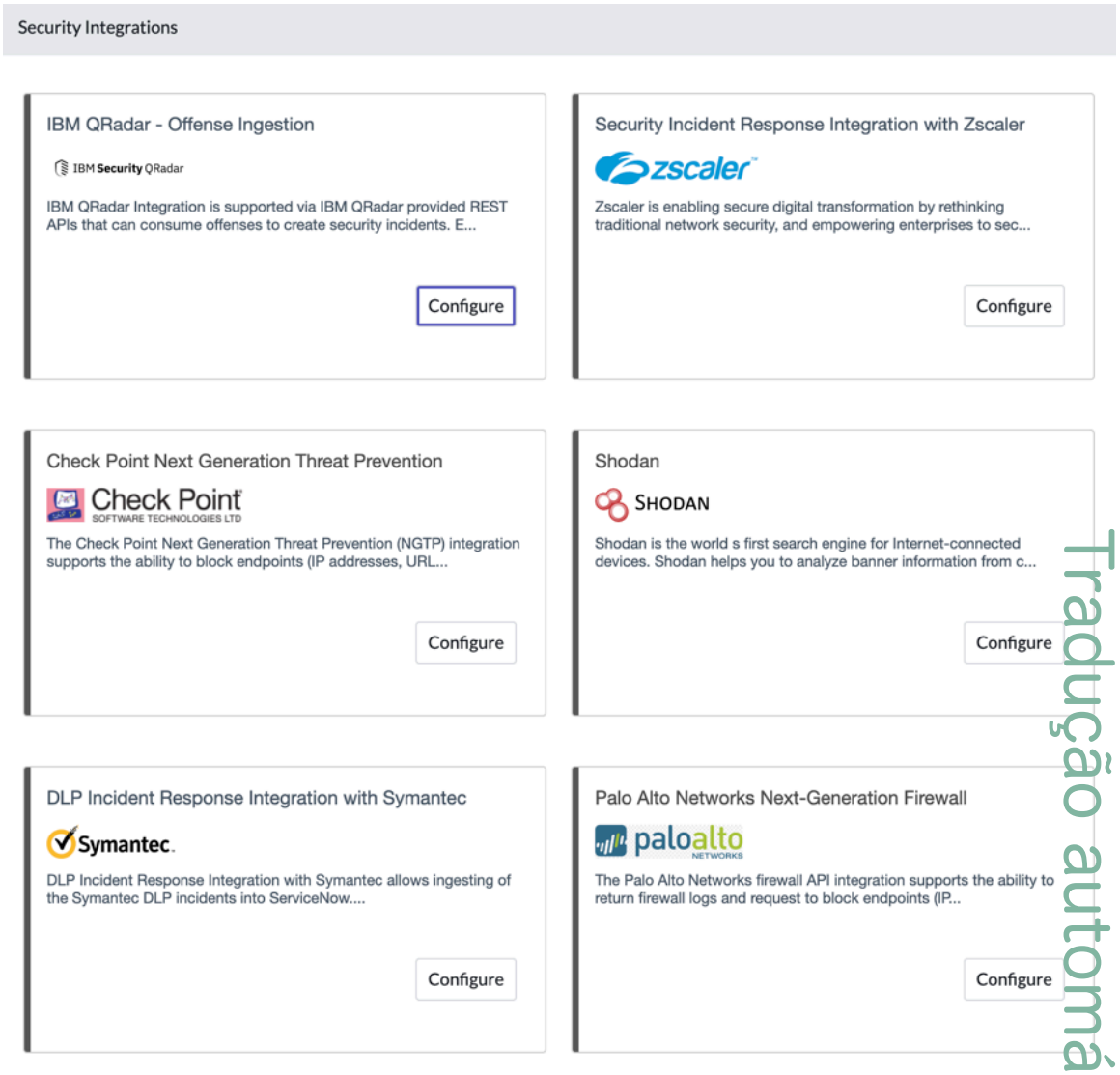
Procedimento

1. Navegar até **Security Operations** > **Integrações** > **Configurações de Integração** depois de instalar a aplicação da ServiceNow Store.
   Os blocos de configuração das integrações são exibidos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

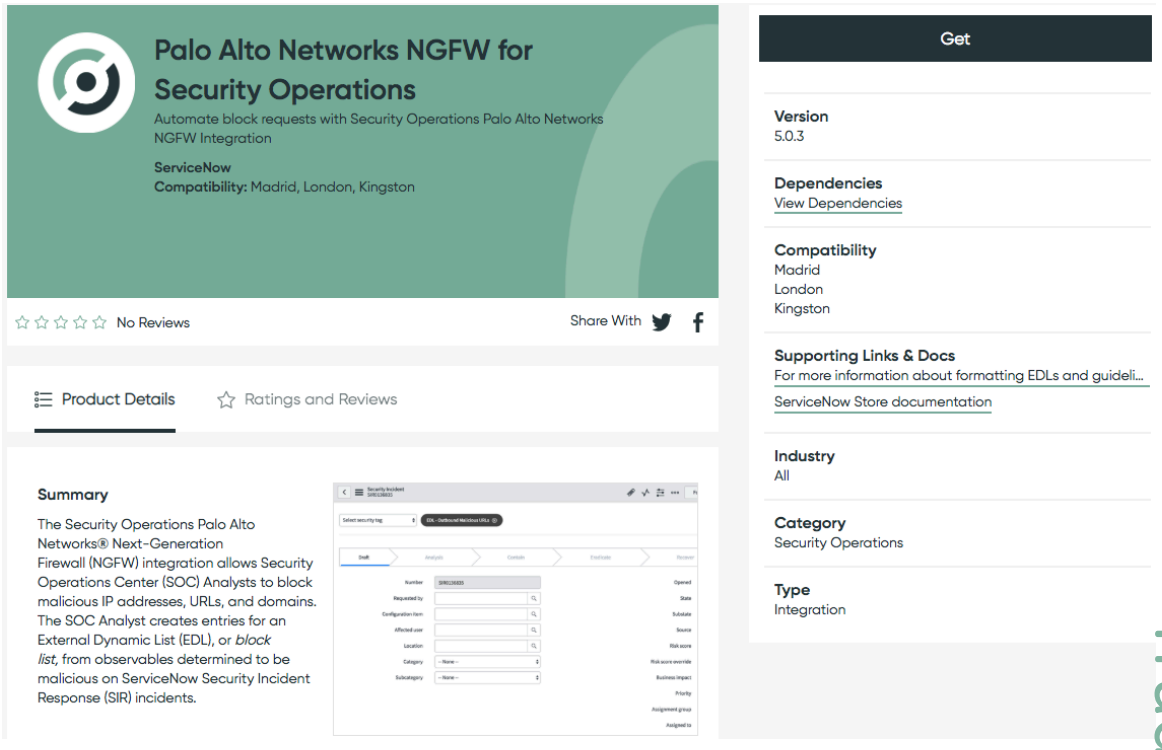
Nota:



2. Localize a integração que você deseja instalar e clique em **Configurar**.
A integração selecionada é mostrada no ServiceNow Store

Tradução automática

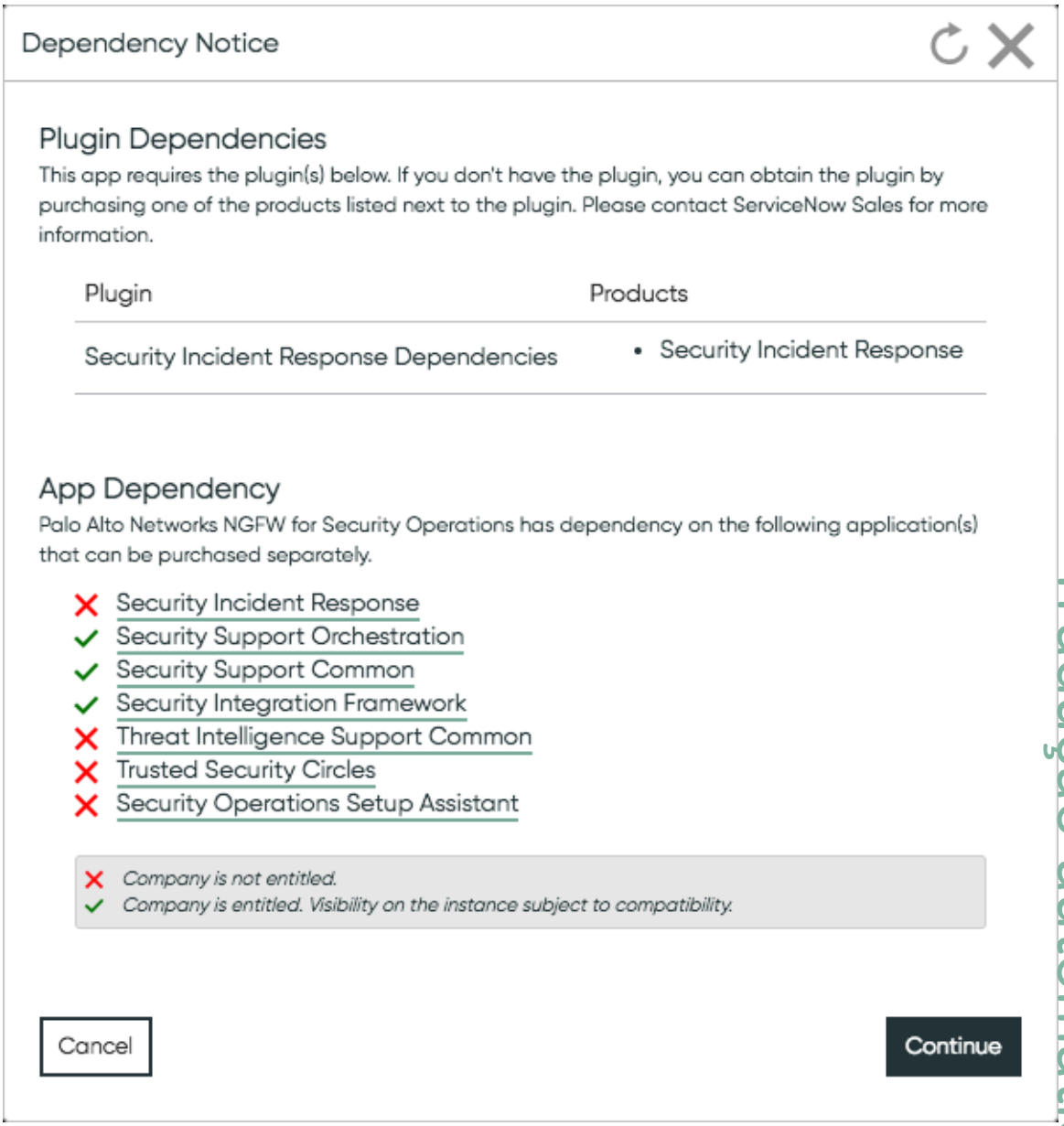
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique **em Exibir dependências** e revise as dependências da aplicação listadas.

Tradução automática

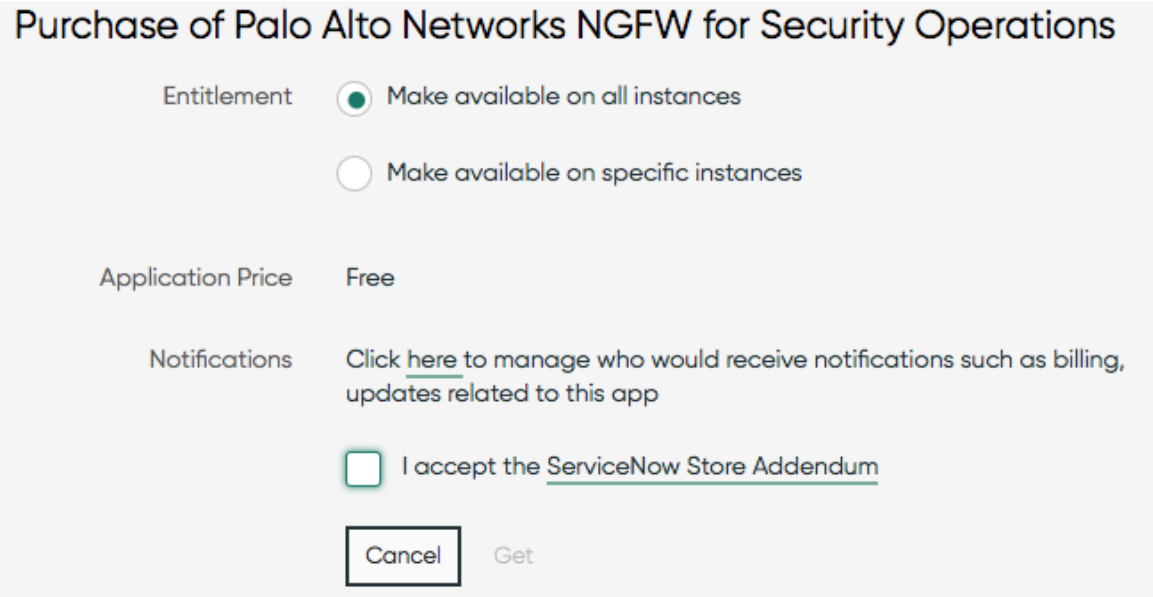
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Se a integração tiver alguma dependência da aplicação principal, como Security Incident Response, para a qual sua empresa ainda não tem direito:
   a. Siga estas instruções para obter direitos, baixar plug-ins de dependência e ativar as aplicações.
   b. Retorne a este procedimento.
   c. Clique em **Continuar**.
5. Clique **em Obter**.
   Os Termos e Condições da ServiceNow são exibidos.
6. Clique em **Continuar**.
   Uma tela de compra semelhante à seguinte é aberta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Identifique em quais instâncias você deseja que a integração esteja disponível, gerencie suas notificações e marque a caixa de seleção do adendo da **ServiceNow Store**.
8. Clique **em Obter**.

> **Nota:**
> Se você estiver baixando uma aplicação para compra, clique em **Comprar**. Se você estiver baixando uma aplicação que requer aprovação prévia do fornecedor, clique em **Solicitar aplicação**.

9. Insira o nome da instância e um motivo para a solicitação e clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
10. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
    Uma lista de aplicações disponíveis para instalação é exibida.
11. Localize a aplicação, selecione-a e clique em **Instalar**.
    Sua integração é instalada automaticamente na sua instância.

Atualizar uma aplicação baixada anteriormente do ServiceNow Store

Se você baixou anteriormente uma aplicação de ServiceNow Store e uma nova versão estiver disponível, você poderá atualizá-la em sua instância.

Antes de Iniciar

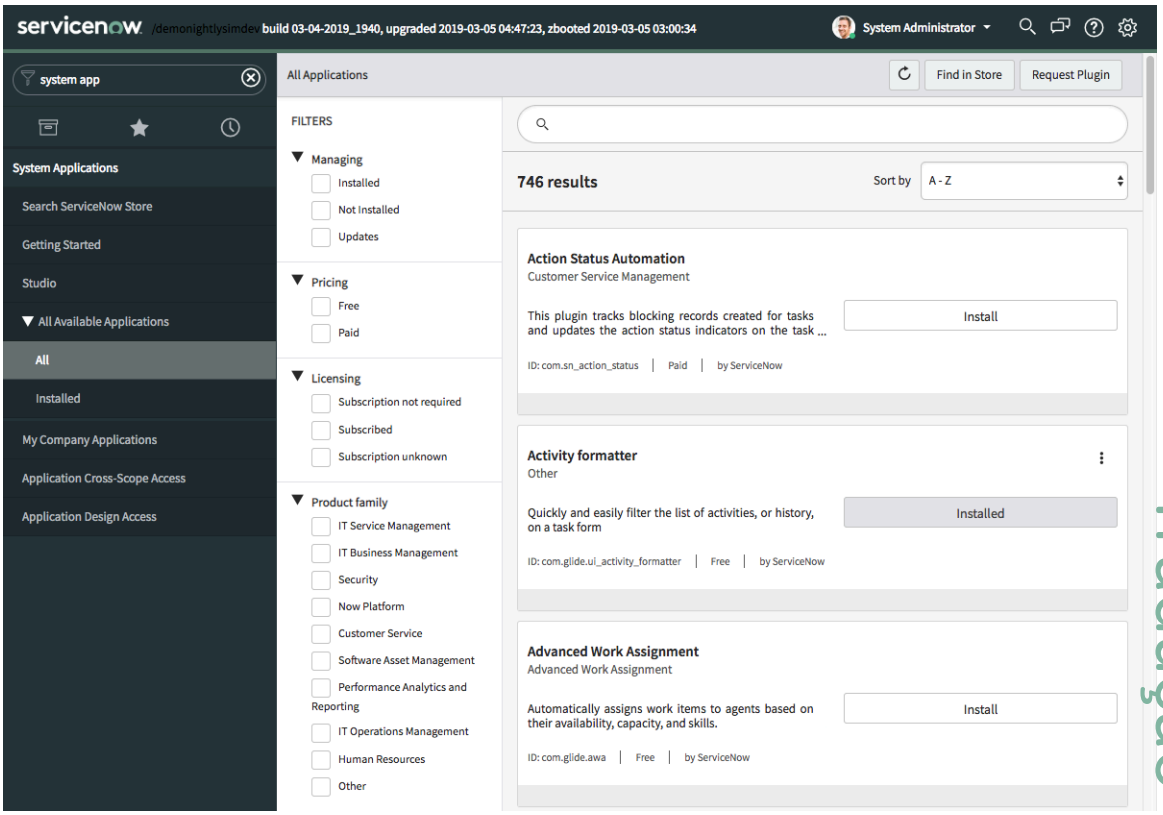
Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.



2. Pesquise a aplicação que você deseja atualizar.
3. Selecione a versão para a qual deseja atualizar e clique em **Atualizar**.
   Sua aplicação é instalada automaticamente na sua instância.

Atualize sua instância para a próxima versão da família

Se você estiver executando uma versão da família (Londres, por exemplo) e quiser atualizar para a próxima versão, não será necessário adquirir as aplicações da ServiceNow Store. A aplicação é atualizada automaticamente quando a plataforma é atualizada para a versão mínima necessária.

Antes de Iniciar

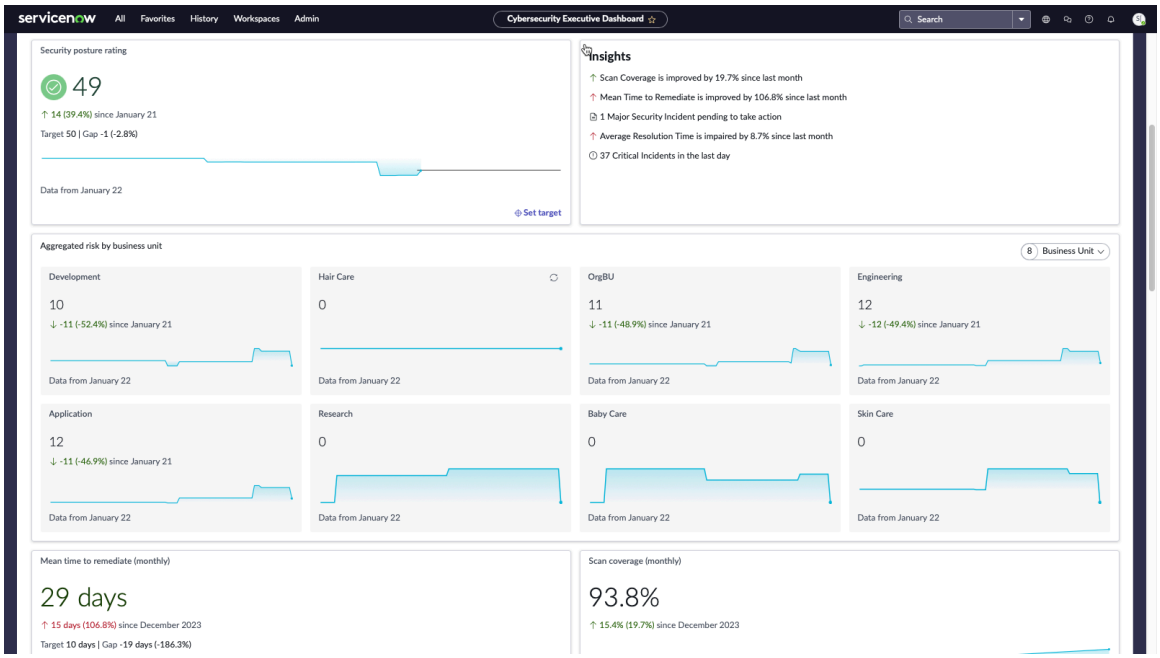
Função necessária: administrador

Painel executivo de segurança cibernética

O painel executivo de segurança cibernética é uma solução abrangente que capacita os diretores de segurança da informação (CISOs) e os executivos de segurança cibernética com visibilidade sobre a postura e as iniciativas de segurança da organização. O painel consolida dados de vários produtos no pacote ServiceNow Security Operations.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O painel fornece os seguintes recursos:

- Pontuação de postura de segurança em toda a organização
- Avaliações de risco por unidade de negócios
- Monitoramento personalizável
- Exibição unificada do cenário de segurança de uma organização
- Parâmetro de Comparação
- Interface amigável
- Visibilidade das métricas de simulação de phishing do KnowBe4 e do Microsoft Defender para Office 365

Esses recursos permitem a tomada de decisão proativa, fornecendo acesso rápido a métricas de segurança críticas. Portanto, é uma ferramenta essencial para aprimorar a resiliência e a prontidão geral da segurança.

Funções necessárias de Now Platform

- sn_bod.ciso para exibir e compartilhar o painel.
- sn_bod.ciso_admin para exibir, compartilhar o painel, configurar pesos para classificação de postura de segurança.

Acesse o painel executivo de segurança cibernética

Para abrir o painel, navegue até **Todos** > **Painel executivo de segurança cibernética** > **Painel executivo de segurança cibernética**.

Casos de uso

Para obter exemplos de como diferentes pessoas de sua organização podem usar este painel, consulte estes casos de uso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuário	Uso do painel
Diretores de segurança da informação (CISOs)	Os CISOs obtêm informações sobre gestão de vulnerabilidades, gestão de incidentes, postura de segurança da organização, métricas de simulação de phishing e assim por diante, para suas organizações.

Indicadores

ANS de host – Encerrado

Este indicador é calculado diariamente. Ele considera todas as vulnerabilidades de host que estão encerradas no momento do cálculo.

ANS de contêiner - Encerrado

Este indicador é calculado diariamente. Ele considera todas as vulnerabilidades de contêiner que estão fechadas no momento do cálculo.

ANS da aplicação - Encerrado

Este indicador é calculado diariamente. Ele considera todas as vulnerabilidades da aplicação que estão encerradas no momento do cálculo.

ANS do resultado de testes - Aprovado

Este indicador é calculado diariamente. Ele considera todas as vulnerabilidades de resultado de testes aprovadas no momento do cálculo.

ANS de host – Contagem encerrada

Este indicador é calculado diariamente. Ele considera a contagem de todas as vulnerabilidades de host que estão encerradas no momento do cálculo.

ANS de contêiner – Contagem de encerrados

Este indicador é calculado diariamente. Ele considera a contagem de todas as vulnerabilidades de contêiner que estão fechadas no momento do cálculo.

ANS de aplicação – Contagem de encerrados

Este indicador é calculado diariamente. Ele considera a contagem de todas as vulnerabilidades da aplicação que estão encerradas no momento do cálculo.

ANS do resultado de testes - Contagem de aprovados

Este indicador é medido diariamente. Ele considera a contagem de todas as vulnerabilidades de resultado de testes aprovadas no momento do cálculo.

Ativos verificados

Este indicador é calculado diariamente. Ele considera a soma dos ativos de fonte de dados (cobertura da verificação) no momento do cálculo.

Ativos verificáveis

Este indicador é calculado diariamente. Ele considera a soma dos ativos de fonte de dados (cobertura da verificação) em que o verificável não é nenhum no momento do cálculo.

Itens vulneráveis

Este indicador é calculado diariamente. Ele considera os itens vulneráveis ativos no momento do cálculo.

Item vulnerável da aplicação

Este indicador é calculado diariamente. Ele considera os itens vulneráveis da aplicação ativos no momento do cálculo.

Item vulnerável de contêiner

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este indicador é calculado diariamente. Ele considera os itens vulneráveis do contêiner ativo no momento do cálculo.

Soma da idade dos itens vulneráveis

Este indicador é calculado diariamente. Ele considera a soma da idade ativa dos itens vulneráveis no momento do cálculo.

Soma da idade dos itens vulneráveis da aplicação

Este indicador é calculado diariamente. Ele considera a soma da idade ativa dos itens vulneráveis da aplicação no momento do cálculo.

Itens vulneráveis aberto

Este indicador é calculado diariamente. Ele considera os itens vulneráveis em aberto no momento do cálculo.

Itens vulneráveis de contêiner em aberto

Este indicador é calculado diariamente. Ele considera os itens vulneráveis do contêiner aberto no momento do cálculo.

Itens vulneráveis de aplicação em aberto

Este indicador é calculado diariamente. Ele considera os itens vulneráveis da aplicação em aberto no momento do cálculo.

VITs adiados

Este indicador é calculado diariamente. Ele tem uma origem de indicador como item vulnerável de host.

AVITs adiados

Este indicador é calculado diariamente. Ele tem uma origem de indicador como um item vulnerável da aplicação.

CVITs adiados

Este indicador é calculado diariamente. Ele tem uma origem de indicador como um item vulnerável de contêiner.

Aguardando implementação dos IVs ativos

Este indicador é calculado diariamente. Ele considera os itens vulneráveis que têm um estado como Aguardando implementação no momento do cálculo.

Problemas de configuração em aberto – Resultados de testes

Este indicador é calculado diariamente. Ele tem uma origem de indicador como resultado de teste para o painel unificado do Vulnerability Response.

SI-Tempo médio para identificar

Este indicador é calculado diariamente. Ele considera o incidente de segurança em que a definição é hora de identificar no momento do cálculo.

Incidente de segurança: tempo médio de duração

Este indicador é calculado diariamente. Ele considera o incidente de segurança em que a definição é uma duração de estado de incidente no momento do cálculo.

Número de incidentes de segurança importantes em aberto

Este indicador é calculado diariamente. Ele considera os incidentes de segurança graves em aberto no momento do cálculo.

Número de incidentes de segurança encerrados

Este indicador é calculado diariamente. Ele considera os incidentes de segurança encerrados no momento do cálculo.

Itens vulneráveis da aplicação encerrados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este indicador é calculado diariamente. Ele considera itens vulneráveis da aplicação encerrados no momento do cálculo.

Itens vulneráveis do contêiner encerrados

Este indicador é calculado diariamente. Ele considera itens vulneráveis de contêiner encerrados no momento do cálculo.

Itens vulneráveis encerrados

Este indicador é calculado diariamente. Ele considera itens vulneráveis encerrados no momento do cálculo.

Obter pontuação de risco máximo para itens vulneráveis

Este indicador é calculado diariamente. Ele considera a pontuação de risco máximo para itens vulneráveis no momento do cálculo.

Obter pontuação de risco máximo para item vulnerável de contêiner

Este indicador é calculado diariamente. Ele considera a pontuação de risco máximo para itens vulneráveis de contêiner no momento do cálculo.

Obter pontuação de risco máximo para itens vulneráveis de aplicação

Este indicador é calculado diariamente. Ele considera a pontuação de risco máximo para itens vulneráveis da aplicação no momento do cálculo.

Soma da pontuação de risco de VITs

Este indicador é calculado diariamente. Ele considera a soma das pontuações de risco de itens vulneráveis no momento do cálculo.

Soma da pontuação de risco de AVIs

Este indicador é calculado diariamente. Ele considera a soma das pontuações de risco dos itens vulneráveis da aplicação no momento do cálculo.

Soma da pontuação de risco de CVIs

Este indicador é calculado diariamente. Ele considera a soma das pontuações de risco dos itens vulneráveis do contêiner no momento do cálculo.

Obter pontuação de risco máximo para incidentes de SI

Este indicador é calculado diariamente. Ele considera as pontuações de risco máximo dos incidentes de segurança no momento do cálculo.

Obter pontuação máxima de risco para resultados de testes de configuração incorreta

Este indicador é calculado diariamente. Ele considera as pontuações de risco máximo para configuração incorreta de resultados de testes no momento do cálculo.

Obter pontuação média de risco para resultados de testes de configuração incorreta

Este indicador é calculado diariamente. Ele considera as pontuações de risco médio para configuração incorreta de resultados de testes no momento do cálculo.

Número de incidentes de segurança em aberto

Este indicador é calculado diariamente. Ele considera os incidentes de segurança em aberto no momento do cálculo.

Visão geral do phishing

Este indicador é calculado diariamente. Ele considera a contagem de métricas de simulação de segurança no momento do cálculo.

MTTR agregado

Calcula o tempo médio necessário para encerrar vulnerabilidades (hosts, contêineres e aplicações) e o tempo necessário para encerrar os resultados de testes em dias. [[ANS de host - Encerrado]] + [[ANS de aplicativo - Encerrado]] + [[ANS de contêiner - Encerrado]] + [[ANS

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de resultado de teste - Aprovado]]) / ([[ANS de host - Contagem de encerrados]] + [[ANS da aplicação - Contagem encerrada]] + [[ANS do resultado de testes - Contagem aprovada]] + [[ANS do contêiner - Contagem encerrada]])

Cobertura de verificação atual

Calcula o percentual de cobertura da verificação usando a proporção entre o número de itens verificados mensalmente e o número total de itens qualificados para verificação durante o mesmo período. var monthScannedItems = [[Ativos verificados / Por MÉDIA de meses +]]; var monthScannableItems = [[Ativos verificáveis / Por MÉDIA de meses +]]; res de var; se (monthlyScannedItems == 0) res = 0; caso contrário, res = monthScannedItems / monthScannableItems * 100; se (res > 100) res = 100; res;

Idade média dos itens vulneráveis ativos

Calcula a idade média de todos os itens vulneráveis ativos (hosts, contêineres e aplicações) em dias. ([[Idade somada dos itens vulneráveis]] + [[Idade somada dos itens vulneráveis da aplicação]] + [[Idade somada dos itens vulneráveis do contêiner]]) / ([[Itens vulneráveis]] + [[Itens vulneráveis da aplicação]] + [[Itens vulneráveis do contêiner]])

VITs ativos por idade e classificação de risco

Calcula a contagem total de todos os itens vulneráveis ativos (hosts, contêineres e aplicações) categorizados por idade e nível de avaliação de risco. [[Itens vulneráveis em aberto]] + [[Itens vulneráveis de contêiner em aberto]] + [[Itens vulneráveis da aplicação em aberto]]

Itens vulneráveis com postergação

Calcula a contagem total de todos os itens vulneráveis (hosts, contêineres e aplicações) com o estado como "Adiado". [[VITs adiados]] + [[AVITs adiados]] + [[CVITs adiados]]

Média de tempo de resolução de incidentes de segurança em aberto

Calcula o tempo médio necessário para fechar os incidentes de segurança em dias. ([[Duração somada dos incidentes de segurança encerrados]] / [[Número de incidentes de segurança encerrados]]) /24

Classificação de postura de segurança

Calcula as classificações gerais de segurança diariamente. É calculado com base na pontuação de risco acumulada. var secPostureRating = 100 - [[Pontuação de risco acumulada]]; secPostureRating;

Pontuação de risco acumulada

Calcula a pontuação de risco acumulada final em que a pontuação de risco de acúmulo de itens vulneráveis, configurações incorretas, incidentes de segurança e incidentes de segurança graves é multiplicada pelos respectivos pesos que são obtidos da tabela de acúmulo de postura de segurança. var numMajorIncidents = [[Número de incidentes de segurança graves em aberto]], majorSIRiskScore, rollUpRiskScore; se (numMajorIncidents > 0) majorSIRiskScore = 100; caso contrário, majorSIRiskScore = 0; rollUpRiskScore = ([[Pontuação de risco acumulada de vulnerabilidade]] * 20 + [[Pontuação de risco acumulada de configuração incorreta]] * 20 + [[Obter pontuação máxima de risco para incidentes de SI]] * 20 + majorSIRiskScore * 40)/100; rollUpRiskScore;

Pontuação de risco acumulado de vulnerabilidade

Calcula a pontuação de risco de vulnerabilidade acumulada em que a pontuação de risco máxima, a pontuação de risco média de itens vulneráveis e a contagem de itens vulneráveis são multiplicadas com seus respectivos pesos. var maxRiskScore = 100; var count = [[VITs ativos por idade e classificação de risco]]; var countRiskScore; se (0 == contagem) countRiskScore = 0; caso contrário, se (contagem > 10000) countRiskScore = maxRiskScore; else if (count > 1000) countRiskScore = (maxRiskScore * 0.80); caso contrário, se (contagem > 100) countRiskScore = (maxRiskScore * 0.60); caso contrário, se (contagem > 10) countRiskScore = (maxRiskScore * 0.40); caso contrário, countRiskScore = (maxRiskScore * 0.20); var vulRiskScore = ([[Obter

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

pontuação máxima de todos os itens vulneráveis]] * 0 + [[Pontuação de risco média de todos os itens vulneráveis]] * 100 + countRiskScore * 0)/100; vulRiskScore;

Obter pontuação máxima de todos os itens vulneráveis

Calcula a pontuação de risco de vulnerabilidade acumulada em que a pontuação de risco máxima, a pontuação de risco média de itens vulneráveis e a contagem de itens vulneráveis são multiplicadas com seus respectivos pesos. var maxScoreForVI = [[Obter pontuação máxima de risco para itens vulneráveis]], maxScoreForCVI = [[Obter pontuação máxima de risco para item vulnerável de contêiner]], maxScoreForAVI = [[Obter pontuação máxima de risco para itens vulneráveis da aplicação]], maxScore; se (maxScoreForVI >= maxScoreForCVI && maxScoreForVI >= maxScoreForAVI) maxScore = maxScoreForVI; caso contrário, se (maxScoreForCVI >= maxScoreForVI && maxScoreForCVI >= maxScoreForAVI) maxScore = maxScoreForCVI; else maxScore = maxScoreForAVI; pontuação máxima;

Pontuação de risco médio de todos os itens vulneráveis

Calcula a pontuação de risco médio de todos os itens vulneráveis (hosts, contêineres e aplicações). var summedRiskScore = [[Summed Risk Score of VITs]] + [[Summed Risk Score of AVIs]] + [[Summed Risk Score of CVIs]], avgRiskScore; var totalVulCount = [[Itens vulneráveis em aberto]] + [[Itens vulneráveis da aplicação em aberto]] + [[Itens vulneráveis do contêiner em aberto]]; se (summedRiskScore == 0) avgRiskScore = 0; caso contrário, se (totalVulCount .=0) avgRiskScore = summedRiskScore / totalVulCount; PontuaçãoDeRisco médio;

Pontuação de risco acumulada de configuração incorreta

Calcula a pontuação de risco acumulada da configuração incorreta usando os resultados de teste categorizados como Falha, Erro ou Desconhecido. var maxRiskScore = 100; var count = [[Abrir problemas de configuração - Resultados de testes]]; var countRiskScore; se (0 == contagem) countRiskScore = 0; caso contrário, se (contagem > 10000) countRiskScore = maxRiskScore; else if (count > 1000) countRiskScore = (maxRiskScore * 0.80); caso contrário, se (contagem > 100) countRiskScore = (maxRiskScore * 0.60); caso contrário, se (contagem > 10) countRiskScore = (maxRiskScore * 0.40); caso contrário, countRiskScore = (maxRiskScore * 0.20); var miRiskScore = ([[Obter pontuação máxima de risco para resultados de testes de configuração incorreta]] * 0 + [[Obter pontuação média de risco para resultados de teste de configuração incorreta]] * 100 + countRiskScore * 0)/100; PontuaçãoDeRisco incorreta;

Tempo médio para eliminar

Calcula o tempo médio necessário para erradicar incidentes de segurança em dias [[Incidente de segurança - tempo médio de duração > Estado do incidente de segurança = erradicar]] / 1440

Tempo médio para identificar

Calcula o tempo médio necessário para identificar incidentes de segurança em dias. [[Incidente de segurança - Tempo médio de identificação]] / 1440

Tempo médio de contenção

Calcula o tempo médio necessário para conter incidentes de segurança em dias. [[Incidente de segurança - Tempo médio de duração > Estado do incidente de segurança = Contêm]] / 1440

Cumprimento da meta de correção

Calcula a porcentagem mensal de adesão da meta de correção a partir de resultados de testes, itens vulneráveis, itens vulneráveis de contêiner e itens vulneráveis da aplicação. A adesão à meta é determinada pelo número de itens que cumpriram a meta definida. ([[Resultados de testes encerrados > Status da meta de correção (Encerrado) = Meta atingida]] + [[Itens vulneráveis do contêiner encerrados > Status da meta de correção (Encerrado) = Meta atingida]] + [[Itens vulneráveis da aplicação encerrados > Status da meta de correção (Encerrado)) = Meta atingida]] + [[Item vulnerável encerrado > Status da meta de correção (Encerrado) = Meta atingida]]) / ([[Resultados de testes encerrados]] + [[Itens vulneráveis de contêiner encerrados]] + [[Itens vulneráveis da aplicação encerrados]] + [[Item vulnerável encerrado]]) * 100;

Eficiência de correção mensal (todos os itens vulneráveis)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Calcula a porcentagem mensal de itens vulneráveis encerrados, itens vulneráveis de contêiner e itens vulneráveis da aplicação em contraste com os recém-identificados. var monthClosedItems = [[Item vulnerável encerrado / Por SOMA de meses +]] + [[Itens vulneráveis de contêiner encerrados / Por SOMA de meses +]] + [[Itens vulneráveis da aplicação encerrados / Por SOMA de meses +]]; var monthNewItems = [[Itens vulneráveis / Por SOMA de meses +]] + [[Itens vulneráveis do contêiner / Por SOMA de meses +]] + [[Itens vulneráveis da aplicação / Por SOMA de meses +]], res; se (monthlyClosedItems == 0) res = 0; caso contrário, se (monthlyNewItems .=0) res = monthClosedItems / monthNewItems * 100; se (res > 1000) res = 1000; res;

Detalhamentos

- Unidade de Negócios
- Pontuação de risco
- Faixa etária
- Grupo de atribuição (unificado)
- Status da Meta de Correção (Encerrado)
- Classe de ativo
- Categoria de ativo
- Classificação de risco (unificada)
- Motivo adiado (unificado)
- Estado do Incidente de segurança
- Prioridade de Incidente de segurança
- Categoria de Incidente de segurança
- Evento de phishing

Visualização de dados

Métricas	Tipo	Descrição
Metas	Medidor	Mostra o destino definido a ser coberto por uma métrica. Para obter mais informações, consulte Definir metas.
Classificação da postura de segurança	Pontuação Única	Pontuação geral da postura de segurança da organização, considerando itens vulneráveis, incidentes de segurança, incidentes de segurança graves e configurações incorretas.
Informações	Realces	Destaques de todo o painel.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métricas	Tipo	Descrição
Risco agregado por unidade de negócios	Pontuação Única	Risco consolidado para cada unidade de negócios, considerando itens vulneráveis, incidentes de segurança, incidentes de segurança graves e configurações incorretas associadas à unidade de negócios. Você pode exibir as informações de no máximo 10 unidades de negócios. As pontuações são calculadas com base no acúmulo de postura de segurança. Navegar até **Todos** > **Painel executivo de segurança cibernética** > **Acúmulos de postura de segurança** para exibir a ponderação de cada categoria. O cálculo da classificação de postura de segurança é o seguinte: Classificação de postura de segurança = 100 - Pontuação de risco agregado. A pontuação de risco agregado é determinada pela média ponderada dos seguintes componentes: • A pontuação de risco acumulada de todos os itens vulneráveis ativos (RVIT). • A pontuação de risco acumulada de todos os resultados de testes de configuração ativos (RCTR). • A pontuação de risco máximo entre todos os incidentes de segurança (RSI) ativos. • Se pelo menos um incidente de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métricas	Tipo	Descrição
		grave estiver ativo, o RMSI será definido como 100. Se nenhum incidente de segurança grave estiver ativo, o RMSI será definido como 0 (RMSI). Para saber mais sobre o cálculo de acúmulo de itens vulneráveis e configurações incorretas, consulte Vulnerability Response Calculadoras de Rollup.
Vulnerabilidades	Pontuação Única	Risco agregado para uma determinada unidade de negócios, considerando somente os itens vulneráveis.
Erros de configuração	Pontuação Única	Risco agregado para uma determinada unidade de negócios, considerando somente configurações incorretas.
Incidentes de segurança	Pontuação Única	Risco agregado para uma determinada unidade de negócios, considerando somente os incidentes de segurança.
Incidentes de segurança graves	Pontuação Única	Risco agregado para uma determinada unidade de negócios, considerando somente os incidentes de segurança graves.
Tempo médio para correção (mensal)	Pontuação Única	Tempo médio para fechar vulnerabilidades e resultados de testes com falha em todos os ativos (hosts, contêineres e aplicações) em um mês. Ele também fornece as seguintes métricas:

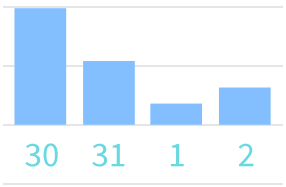
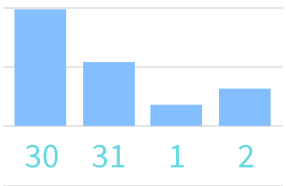
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métricas	Tipo	Descrição
		• Mudança de percentual em relação ao mês anterior. • Meta: meta definida em dias para corrigir as vulnerabilidades. • Lacuna: diferença em dias entre o tempo de destino e o real para corrigir as vulnerabilidades. • Parâmetro de comparação do setor: média da métrica de pares no mesmo setor. • Parâmetro de comparação global: média da métrica de pares no mercado global Consulte Aceitação de pontuações de parâmetro de comparação sobre como exibir as pontuações do parâmetro de comparação.
Idade média das vulnerabilidades ativas (mensal)	Pontuação Única	Idade média mensal dos três tipos de itens vulneráveis. Ele também fornece uma comparação da idade do mês atual com o mês anterior. Ele também fornece as seguintes métricas: • Mudança de percentual em relação ao mês anterior. • Parâmetro de comparação do setor: média da métrica de pares no mesmo setor. • Parâmetro de comparação global: média da métrica de pares no mercado global
Vulnerabilidades por classificação de risco e idade	Mapa térmico	Detalhamento de vulnerabilidades ativas em hosts, contêineres e aplicações por classificação de risco e idade.

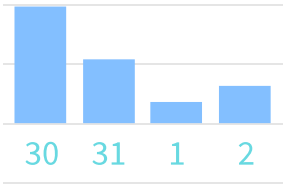
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métricas	Tipo	Descrição
Cumprimento da meta de correção por grupo de atribuição	Barra  Vertical	Proporção da soma de VITs encerrados, AVITs, CVITs e resultados de testes em que o status do destino é meta atingida para a soma de VITs encerrados, AVITs, CVITs e resultados de testes.
Cobertura de verificação (mensal)	Pontuação Única	Percentual de ativos verificados mensalmente de todos os ativos. Ele também fornece uma comparação da porcentagem do mês atual com o mês anterior. Ele também fornece as seguintes métricas: • Mudança de percentual em relação ao mês anterior. • Parâmetro de comparação do setor: média da métrica de pares no mesmo setor. • Parâmetro de comparação global: média da métrica de pares no mercado global
Verificados versus CMDB ativos	Barra  Vertical	Contagem mensal dos ativos verificados e Configuration Management Database (CMDB) por classes de IC.
Vulnerabilidades por classificação de risco e idade	Mapa térmico	Contagem de itens vulneráveis em aberto, itens vulneráveis de contêiner e itens vulneráveis de aplicação, que são categorizados por classificação de risco e idade.

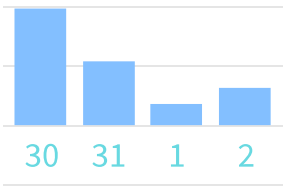
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métricas	Tipo	Descrição
Vulnerabilidades por categoria de ativo e classificação de risco	Barra  Vertical	Contagem de itens vulneráveis em aberto, itens vulneráveis de contêiner e itens vulneráveis de aplicação que são categorizados pela categoria de ativo e classificação de risco (crítico, alto e médio).
Idade média das vulnerabilidades ativas (mensal)	Pontuação Única	Idade média mensal dos três tipos de itens vulneráveis. Ele também fornece uma comparação da idade do mês atual com o mês anterior.
Tendência de vulnerabilidades críticas e altas ativas	linha	Tendência diária do número de itens vulneráveis, itens vulneráveis de contêiner e itens vulneráveis de aplicação que têm classificação de risco crítica e alta.
Tendência de erro de configuração crítica e alta ativa	linha	Tendência diária de configurações incorretas, que têm uma classificação de risco crítica e alta.
Eficiência de correção (mensal)	Pontuação Única	Percentual de itens vulneráveis encerrados mensalmente para itens vulneráveis ativos mensais. Ele também fornece as seguintes métricas: • Mudança de percentual em relação ao mês anterior. • Meta: meta definida em porcentagem para corrigir as vulnerabilidades. • Lacuna: a lacuna entre a meta e a pontuação atual. • Parâmetro de comparação do setor: média da métrica de pares no mesmo setor. • Parâmetro de comparação global: média da métrica de pares no mercado global

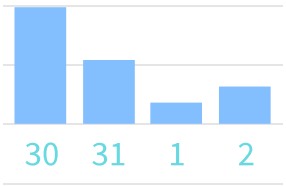
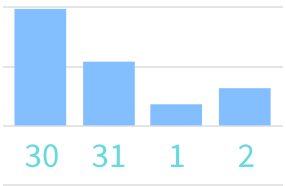
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métricas	Tipo	Descrição
Adiado por motivo e grupo de atribuição	Barra  Vertical	Contagem de itens vulneráveis, itens vulneráveis de contêiner e itens vulneráveis de aplicação que estão no estado adiado. Eles são categorizados por motivo e grupo de atribuição.
Incidentes de segurança graves	Pontuação Única	Número de incidentes de segurança graves em aberto.
Média de tempo de resolução de incidentes de segurança (mensal)	Pontuação Única	Tempo médio de resolução mensal em dias de incidentes de segurança encerrados. Ele também fornece as seguintes métricas: • Mudança de percentual em relação ao mês anterior. • Meta: meta definida em dias para corrigir as vulnerabilidades. • Lacuna: a lacuna entre os dias reais para resolver e o destino definido para corrigir. • Parâmetro de comparação do setor: média da métrica de pares no mesmo setor. • Parâmetro de comparação global: média da métrica de pares no mercado global
Tempo médio para eliminar (mensal)	Pontuação Única	Resolução média mensal em dias para erradicar incidentes de segurança.
Tempo médio para identificar (mensal)	Pontuação Única	Resolução média mensal em dias para identificar os incidentes de segurança.
Tempo médio de contenção (mensal)	Pontuação Única	Resolução média mensal em dias para conter incidentes de segurança.
Incidentes ativos por prioridade e categoria	Mapa térmico	Contagem de incidentes de segurança ativos, que são categorizados por prioridade e categoria.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métricas	Tipo	Descrição
Tendência de incidentes encerrados e em aberto	linha	Tendência mensal do número de incidentes de segurança que estão sendo fechados e abertos.
Incidentes ativos por estados	Barra  Vertical	Contagem de incidentes de segurança ativos para cada estado.
Visão geral da simulação de phishing mensal (KnowBe4)	Barra  Vertical	Soma de usuários que executaram ações como abrir, selecionar e relatar na simulação de phishing junto com a soma do total de usuários de cada simulação no mês anterior.

Aplicações a serem instaladas

Você deve instalar os seguintes aplicativos para preencher a pontuação nos widgets. Com base na aplicação que você está usando, talvez seja necessário instalar as aplicações dependentes.

Se estiver usando	Instalar
Vulnerability Response	• Performance Analytics for Vulnerability Response • Comum do Vulnerability Response • Vulnerability Response • Vulnerability Response e Configuration Compliance para contêineres • Configuration Compliance
Integrações de phishing	• Security Simulation and Training Integration for SecOps • Integração KnowBe4 para SecOps • Microsoft Defender for Office365 Integration for SecOps

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se estiver usando	Instalar
Security Incident Response	• Performance Analytics para Security Incident Response • Security Incident Response • Gestão de incidentes graves de segurança

Trabalhos programados para coleta de dados

Os trabalhos programados a seguir são executados para coletar pontuações em novos dados automaticamente.

Trabalho programado	Frequência	Descrição
Carregar as pontuações do parâmetro de comparação	Sob demanda	Coleta pontuações da instância e publica na instância central. Os algoritmos de parâmetro de comparação calculam as melhores pontuações do setor.
Baixar as pontuações do parâmetro de comparação	Sob demanda	Baixa as pontuações do parâmetro de comparação. Está disponível na tabela Pontuações de parâmetro de comparação [sn_bm_client_score_list].

Aceitação de pontuações de parâmetro de comparação

Obtenha pontuações de parâmetro de comparação registrando sua instância na instância central ServiceNow. Este último mantém informações de vários setores para fornecer a pontuação de parâmetro de comparação.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Para registrar sua instância com a instância central, siga estas etapas:

a. Navegar até **Todos** > **Propriedades do sistema**

b. Selecione *`sn_bm_client.central_instance_url`* propriedade do sistema.

c. No campo **Valor**, insira o URL da instância central do parâmetro de comparação.

> **Nota:**
> Se a instância for provisionada, seus detalhes serão enviados para a instância central automaticamente.

d. Selecione **Aceitar no** widget para validar e estabelecer uma conexão com a instância central.

2. Para carregar sua pontuação na instância central, siga estas etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegar até **Todos** > **Scheduler do Sistema** > **Trabalhos programados**

b. Selecione o *`Upload the benchmark scores`* trabalho programado.

c. Selecione **Atualizar**.
As pontuações são carregadas na instância central. No entanto, os trabalhos programados pela instância central são executados uma vez por mês para atualizar as pontuações nos widgets do painel.

3. Para baixar a pontuação da instância central, siga estas etapas:

a. Navegar até **Todos** > **Scheduler do Sistema** > **Trabalhos programados**

b. Selecione o *`Download the benchmark scores`* trabalho programado.

c. Selecione **Executar agora**.
As pontuações estão disponíveis na tabela Pontuações de parâmetro de comparação [sn_bm_client_score_list], que é refletida nos widgets do painel.

Definir metas

Defina metas em dias para corrigir vulnerabilidades, incidentes de segurança e configurações incorretas.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Selecione **Definir destino** no widget.
2. Selecione o ícone **Destinos** na página de Detalhes de KPI.
3. Marque a caixa **Para todos**.
4. No campo **Meta**, insira o número de dias em que você deseja atingir a meta.
5. Selecione a data de início da meta.
6. Selecione a data de revisão da meta.
7. Selecione **Atualizar**.

Security Simulation and Training Integration for Security Operations

Reforce a defesa da sua organização contra ameaças importantes à segurança cibernética incorporando integrações de phishing ao painel executivo de segurança cibernética. As integrações de phishing aprimoram o painel executivo de segurança cibernética incorporando dados de ferramentas de simulação de phishing de terceiros, como KnowBe4 e Microsoft Defender for Office 365.

As integrações a seguir elevam as capacidades do painel executivo de segurança cibernética, fornecendo uma perspectiva unificada sobre a postura de segurança da sua organização, a prontidão dos funcionários e a suscetibilidade a ataques de phishing:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Integração KnowBe4
- Integração do Microsoft Defender para Office 365

Configurar integração do Knowbe4

Obtenha informações imediatas sobre a vulnerabilidade de sua equipe a ataques de phishing integrando ao KnowBe4, uma plataforma líder de treinamento de conscientização de segurança cibernética. Por meio da integração do KnowBe4, identifique tendências e áreas de melhoria em seus programas de treinamento de segurança cibernética, monitore a resiliência geral do phishing e reforce proativamente as medidas de segurança da sua organização.

Antes de Iniciar

Função necessária: sn_sec_phish.admin e sn_sec_phish_kb4.kb4_admin

Procedimento

1. Navegar até **Todos** > **Integração KnowBe4** > **Configurações do KnowBe4**.
2. Selecione **Novo**.
3. No formulário, preencha os detalhes:

Formulário de configuração do KnowBe4

Campo	Descrição
Instância de Integração	Nome da instância de integração. Selecione a instância de integração usando o ícone de pesquisa.
URL base	URL para integrar com KnowBe4.
Chave de API	Chave de API adquirida da conta KnowBe4.
Página	Número da página de onde as simulações devem ser buscadas.
Tamanho da Página	Número de simulações que devem ser incluídas.

   a. Selecione **Novo** se nenhuma instância de integração estiver disponível.

   b. No formulário, preencha os detalhes:

Formulário de instância de integração

Campo	Descrição
Nome	Nome da instância de integração.
Aplicação	Nome da aplicação (KnowBe4 Integration for SecOps).
Integração	KnowBe4 é o padrão.
Ativo	O padrão é ativado (selecionado). Se desmarcada, a instância não está ativa.
Descrição	Descrição resumida da instância de integração.

4. Selecione **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Navegar até **Todos** > **Simulação e treinamento de segurança** > **Integrações**.
6. Selecione Integração do Knowbe4.
7. Selecione **Executar agora** para executar e coletar dados do KnowBe4.

Configurar integração do Microsoft Defender para Office 365

Obtenha informações valiosas sobre métricas de simulação de phishing diretamente no painel executivo de segurança cibernética por meio da integração perfeita com o Microsoft Defender para Office 365.

Antes de Iniciar

Função necessária: sn_sec_phish_msatk.ms_admin

Procedimento

1. Navegar até **Todos** > **Integração de ataque da Microsoft** > **Configurações de ataque da Microsoft**.
2. Selecione **Novo**.
3. No formulário, preencha os detalhes:

Formulário Configuração de ataque da Microsoft

Campo	Descrição
Instância de Integração	Nome da instância de integração. Selecione a instância de integração usando o ícone de pesquisa.
ID de locatário	ID do locatário da aplicação criada no portal do Microsoft Azure.
ID de cliente	ID de cliente da aplicação criada no portal do Microsoft Azure.
Segredo do Cliente	Segredo do cliente da aplicação criada no portal do Microsoft Azure.
Marcador	Data a partir da qual as simulações devem ser buscadas.
URL de token	URL base de onde o token é criado para acessar a API de simulações da Microsoft.
URL de todas as simulações	URL base da API de simulações da Microsoft.

   a. Selecione **Novo** se nenhuma instância de integração estiver disponível.

   b. No formulário, preencha os detalhes:

Formulário de instância de integração

Campo	Descrição
Nome	Nome da instância de integração.
Aplicação	Nome da aplicação (Microsoft Defender for Office 365).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Integração	Referência de integração de terceiros (integração de ataque da Microsoft).
Ativo	O padrão é ativado (selecionado). Se desmarcada, a instância não está ativa.
Descrição	Descrição resumida da instância de integração.

4. Selecione **Enviar**.
5. Navegar até **Todos** > **Simulação e treinamento de segurança** > **Integrações**.
6. Selecione Integração de ataque da Microsoft.
7. Selecione **Executar agora** para executar e coletar dados da Microsoft.

Security Incident Response

A aplicação ServiceNow® Security Incident Response rastreia o andamento dos incidentes de segurança desde a descoberta e a análise inicial, passando pela contenção, erradicação e recuperação, até a revisão pós-incidente final, a criação e o fechamento do artigo da base de conhecimento.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Explorar • Washington DC • Noções básicas do Security Incident Response • Separação de domínios e Security Incident Response • IU de segurança (vídeo)	Configurar • Instalar e configurar Security Incident Response • Noções básicas sobre a definição de processo do Security Incident Response	Administrar • Outras tarefas de configuração Security Incident Response adicionais • Relatório do Security Incident Response
Usar • Gerenciamento de incidentes de segurança e solicitações de entrada • Gerenciar pesquisas e verificações • Gerenciar atividades pós-incidente • Experiência Móvel para Security Incident Response	Desenvolver • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação • Orquestração de resposta de incidente de segurança	Integrar • Integrações do Security Incident Response • ServiceNow Security Operations diretrizes de desenvolvimento de integração • Dicas para escrever integrações
Solução de problemas e obter ajuda		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Faça ou responda perguntas na comunidade do Security Operations
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Solicitar um aplicativo Security Operations na Store

Se você é um novo cliente [Security Operations no London Patch 6 ou posterior, visite o ServiceNow Store site para exibir todos os aplicativos disponíveis e para obter informações sobre como enviar solicitações para a loja.

Noções básicas do Security Incident Response

Com Security Incident Response (SIR), gerencie o ciclo de vida de seus incidentes de segurança, desde a análise inicial até a contenção, erradicação e recuperação. O Security Incident Response permite que você obtenha uma compreensão abrangente dos procedimentos de resposta do incidente realizados por seus analistas e entenda as tendências e os gargalos nesses procedimentos com painéis e relatórios orientados por análise.

Uma introdução ao Security Incident Response, mostrando como começar a usar a aplicação.

Assista a este vídeo de nove minutos para saber mais sobre o processo de SIR, usando Security Incident Response para impedir ataques e exibindo a atividade de segurança no Security Incident Response Explorer.

Integrações integradas com soluções de segurança cibernética de terceiros e integrações desenvolvidas por parceiros da ServiceNow Store permitem automação e orquestração de segurança para uma resposta do incidente precisa e eficiente.

Para proteger suas investigações e manter os incidentes de segurança privados, Security Incident Response fornece os meios para restringir o acesso ao sistema a funções e ACLs relacionadas à segurança específicas. Os administradores que não sejam de segurança podem ter acesso restrito, a menos que você permita expressamente a entrada.

Nota:
Os administradores do sistema de TI [admin] podem representar usuários da ServiceNow. No entanto, ao representar um usuário com uma função de administrador de aplicação para o Security Incident Response, um administrador não pode acessar os recursos concedidos por essa função, incluindo incidentes de segurança e informações de perfil. O acesso a módulos e aplicações na barra de navegação também é restrito. Além disso, o administrador não pode mudar a senha de qualquer usuário com uma função de administrador de aplicação para o Security Incident Response.

Fluxo de informações de SIR

O Security Incident Response emprega o seguinte fluxo de informações, desde a integração até a investigação e, em seguida, até a resolução e a revisão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de informações do Security Incident Response

Discovery

Os incidentes de segurança podem ser registrados em log ou criados das seguintes maneiras.

- No formulário de Incidente de segurança
- De eventos gerados internamente ou criados por monitoramento externo ou sistemas de acompanhamento de vulnerabilidades por meio de regras de alerta ou manualmente
- De sistemas externos de monitoramento ou acompanhamento
- No catálogo de serviços

Análise

Dependendo da exibição selecionada que você está usando (padrão, Segurança não relacionada a TI, Segurança ITIL e assim por diante), o formulário de Incidente de segurança pode mostrar qualquer combinação de vulnerabilidades, incidentes, mudanças, problemas, tarefas no IC afetado e no IC afetado grupos. O sistema pode identificar malware, vírus e outras áreas de vulnerabilidade por referência cruzada ao banco de dados do Instituto Nacional de Padrões e Tecnologia (NIST) ou outro software de detecção de terceiros. Conforme os incidentes de segurança são resolvidos, você pode usar qualquer incidente para criar um artigo da base de conhecimento de segurança para referência futura.

Realize análises adicionais usando um mapa de serviços de negócios para localizar outros sistemas afetados ou serviços de negócios que podem estar infectados.

Contenção, Erradicação e Recuperação

Ao monitorar e analisar vulnerabilidades, você pode criar e atribuir tarefas a outros departamentos. Você pode usar um mapa de serviço de negócios para criar tarefas, problemas ou mudanças para todos os sistemas afetados, documentos, atividades, mensagens SMS, chamadas em ponte e assim por diante.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Revisar

Depois que o incidente for resolvido, outras etapas podem ocorrer antes do fechamento. Você pode executar uma revisão pós-incidente. Criar artigos da base de conhecimento pode ajudar em incidentes semelhantes futuros. Incidentes significativos podem exigir uma revisão de resolução pós-incidente. Esta revisão pode assumir várias formas. Por exemplo:

- Conduza uma reunião para discutir o incidente e coletar respostas.
- Escreva e distribua para as equipes que trabalharam em um incidente uma lista de perguntas de revisão de resolução projetadas para cada categoria ou prioridade de incidente.
- Os gerentes de incidentes podem escrever o relatório e coletar informações por conta própria.

Um relatório de revisão de resolução de incidente pode ser gerado automaticamente, incluindo:

1. um resumo do que foi feito
2. a linha do tempo
3. o tipo de incidente de segurança encontrado
4. todos os incidentes relacionados, mudanças, problemas, tarefas, grupos de IC
5. os detalhes da resolução

Além disso, um sistema de pesquisa de revisão de resolução de incidente de segurança automatizado está disponível. Ele reúne os nomes de todos os usuários atribuídos a um incidente de segurança e envia uma pesquisa personalizada para coletar dados sobre o tratamento do incidente. Esses dados podem ser disponibilizados em um relatório de revisão de incidente de segurança gerado, que você pode editar em um rascunho final. Dados semelhantes podem ser adicionados a um artigo da base de conhecimento para conter as lições aprendidas e as etapas a serem executadas para resolver problemas semelhantes no futuro.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Terminologia do Security Incident Response

Os termos a seguir são usados em Security Incident Response.

Termo	Definição
Ativo	Qualquer incidente de segurança que não esteja no estado encerrado ou cancelado.
Bloqueio de administrador	A capacidade de restringir o acesso Security Incident Response ao pessoal com funções relacionadas à segurança e ACLs.
Solicitações de segurança de entrada	Solicitações enviadas para demandas de segurança de baixo impacto, como solicitar um novo crachá eletrônico.
Gerenciar atividades pós-incidente	Uma revisão das origens e do tratamento de um incidente de segurança. O produto final é um relatório pós-incidente, que documenta todas as ações realizadas e os motivos para realizá-las.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Termo	Definição
Tarefas de resposta	Tarefas atribuídas a um incidente de segurança para rastrear ações em resposta à ameaça.
Noções básicas sobre calculadoras de incidentes de segurança	Calculadoras usadas para atualizar valores de registro quando condições pré-configuradas são atendidas.
Mapas de árvore de incidentes de segurança	Tipo de gráfico que mostra hierarquicamente os dados de incidentes de segurança na forma de retângulos aninhados.
Pesquisa de ameaças	Uma solicitação enviada do catálogo de incidentes de segurança para verificação de arquivos, URLs e endereços IP em busca de malware.
Verificação de vulnerabilidade	Uma solicitação iniciada no formulário de Incidente de segurança para verificar os recursos afetados (servidores, computadores e outros itens de configuração) em busca de vulnerabilidades.

Separação de domínios e Security Incident Response

Separação de domínios é compatível com Security Incident Response. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Padrão

- Inclui nível de suporte **Básico**.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Visão geral

Na aplicação Security Incident Response, a separação de domínio permite que os provedores de serviço (SPs) padronizem os procedimentos SOC (Security Operations Center) e Security Incident Response (SIR) em toda a base de clientes que atendem com custos operacionais reduzidos e uma qualidade de serviço superior. Separar espaços do cliente para fluxos de trabalho, painéis, relatórios e assim por diante garante que os dados do cliente sejam separados e nunca expostos a outros clientes.

Suporte à separação de domínio no Security Incident Response por versões

Liberação	Nível de suporte	Anotações
Genebra, Helsinki	Sem suporte	Início da separação de domínios no nível de dados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Suporte à separação de domínio no Security Incident Response por versões

Liberação	Nível de suporte	Anotações
Istambul	Somente dados	
Jakarta	Nível 2 (Dados, Solicitante, Executante)	**Novos recursos**: suporte a integrações de terceiros com separação de domínio de nível 2 em uma única instância de integração, incluindo integrações de Inteligência contra ameaças
Kingston	Nível 2 (Dados, Solicitante, Executante)	**Novos recursos**: a integração do Sighting Search para SIR é habilitada com várias instâncias, mas todas as instâncias ainda estão em um único domínio. Exemplo: se houver duas instâncias de uma integração Splunk configurada (SplunkCLOUD e SplunkCORP), ambas ainda serão aproveitadas para atividades de resposta do incidente em um único domínio, onde a implementação foi configurada originalmente.
Londres	Nível 2 (Dados, Solicitante, Executante)	**Novos recursos**: todas as integrações residem em vários domínios
Madri	Nível 2 (Dados, Solicitante, Executante)	Todas as integrações agora podem residir em vários domínios. No exemplo acima, SplunkCloud pode ser domain1 e SplunkCORP domain2.
Nova York	Nível 2 (Dados, Solicitante, Executante)	Todas as integrações residem em vários domínios.
Orlando	Padrão	Todas as integrações residem em vários domínios.
Paris	Padrão	Todas as integrações residem em vários domínios.

A separação de domínio para a aplicação Security Incident Response abrange a seguinte funcionalidade do produto:

- Os alertas de segurança são direcionados para o domínio apropriado do usuário cujo ID/credencial/escopo gera o incidente e é registrado como um incidente de segurança.
- Os alertas geram "observáveis", que representam propriedades com estado ou eventos mensuráveis: fluxos de trabalho de segurança no domínio do incidente de segurança são usados para orquestrar a resposta.
- As integrações são configuradas no domínio do incidente de segurança para automação de resposta.
- As capacidades são configuradas no domínio do incidente de segurança para automação de resposta. Esses recursos (a partir da versão Kingston) incluem:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

  - Pesquisa de ameaças
  - Aprimorar Observável
  - Aprimorar item de configuração
  - Obter processo em execução
  - Obter Estatísticas de Rede
  - Bloquear Solicitação
  - Isolar Host
  - Pesquisa de Vistas
  - Pesquisa e Exclusão de E-mails
  - Publicar na Watchlist
- Os resultados da automação de resposta (como Pesquisa de ameaças ou Pesquisa de detecções) são armazenados no domínio do incidente de segurança.
- Outros incidentes de segurança são referenciados cruzadamente no mesmo domínio do incidente de segurança com base em um conjunto compartilhado de observáveis.
- Outros usuários têm referência cruzada no domínio do incidente de segurança.
- Os itens de configuração são referenciados cruzadamente no mesmo domínio do incidente de segurança.
- Tarefas de resposta manuais são adicionadas ao domínio do incidente de segurança.
- Os artigos da base de conhecimento e os livros de execução são referenciados no domínio do incidente de segurança.
- As métricas do Security Incident Response pertinentes aos incidentes no domínio são exibidas em painéis, bem como em relatórios.

Nota:
Nos casos anteriores, os princípios abrangentes de visibilidade em domínios separados na NOW Platform se aplicam. Como sempre, um incidente no domínio primário pode fazer referência a artefatos no domínio secundário, mas não o contrário.

Como a separação de domínio funciona no Security Incident Response

A aplicação Security Incident Response gerencia o ciclo de vida de um incidente de segurança de ponta a ponta. Os casos de uso a seguir reconhecem a separação de domínio:

- **Ingestão de eventos e alertas** para criar incidentes de segurança para o analista no SOC do cliente ou no MSP responder:
  - Analisadores de e-mail (baseado em plataforma, phishing relatado pelo usuário, personalizado)
  - Eventos/alertas de desduplicação antes da criação do incidente
  - Extração automática de observáveis
  - Aplicações na loja SIEM de terceiros
- **Aprimoramento** de artefatos envolvidos nos incidentes (IP, URLs, domínios, hashes de arquivo):

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Aprimoramento de ativos (CMDB)
- Usuários (plataforma)
- Automação: aprimoramento de observável (por exemplo: WhoIs)

- **Investigar** os incidentes com a ajuda dos artefatos e sua reputação ou associação com ameaças conhecidas
  - Orchestrate: Playbooks e artigos da base de conhecimento
  - Automação: pesquisa de ameaças (por exemplo: VirusTotal), pesquisa de detecções (por exemplo: Splunk), obter processos em execução (por exemplo: Carbon Black)
- **Erradicar** os artefatos relacionados à ameaça envolvidos no incidente com base na investigação realizada
  - Orchestrate: Playbooks e artigos da base de conhecimento
  - Automação: pesquisa e exclusão de e-mail (por exemplo: Microsoft Exchange), Bloqueio de IP (por exemplo: firewall da Palo Alto)
- **Medir** a eficiência ou as operações de resposta a incidentes
  - Painéis de Performance Analytics: produtividade e tendências de incidentes
  - Reconstrução de etapas de investigação de incidentes a partir de anotações de trabalho
  - Revisão pós-incidente

Configuração do Domain Separation

Configurar o Domain Separation para Security Incident Response não requer etapas adicionais. Todas as tabelas Security Incident Response adquirem a coluna Domínio depois que a instância é separada por domínio.

Dados separados por domínio

Os dados podem ser separados por domínio, o que significa:

- Os incidentes de segurança em um domínio não podem ser exibidos em outros domínios.
- Os observáveis extraídos do incidente de segurança são colocados no mesmo domínio e não podem ser exibidos em outros domínios.
- Até a versão Kingston, as integrações de terceiros configuradas existem no domínio global e podem ser acessadas por todos os outros domínios na instância.
- Na versão Madrid, as integrações de terceiros podem ser configuradas e ativadas por domínio. Isso significa que a integração ativada e configurada em um domínio não pode ser aproveitada em outro domínio.
- As automações executadas nos observáveis usando integrações de terceiros (para investigação de ameaças, contenção ou erradicação) localizam seus resultados no domínio do incidente de segurança e não podem ser exibidos em outro domínio.
- Fluxos de trabalho de orquestração criados em um domínio não são visíveis em outro domínio.
- As capacidades (conforme delineadas na lista de funções de capacidades anteriores) que são invocadas permanecem genéricas em domínios com implementação específica de domínio da capacidade que está sendo chamada. Por exemplo, uma pesquisa de detecções em um IP pode invocar uma implementação Splunk em um domínio e uma implementação QRadar em outro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração

Todos os aspectos da configuração do produto são autônomos em um ambiente separado por domínio. A configuração pode ser personalizada para domínios individuais.

Nota:
A lógica de negócios e os processos nos itens 2 a 5 abaixo podem ser administrados no domínio do locatário.

As seguintes tarefas devem ser configuradas:

1. Administração do Sistema
   - Atribua funções a usuários e grupos de usuários: funções de usuário instaladas com o Security Incident Response
   - Instale um ou mais plug-ins de integração de terceiros para trabalhar com Security Incident Response: Integrações do Security Incident Response
2. Security Incident Response Administration
   - Adicionar ou revisar funções: Componentes instalados com Security Incident Response
   - Configurar grupos e usuários: Criar um grupo de incidentes de segurança
   - Configurar escalações de incidentes: Escalar um incidente de segurança
   - Configure calculadoras de pontuação de risco de incidente de segurança: Noções básicas sobre calculadoras de incidentes de segurança
   - Configurar acordos de nível de serviço: Criar um Security Incident Response ANS
   - Configure as definições do processo de incidente de segurança: Noções básicas sobre a definição de processo do Security Incident Response
   - Configure processos de revisão pós-incidente: Gerenciar atividades pós-incidente
3. Configurações de e-mail de incidente de segurança
   - Definir a caixa de entrada de análise de e-mail: Security Operations análise de e-mail
   - Configure analisadores de e-mail para ingestão de alertas: Criar analisadores de e-mail no Security Operations
   - Configure regras de correspondência de e-mail para phishing relatado pelo usuário: Criar regras para validar ataques de phishing relatados pelo usuário
   - Configurar ações de e-mail de entrada:ações de e-mail de entrada
4. Configurações do playbook de incidente de segurança
   - Revise e configure documentos do runbook: Criar um runbook do Security Incident Response
   - Configure fluxos de trabalho de incidente de segurança: Security Operations funcionalidade comum
5. Configurações de capacidade
   - Bloquear solicitação: Integração do Security Operations - Capacidade de solicitação de bloqueio
   - Pesquisa e exclusão de e-mail: Integração do Security Operations - Capacidade de pesquisa e exclusão de e-mail
   - Aprimorar item de configuração: Integração do Security Operations - Aprimorar capacidade de IC
   - Aprimorar observável: Integração do Security Operations - Capacidade Aprimorar observável
   - Obter estatísticas de rede: Integração do Security Operations - Obter recurso de estatísticas de rede

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Obter processos em execução: Integração do Security Operations - Obter capacidade de processos em execução
- Isolar host: Integração do Security Operations - Capacidade Isolar host
- Publicar na lista de observação: Integração do Security Operations - Capacidade de publicar na lista de observação
- Pesquisa de detecções: Integração do Security Operations com o recurso Pesquisa de detecções
- Pesquisa de ameaças: Integração do Security Operations - Pesquisa de ameaças

Como os domínios de locatário gerenciam seus dados de aplicação próprios

- Os proprietários de domínio de locatário criam suas próprias regras de análise de e-mail para ingerir incidentes de segurança.
- Os proprietários de domínio de locatário podem configurar integrações específicas exclusivamente para uso no domínio.
- Os proprietários de domínio de locatário podem criar seus próprios fluxos de trabalho de resposta do incidente.
- Os proprietários de domínio de locatário podem criar suas próprias categorias de incidentes, artigos da base de conhecimento de resposta do incidente e runbooks a serem associados aos fluxos de trabalho de resposta do incidente.
- Os usuários do domínio de locatário criam e fecham seus próprios incidentes de segurança.

Lógica de negócios e processos que podem ser separados por domínio pelo proprietário da instância

- Security Incident Response usuários e grupos
- Security Incident Response integrações (começando com a versão Madrid)
- Regras de análise de e-mail para criação de incidente
- Regras de negócios para consolidar vários eventos ou alertas em um incidente de segurança
- Fluxos de trabalho para orquestração de resposta do incidente
- Calculadoras de pontuação de risco de incidente de segurança
- Caminho de escalação de incidente de segurança
- ANS de incidente de segurança
- Definições de processo de incidente de segurança
- Processos de análise pós-incidente de segurança

Tópicos relacionados

Domain Separation para provedores de serviço

Configuração do Security Incident Response

A configuração de Security Incident Response envolve algumas etapas obrigatórias e várias etapas opcionais, dependendo dos seus requisitos específicos. Depois de baixar o Security Incident Response do ServiceNow Store e instalá-lo, você está pronto para executar o

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

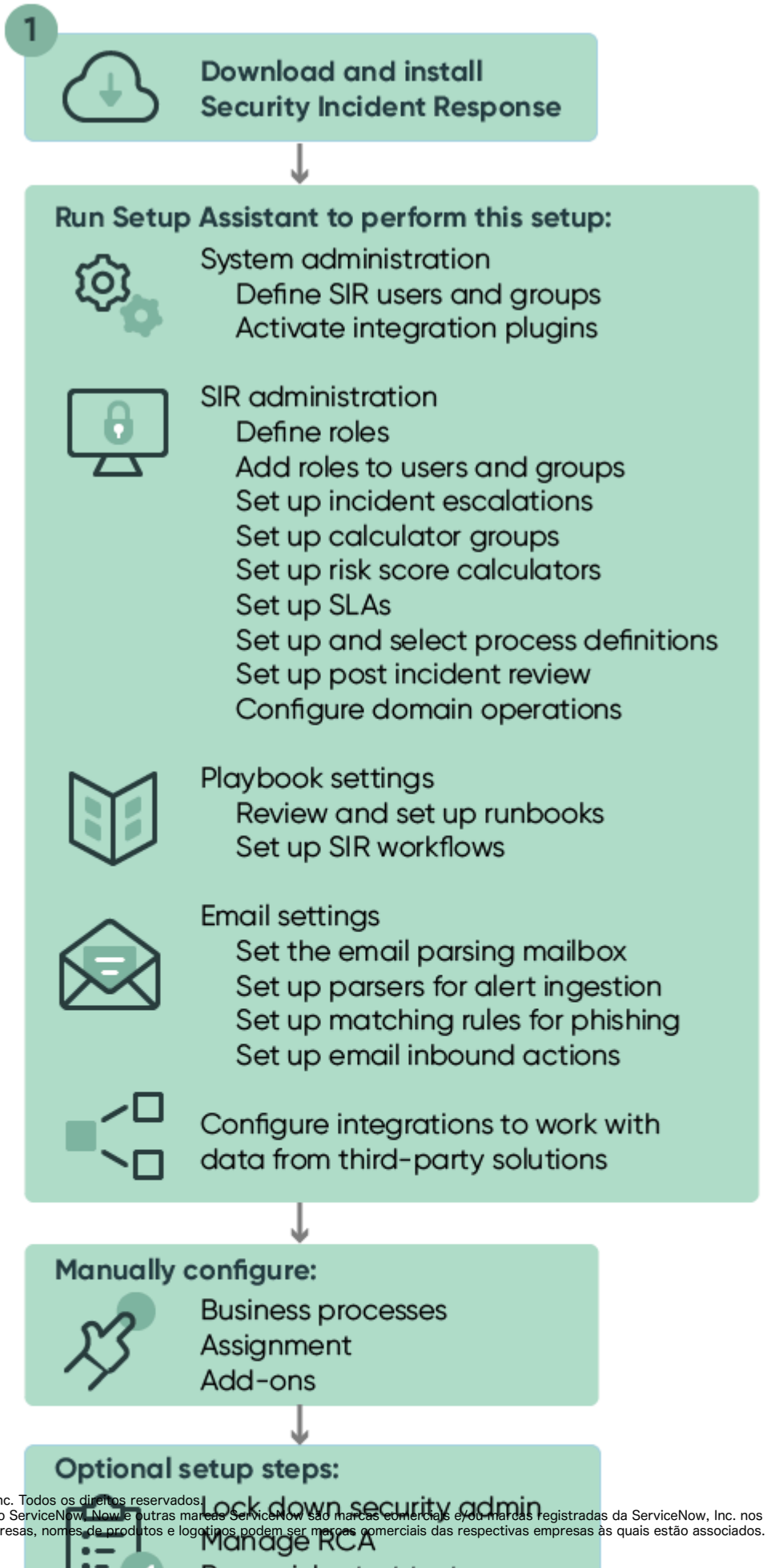
Assistente de configuração para executar a configuração básica do Security Incident Response e integrações de terceiros.

O Security Incident Response processo de configuração

O diagrama a seguir ilustra o processo de configuração. Ele é separado em dois subprocessos, baixando e configurando a aplicação Security Incident Response e, em seguida, baixando e configurando a Espaço do analista de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A primeira etapa da configuração é baixar o Security Incident Response aplicação do ServiceNow Store. Quando o download estiver concluído, vários aplicativos dependentes, incluindo o Assistente de configuração, serão carregados e estarão prontos para uso para configurar Security Incident Response.

Assistente de configuração

O Assistente de configuração Security Incident Response é uma aplicação semelhante a um assistente que orienta você, passo a passo, na configuração da sua instância Security Incident Response.

As etapas de configuração são bastante autoexplicativas; no entanto, se você precisar de explicação adicional, poderá encontrar assistência adicional na referência do Assistente de configuração. Depois de concluir a configuração usando o Assistente de configuração, você pode executar outros procedimentos de configuração opcionais, conforme necessário. Esses procedimentos incluem opções para:

- Como configurar o ciclo de vida da solicitação
- Criação de catálogos e solicitações
- Configurando notificações
- Configuração de atribuição manual e automática
- Habilitar a base de conhecimento, documentos gerenciados e atividades de tarefa

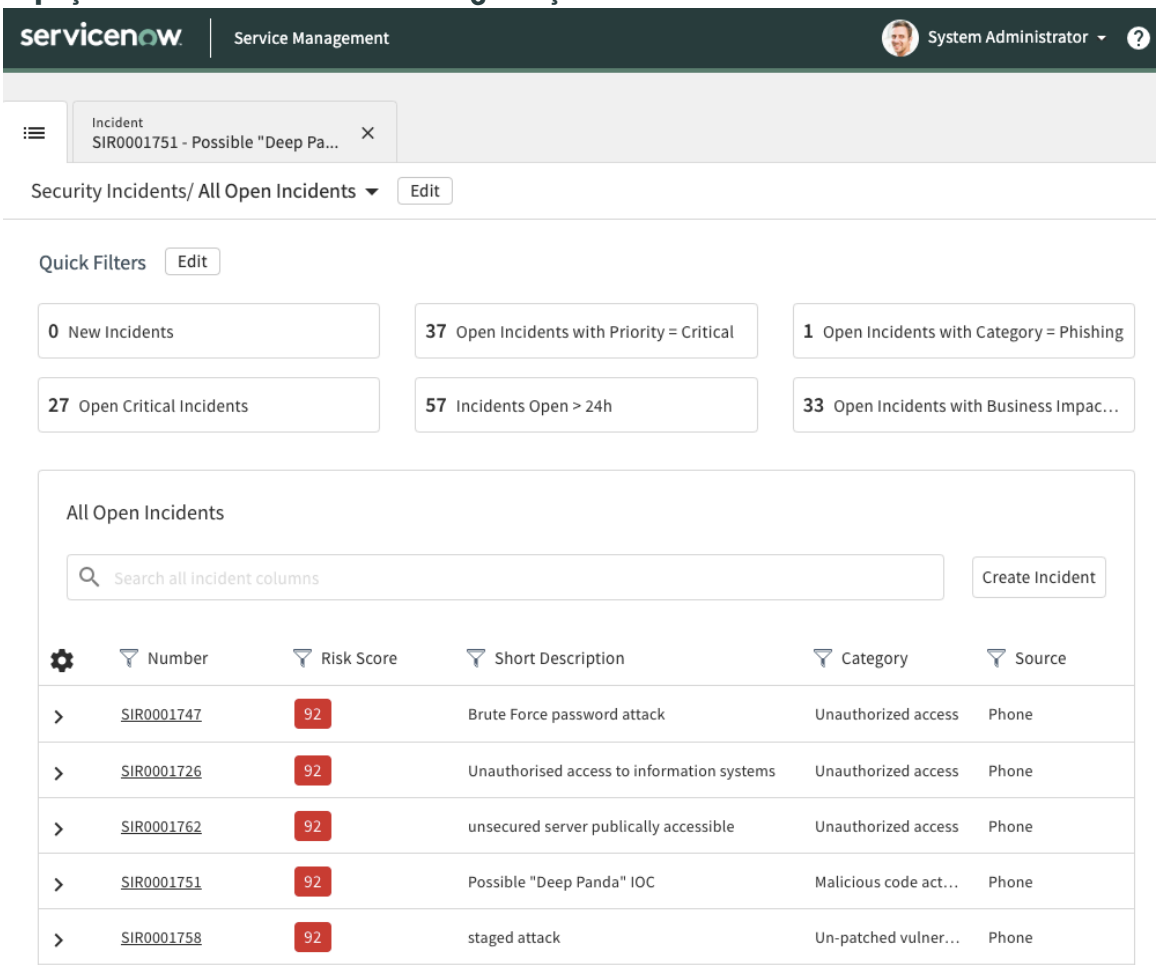
Espaço do analista de segurança

Ao concluir a configuração do Security Incident Response, você está pronto para instalar e configurar o Espaço do analista de segurança, o que simplifica a análise de incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Espaço de trabalho do analista de segurança



Primeiro, você deve baixar a aplicação de ServiceNow Store e configurá-la. O processo de configuração inclui a configuração de filtros primários e secundários para restringir a lista de incidentes de segurança para análise.

Depois de instalar e configurar a aplicação, você pode abrir o Security Analyst Workspace navegando até **Incidente de segurança** > **Incidentes (Nova IU)**.

Instalar e configurar Security Incident Response

Antes de executar Security Incident Response em sua instância, você deve baixá-lo do ServiceNow Store e concluir as etapas de configuração.

Antes de Iniciar

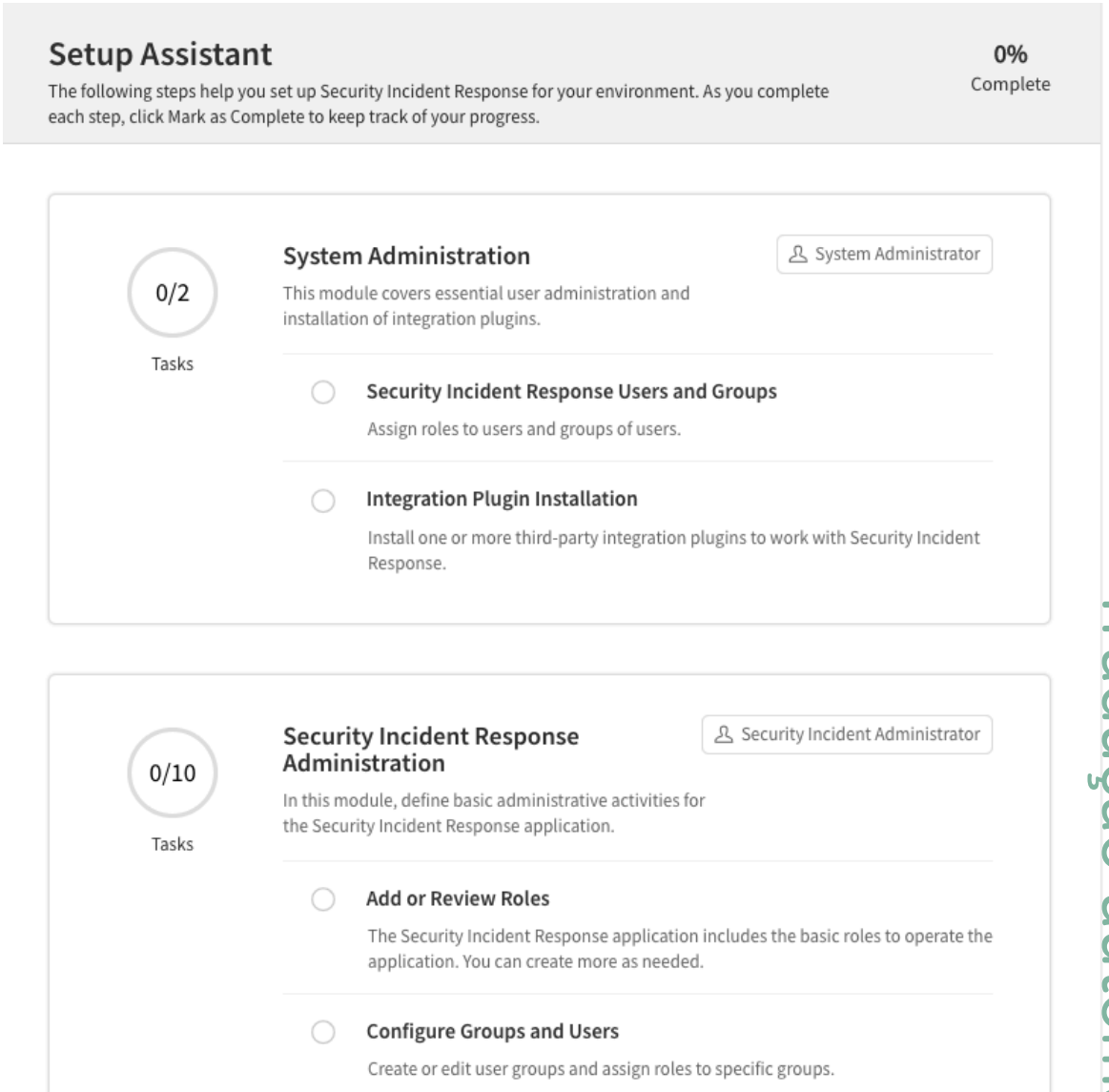
Função necessária: administrador

Procedimento

1. Siga as instruções para download de uma aplicação do ServiceNow Store.
2. Depois de baixar a aplicação Security Incident Response e todas as suas aplicações de dependência, navegue até **Incidente de segurança** > **Configuração do espaço do analista** > **Assistente de configuração**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Siga as instruções nos formulários para configurar o sistema de base Security Incident Response.
   Para obter informações adicionais sobre algumas das tarefas de configuração mais complicadas, consulte Referência do Assistente de configuração, conforme necessário.

Baixe e instale o Security Analyst Workspace

Antes de executar a Security Incident Response nova IU em sua instância, você deve baixá-la do ServiceNow® Store e instalá-la.

Antes de Iniciar

Para garantir uma instalação sem problemas, verifique se você tem as funções ServiceNow necessárias para sua instância. As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados:

- Se ainda não estiver atribuído, o administrador do sistema [admin] instalará a aplicação e atribuirá a função de administrador do Security Incident Response [sn_si.admin].
- O administrador do Security Incident Response [sn_si.admin] supervisiona a configuração e verifica os resultados esperados.

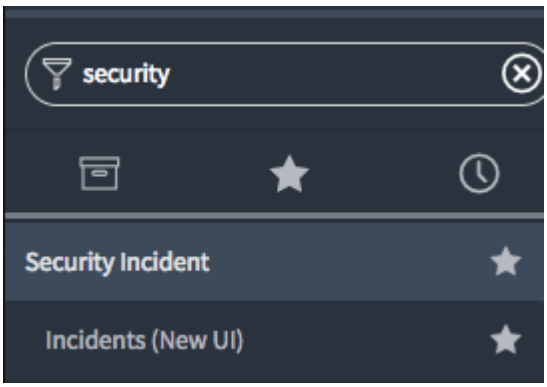
Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Siga as instruções para download de uma aplicação do ServiceNow Store e instale a aplicação **de IU do Security Incident Response**.
2. Após a conclusão da instalação, você pode abrir o Security Analyst Workspace navegando até **Incidente de segurança** > **Incidentes (Nova IU)**



Componentes instalados com Security Incident Response

Vários tipos de componentes são instalados com o download e a ativação da aplicação Security Incident Response, incluindo funções de usuário, tabelas, propriedades e trabalhos programados.

Nota:
A tabela Arquivos da Aplicação lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

Propriedades instaladas

Usuários com a função de administrador do sistema [admin] podem exibir as propriedades. Usuários com a função de administrador de segurança [sn_si.admin] podem modificá-las.

Propriedade	Uso
Hora de início padrão para todos os agentes quando nenhuma programação estiver definida, no formato 08:00 sn_si.default.start.time	• **Tipo**: cadeia de caracteres • **Valor padrão**: 08:00 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Hora de término padrão para todos os agentes quando nenhuma programação estiver definida, no formato 17:00 sn_si.default.end.time	• **Tipo**: cadeia de caracteres • **Valor padrão**: 17:00 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Incluir observáveis do tipo de destino junto com outros observáveis de tipo de contexto no usuário	Determina se um observável de incidente de segurança com um tipo de contexto de Destino é exibido nas guias

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Uso
de incidentes de segurança e relacionamentos de IC sn_si.link_dest_ip	**Itens de configuração** ou **Usuários afetados**. Por padrão, os observáveis com um tipo de contexto de destino são excluídos. Para incluir os observáveis, escolha Sim.
Permitir personalização ao criar um Problema ou uma Solicitação de mudança com base em um Incidente de segurança sn_si.popup	Quando um problema ou uma mudança são criados, esta propriedade abre uma janela pop-up para modificar a solicitação. Se essas propriedades estiverem definidas como **falsas**, o problema ou a solicitação de mudança terão a mesma prioridade, descrição resumida e descrição que o incidente de segurança sem a opção de adicionar ou editar esses campos. • **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Associe resultados de pesquisa de detecções a ICs no CMDB. sn_si.associate_ci_with_sighting_search	Quando definido como verdadeiro, os resultados da pesquisa de vistas incluem itens de configuração associados que estão no seu CMDB. • **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
A pontuação de risco no intervalo é realçada em verde, no formato 0 - 49 sn_si.risk.score.green	Na lista Incidentes de segurança, os incidentes de segurança com uma pontuação de risco entre 0 e 49 são marcados com um ponto verde.
A pontuação de risco no intervalo é realçada em laranja, no formato 50 a 79 sn_si.risk.score.orange	Na lista Incidentes de segurança, os incidentes de segurança com uma pontuação de risco entre 50 e 79 são marcados com um ponto laranja.
A pontuação de risco no intervalo é realçada em vermelho, no formato 80 a 100 sn_si.risk.score.red	Na lista Incidentes de segurança, os incidentes de segurança com uma pontuação de risco entre 80 e 100 são marcados com um ponto vermelho.
Este parâmetro ativa ou desativa as configurações de pesquisa de detecções que têm esse recurso implementado.	Quando definido como verdadeiro, as pesquisas de detecções podem ser realizadas em integrações ativadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Uso
sn_si.enable_sighting_search	• **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
O número de linhas de dados brutos é salvo quando for realizada uma pesquisa de detecções. Intervalo de 0 a 100 sn_si.sighting_search_raw_data_rows	Esta propriedade tem como padrão 50 linhas de dados brutos. Metade das linhas de resultados são relatadas a partir do início do intervalo de tempo de pesquisa e metade a partir do final do intervalo de tempo de pesquisa. Portanto, se você selecionar 50 linhas, 25 virão do início do intervalo de tempo de pesquisa e 25 do fim do intervalo de tempo de pesquisa.
Avançar automaticamente o Estado do Incidente para Conter quando uma Tarefa de Resposta avançar para Trabalho em Andamento sn_si.rollup_task_state	Ao usar fluxos ou fluxos de trabalho, considere definir esta propriedade como **falso**. Isso permite que você controle o Estado do incidente de dentro de fluxos ou fluxos de trabalho. Também ajuda a evitar possíveis conflitos durante a transição de um estado de incidente para outro. • **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Propriedades de atribuição do Security Incident Response	
Peso do local sn_si.location.weight	Uma classificação usada ao calcular os critérios a serem usados para atribuir automaticamente um analista de segurança. Se, por exemplo, o local for considerado para uma tarefa, o valor do peso do local será adicionado à classificação do analista de segurança. • **Tipo**: inteiro • **Valor padrão**: 10 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Peso das Habilidades sn_si.skills.weight	Uma classificação usada ao calcular os critérios a serem usados para atribuir automaticamente um analista de segurança. Se, por exemplo, habilidades forem consideradas para uma tarefa, o valor do peso das habilidades será adicionado à classificação do analista de segurança. • **Tipo**: inteiro • **Valor padrão**: 10 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Uso
Definir o número máximo de analistas de segurança a serem processados pela atribuição automática de uma vez sn_si.max.agents.processed	O sistema tem um limite absoluto de 300 analistas de segurança. Se você especificar mais de 300, ele definirá o valor para esse nível. O sistema não pode expedir automaticamente uma tarefa para um grupo de expedição que contém mais analistas de segurança do que o valor configurado. • **Tipo**: inteiro • **Valor padrão**: 100 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Peso do Fuso horário sn_si.timezone.weight	Uma classificação usada ao calcular os critérios a serem usados para atribuir automaticamente um analista de segurança. Se, por exemplo, o fuso horário do analista de segurança for considerado para uma tarefa, o valor do peso do fuso horário será adicionado à classificação do analista de segurança. • **Tipo**: inteiro • **Valor padrão**: 10 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Quantidade de tempo (em minutos) para adicionar entre o final de uma tarefa e o início da próxima viagem. sn_si.work.spacing	Um exemplo de valor de tempo válido é 10. • **Tipo**: inteiro • **Valor padrão**: 0 • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Campos de diário especificados que contenham marcadores de código que renderizem o conteúdo como HTML. sn_si.journal_field.html_enabled	• **Tipo**: cadeia de caracteres • **Valor padrão**: work_notes, comentários • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Calcule os serviços afetados em segundo plano. sn_si.refresh_impacted.event	A lista relacionada de Serviços afetados/ICs afetados é gerada por meio de eventos. Quando habilitada, a atualização é executada em segundo plano e os marcadores de segurança são adicionados ao incidente. Defina o valor como **verdadeiro** para executar a operação em segundo plano.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Uso
	• **Tipo**: verdadeiro | falso • **Valor-padrão**: falso • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**
Recupere o serviço essencial a partir de dados pré-calculados. sn_si.critical_service.calculator.use_cache	Permite que a calculadora de serviço essencial use dados pré-calculados de itens de configuração. Defina o valor como **verdadeiro** para pesquisar a partir de dados pré-calculados • **Tipo**: verdadeiro | falso • **Valor-padrão**: falso • **Local**: **Incidente de segurança** > **Administração** > **Propriedades**

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
Administrador de Incidente de segurança [sn_si.admin]	Controle total sobre todos os dados de Security Incident Response. Também gerencia territórios e habilidades, conforme necessário. **Nota:** No sistema de base, o administrador também tem acesso a sn_si.admin. Security Incident Response pode ser restringido pelo administrador, desde que pelo menos outro usuário tenha a função de administrador de segurança atribuída.	• assessment_admin • catalog_admin • decisão_tabela_admin • leitor_de_tabela_decisão • filter_admin • flow_designer • pd_author • pd_content_author • pd_operator • skill_admin • skill_model_admin • sn_si.analyst • sn_si.knowledge_admin • sn_si.manager • sn_sec_cmn.admin • sn_si.restriction_access_manager • sn_si.special_access_read_manager • sn_si.special_access_write_manager • sn_ti.malicious_attachment_access

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
		• sn_ti.observável.admin • tags_admin • template_admin • territory_admin • treemap_admin • user_admin
Analista de incidentes de segurança [sn_si.analyst]	Gerenciar incidentes de segurança. Função subjacente para acesso de segurança básico. Usuários com esta função podem criar e atualizar incidentes de segurança, solicitações e tarefas, bem como problemas, mudanças e indisponibilidades relacionadas a seus incidentes.	• pd_operator • snc_platform_rest_api_access • sn_msi.promotor • sn_msi.proposer • sn_si.basic • sn_ti.malicious_attachment_access
Incidente de segurança básico [sn_si.basic]	Função subjacente para acesso de segurança básico. Usuários com esta função podem criar e atualizar incidentes de segurança, solicitações e tarefas, bem como problemas, mudanças e indisponibilidades relacionadas a seus incidentes.	• canvas_user • document_management_user • e-mail_composer • flow_operator • Inventory_user • pa_viewer • service_fullfiller • skill_user • sn_sec_cmn.write • sn_si.read • sn_ti.observable.read • sn_ti.observable.write • sn_ti.read • task_activity_writer • task_editor • treemap_user

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
Diretor de segurança da informação (CISO) [sn_si.ciso]	Exibir e manipular o painel do CISO. Além disso, se o plug-in Vulnerability Response estiver ativado, os usuários com esta função poderão adicionar mapas de árvore de definição de significância de vulnerabilidade ao painel. Você também pode fazer o mesmo com o plug-in Security Incident Response.	• pa_viewer • sn_si.basic • sn_si.read
Incidente de segurança externo [sn_si.external]	Exibir todos os incidentes de segurança que pertencem ao grupo específico. **Nota:** As duas regras a seguir são aplicáveis em ServiceNow independentemente do administrador com escopo ou do app do escopo. • Ao adicionar qualquer usuário a um grupo, você também está atribuindo funções a esse grupo. Da mesma forma, quando você remove um usuário de um grupo, as funções herdadas também são removidas. • Cada função é atribuível por alguma função de precedência mais alta.	service_fulfiller

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
Usuário de integração de incidente de segurança [sn_si.integration_user]	Ferramentas externas podem fornecer novos registros de incidentes de segurança e atualizar registros de incidentes de segurança.	import_transformer
Administrador de conhecimento do incidente de segurança [sn_si.knowledge_admin]	Gerencie, atualize e exclua as informações na base de conhecimento do Incidente de Segurança.	• knowledge_admin • sn_si.read
Gerenciador de Incidentes de segurança [sn_si.manager]	Mesmo acesso que os analistas de segurança.	• pd_author • pd_operator • sn_si.basic
Leitura de incidente de segurança [sn_si.read]	Ler incidentes de segurança.	• canvas_user • sn_sec_cmn.read • sn_templated_snip.template_snippet_reader • sn_ti.observable.read • workspace_user
Gerenciador de acesso de restrição de segurança [sn_si.restriction_access_manager]	Permite que usuários ou grupos "imponham restrição" em incidentes de segurança. Isso se aplica somente à mudança de campo.	N/D
Acesso especial a incidente de segurança sn_si.special_access	Fornece acesso a incidentes de segurança específicos para usuários fora da organização do Security Operations.	N/D
Habilitador de acesso especial de segurança [sn_si.special_access_enabler]	Fornece função de acesso especial a um usuário fora da organização do Security Operations para incidentes de segurança específicos.	N/D
Gerenciador de leitura de acesso especial a incidentes de segurança [sn_si.special_access_read_manager]	Gerencie a função de acesso especial a incidentes de segurança [sn_si.special_access]. Use esta função para modificar o campo **Acesso de leitura** no formulário de incidente de segurança. Esta	sn_si.special_access_enabler

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
	função pode ser atribuída por sn_si.admin.	
Gerenciador do gravador de acesso especial a incidentes de segurança [sn_si.special_access_write_manager]	Gerencie a função de acesso especial a incidentes de segurança [sn_si.special_access]. Use esta função para modificar o campo **Acesso privilegiado** no formulário de incidente de segurança. Esta função pode ser atribuída por sn_si.admin.	sn_si.special_access_enabler

Trabalhos programados instalados

Trabalho programado	Descrição
Pesquisar observáveis de incidente de segurança	Executa uma pesquisa de observáveis em uma programação definida pelo usuário.

Tabelas instaladas

Tabela	Descrição
Configuração do Feed de Notícias [sn_si_feed_configuration]	Registros de configuração usados para definir o conteúdo exibido no feed de notícias de incidentes de segurança.
Regra de Atribuição de Análise Pós-incidente [sn_si_pir_condition]	Automatiza a seleção de participantes de uma pesquisa de revisão pós-incidente quando um incidente de segurança é encerrado.
Incidente de Segurança [sn_si_incident]	Armazena um incidente de segurança, as respostas ao incidente, todas as tarefas vinculadas, mudanças, problemas e incidentes relacionados a este incidente de segurança.
Vetores de Ataque do Incidente de Segurança [sn_si_attack_vector]	Opções de vetor de ataque.
Log de Auditoria de Incidentes de Segurança [sn_si_audit_log]	Armazena logs de auditoria de aprimoramento de incidentes de segurança.
Calculadora de Incidentes de Segurança [sn_si_calculator]	Uma calculadora para definir determinados campos de incidente de segurança quando certas condições são atendidas.
Grupo de Calculadoras de Incidentes de Segurança [sn_si_calculator_group]	Um agrupamento de calculadoras de incidente de segurança. A ordem do grupo de calculadoras

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
	determina qual grupo é avaliado primeiro e, em cada grupo, uma calculadora é usada no máximo.
Firewall de aprimoramento de incidente de segurança [sn_si_enrichment_firewall]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos do Firewall da Palo Alto Networks.
Resultados de malware de aprimoramento de incidente de segurança [sn_si_enrichment_malware]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos do malware.
Estatísticas de Rede de Aprimoramento de Incidente de Segurança [sn_si_enrichment_network_statistics]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos das estatísticas de rede.
Processos em execução de Aprimoramento de Incidente de Segurança [sn_si_enrichment_running _processes]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos para processos em execução.
Serviços de Execução de Aprimoramento de Incidente de Segurança [sn_si_enrichment_running_service]	Estende a partir da tabela base (sn_sec_cmn_enrichment_data_base) e inclui todos os registros de aprimoramento específicos para serviços em execução.
Pesquisa de E-mail de Incidente de Segurança [sn_si_m2m_incident_email_search]	Mapeia registros de pesquisa de e-mail para incidentes de segurança.
Importação de incidentes de segurança [sn_si_incident_import]	Tabela de importação para incidentes de segurança. Usado para criar incidentes de segurança a partir de sistemas externos.
Definição do Processo de Incidentes de Segurança [sn_si_process_definition]	Armazena a configuração dos fluxos do processo de incidente de segurança.
Seletor de Definição do Processo de Incidentes de Segurança [sn_si_process_definition_selector]	Armazena a definição do processo de incidente de segurança a ser usada para incidentes de segurança.
Caso do Atendimento ao cliente relacionado ao incidente de segurança [sn_si_m2m_incident_customerservice_case]	Mapeia casos de atendimento ao cliente e incidentes de segurança
Dados de aprimoramento relacionados ao Incidente de Segurança [sn_si_m2m_incident_enrichment]	Mapeia incidentes de segurança e registros de dados de aprimoramento relacionados.
Tarefa Security Incident Response [sn_si_task]	Gerencia subtarefas relacionadas à manipulação de um incidente de segurança. Essas tarefas podem ser atribuídas ao pessoal de segurança ou a pessoas em

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
	outros departamentos, para gerenciar a comunicação entre departamentos e o acompanhamento de tarefas.
Modelo de tarefas Security Incident Response [sn_si_task_template]	Usado para criar uma tarefa Security Incident Response. Esses modelos geralmente são usados em entradas do catálogo para criar automaticamente um conjunto de subtarefas apropriadas para um tipo específico de incidente de segurança.
Documento de runbook de incidente de segurança [sn_si_runbook_document]	Associa condições ou filtros de incidente de segurança a um artigo de conhecimento. Usado para especificar procedimentos de runbook para correção de incidente de segurança.
Modelo de Incidente de Segurança [sn_si_incident_template]	Usado para criar um incidente de segurança. Esses modelos geralmente são usados em entradas do catálogo para criar um incidente de segurança pré-criado.
Requisição de Segurança [sn_si_request]	Uma solicitação relacionada à segurança para a equipe de segurança.
Solicitação de Verificação de Segurança [sn_si_scan_request]	Uma solicitação de pesquisa de ameaças.
Calculadora de Gravidade sn_si_severity_calculator	Define os valores de severidade, impacto, risco e criticalidade de um incidente de segurança.
Usuário Afetado pela Tarefa [sn_si_m2m_task_affected_user]	Uma tabela muitos para muitos que associa incidentes de segurança aos usuários afetados.
Avaliador de Resultado de Atividade de Fluxo de Trabalho de Modelo [sn_si_wf_activity_outcome_evaluator]	Mapeia um recurso com um script de avaliação. Um novo subfluxo pode ser adicionado a um fluxo de trabalho de modelo para definir um resultado de tarefa de resposta em vez de ter um analista para defini-lo manualmente.

Tradução automática

Outras tarefas de configuração Security Incident Response adicionais

Se você for um administrador no domínio global, configure como Security Incident Response lida com as operações diárias.

Antes de Iniciar
Função necessária: sn_si.admin

Nota:

Essas opções são padrão para muitos aplicativos de gerenciamento de serviços e, como tal, eles usam a terminologia de gerenciamento de serviços. Por exemplo, Solicitação é usada para a tarefa principal (ou seja, o incidente de segurança) e Tarefa é usada para subtarefas ou Tarefas de resposta.

Se você for um administrador em um domínio inferior ao domínio global, poderá exibir a tela Configurações, mas modificar as configurações.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Administração** > **Configuração**.
   As opções para configurar as aplicações são organizadas nestas guias:
   - A guia **Processo de negócios** contém opções para configurar o ciclo de vida da solicitação, criar catálogos e solicitações e configurar notificações.
   - A guia **Atribuição** contém opções para configurar atribuições manuais e automáticas.
   - A guia **Complementos** contém opções para habilitar a base de conhecimento, documentos gerenciados e atividades de tarefa.
2. Preencha os campos na guia **Processo de negócios**.

Tela de configuração — Guia Processo de negócios

Campo	Descrição
Ciclo de vida	
As Anotações de trabalho são necessárias para fechar ou cancelar uma solicitação ou tarefa	Habilite esta opção para exigir que o usuário insira anotações de trabalho antes que um incidente de segurança ou tarefa de resposta possa ser fechado ou cancelado.
Copiar anotações de trabalho da tarefa para solicitação	Habilite esta opção para sincronizar as anotações de trabalho da tarefa de resposta com as anotações de trabalho no incidente de segurança. Portanto, quando as anotações de trabalho na tarefa são adicionadas, as mesmas anotações de trabalho aparecem no incidente de segurança primário.
Criação de Solicitação e Catálogo	
Criar ou atualizar solicitações por e-mail de entrada	Habilite esta opção para criar ou atualizar incidentes de segurança de e-mails de entrada.
As solicitações são criadas usando	Selecione **catálogo ou formulário regular** para ativar o catálogo e habilitar a publicação automática de modelos de incidente de segurança no catálogo. Selecione **o formulário regular somente** para desativar o catálogo e desabilitar a publicação automática de modelos de incidente de segurança no catálogo.
Os modelos criam um item do catálogo dedicado	Habilite esta opção para ativar a publicação automática de itens do catálogo para a aplicação.
Notificações	
Para uma solicitação ou tarefa, quando o campo selecionado for alterado, envie uma notificação aos destinatários	Você pode configurar notificações a serem enviadas para destinatários específicos quando os campos selecionados em incidentes de segurança e tarefas de resposta forem alterados. **a.** Na **Tabela**, selecione **Solicitação (incidente de segurança** ou **Tarefa (tarefa de resposta)**. **b.** Em **Campo**, selecione o campo a ser usado para gerar notificações. Quando uma mudança é feita no campo selecionado, uma notificação é enviada aos destinatários identificados. **c.** Em **Destinatários**, selecione um ou mais destinatários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	d. Se você selecionar **um usuário** ou **grupo específico**, será solicitado a selecionar um usuário ou grupo. **e.** Para definir mais notificações usando outros campos ou destinatários, repita as etapas anteriores para o próximo conjunto de configurações de notificação. **f.** Para remover uma notificação, clique no ícone de ⊖ à direita da notificação.

3. Clique na guia **Atribuição** e preencha os campos.

Tela de configuração — Guia Atribuição

Campo	Descrição
Método de atribuição para solicitações	Selecione o método para atribuir incidentes de segurança: ○ **usando atribuição automática**: os incidentes de segurança são atribuídos automaticamente. ○ **usando um fluxo de trabalho**: os incidentes de segurança são atribuídos pelo fluxo de trabalho selecionado. ○ **manualmente**: os incidentes de segurança são atribuídos manualmente.
Use este fluxo de trabalho para atribuir solicitações	Selecione o fluxo de trabalho para expedir incidentes de segurança. Este campo aparece quando **o uso de um fluxo de trabalho** é selecionado na lista **Método de atribuição para solicitações**.
Método de atribuição para tarefas	Selecione o método para atribuir tarefas de resposta: ○ **usando atribuição automática : as**tarefas de resposta são atribuídas automaticamente. ○ **usando um fluxo de trabalho**: as tarefas de resposta são atribuídas pelo fluxo de trabalho selecionado. ○ **manualmente**: as tarefas de resposta são atribuídas manualmente.
Use este fluxo de trabalho para atribuir tarefas	Selecione o fluxo de trabalho para atribuir tarefas de resposta. Este campo aparece quando **o uso de um fluxo de trabalho** é selecionado na lista **Método de atribuição para tarefas**.
Atribuir solicitações ou tarefas com base nas áreas cobertas do grupo de atribuições	Habilite esta opção para limitar a atribuição de incidentes de segurança e tarefas de resposta a grupos que cobrem o local da tarefa.
Programando	
A seleção automática de agentes considera o fuso horário das tarefas	Habilite esta opção para considerar o fuso horário do agente ao atribuir uma tarefa. Este campo aparece quando a atribuição automática é selecionada para incidentes de segurança ou tarefas de resposta.
Fatores adicionais	

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
A seleção automática de agentes considera a localização dos agentes	Habilite esta opção para dar preferência aos agentes que estão mais próximos do local da tarefa ao atribuir tarefas. Este campo aparece quando a atribuição automática é selecionada para incidentes de segurança ou tarefas de resposta.
A seleção automática de agentes requer que eles tenham habilidades	Selecione o grau em que as habilidades do agente devem corresponder a uma tarefa ao determinar a atribuição automática. ○ Selecione **tudo** para exigir que um agente atribuído tenha todas as habilidades para executar a tarefa. Um agente que não tem pelo menos uma habilidade é eliminado. ○ Selecione **alguns** se quiser que os agentes tenham a maioria das habilidades necessárias para executar a tarefa. ○ Selecione **Nenhum** se quiser atribuir automaticamente os agentes sem levar em conta as habilidades. Este campo aparece quando a atribuição automática é selecionada para incidentes de segurança ou tarefas de resposta.
Tentativa de seleção automática de atribuir o mesmo agente a todas as tarefas em uma solicitação	Habilite esta opção para atribuir automaticamente todas as tarefas de resposta de um incidente de segurança ao mesmo agente.

4. Clique na guia **Complementos** e preencha os campos.

Tela de configuração — Guia Complementos

Campo	Descrição
Documentação	
Habilitar uma base de conhecimento dedicada	Habilite esta opção para ativar a base de conhecimento para Security Incident Response.
Habilitar documentos gerenciados	Habilite esta opção para adicionar uma lista relacionada a documentos gerenciados.
Habilitar atividades da tarefa	Habilite esta opção para registrar interações e comunicações de tarefa, como chamadas telefônicas e mensagens de e-mail.

5. Clique em **Salvar**.

Bloquear administração de segurança

Para proteger as investigações e manter os incidentes de segurança privados, você pode restringir o acesso Security Incident Response a funções e ACLs específicas de segurança. Os administradores que não sejam de segurança podem ter acesso restrito, a menos que você permita expressamente a entrada.

Antes de Iniciar

Quando a aplicação Security Incident Response é ativada, o usuário Administrador do sistema recebe a função sn_si.admin por padrão. O administrador do sistema é o único administrador que pode configurar grupos de segurança e usuários.

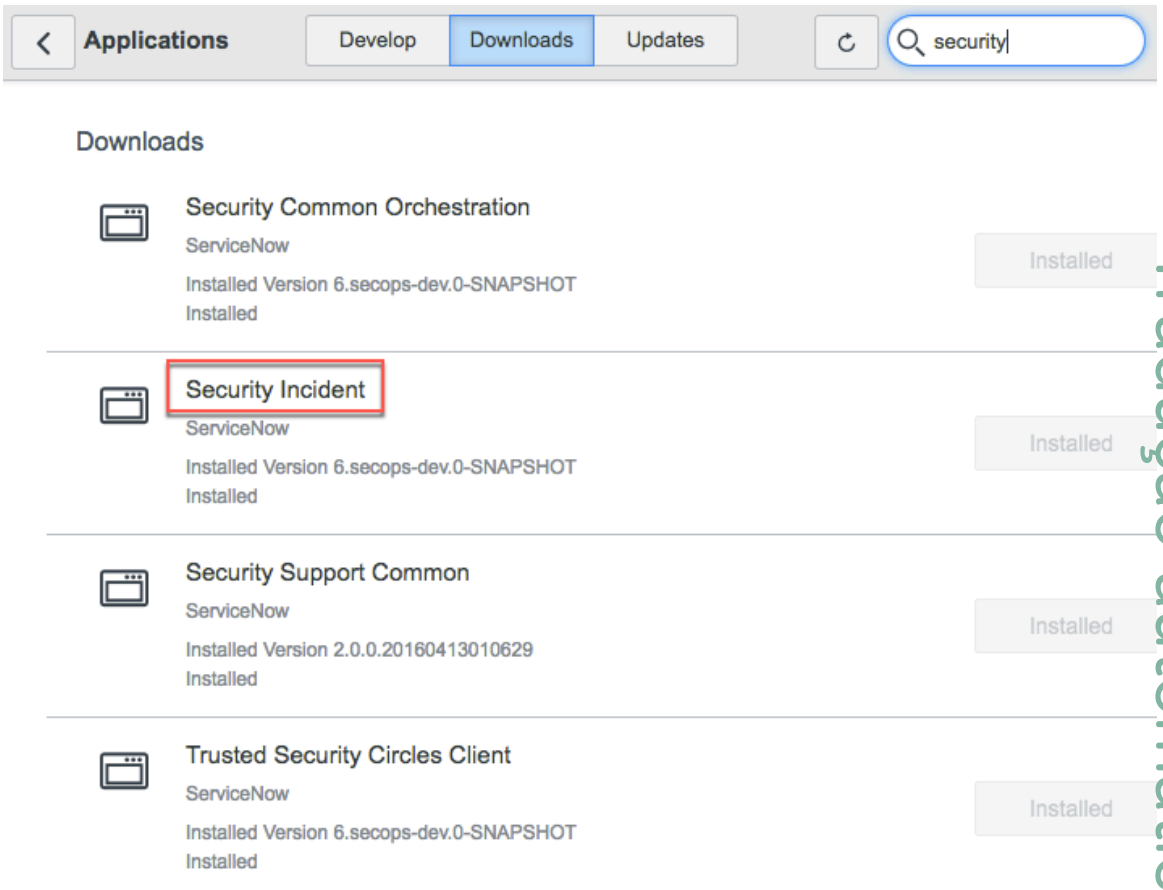
Uma função de segurança é necessária para ter acesso a Security Incident Response recursos e registros.

Função necessária: sn_si.admin

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Depois que o plug-in Security Incident Response tiver sido ativado, um usuário com a função de administrador atribuirá a função de administrador com escopo (sn_si.admin) a pelo menos um usuário.
2. O usuário com a função de administrador muda para o escopo do Incidente de segurança.
3. Navegar até **Aplicações do sistema** > **Aplicações**.
4. Clique **em Downloads**.
5. Digite **segurança** no campo **Pesquisar aplicações**.



6. Clique **em Incidente de segurança**.
7. Role para baixo até **Links relacionados** e clique em **Remover da função contida pelo administrador**.
8. Saia e faça login novamente.
   O usuário administrador não pode acessar a aplicação Security Incident Response.

Tópicos relacionados

Administração de aplicação

Gerenciar acesso restrito de solicitante

O recurso Acesso Restrito de Chamador (RCA) permite que um administrador defina o acesso entre escopos a uma aplicação ou recurso de aplicação e permita ou negue solicitações de acesso. Este recurso é habilitado em Security Incident Response por padrão para que os analistas de segurança possam proteger informações confidenciais relacionadas à segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um campo chamado **Acesso** do solicitante foi adicionado a todas as tabelas e inclusões de script em Security Incident Responsee o campo é padronizado como **Rastreamento de chamadas**. Esta configuração significa que os escopos da aplicação têm permissão para acessar Security Incident Response tabelas e inclusões de script. No entanto, um registro de acompanhamento é criado para cada registro e armazenado na tabela Privilégio de acesso restrito do solicitante [sys_restricted_caller_access].

Nota:
Tenha cuidado ao mudar registros de **Rastreamento** de **chamador para Restrito**ao chamador. Registros com este status não podem ser acessados até que um administrador permita o acesso manualmente. O administrador deve navegar até **Aplicações do sistema** > **Acesso de chamador restrito a aplicação**, localize a tabela ou inclusão de script para a qual o acesso foi solicitado e altere o campo **Status** de **Solicitado** para **Permitido**.

Tópicos relacionados

Configurações de privilégio de acesso de chamador restrito

Definir o escopo da aplicação, o recurso da aplicação e o acesso ao evento

Executar testes de início rápido para Security Incident Response

Valide se Security Incident Response ainda funciona depois de fazer mudanças de configuração, como aplicar uma atualização ou desenvolver uma aplicação. Copie e personalize esses testes de início rápido para aprovar ao usar seus dados específicos da instância.

Os testes de início rápido Security Incident Response exigem a ativação do plug-in Security Incident Response (com.snc.security_incident) e o carregamento dos dados de demonstração.

Testes Security Incident Response

Teste	Descrição	Versão de lançamento
SIR: criar incidente de segurança	Determine se um usuário pode criar um incidente de segurança com êxito a partir do formulário de incidente de segurança.	Washington DC
SIR: criar incidente de segurança por meio do catálogo de incidentes de segurança	Determine se um usuário pode criar um incidente de segurança com êxito a partir do formulário de incidente de segurança.	Washington DC
SIR: ciclo de vida do incidente de segurança	Valide as tarefas de resposta do fluxo de trabalho de violação de política.	Washington DC
SIR: pesquisa de ameaças	Valida a funcionalidade de pesquisa de ameaças.	Washington DC
SIR: configuração OOTB das avaliações de PIR	Use este teste para validar avaliações de PIR e configurações de sistema de base.	Washington DC
SIR: configuração condicional das avaliações de PIR	Verifique se incidentes de segurança correspondentes à regra condicional obrigatória não são	Washington DC

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes Security Incident Response

Teste	Descrição	Versão de lançamento
	encerrados sem a conclusão da avaliação pós-incidente. Verifique se os incidentes de segurança correspondentes à regra condicional opcional podem ser encerrados sem a conclusão da avaliação pós-incidente. Verifique se as avaliações não são geradas para os incidentes de segurança que não correspondem a nenhuma regra.	
SIR: verificação do tempo de execução do PIR	Verifique se os relatórios PIR estão configurados e anexados aos incidentes de segurança de acordo com o novo design.	Washington DC
SIR: verificação de configuração do tempo de design do PIR	Verifique se o incidente de segurança está mapeado com o modelo de relatório baseado na configuração do administrador.	Washington DC
SIR: Vincular o incidente de segurança a um importante incidente de segurança existente	Vincule um Incidente de Segurança a um Incidente de Segurança Importante existente e valide os dados do Incidente de Segurança implementados no Incidente de Segurança Importante.	Washington DC
SIR: promover o incidente de segurança como um incidente de segurança importante	Promova um Incidente de Segurança como um Incidente de Segurança Importante e valide os dados do Incidente de Segurança implementados no Incidente de Segurança Importante.	Washington DC
SIR: propor Incidente de Segurança como Incidente de Segurança Importante	Proponha um Incidente de Segurança como Incidente de Segurança Importante e valide os dados de Incidente de Segurança implementados no Incidente de Segurança Importante.	Washington DC
Verifique se somente Membros permitidos podem acessar o incidente de segurança quando a opção Impor restrição estiver ATIVADA	Verifique se somente os membros permitidos podem acessar o incidente de segurança quando a opção Impor restrição estiver habilitada.	Washington DC
Verifique se somente grupos permitidos podem acessar o incidente de segurança quando	Verifique se somente os grupos permitidos podem acessar o incidente de segurança quando	Washington DC

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes Security Incident Response

Teste	Descrição	Versão de lançamento
a opção Impor restrição estiver ATIVADA	a opção Impor restrição estiver habilitada.	
Validar acesso de leitura	Valide o acesso de exibição.	Washington DC
Validar acesso de gravação	Valide o acesso de edição.	Washington DC

Tópicos relacionados

Testes de início rápido

Referência do Assistente de configuração

O Assistente de configuração orienta você nas etapas necessárias para configurar o sistema de base Security Incident Response. Esta seção fornece informações adicionais sobre as etapas complicadas para as quais você pode precisar de mais explicações.

Criar uma definição de processo Security Incident Response

Você pode criar uma definição de processo para definir a maneira como os incidentes de segurança fazem a transição de um estado para o próximo. As definições de processo ajudam as centrais de serviços e os usuários finais a rastrear o problema durante todo o ciclo de vida.

Antes de Iniciar

Função necessária: sn.si_admin

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Administração** > **Definição de Processo**.
2. Clique em **Nova**.
3. Preencha os campos, se for o caso.

Criando definições de processo

Campo	Descrição
Nome	Nome do registro que descreve o processo codificado no arquivo de inclusão de script. O nome é exibido como uma opção na lista do **Seletor de definição de processo**.
Script Include	O nome (incluindo o prefixo `sn_si.`) da inclusão de script que contém a definição do processo. O script deve estar no escopo da aplicação Incidente de segurança (`sn_si`). Para obter mais informações, consulte Criar uma inclusão de script de definição de processo personalizada Security Incident Response. Se este campo não contiver um nome de inclusão de script válido, a definição padrão de ProcessDefinition_NIST_Stateful será usada.
Descrição	Informações úteis sobre a inclusão de script.
Ordem	Determina a posição na lista de definição de processo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Quando marcada, torna esta definição de processo selecionável na página **Seletor de definição** de processo.

4. Clique em **Enviar**.

Tópicos relacionados

Seleção de processo do Security Incident Response

Noções básicas sobre a definição de processo do Security Incident Response

Noções básicas sobre a definição de processo do Security Incident Response

Security Incident Response Definição de Processo substitui fluxos de estado e fornece aos usuários finais e centrais de serviços o status de um problema. Uma definição de processo ajuda a rastrear o problema durante seu ciclo de vida. Security Incident Response é uma aplicação Service Management (SM), que tem seu próprio conjunto de estados. Estados inválidos são relatados como parte de Seleção de processo.

Definição de processo do Security Incident Response

A definição de processo padrão (NIST Stateful) define os seguintes estados de incidente:

Nota:
Os estados disponíveis variam de acordo com o estado atual do incidente.

Estados de definição do processo de Incidente de segurança

Estado	Descrição
Rascunho	O iniciador da solicitação adiciona informações sobre o incidente de segurança, mas ainda não está pronto para ser trabalhado.
Análise	O incidente foi atribuído e o problema está sendo analisado.
Contém	O problema foi identificado e a equipe de segurança está trabalhando para contê-lo e executar o controle de danos. Essas ações podem incluir colocar os servidores off-line, desconectar equipamentos da Internet e verificar se existem backups.
Erradicar	O problema foi contido e a equipe de segurança está tomando medidas para corrigir o problema.
Recuperar	O problema foi resolvido e a prontidão operacional dos sistemas afetados está sendo verificada.
Revisar	O incidente de segurança foi concluído e todos os sistemas estão de volta à função normal. No entanto, uma revisão pós-incidente ainda é necessária.
Encerrado	O incidente está concluído, mas antes que um incidente de segurança possa ser encerrado, você deve preencher as informações na guia **Informações de fechamento**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definições de processo de tarefa de Incidente de segurança

As definições de processo a seguir são usadas para tarefas de incidente de segurança.

Estados da definição do processo da tarefa

Estado	Descrição
Pronto	A tarefa está pronta para ser trabalhada depois de ser atribuída a um agente.
Atribuído em	A tarefa é atribuída a um agente.
Trabalho em andamento	O agente atribuído está trabalhando na tarefa.
Concluir	A tarefa está concluída.
Cancelado	A tarefa foi cancelada.

O NIST oferece suporte aos dois modelos a seguir:

- **NIST com estado**

  Esta definição de processo permite que os analistas passem de um estado para outro em uma ordem sequencial sem ignorar nenhuma etapa. Por exemplo, se o Analista iniciar com o estado **Rascunho**, a ordem sequencial desta definição de processo será **Rascunho**>**Análise**>**Conter**>**Erradicar**>**Recuperar**. Portanto, a definição do processo com estado do NIST é unidirecional e permite que os analistas avancem somente para os estados avançados.

  Aqui está outro exemplo, se o Analista iniciar com o estado Análise, a ordem sequencial desta definição de processo será **Análise**>**Conter**>**Erradicar**>**Recuperar**.

- **NIST em aberto**

  Esta definição de processo permite que os analistas passem de um estado para outro, seja para frente ou para trás. Por exemplo, se o Analista iniciar com o estado **Análise**, a ordem da definição do processo poderá ser **Análise**>**Conter**>**Erradicar**>**Recuperar** ou **Análise**>**Rascunho**. Portanto, a definição do processo NIST Open é bidirecional e permite que os analistas avancem ou retrocedam, dependendo dos requisitos.

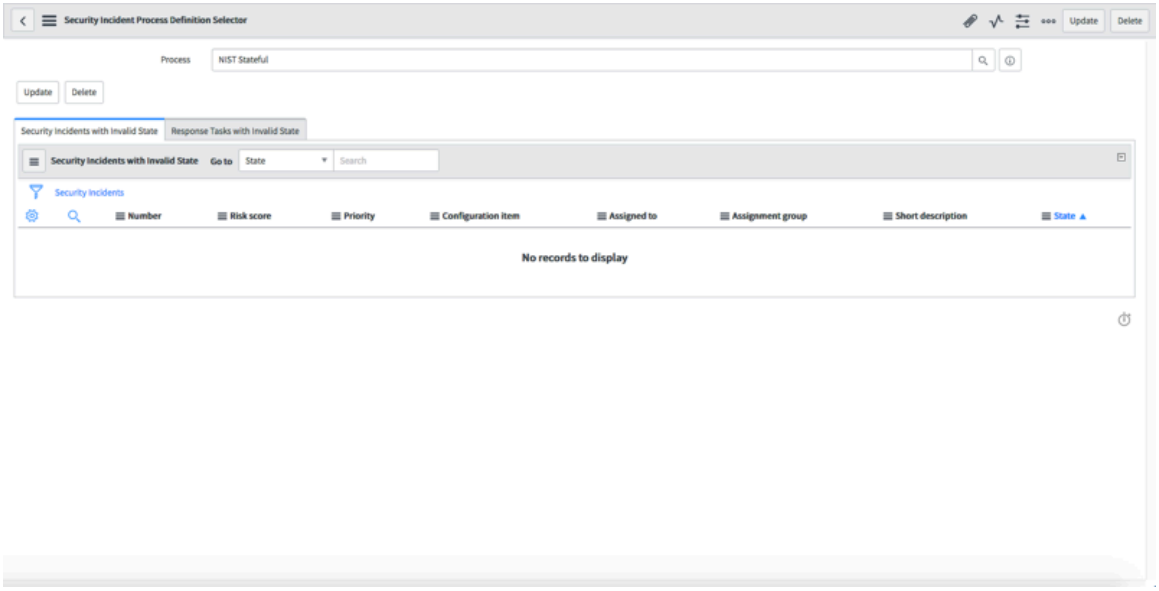
Seleção de processo do Security Incident Response

Seleção de processo lista processos com estados inválidos para incidentes de segurança e tarefas de resposta.

Um administrador pode corrigir o incidente ou a tarefa para estados válidos manualmente ou usando um script. Uma lista relacionada vazia (sem incidentes; sem tarefas) indica que todas as tarefas ativas estão em um estado válido. Os estados disponíveis variam de acordo com o estado atual do incidente. Para obter mais informações, consulte Corrigir um incidente de segurança ou estado de tarefa inválido com a definição de processo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Selecione uma definição de processo Security Incident Response

Você pode selecionar a definição de processo a ser usada para os estados apropriados para os incidentes de segurança e as tarefas de resposta da sua empresa.

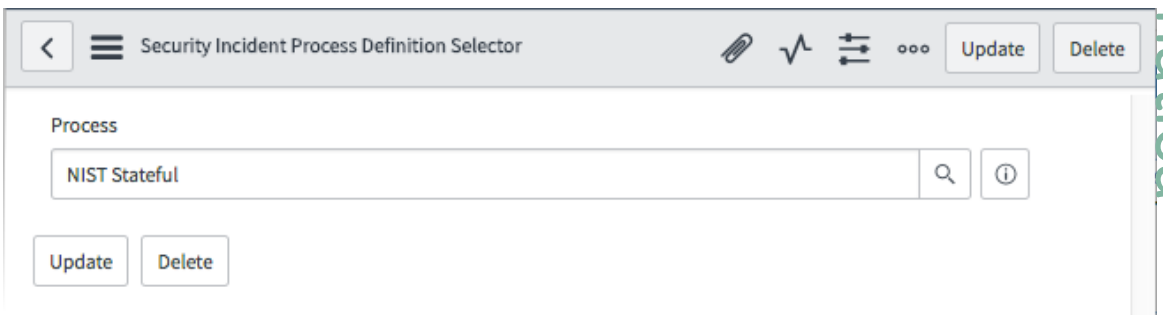
Antes de Iniciar

Função necessária: admin e sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Navegar até **Todos** > **Security Incident Response** > **Administração** > **Seleção de processo**.
2. Clique no ícone de pesquisa para listar as definições de processo disponíveis.



3. Selecione uma definição de processo.
4. Clique em **Atualizar**.

Criar uma inclusão de script de definição de processo personalizada Security Incident Response

Crie um script de Definição de processo personalizado para os estados apropriados para os incidentes de segurança e as tarefas de resposta da sua empresa.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

O script principal sn_si.ProcessDefinition inclui controles e definições de processo. **A definição de processo** determina qual definição está em uso (usando a **seleção de processo**). Ele chama o arquivo de inclusão de script apropriado para determinar os estados iniciais e as transições para incidentes de segurança e tarefas de resposta.

Procedimento

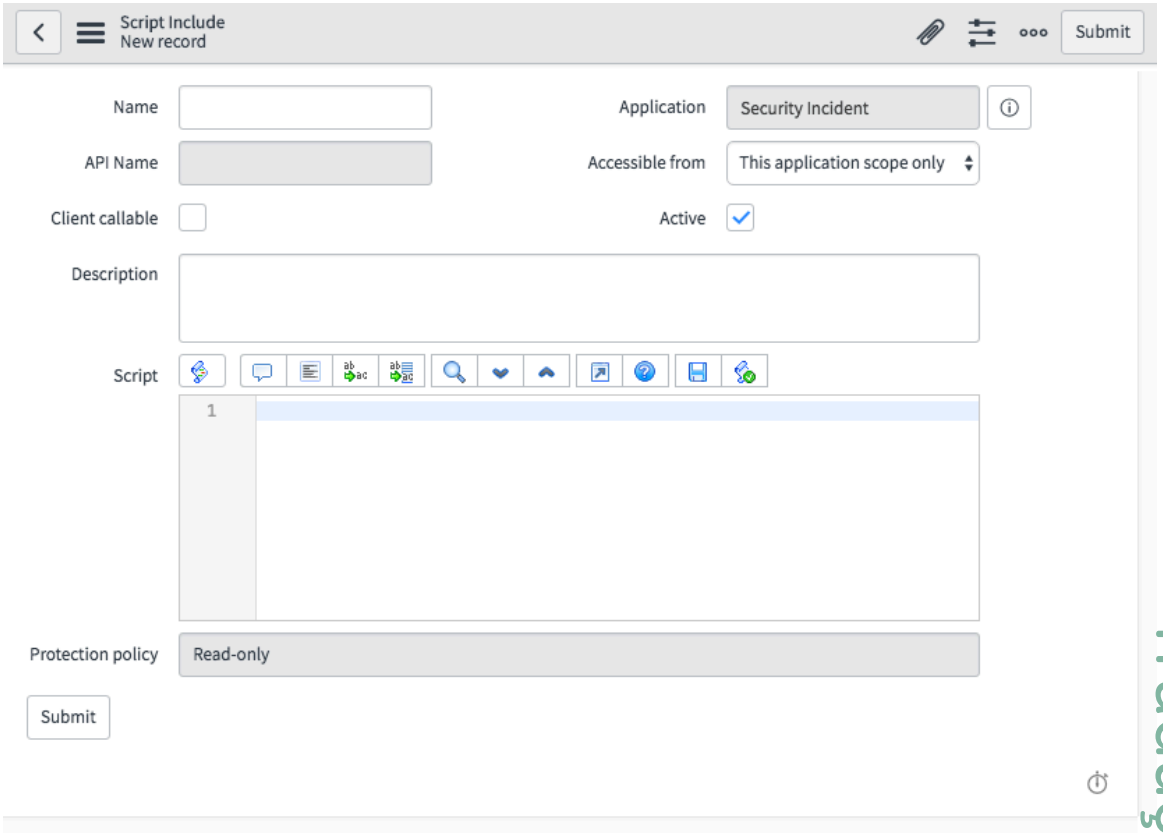
1. Navegar até **Tudo** > **Definição do Sistema** > **Inclusões de script**.
2. Clique em **Novo.**
3. Preencha os campos, se for o caso.

Criando definições de processo

Campo	Descrição
Nome	Nome desta inclusão de script.
Nome da API	Criado com base no nome da inclusão de script.
Cliente chamável	Disponibiliza a inclusão de script para Client scripts, filtros de lista e relatório, qualificadores de referência ou, se especificado, como parte do URL.
Aplicação	Incidente de segurança
Acessível de	Escolha **Somente este escopo da aplicação** .
Ativo	Quando marcada, torna esta inclusão de script selecionável na página **Definição de processo**.
Descrição	Informações úteis sobre a inclusão de script.
Script	Define o script do lado do servidor a ser executado quando chamado de outros scripts. O script deve definir uma única classe JavaScript ou uma função global. O nome da classe ou da função deve corresponder ao campo Nome. Para obter informações sobre o conteúdo do script, consulte Inclusão de script de definição de processo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em **Enviar**.

Tópicos relacionados

Inclusão de script de definição de processo

Inclusão de script de definição de processo

O script include de definição de processo fornece métodos para definir uma definição de processo.

Implemente as constantes, atributos, matrizes e chamadas de método descritas aqui para personalizar uma inclusão de script de definição de processo.

Onde usar

Use esta inclusão de script para criar uma definição de processo.

Corpo da inclusão de script

O corpo da inclusão de script é composto por três seções:

- Constantes: definições de estado inicial
- Security Incident and Response Task: matrizes de definição de processo
- Chamadas de método: recuperando informações

Constantes

As constantes são usadas para definir os estados iniciais de incidentes de segurança e tarefas de resposta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O uso de constantes é opcional, mas recomendado para facilitar a leitura. Por exemplo:

```
INITIAL_INCIDENT_STATE: 10,
INITIAL_TASK_STATE: 1,
```

Que são usados posteriormente pelos seguintes métodos:

```
getInitialIncidentState: function() {
return this.INITIAL_INCIDENT_STATE;
},
getInitialTaskState: function() {
return this.INITIAL_TASK_STATE;
},
```

O próximo conjunto de constantes define os estados dos incidentes de segurança e das tarefas de resposta.

Cada matriz também contém a definição de quais estados estão disponíveis quando o incidente ou a tarefa está em um estado específico.

Por exemplo:

```
TASK_STATES: [{state:1, label:"Draft", choice:[1, 10]},
 {state:10, label:"Ready", choice:[10, 16]},
 {state:16, label:"Assigned", choice:[16, 18]},
 {state:18, label:"Work in Progress", choice:[18, 3]},
 {state:3, label:"Close Complete", choice:[]},
 {state:7, label:"Cancelled", choice:[]},
 ],
```

O exemplo é uma matriz de objetos. Cada objeto define um estado e possíveis estados de transição.

A ordem do objeto do estado determina a ordem desejada para o fluxo.

Quando a tarefa está no estado "Rascunho" (valor 1), os estados possíveis são: 1 (Rascunho, que não é mudança) e 10 (Pronto, a próxima etapa no processo).

Não há limite para o número de transições de um estado. O estado "Encerrar concluído" e "Cancelado" são estados finais e, portanto, não têm transições de estado possíveis.

A ordem dos atributos no objeto não é importante. Se isso tornar a definição mais clara, coloque o rótulo primeiro.

Atributos

Os atributos obrigatórios em um objeto de definição de estado são:

- estado: valor numérico do estado
- rótulo: texto legível associado ao estado
- opção: uma matriz de valores de estado para os quais o estado pode fazer a transição (determina o conteúdo do menu suspenso de estado)

Os atributos opcionais são:

- obrigatório: lista de IDs de campo que se tornam obrigatórios neste estado
- readonly: lista de IDs de campo que se tornam somente leitura neste estado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- visível: lista de IDs de campo que se tornam visíveis neste estado
- notmandatory: lista de IDs de campo que se tornaram não obrigatórios neste estado
- notvisible: lista de IDs de campo que não estariam mais visíveis neste estado

Nota:

Se atributos opcionais forem usados, será responsabilidade do autor garantir que os campos fiquem visíveis/invisíveis, obrigatórios/não obrigatórios, visíveis/ocultos ou somente leitura adequadamente entre os estados.

Por exemplo, ocultar um campo em um estado não o torna visível em outro estado mais tarde, a menos que o atributo "visível" seja usado.

Matrizes de definição de fluxo de processo

Para definir as informações exibidas no formatador de fluxo do processo (a barra na parte superior dos formulários de tarefa de incidente e resposta de segurança), o sistema requer informações sobre o que exibir para cada estado.

Por exemplo:

```
TASK_PF: [{label:"Draft", condition:"state=1^EQ", description:"<p>Security Incident Response Task is in draft</p>"},
{label:"Ready", condition:"state=10^EQ", description:"<p>Security Incident Response Task is ready to be assigned</p>"},
{label:"Assigned", condition:"state=16^EQ", description:"<p>Security Incident Response Task is assigned</p>"},
{label:"Work in Progress", condition:"state=18^EQ", description:"<p>Work has started on this Security Incident Response Task</p>"},
{label:"Closed", condition:"state=3^ORstate=4^ORstate=7^EQ", description:"<p>Security Incident Response Task is complete</p>"},
],
```

A matriz TASK_PF é uma coleção de rótulos, condições e descrições usadas para determinar o texto exibido na barra do formatador de processo (incluindo ordem e atividade).

No exemplo, o texto "Pronto" é o segundo item exibido. Ele é realçado quando a tarefa atende à condição 'state=10^EQ'.

Quando o ponteiro do mouse passa sobre o texto, a descrição "A tarefa do Security Incident Response está pronta para ser atribuída" é exibida.

Nota:

Os estados podem ser combinados em um único estado de formatador.

No exemplo, os estados "Encerrado concluído" e "Cancelado" são exibidos como "Encerrado" na barra superior.

Chamadas de método

Os seguintes métodos devem estar presentes na inclusão de script, pois são usados por sn_si.ProcessDefinition:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipo de retorno	Resumo do método	Descrição
Cadeia de caracteres	getInitialIncidentState: função ()	retornar o valor numérico do estado do incidente inicial
Cadeia de caracteres	getInitialTaskState: função():	retornar o valor numérico do estado inicial da tarefa
Matriz de cadeia de caracteres	getIncidentStates: função ():	retornar a matriz do estado do incidente
Matriz de cadeia de caracteres	getTaskStates: função ():	retornar a matriz do estado da tarefa
Matriz de objetos	getIncidentProcessFlows: função ():	retornar a matriz de definição de fluxo do processo de incidente
Matriz de objetos	getTaskProcessFlows: função ():	retornar a matriz de definição de fluxo do processo de tarefa

O próximo conjunto de métodos é chamado sempre que um incidente ou uma tarefa é atualizado e permite que ações sejam executadas em transições de mudança específicas.

Tipo de retorno	Resumo do método	Descrição
vazio	performanceIncidentStateChange: função (atual, anterior)	Nos exemplos, este método é usado para definir valores relacionados ao SM e garantir que um incidente avance para fora de "Rascunho" quando alguém for atribuído a ele.
vazio	performanceTaskStateChange: função (atual, anterior)	No exemplo, este método é usado para atualizar carimbos de data/hora (na atribuição e no fechamento) e avançar a tarefa de "Pronto" para "Atribuído" depois que o campo assigned_to estiver preenchido.

As mesmas ações realizadas por esses dois métodos podem ser realizadas usando uma regra de negócios. Ao defini-los na inclusão de script, a alternância das definições de processo é facilitada.

Corrigir um incidente de segurança ou estado de tarefa inválido com a definição de processo

Um administrador pode corrigir o incidente de segurança ou a tarefa para estados válidos, manualmente ou usando um script. Os estados disponíveis variam de acordo com o estado atual do incidente.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Depois de alternar as definições de processo, a nova definição pode não oferecer suporte a alguns dos estados antigos. Para corrigir os estados de tarefa ou incidente órfãos, você pode mudar a definição do processo, editar a inclusão de scriptou abrir manualmente cada incidente ou tarefa para atualizar o estado. Geralmente, atualizar o estado (que pode ser feito em massa) é a solução mais fácil.

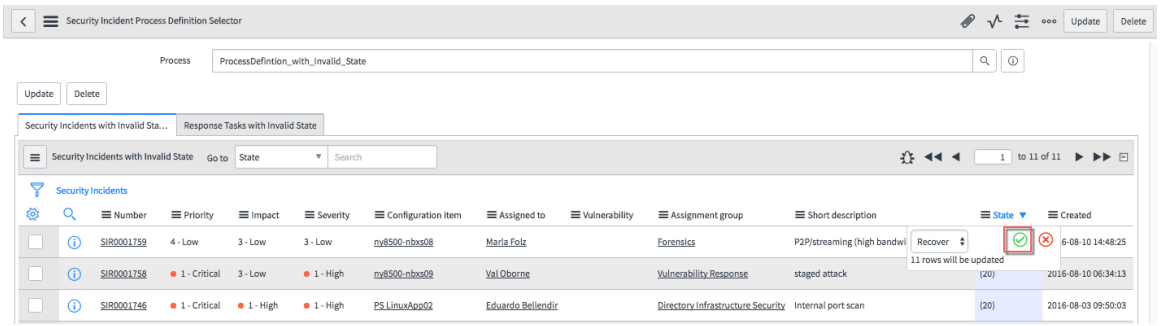
Para mudar os estados em massa, faça o seguinte:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Seleção de processo**.
2. Realce o campo **Estado** para os incidentes ou tarefas que você deseja mudar.
3. Clique duas vezesno campo **Estado** no primeiro registro, selecione o novo **Estado** e clique na marca de seleção) para concluir a mudança.



4. Clique em **Atualizar**.

Criar um grupo de incidentes de segurança

Configure um grupo de incidentes de segurança e atribua as funções e os usuários apropriados ao grupo.

Antes de Iniciar

Funções necessárias:

- Se você tiver a função user_admin, poderá criar grupos de atribuição de incidentes de segurança.
- Se você tiver a função sn_si.admin, poderá criar e editar grupos de atribuição de incidentes de segurança.

Por Que e Quando Desempenhar Esta Tarefa

Os usuários de um grupo herdam as funções do grupo, portanto, você não precisa atribuir funções a cada usuário separadamente.
É uma prática recomendada criar quantos grupos forem necessários em sua organização. Também é uma prática recomendada criar um grupo para administradores e atribuir a função de administrador somente a este grupo.

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Grupos** ou **Incidente de segurança** > **Configuração** > **Grupos**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Nota:

Para obter mais informações, consulte Criar um grupo de usuários .

4. Certifique-se de selecionar o tipo de **incidente de segurança** para este grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Se o campo **Tipo** não estiver visível, configure o formulário para adicioná-lo.

b. Clique no ícone de cadeado ao lado do campo **Tipo**.

c. Clique no ícone de pesquisa de referência ( )

d. Pesquise e selecione o tipo de **incidente de segurança**.

5. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
6. Na lista relacionada **Funções**, adicione as funções que cada membro deste grupo recebe.
   Por exemplo, se você estiver criando um grupo para Security Incident Response membros da equipe, adicione sn_si.analyst. Se você estiver criando um grupo para administradores Security Incident Response, adicione sn_si.admin.
7. Na lista relacionada **Membros do Grupo**, adicione usuários a este grupo.
8. Clique em **Atualizar**.

Criar um grupo de calculadoras de incidentes de segurança

Grupos de calculadoras de incidentes de segurança são usados para agrupar calculadoras.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Configuração** > **Grupos de calculadoras de incidentes de segurança**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Nome	O nome da calculadora de incidente de segurança.
Aplicação	A aplicação que contém este registro.
Pedido	A ordem na qual a calculadora de incidente de segurança é executada. Uma calculadora com uma entrada de ordem de 100 é executada antes de uma calculadora com uma entrada de ordem de 200.
Descrição	Uma descrição deste grupo de calculadoras.
Criado por	Insira o nome do usuário que criou

4. Clique em **Enviar**.

Criar uma calculadora de incidente de segurança

As calculadoras de incidente de segurança permitem calcular a gravidade de um incidente de segurança com base em fórmulas predefinidas. Você pode definir suas próprias calculadoras de incidente de segurança, conforme necessário.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Configuração** > **Grupos de calculadoras de incidentes de segurança**.
2. Clique no nome do grupo para o qual você deseja criar uma calculadora ou crie um grupo de calculadoras.
3. Clique em **Nova**.
4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Nome	O nome da calculadora de incidente de segurança.
Grupo de Calculadoras	Nome do grupo ao qual esta calculadora pertence. **Nota:** Criar ou alterar o grupo de calculadoras se torna disponível depois que você insere um **Nome** e uma **Tabela**.
Tabela	Selecione a tabela a ser usada para esta calculadora. Ao adicionar calculadoras a tabelas diferentes de Vulnerabilidade [sn_vul_vulnerability] e Item vulnerável [sn_vul_vulnerable_item], você deve adicionar regras de negócios e ações de IU a essas tabelas. Para ver exemplos: ○ Navegar até **Definição do Sistema** > **Regras de negócios**e localize a regra de negócios **Calcular severidade** na tabela Item vulnerável [sn_vul_vulnerable_item]. ○ Navegar até **IU do Sistema** > **Ações de IU**e localize a ação de IU **Calcular severidade** na tabela Item vulnerável [sn_vul_vulnerable_item]. Além disso, a função de administrador de vulnerabilidades deve receber recursos completos de leitura, gravação (ou save_as_template) em qualquer tabela usada por uma calculadora para ver corretamente os valores a serem aplicados ao modelo.
Aplicação	A aplicação com escopo à qual a calculadora pertence.
Pedido	A ordem na qual a calculadora de incidente de segurança é executada. Uma calculadora com uma entrada de ordem de 100 é executada antes de uma calculadora com uma entrada de ordem de 200.
Ativo	Liga ou desliga a calculadora.
Descrição	Uma descrição desta calculadora.

5. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
   As guias **Condições** e **Valores a serem** aplicados são exibidas.
6. Preencha os campos na guia **Condições**, conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Usar grupo de filtros	Marque esta caixa de seleção para usar um grupo de filtros predefinido ou criar um novo grupo de filtros para definir os critérios da calculadora.
Grupo de filtros	Selecione o grupo de filtros a ser usado para definir uma calculadora. Este campo aparecerá somente se você marcar a caixa de seleção **Usar grupos de filtros**.
Usar a condição avançada	Marque esta caixa de seleção para indicar que uma condição de script é usada para determinar quando esta calculadora é aplicada. Quando você marca a caixa de seleção, um campo de script **de condição avançada** é exibido. Se você marcou a caixa de seleção **Usar grupo de filtros**, este campo ficará oculto. **Nota:** Antes de definir condições avançadas e escrever scripts para determinar quando as calculadoras de incidentes de segurança são aplicadas, retorne à lista Calculadoras de incidentes de segurança. Explore os registros da calculadora enviados com o sistema de base.
Condição	Define condições básicas de filtro para determinar se a calculadora é usada. Se você selecionou uma das caixas de seleção **Usar grupo de filtros** ou **Usar condições avançadas**, este campo ficará oculto.

7. Clique na guia **Valores a serem aplicados** e preencha os campos no formulário, conforme apropriado. Você tem a opção de criar um script para definir os valores a serem aplicados ao cálculo ou definir um modelo com base nos campos da tabela selecionada.

Campo	Descrição
Usar valores de script	Marque esta caixa de seleção para definir valores de campo com um script.
Valores de Script	Define a quais valores os cálculos serão aplicados. Este campo aparecerá somente se você marcar a caixa de seleção **Usar valores de script**.
Modelo	Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**. Selecione os campos e valores que você deseja usar para a calculadora.

8. Quando tiver concluído todas as entradas, clique em **Enviar**.

Noções básicas sobre calculadoras de incidentes de segurança

Calculadoras de incidentes de segurança são usadas para atualizar valores de registro quando condições predefinidas são atendidas. As calculadoras são agrupadas com base nos critérios usados para determinar como os registros são atualizados.

O sistema de base Security Incident Response inclui os seguintes grupos de calculadoras de incidente de segurança e calculadoras. A primeira calculadora que corresponde às condições é executada em cada grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Calculadoras de incidentes de segurança no sistema de base

Nome do Grupo da Calculadora de Incidentes de Segurança	Calculadoras incluídas no grupo	Descrição
Impacto nos negócios	Agregar de calculadoras de severidade	Esta calculadora delega para a Calculadora de Criticidade de Segurança que determina a criticidade ponderando os valores de outros campos.
Gravidade	Negócios afetados	Esta calculadora de severidade define seus critérios de seleção usando um construtor de condição simples.
	Serviço crítico afetado	Esta calculadora de severidade define seus critérios de seleção usando uma condição avançada. Se o item de configuração no incidente de segurança estiver associado a um serviço de negócios altamente crítico, os campos **Pontuação de risco**, **Impacto nos negócios**e **Prioridade** serão elevados conforme definido pela calculadora.
	Mudanças críticas de serviço	Esta calculadora de severidade define seus critérios de seleção usando uma condição avançada. Se o incidente de segurança atender às condições, um script será executado para definir os níveis para os quais os campos serão elevados. Se o item de configuração no incidente de segurança estiver associado a um serviço de negócios mais crítico ou um pouco crítico, os campos **Pontuação de risco**, **Impacto nos negócios**e **Prioridade** serão elevados conforme definido pela calculadora.
	Vetores de ataque múltiplo	Esta calculadora de severidade define seus critérios de seleção usando um construtor de condição simples. Se o item de configuração no incidente de segurança estiver associado a vetores de ataque da Web, e-mail e representação, os campos **Pontuação de risco**, **Impacto nos negócios**e **Prioridade**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Calculadoras de incidentes de segurança no sistema de base

Nome do Grupo da Calculadora de Incidentes de Segurança	Calculadoras incluídas no grupo	Descrição
		serão elevados conforme definido pela calculadora.
	Definir prioridade com categoria e serviços	Esta calculadora de severidade define seus critérios de seleção usando um construtor de condição avançado. A prioridade do incidente de segurança é definida como **1 - Crítica** quando as seguintes condições são atendidas: • O incidente de segurança tem serviços afetados associados e um deles é crítico. • A categoria de incidente de segurança é uma das seguintes: ◦ Negação de serviço ◦ Spear Phishing ◦ Atividade de código malicioso **Nota:** Esta calculadora está disponível no sistema de base quando você tem o tipo de preço da Operação de segurança inicial.
	Definir prioridade com observáveis	Esta calculadora de severidade define seus critérios de seleção usando um construtor de condição avançado. A prioridade do incidente de segurança é definida como **1 - Crítica** quando as seguintes condições são atendidas: • O incidente de segurança tem serviços afetados associados e um deles é crítico. • A categoria de incidente de segurança é uma das seguintes: ◦ Negação de serviço ◦ Spear Phishing ◦ Atividade de código malicioso • Um dos observáveis ou indicadores associados tem uma contagem de vistas que excede

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Calculadoras de incidentes de segurança no sistema de base

Nome do Grupo da Calculadora de Incidentes de Segurança	Calculadoras incluídas no grupo	Descrição
		duas vistas com indicadores ativos (ou seja, os observáveis ou indicadores são confirmados como incorretos por várias fontes). **Nota:** Esta calculadora está disponível no sistema de base quando você tem o tipo de preço Advanced Security Operation e ativa o plug-in Threat Feeds.
Criticidade do usuário	Obter criticalidade do usuário	Esta calculadora de severidade define seus critérios de seleção usando um construtor de condição simples. Esta calculadora de severidade faz com que a criticalidade dos negócios do usuário seja alterada para **1 - Crítica** quando o campo **Departamento** é alterado para **Finanças**.
	Obter criticidade do grupo de usuários	Esta calculadora de severidade define seus critérios de seleção usando um construtor de condição avançado. Esta calculadora de severidade fornece um exemplo de uma calculadora que é executada em dados em uma lista relacionada.

Tradução automática

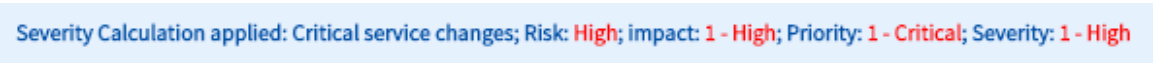
Calculadoras de severidade

Quando você cria um incidente de segurança, os campos **Pontuação de risco**, **Impacto nos negócios**e **Prioridade** contêm valores padrão. Quando você salva o incidente, uma regra de negócios valida automaticamente as informações no incidente de segurança em relação às condições definidas em cada uma das calculadoras de severidade ativas. Eles são validados em uma calculadora de segurança de cada vez, na ordem definida pelo campo **Ordem** em cada calculadora. Se as informações no incidente de segurança corresponderem às condições definidas em uma das calculadoras, os valores do campo de severidade serão atualizados de acordo com as regras configuradas na calculadora.

Por exemplo, suponha que você crie um incidente de segurança para um IC afetado e o IC seja altamente crítico. Quando o incidente de segurança é salvo, as informações do IC são comparadas com as condições definidas nas calculadoras de severidade. Quando o incidente de segurança é validado em relação à calculadora de severidade do **serviço crítico**

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

afetado, os campos de severidade são atualizados automaticamente e uma mensagem semelhante à seguinte aparece na parte superior do incidente de segurança.



Você pode usar essas calculadoras de severidade como estão ou editá-las para atender melhor às necessidades do seu negócio. Por exemplo, se você quiser identificar ameaças da Web e de e-mail específicas à unidade de negócios Finanças, poderá alterar as condições da calculadora de **Vetores de vários ataques** :

- [Vetor de ataque] [contém] [Web]
- [Vetor de ataque] [contém] [E-mail]
- [Unidade de negócios] [contém] [Finanças]

Você também pode atualizar os valores de severidade em um incidente de segurança existente a qualquer momento, abrindo o registro e clicando no link relacionado **Calcular severidade**.

Calculadoras de pontuação de risco de incidente de segurança

As calculadoras **Definir prioridade com categoria e serviços** e **Definir prioridade com observáveis** são usadas para calcular uma pontuação de risco para um incidente de segurança.

Calculadoras de criticalidade do usuário

As duas calculadoras no grupo **de criticalidade do usuário** (**Obter criticalidade do usuário** e **Obter criticalidade de grupo de usuários**) fornecem exemplos de como você pode direcionar a criticalidade com base em critérios definidos em um registro de usuário ou com base no grupo ao qual um usuário pertence.

Eles podem ser editados conforme necessário ou novas calculadoras de criticidade do usuário podem ser criadas.

A calculadora **Obter criticidade do** usuário faz com que a criticalidade dos negócios do usuário seja alterada para **1 - Crítica** quando o campo **Departamento** é alterado para **Finanças**.

A calculadora **Obter criticidade do grupo de** usuários faz com que a criticalidade dos negócios do usuário seja alterada para **1 - Crítica** quando o usuário é adicionado ao grupo Banco de **dados**.

Nota:
Obter criticidade de grupo de usuários é um exemplo de uma calculadora que é executada em dados em uma lista relacionada. Se você quiser adicionar mais grupos para iniciar uma mudança de criticalidade, adicione uma lista separada por vírgulas de sys_ids de grupo na primeira linha do script. Exemplo: `var CRITICAL_GROUPS = [group1_sys_id, group2_sys_id, group3_sys_id];`.

Cálculos de pontuação de risco de incidente de segurança

A pontuação de risco é calculada como uma média aritmética que representa o risco com base na prioridade de um incidente de segurança, no tipo de incidente de segurança (Negação de serviço, Spear Phishing ou atividade de código malicioso) e no número de origens que acionaram uma falha pontuação de reputação em um indicador.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A pontuação de risco ajuda a priorizar o trabalho de incidente de segurança para os analistas.

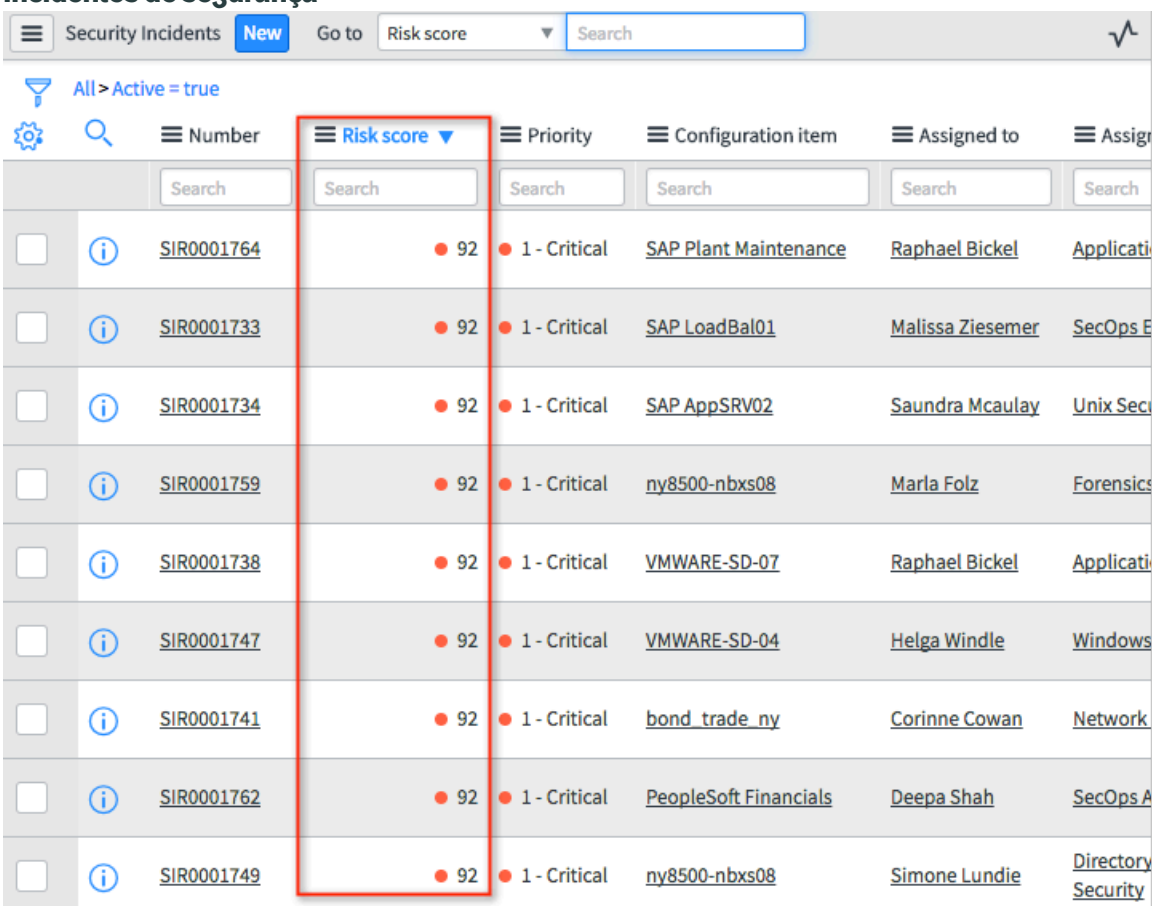
As calculadoras de incidente de segurança **Definir prioridade com categoria e serviços** e **Definir prioridade com observáveis** são usadas para calcular uma pontuação de risco para um incidente de segurança. Além disso, as seguintes regras de negócios acionam o cálculo automático de pontuações de risco:

- Calcular Gravidade
- Atualizar pontuação de risco
- Atualizar pontuação de risco de SI

Nota:
A calculadora de risco disponível no sistema de base depende do seu tipo de preço do Security Operations.

Ao observar uma lista de incidentes de segurança no sistema de base, observe a coluna **Pontuação de risco**.

Incidentes de segurança

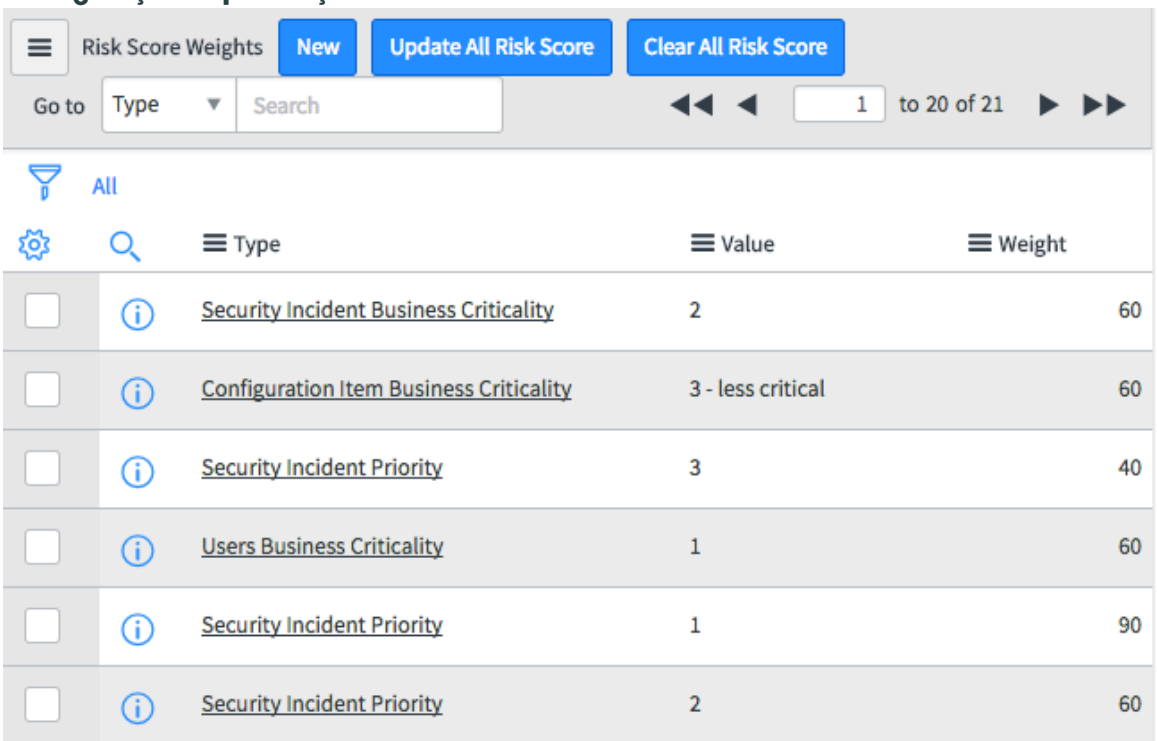


A pontuação de risco é calculada usando pesos definidos na **configuração de pontuação de risco**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de pontuação de risco



Por exemplo, se um incidente de segurança tiver um **Impacto nos negócios** definido como **2-Alto** e uma **Prioridade** definida como **3-Moderado**, os respectivos pesos na tabela Ponderações de pontuação de risco serão pesquisados e calculados da seguinte forma:

Impacto do incidente de segurança nos negócios com um valor de 2 = um peso de 60.

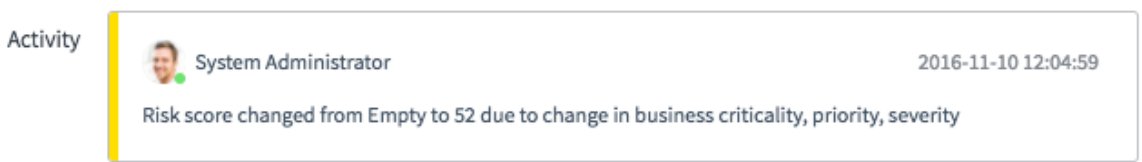
Prioridade de incidente de segurança com um valor de 3 = um peso de 40.

(60 + 40)/2 = uma pontuação de risco de 50.

A posição do incidente de segurança na lista de incidentes de segurança é reordenada com base em sua pontuação de risco atualizada.

Se, no exemplo acima, o **Impacto nos negócios** ou a **Prioridade** do incidente de segurança forem alterados, a pontuação de risco será recalculada e as mudanças serão refletidas nas anotações de trabalho.

Anotações de trabalho



As anotações de trabalho são atualizadas quando os seguintes campos são alterados (fazendo com que a pontuação de risco seja atualizada):

- **Impacto nos negócios** no formulário de Incidente de segurança
- **Prioridade** no formulário de Incidente de segurança
- **Severidade** no formulário de Incidente de segurança (oculta por padrão)
- **Impacto nos negócios** na lista relacionada de **Usuários afetados**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Impacto nos negócios** na lista relacionada de **Serviços afetados**
- **Impacto nos negócios** sobre vulnerabilidades na lista relacionada de **itens vulneráveis**

Além disso, as anotações de trabalho são atualizadas nas seguintes situações:

- Quando uma associação entre usuários afetados e um incidente de segurança é criada ou modificada
- Quando uma associação entre serviços afetados e um incidente de segurança é criada ou modificada
- Quando uma associação entre itens vulneráveis e um incidente de segurança é criada ou modificada

As anotações de trabalho também são atualizadas sempre que **Atualizar todas as pontuações de risco** e **Limpar todas as pontuações de risco** no formulário Ponderações de pontuação de risco são clicados.

Manter pesos de pontuação de risco

Os pesos de pontuação de risco usados para calcular pontuações de risco em incidentes de segurança podem ser removidos ou atualizados individualmente. Eles também podem ser removidos ou atualizados para todos os incidentes de segurança. A capacidade de removê-los de incidentes de segurança é útil ao alterar valores de peso.

Antes de Iniciar

Função necessária: sn_sec_cmn.admin

Nota:
Usuários com a função sn_si.read podem exibir a configuração de pontuação de risco em Security Incident Response.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Configuração** > **Configuração de pontuação de risco**.

   Nota:
   Usuários com a função sn_si.read podem exibir a configuração de pontuação de risco navegando até **Incidente de segurança** > **Alertas e eventos** > **Configuração de pontuação de risco**.

2. Para adicionar um novo peso de pontuação de risco, clique em **Novo** e insira as informações nos campos.

Campo	Descrição
Tipo	Selecione o tipo de pontuação de risco que você está definindo.
Valor	Especifique o valor associado ao tipo selecionado. Se vários valores estiverem disponíveis para o tipo, convém definir vários registros de peso de pontuação de risco. Exemplo: prioridade de incidente de segurança com um valor de 1, prioridade de incidente de segurança com um valor de 2 e assim por diante.
Ponderação	O peso associado ao par de tipo/valor selecionado. As entradas válidas estão entre 0 e 100, sendo 0 o menor peso e 100 o maior.

3. Clique em **Enviar**.
4. Execute qualquer uma dessas etapas, conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para limpar um registro de ponderação de pontuação de risco, abra-o na lista e clique em **Excluir**.
- Para limpar todos os registros de ponderação de pontuação de risco, clique em **Limpar todas as pontuações de risco**.
- Para atualizar todos os registros de ponderação de pontuação de risco, clique em **Atualizar todas as pontuações de risco**.

Criar um Security Incident Response ANS

Você pode definir um Acordo de nível de serviço (ANS) para Security Incident Response.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Configuração** > **SLAs**.
2. Clique em **Nova**.
   Para obter descrições de campo e instruções detalhadas, consulte Create an SLA definition .

Reparar ANS de incidente de segurança

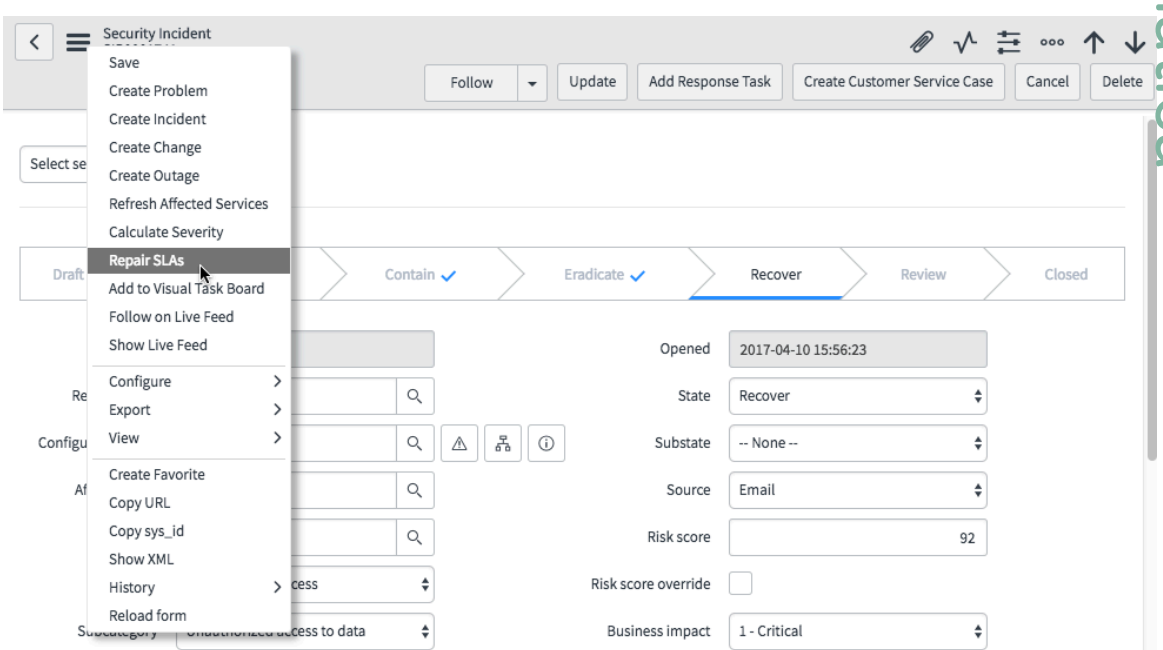
Você pode reparar registros de SLA para garantir que as informações de tempo e duração do SLA sejam precisas.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança para o qual você deseja reparar SLAs.
2. Clique no menu de contexto do cabeçalho do formulário e selecione **Reparar ANS**:



3. Clique em **OK** na caixa de confirmação Aviso.
   Para obter mais informações, consulte Reparar ANS .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar um runbook do Security Incident Response

Um runbook é uma associação entre um artigo de conhecimento publicado e uma tarefa específica. Enquanto você está executando a tarefa, um artigo de conhecimento no runbook é aberto automaticamente, fornecendo informações pertinentes à tarefa.

Antes de Iniciar

Deve haver artigos de conhecimento na base de conhecimento do Security Incident Response Runbook. Ao criar um artigo de conhecimento de incidente de segurança, certifique-se de selecionar **Runbook do Security Incident Response** no campo **Base de conhecimento**. Depois de publicar o artigo, você pode clicar no botão **Criar Runbook**.

Função necessária: sn.si.knowledge_admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar runbooks durante o incidente de segurança ou processos de criação de tarefa de resposta, ou pode associar os artigos da base de conhecimento em um runbook com tarefas no playbook.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Runbook Manual** > **Criar Novo Runbook**.
2. Preencha os campos, se for o caso.

Campo	Descrição
Artigo de conhecimento	Selecione um artigo de conhecimento para incluir no runbook.
Ativo	Marque a caixa para disponibilizar o runbook no **Navegador de filtro**.
Usar grupo de filtros	Marque esta caixa de seleção para usar um grupo de filtros predefinido ou criar um novo grupo de filtros para definir os critérios do runbook.
Grupo de filtros	Selecione o grupo de filtros a ser usado para definir um runbook. Este campo aparecerá somente se a caixa de seleção **Usar grupos de filtros** estiver marcada.
Tabela	Selecione Incidente de segurança [sn_si_incident] ou Security Incident Response Tarefa [sn_si_task]. Se você marcou a caixa de seleção **Usar grupo de filtros** e selecionou um grupo de filtros, este campo será padronizado para a tabela associada ao grupo de filtros selecionado.
Condição	Defina as condições que conectam este runbook ao incidente ou tarefa. Se você marcou a caixa de seleção **Usar grupo de filtros** e selecionou um grupo de filtros, os campos **Condição** não serão exibidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
   A guia Detalhes do artigo de conhecimento e uma série de botões são exibidos.
4. Para exibir os detalhes do runbook, clique na guia **Detalhes da Base de Conhecimento**.
5. Para ver o artigo de conhecimento como ele aparecerá para o usuário, clique em **Exibir artigo**.
6. Para edite os detalhes do artigo de conhecimento , clique em **Editar artigo**.

Criar regras para validar ataques de phishing relatados pelo usuário

Quando seus funcionários recebem e-mails que parecem ser ataques de phishing, eles podem relatá-los para você usando um endereço de e-mail de phishing. O e-mail suspeito é validado usando regras definidas pela sua organização.

Antes de Iniciar

Antes que as regras de correspondência de e-mail possam ser usadas para identificar possíveis ataques de phishing, defina um endereço de e-mail para o qual os e-mails encaminhados de seus funcionários serão enviados para processamento. Você tem as seguintes opções para definir este endereço de e-mail (supondo que o domínio de e-mail da sua empresa seja acme.com):

- Defina um endereço de e-mail como **acme+phishing@service-now.com**. O marcador **+phishing** é compatível com o SMTP para habilitar a filtragem e sua instância pode receber e-mails enviados para ela.
- Defina um endereço de e-mail, como **phishing@acme.com** (sua caixa de correio do Exchange), que por sua vez o encaminha para **acme+phishing@service-now.com** (sua caixa de correio de instância definida por meio de uma regra de encaminhamento de e-mail).

Função necessária: sn_sec_cmn.write

Por Que e Quando Desempenhar Esta Tarefa

Quando um funcionário encontra um e-mail suspeito, ele deve encaminhá-lo como um anexo para o seu endereço de e-mail de phishing. Se o e-mail anexado corresponder a uma regra que define uma ameaça, um incidente de segurança será criado.

Procedimento

1. Navegar até **Tudo** > **Security Operations** > **Processamento de E-mails** > **Phishing relatado pelo usuário**.
2. Clique em **Nova**.
3. Preencha os campos, conforme necessário.

Formulário Regras de correspondência de e-mail

Campo	Descrição
Nome	Nome para esta regra de correspondência de e-mail. Por exemplo, Phishing relatado pelo usuário.
Condições	Use o Construtor de condição para validar se um e-mail enviado para o endereço de e-mail de phishing da sua empresa é um ataque de phishing. Veja o exemplo a seguir.

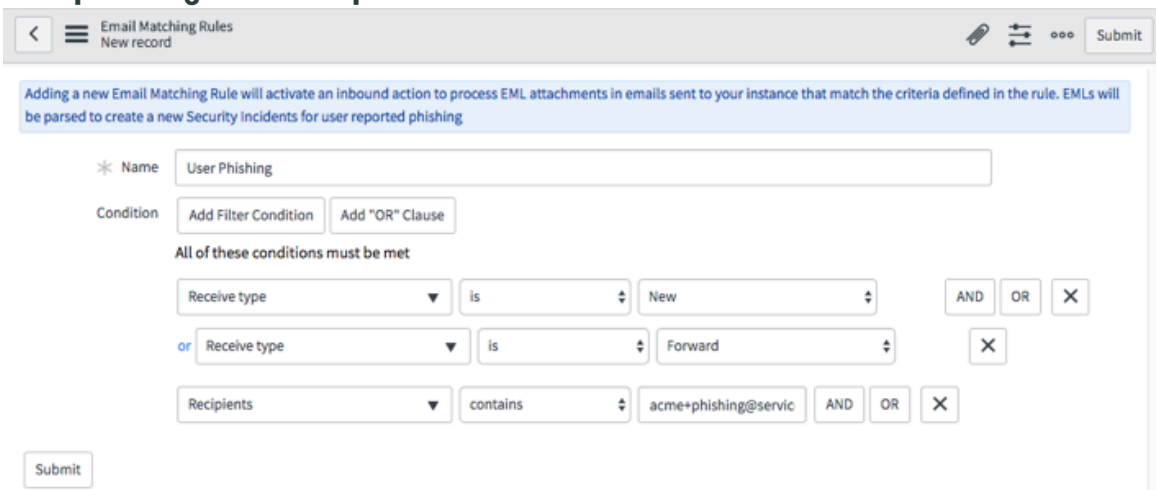
4. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example:
Este exemplo mostra uma regra de correspondência para lidar com phishing relatado pelo usuário.

Exemplo de regra de correspondência de e-mail



Configurar o Espaço do analista de segurança

Configure a interface do usuário do registro de Incidente no Espaço do analista de segurança para especificar os campos que você deseja exibir.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Especifique os campos a serem exibidos em seu registro de incidente e a ordem na qual os campos devem aparecer no formulário de incidente de segurança e no formulário de tarefa de resposta. Você também pode definir um limite para o número de campos que deseja exibir.

Nota:
Você pode criar regras para determinar qual exibição deve ser usada para um formulário específico. Várias exibições estão incluídas no sistema de base, incluindo as exibições de IU padrão e Novo SIR. Várias regras de exibição também são enviadas com o sistema de base, incluindo a regra de tarefa de resposta de todos os outros. Esta regra impõe a exibição Padrão no formulário de tarefa de resposta quando a condição especificada na regra de exibição é atendida. O Espaço do analista de segurança usa a exibição Nova IU do SIR. Se os campos de formulário exibidos no Espaço do analista de segurança não corresponderem aos campos de formulário no ambiente clássico, uma regra de exibição provavelmente será aplicada. Para usar a exibição de **nova IU do SIR** para o formulário, você deve desabilitar a regra de exibição. Consulte Controle quando o sistema exibe uma exibição para obter detalhes.

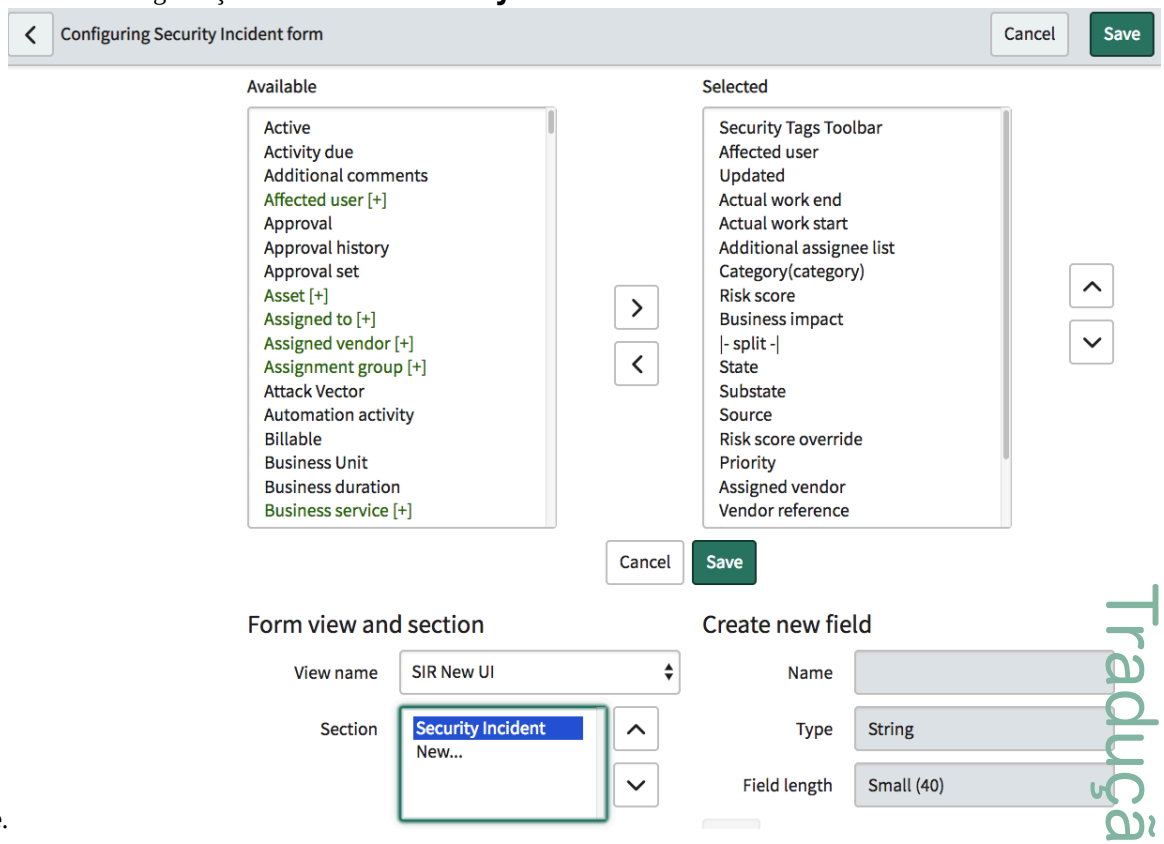
Procedimento

1. Navegue até qualquer lista de incidentes de segurança (por exemplo, **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar Todos os Incidentes**).
2. Para abrir o registro do incidente de segurança, clique em um link de incidente de segurança.
3. Para navegar até a página do formulário Configuração de Incidente de segurança, clique no ícone de menu Menu de e selecione **Configurar** > **Layout do formulário**.
4. Na lista **Exibir nome**, selecione **SIR Nova IU**.
5. No campo **Seção**, selecione a seção apropriada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pode ser **Incidente** de segurança ou **Tarefa do Security Incident**



Response.

6. Selecione os campos e a ordem em que você deseja que eles apareçam na faixa de Incidentes na nova IU.
7. Clique em **Salvar**.

Nota:

- Certos campos estão ocultos por padrão nas faixas de Incidente e Tarefa de resposta. Altere os campos que estão ocultos ou exibidos modificando as propriedades `sn_app_secops_ui.form.excluded_fields.incident` e `sn_app_secops_ui.form.excluded_fields.response_task` conforme descrito em Propriedades do Espaço do analista de segurança.
- Especifique o número de campos que podem ser exibidos nas faixas Incidente e Tarefa de resposta e na primeira linha da faixa Incidente definindo estas propriedades:
  - sn_app_secops_ui.task_summary.single_summary.limit.incident
  - sn_app_secops_ui.task_summary.single_summary.limit.response_task
  - sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line

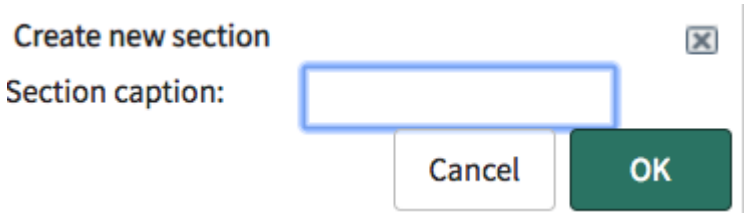
8. Para configurar os estilos dos círculos pontilhados que aparecem ao lado de um valor de campo no registro de Incidente, por exemplo, navegue até **IU do Sistema** > **Estilos de Campo** e modificam ou criam um novo registro de estilo para a tabela específica e o nome do campo.
   A propriedade cor de fundo no campo Estilo do registro de estilo determina a cor do círculo pontilhado.
9. Para exibir a faixa de incidentes atualizada, clique em **Incidentes de segurança** > **Incidentes (Nova IU)** para navegar até o registro do Incidente no Espaço do analista de segurança e atualizar a página para exibir a faixa do Incidente atualizada.
10. Para configurar a faixa de tarefa de resposta no registro de incidente, navegue até **Incidentes de segurança** > **Tarefas de resposta** > **Mostrar Todas as Tarefas** e repita as etapas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

11. Se você estiver criando uma nova tabela de tarefas que se estende da tabela de tarefas do Security Incident Response base, também deverá adicionar a exibição Nova IU do SIR à tabela.

    a. Na lista **Exibir nome**, selecione **Novo**.



    b. Insira **SIR New UI** (diferencia maiúsculas de minúsculas) na janela Criar nova exibição e clique em **OK**.

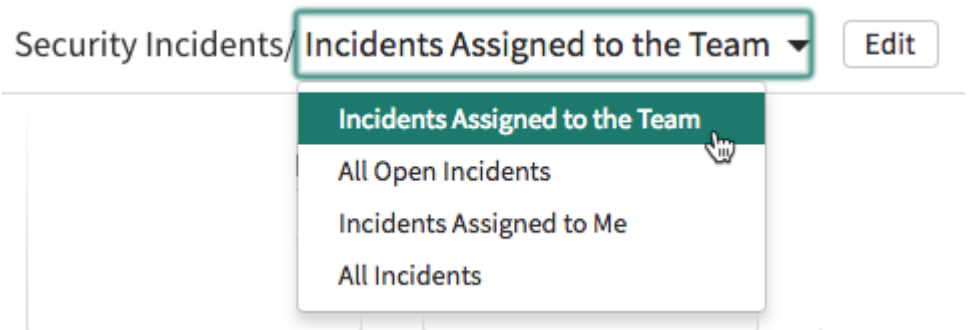
Resultado
Os incidentes de segurança e as faixas de tarefa de resposta são atualizados no Espaço do analista de segurança (Gerenciar ameaças à segurança usando o Espaço do analista de segurança).

Configurar filtros primários e secundários para Espaço do analista de segurança

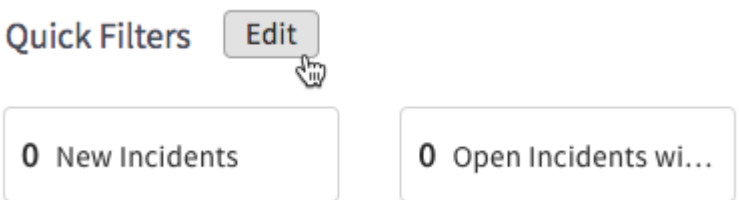
O sistema base Espaço do analista de segurança inclui um conjunto de filtros primários para restringir a lista de incidentes de segurança para análise (para incidentes de segurança atribuídos a você, todos os incidentes em aberto e assim por diante) e um conjunto de filtros rápidos (ou secundários) para restringir a lista ainda mais (por novos incidentes, incidentes abertos, somente incidentes críticos e assim por diante).

Antes de Iniciar
Você pode usar o ambiente Clássico para definir filtros primários e secundários adicionais.

Ao definir os filtros a serem usados no Espaço do analista de segurança, você pode atribuir marcadores para indicar se eles podem ser usados como filtros primários ou secundários. Os filtros primários são mostrados na parte superior da lista de incidentes de segurança.



Clique em **Editar** ao lado da opção Filtros rápidos para selecionar filtros secundários (ou rápidos).



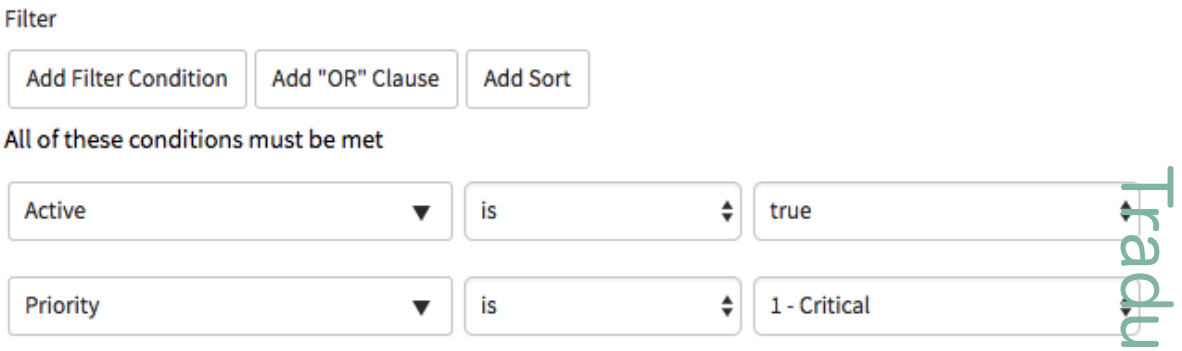
Função necessária: admin ou sn_sec_cmn.write

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Filtros**.
2. Clique em **Novo** e conclua as etapas a seguir.
   a. Insira um **Título**.
   b. Selecione **Incidente de segurança [sn_si_incident]** na lista de seleção **Tabela**.
   c. Adicione suas condições de filtro.
   Por exemplo, o filtro **Incidentes em aberto com prioridade = crítica** usa essas condições.



   d. Clique em **Enviar**.
3. Se a coluna **Marcadores** não estiver visível na lista de filtros, clique no ícone de engrenagem e personalize a exibição para adicioná-la.
4. Localize o filtro que você criou e adicione um dos marcadores a seguir para indicar como o filtro deve aparecer no Espaço do analista de segurança.
   - **SN_SI_Primary**: se este marcador for selecionado, o filtro poderá ser selecionado na interface de caixa de listagem primária do filtro primário no Espaço do analista de segurança.
   - **SN_SI_Primary_OOB**: se este marcador for selecionado, o filtro aparecerá no lado **Selecionado** do filtro primário slushbucket por padrão.
   - **SN_SI_Secondary**: se este marcador for selecionado, o filtro poderá ser selecionado na interface de caixa de listagem secundária (rápida).
   - **SN_SI_Secondary_OOB**: se este marcador for selecionado, o filtro aparecerá no lado **Selecionado** da interface de caixa de listagem primária do filtro primário por padrão.

Tópicos relacionados

Criar e editar filtros

Propriedades do Espaço do analista de segurança

Essas propriedades do sistema são usadas para configurar o Security Analyst Workspace.

Existem dois tipos de propriedades:

- Propriedades que normalmente não são modificadas, como sys_ids e chaves de produto.
- Propriedades que são modificadas conforme necessário, como longos intervalos de pesquisa e configurações de interface do usuário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
As propriedades do Security Analyst Workspace estão localizadas neste local: **Incidente de segurança** > **Configuração do espaço do analista** > **Propriedades do espaço do analista**.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
Campos que estão ocultos por padrão na faixa de tarefa de resposta. sn_app_secops_ui.form.excluded_fields.response_task	• **Tipo**: cadeia de caracteres • **Valor padrão**: ◦ número ◦ descrição resumida ◦ comentários ◦ work_notes ◦ comentários_e_anotações_de_trabalho ◦ lista_anotações_trabalho ◦ automação_atividade
Campos que estão ocultos por padrão na faixa de incidentes. sn_app_secops_ui.form.excluded_fields.incident	• **Tipo**: cadeia de caracteres • **Valor padrão**: ◦ número ◦ descrição resumida ◦ comentários ◦ work_notes ◦ comentários_e_anotações_de_trabalho ◦ lista_anotações_trabalho ◦ automação_atividade ◦ security_tags
O estilo de cor de fundo é aplicado aos campos listados aqui. sn_app_secops_ui.form.color_coded_fields	• **Tipo**: cadeia de caracteres • **Valor padrão**: ◦ criticalidade dos negócios ◦ impacto ◦ prioridade ◦ risk_score ◦ severidade
Se verdadeiro, as tabelas estendidas da tabela de tarefas de resposta base sn_si_task também terão acesso aos	• **Tipo**: verdadeiro | falso • **Valor padrão**: verdadeiro

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
modelos de e-mail criados para a tabela de tarefas de resposta base. sn_app_secops_ui.extend.base.response_task.email_templates	
Define a largura de cada campo de resumo em cada faixa de tarefa de resposta. sn_app_secops_ui.task_summary.single_summary.width.response_task	• **Tipo**: inteiro • **Valor padrão**: 10
Define a largura de cada campo de resumo em cada faixa de incidente. sn_app_secops_ui.task_summary.single_summary.width.incident	• **Tipo**: inteiro • **Valor padrão**: 15
Define um limite para o número de campos de resumo permitidos na faixa de incidentes. sn_app_secops_ui.task_summary.single_summary.limit.incident	• **Tipo**: inteiro • **Valor padrão**: 12
Define um limite para o número de campos de resumo permitidos na faixa de tarefa de resposta. sn_app_secops_ui.task_summary.single_summary.limit.response_task	• **Tipo**: inteiro • **Valor padrão**: 12
Define um limite para o número de campos de resumo permitidos na primeira linha da faixa de incidentes. sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line	• **Tipo**: inteiro • **Valor padrão**: 3
Lista separada por vírgulas de campos que podem ter fotos do usuário. sn_app_secops_ui.form.user_fields	• **Tipo**: cadeia de caracteres • **Valor padrão**: ◦ afetado_usuário ◦ Solicitante ◦ sys_updated_by ◦ sys_created_by ◦ opened_by ◦ closed_by ◦ enviado_por

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
Define a largura de cada campo de resumo em cada exibição de inspeção de incidente. sn_app_secops_ui.task_summary.single_summary.width.incident_peek	• **Tipo**: inteiro • **Valor padrão**: 13,5

Lista separada por vírgulas de campos que exibem a hora.
 	
sn_app_secops_ui.form.time_fields
	• **Tipo**: cadeia de caracteres
	• **Valor padrão**:
	  ○ opened_at
	  ○ sys_created_on
	  ○ sys_updated_on

Controla a frequência (em milissegundos) com que os resultados da pesquisa de vista são atualizados. sn_app_secops_ui.poller_interval.search_action	• **Tipo**: inteiro • **Valor padrão**: 30000 **Mínimo**: 15000
Controla a frequência (em milissegundos) com que a contagem ou os dados de consulta são atualizados. sn_app_secops_ui.poller_interval.related_list	• **Tipo**: inteiro • **Valor padrão**: 30000 **Mínimo**: 15000
Controla a frequência (em milissegundos) com que os dados de resultado são atualizados (para o playbook). sn_app_secops_ui.poller_interval.playbook_tasks	• **Tipo**: inteiro • **Valor padrão**: 30000 **Mínimo**: 15000
ID do fluxo de trabalho Integração do Security Operations - Isolar host. sn_app_secops_ui.workflow.id.Isolate_host	• **Tipo**: cadeia de caracteres • **Valor padrão**: d72041f1ff203200c68c84648e94fa5e
ID do fluxo de trabalho Integração do Security Operations - Lista de observação. sn_app_secops_ui.workflow.id.publish_to_watchlist	• **Tipo**: cadeia de caracteres • **Valor padrão**: 35800c0eff343200c68c84648e94fa85
ID do fluxo de trabalho Integração do Security Operations - Solicitação de bloqueio. sn_app_secops_ui.workflow.id.block_request	• **Tipo**: cadeia de caracteres • **Valor padrão**: 11a6a5270b9032008f9108e3c5673a24

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
ID da função do usuário sn_si_analyst. sn_app_secops_ui.roles.id.sn_si.write	• **Tipo**: cadeia de caracteres • **Valor padrão**: 66878663ff123100158bfffffffff8d
ID da função do usuário sn_si_read. sn_app_secops_ui.roles.id.sn_si.read	• **Tipo**: cadeia de caracteres • **Valor padrão**: ae878663ff123100158bfffffffff8e
ID da função do usuário sn_si_admin. sn_app_secops_ui.roles.id.sn_si.admin	• **Tipo**: cadeia de caracteres • **Valor padrão**: 22878663ff123100158bfffffffff8d
ID do fluxo de trabalho Microsoft Exchange - Executar pesquisa e exclusão de e-mail. sn_app_secops_ui.email.phishing.manual.workflow	• **Tipo**: cadeia de caracteres • **Valor padrão**: ed9f289cc310220031fbdccdf3d3aeb4
ID da ação personalizada Adicionar à lista de proibições na guia Explorar no Espaço do analista de segurança. sn_app_secops_ui.explore.action.direct.id.deny_list	• **Tipo**: cadeia de caracteres • **Valor padrão**: DENY_e9bd0ac50b632200263a089b37673a0b
ID da ação personalizada Adicionar à lista de permissões na guia Explorar do Espaço do analista de segurança sn_app_secops_ui.explore.action.direct.id.allow_list	• **Tipo**: cadeia de caracteres • **Valor padrão**: ALLOWLIST_e9bd0ac50b632200263a089b37673a0b
ID da ação de IU Executar pesquisa de ameaças. sn_app_secops_ui.explore.action.id.run_threat_lookup	• **Tipo**: cadeia de caracteres • **Valor padrão**: da5ff4420b540300263a089b37673ae7
ID da capacidade de integração da Pesquisa de ameaças. sn_app_secops_ui.explore.capability.id.threat_lookup	• **Tipo**: cadeia de caracteres • **Valor padrão**: 39344d4f0b273200263a089b37673ab1
ID da ação personalizada Aprimoramento de observável na guia Explorar no Espaço do analista de segurança.	• **Tipo**: cadeia de caracteres • **Valor padrão**: OBS_ENRICHMENT_54e2f5d60b5003009f66e94685673

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
sn_app_secops_ui.explore.action.id.observable_enrichment	
ID da capacidade de integração Aprimorar observável. sn_app_secops_ui.explore.capability.id.observable_enrichment	• **Tipo**: cadeia de caracteres • **Valor padrão**: 9ad183640b1003009f66e94685673af4
ID da Ação de IU Publicar na Lista de Observação. sn_app_secops_ui.explore.action.id.publish_to_watchlist	• **Tipo**: cadeia de caracteres • **Valor padrão**: 8ee94002ff743200c68c84648e94faf9
ID da ação de IU de solicitação de bloqueio. sn_app_secops_ui.explore.action.id.block_request	• **Tipo**: cadeia de caracteres • **Valor padrão**: 7158f6e40b2032008f9108e3c5673adf
ID da ação de IU Executar pesquisa de detecções. sn_app_secops_ui.explore.action.id.sightings_search	• **Tipo**: cadeia de caracteres • **Valor padrão**: 43f91a6f0b032200b97c67d985673a2c
ID da ação de IU Criar incidente de segurança secundário. sn_app_secops_ui.explore.action.id.create_child_incident	• **Tipo**: cadeia de caracteres • **Valor padrão**: 5a6882645363530099d5ddeeff7b1272
ID da ação de IU Adicionar anotação de segurança. sn_app_secops_ui.explore.action.id.add_security_annotation	• **Tipo**: cadeia de caracteres • **Valor padrão**: 1e3a3e723b5332005a9149a4d2efc4eb
ID da Ação Personalizada de Aprimoramento de IC na guia Explorar no Espaço do analista de segurança. sn_app_secops_ui.explore.action.id.ci_enrichment	• **Tipo**: cadeia de caracteres • **Valor padrão**: CI_ENRICHMENT_54e2f5d60b5003009f66e94685673a1
ID da ação de IU Isolar Host. sn_app_secops_ui.explore.action.id.Isolate_host	• **Tipo**: cadeia de caracteres • **Valor padrão**: d6244e0aff203200c68c84648e94fad3

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do Espaço do analista de segurança

Nome da Propriedade	Descrição
ID da ação de IU Adicionar vários observáveis. sn_app_secops_ui.explore.action.id.multiple_observable	• **Tipo**: cadeia de caracteres • **Valor padrão**: 138de478d78322007a6de294de6103aa
Chave do produto para ag-Grid-Enterprise. sn_app_secops_ui.ag-grid-license	• **Tipo**: cadeia de caracteres • **Valor padrão**: ServiceNow_ServiceNow_5Devs2_August_2018__MTUzM:

Configuração adicional do espaço do analista de segurança

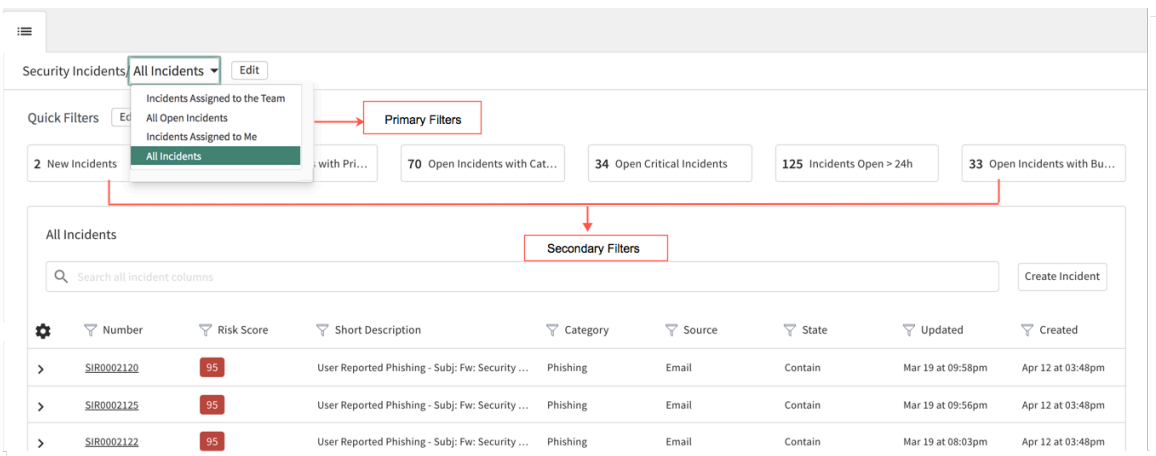
Configure o Espaço do analista de segurança e defina filtros, ações de IU e listas relacionadas.

- Configuração de filtro da página principal
- Habilitar ações de IU
- Ações de IU de formulário
- Configuração da Lista relacionada
- Ações de IU da Lista relacionada
- Propriedades do sistema de configuração de formulário
- Habilitar playbooks para seleção do analista

Configuração de filtro da página principal

Você pode adicionar novos filtros ou modificar os filtros existentes que aparecem no Espaço do analista de segurança.

O Espaço do analista de segurança tem filtros primários e secundários que permitem filtrar a lista de incidentes de segurança para que você possa encontrar rapidamente os incidentes de segurança que deseja analisar. Para obter mais informações, consulte Gerenciar ameaças à segurança usando o Espaço do analista de segurança.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar um novo filtro

1. Navegar até **Incidentes de segurança** > **Configuração do espaço de analista (nova IU)** > **Configuração de filtro da página principal**.
2. Clique em **Nova**.
3. Insira um título para o filtro, especifique a condição do filtro e clique em **Enviar** para retornar à página anterior.

   Você verá o filtro recém-adicionado listado na página.
4. Adicione um marcador a este filtro para indicar se é um filtro primário ou secundário. Os seguintes marcadores estão disponíveis:
   - SN_SI_Primário
   - SN_SI_Secundário

Editar filtros existentes

Você também pode fazer o seguinte:

- Modificar filtros existentes: clique no título de um filtro existente. Modifique o título e a condição do filtro e clique em **Atualizar**.
- Modificar marcadores: selecione um filtro e clique na coluna Marcador na configuração do filtro da página principal. Você pode excluir o marcador existente ou adicionar um novo marcador para o filtro.

Habilitar ações de IU

Antes de configurar qualquer Ação de IU, você deve executar determinadas etapas para habilitá-las para que fiquem disponíveis para configuração no Espaço do analista de segurança.

Nota:
Para modificar as ações de IU, faça login como um usuário com as seguintes funções:

- ui_action_admin
- ui_page_admin
- web_service_admin

Existem dois tipos de ações de IU que podem ser configuradas para o Espaço do analista de segurança:

- Ação de IU baseada em diálogo
- Ação de IU do lado do servidor

Ação de IU baseada em diálogo

Para habilitar ações de IU baseadas em diálogo no Espaço do analista de segurança, faça as seguintes mudanças nas páginas de IU associadas às respectivas ações de IU padrão.

1. **Seção HTML**: modifique a seção HTML para incluir o marcador de entrada de *`reação`*. O valor do marcador de entrada de *`reação`* é usado na seção de script do cliente para identificar se a Página de IU foi iniciada a partir de Espaço do analista de segurança. Um exemplo é mostrado abaixo:

```
<input id="react" name="react" type="hidden"
value="${JS,HTML:sysparm_react}" />
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. **Script do cliente**: a lógica adicional precisa ser gravada no script do cliente quando o sinalizador de *reação* é verdadeiro. Isso é necessário para lidar com os eventos do botão **Enviar** e **Cancelar** mostrados como parte da janela de diálogo.
   a. O manipulador de eventos onCancel () precisa expedir o evento "SIR_WORKBENCH_POPUP_CANCEL" do Espaço do analista de segurança
   b. O manipulador de eventos onSubmit () precisa expedir o evento "SIR_WORKBENCH_POPUP_SUBMIT" do Espaço do analista de segurança
3. A execução do script de processamento é ignorada do contexto Espaço do analista de segurança porque a ação "onSubmit" foi modificada para retornar falso quando o valor do marcador de entrada de *reação* for verdadeiro. A lógica do script de processamento precisa ser tratada por meio de um script de cliente chamável (invocado por meio da API GlideAjax) ou do endpoint do recurso REST.

Consulte as seguintes páginas de IU de amostra para obter mais detalhes:

- Exemplo de ação de IU da Lista relacionada: Publicar na lista de observação (nome da página de IU:public_to_watchlist)
- Exemplo de ação de IU de formulário: Criar problema (nome da página de IU: create_prb_change_inc)

Ação de IU do lado do servidor

Para habilitar ações de IU do lado do servidor, você deve fazer o seguinte:

A lógica do script de ação de IU padrão deve ser tratada como parte de um recurso REST de script.

Consulte os seguintes exemplos de ações de IU de formulário para obter mais detalhes:

- Criar indisponibilidade
- Cancelar

Ações de IU de formulário

Você pode configurar as ações de IU que são exibidas no Espaço do analista de segurança.

Pré-requisitos:

Antes de configurar qualquer ação de IU, você deve executar determinadas etapas para habilitá-las para que fiquem disponíveis para configuração no Espaço do analista de segurança. Consulte Habilitar ações de IU para mais detalhes.

Para configurar uma ação de IU de formulário para o Espaço do analista de segurança, siga estas etapas:

1. Navegar até **Incidentes de segurança** > **Configuração do espaço de analista (nova IU)** > **Ações de IU de Formulário**.
2. Insira os seguintes detalhes:

Nome do campo	Descrição
Ação	Selecione uma ação de IU na lista de seleção.
Tipo	Selecione o tipo de ação. Isso pode ser:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do campo	Descrição
	○ Ação baseada em diálogo: este tipo de ação é usado quando a interação do usuário ou as entradas são necessárias para executar a lógica de negócios específica. ○ Ação do lado do servidor: esta ação executa a lógica de negócios necessária sem qualquer entrada adicional do usuário. **Nota:** Antes de configurar qualquer ação de IU, você deve executar determinadas etapas para habilitá-las para que fiquem disponíveis para configuração no Espaço do analista de segurança. Consulte Habilitar ações de IU para mais detalhes.
Aplicação	O nome do escopo da aplicação (IU do Security Incident Response) ao qual a ação de IU está sendo adicionada é exibido aqui.
Ação baseada em diálogo Se você selecionar Ação baseada em diálogo no campo Tipo, insira os seguintes detalhes:	
Página de IU	Selecione a página de IU associada à ação.
Título da Caixa de Diálogo	Insira um título para a ação de diálogo.
Largura e Altura da Caixa de Diálogo	Insira a altura e a largura da caixa de diálogo em pixels.
Script	Para a Página de IU selecionada, você pode especificar parâmetros de consulta adicionais aqui. O modelo fornecido com o sistema de base constrói e retorna somente o parâmetro `sysparm_sys_id`. Você pode substituir isso especificando parâmetros diferentes aqui.
Ação do lado do servidor Se você selecionar Ação do lado do servidor no campo Tipo, insira os seguintes detalhes:	
Recurso Rest de Script	Selecione o recurso Rest de script que define a ação. **Nota:** A ACL **SIR UI ANALYST** deve ser adicionada ao recurso REST.

3. Clique em **Enviar**.
4. Navegar até **Incidentes de segurança** > **Incidentes (Nova IU)** página.
5. Clique em um número de incidente de segurança para exibir o registro do incidente de segurança. Você pode ver a nova ação de IU na parte superior da página.

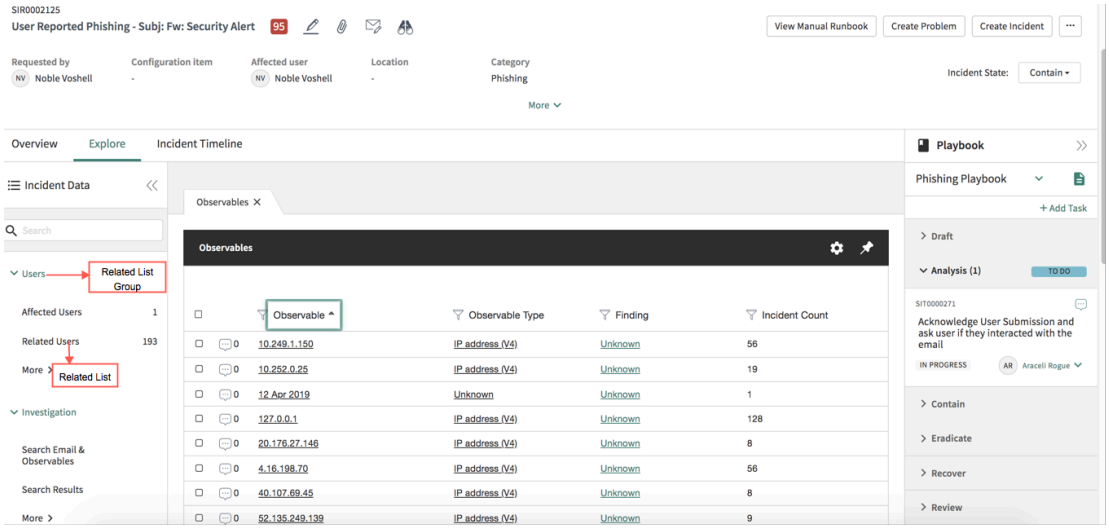
Para modificar uma ação de IU de formulário existente, clique no Nome da ação para navegar até a página Ações de IU de formulário. Você pode modificar o Nome da Ação, o Tipo e o restante dos campos com base no tipo selecionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração da Lista relacionada

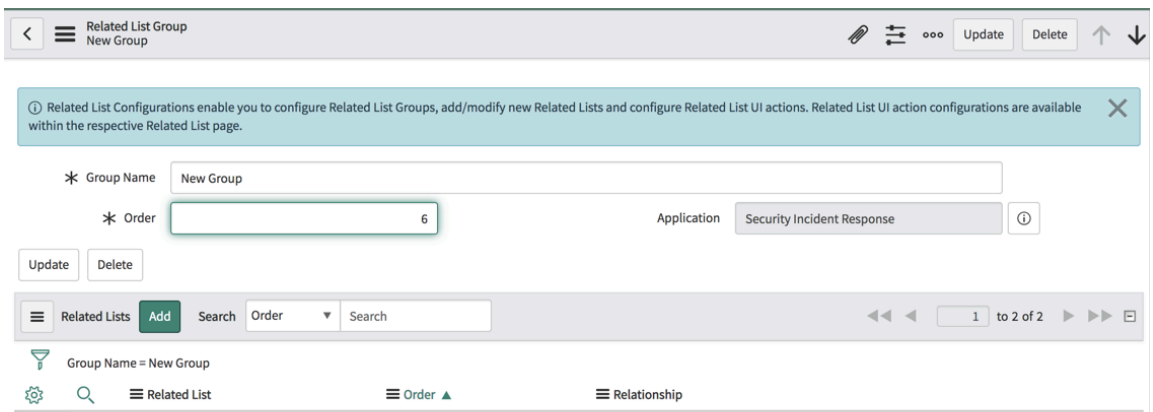
Você pode adicionar novas listas relacionadas ou novos grupos de listas relacionadas e modificar grupos existentes ou listas relacionadas que aparecem no Espaço do analista de segurança.



Adicionar um grupo de lista relacionada

Para adicionar um grupo de lista relacionada, siga estas etapas:

1. Navegar até **Incidentes de segurança** > **Configuração do espaço de analista (nova IU)** > **Configurações de Lista relacionada**.
2. Clique em **Novo** para adicionar um novo Grupo de Lista relacionada. Insira o Nome do Grupo e a Ordem em que ele deve aparecer na página Incidentes (Nova IU).
3. Clique em **Enviar**. O grupo recém-adicionado aparece na página Grupos de lista relacionada.



Adicionar uma Lista relacionada

Para adicionar uma nova Lista relacionada, siga estas etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Clique em um link de Grupo de lista relacionada.
2. Na seção Listas relacionadas, clique em **Adicionar** para adicionar uma nova lista relacionada.

   Se você não vir o botão **Adicionar**, verifique se você está no mesmo escopo da aplicação que o Grupo de Lista relacionada.
3. Selecione a Lista relacionada a ser incluída no grupo.

   Nota:
   Se você não vir uma lista relacionada específica, faça o seguinte:

   a. Navegar até **IU do Sistema** > **Listas relacionadas** e pesquise Listas relacionadas presentes na tabela `sn_si_incident`.
   b. Clique na tabela `sn_si_incident` associada à exibição de **nova IU do SIR**.
   c. Na seção Entradas da lista relacionada, clique em **Novo** para adicionar a Lista relacionada à exibição **Nova IU do SIR**.
4. Especifique a ordem em que ele deve aparecer e clique em **Enviar**.

   A Lista relacionada que você adicionou aparecerá no Espaço do analista de segurança.

Para modificar um Grupo de Lista relacionada existente, clique no Nome do grupo para navegar até a página Grupo de Lista relacionada. Você pode modificar o Nome do Grupo, a Ordem e adicionar ou excluir Listas relacionadas do grupo.

Ações de IU da Lista relacionada

Você pode adicionar novas ações de IU às listas relacionadas que aparecem em Espaço do analista de segurança.

Pré-requisitos:

Antes de configurar qualquer ação de IU, você deve executar determinadas etapas para habilitá-las para que fiquem disponíveis para configuração no Espaço do analista de segurança. Consulte Habilitar ações de IU para mais detalhes.

Para adicionar uma nova ação de IU de Lista relacionada, siga estas etapas:

1. Navegar até **Incidentes de segurança** > **Configuração do espaço de analista (nova IU)** > **Configurações de Lista relacionada**.
2. Clique no Nome do grupo. A página de configuração do Grupo de lista relacionada é exibida.
3. Clique na Lista relacionada à qual você deseja adicionar uma ação de IU.
4. Clique em **Adicionar** na seção Ações de IU da Lista relacionada.
5. Insira os seguintes detalhes:

Nome do campo	Descrição
Ação	Selecione uma ação de IU na lista de seleção.
Tipo	Selecione o tipo de ação. Isso pode ser:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do campo	Descrição
	○ Ação baseada em diálogo: este tipo de ação é usado quando a interação do usuário ou as entradas são necessárias para executar a lógica de negócios específica. ○ Ação do lado do servidor: esta ação executa a lógica de negócios necessária sem qualquer entrada adicional do usuário. **Nota:** Antes de configurar qualquer ação de IU, você deve executar determinadas etapas para habilitá-las para que fiquem disponíveis para configuração no Espaço do analista de segurança. Consulte Habilitar ações de IU para mais detalhes.
Aplicação	O nome do escopo da aplicação (IU do Security Incident Response) ao qual a ação de IU está sendo adicionada é exibido aqui.
Ação baseada em diálogo Se você selecionar Ação baseada em diálogo no campo Tipo, insira os seguintes detalhes:	
Página de IU	Selecione a página de IU associada à ação.
Título da Caixa de Diálogo	Insira um título para a ação de diálogo.
Largura e Altura da Caixa de Diálogo	Insira a altura e a largura da caixa de diálogo em pixels.
Script	Para a Página de IU selecionada, você pode especificar parâmetros de consulta adicionais aqui. O modelo fornecido com o sistema de base constrói e retorna somente os parâmetros `sysparm_incident_id`, `sysparm_record_table`e `sysparm_related_sys_ids`. Você pode substituí-los especificando diferentes parâmetros aqui.
Ação do lado do servidor Se você selecionar Ação do lado do servidor no campo Tipo, especifique o seguinte:	
Recurso Rest de Script	Selecione o recurso Rest de script que define a ação. **Nota:** A ACL **SIR UI ANALYST** deve ser adicionada ao recurso REST.

6. Clique em **Enviar**.
7. Navegar até **Incidentes de segurança** > **Incidentes (Nova IU)** página.
8. Clique em um número de incidente de segurança para exibir o registro do incidente de segurança. Inicie a respectiva Lista relacionada para exibir a nova ação de IU.

Propriedades do sistema de configuração de formulário

Essas propriedades do sistema definem os intervalos de atualização do formulário para as tarefas do playbook.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

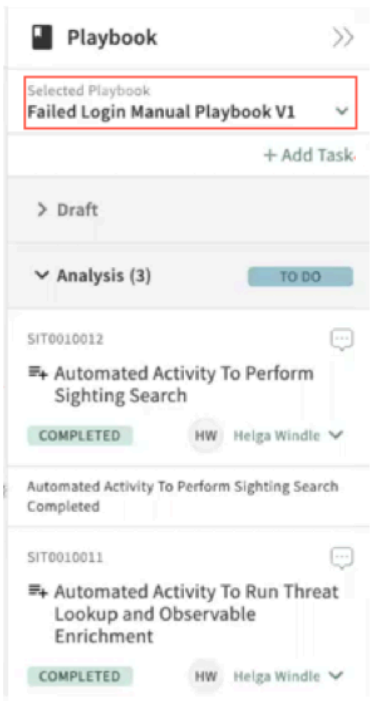
Para configurar essas propriedades, navegue até **Configuração do espaço de analista (nova IU)** > **Propriedades do espaço do analista**.

Propriedade	Valor padrão	Descrição
sn_app_secops_ui.poller_interval.playbook_tasks	10000 ms	O tempo de intervalo usado pelo componente do playbook para atualizar suas tarefas de resposta para cada tempo de intervalo configurado.
sn_app_secops_ui.poller_interval_count.playbook_tasks	9 vezes	O número de vezes que o componente do playbook pesquisa tarefas de resposta.
sn_app_secops_ui.poller_interval.related_lists	30000 ms	Este tempo de intervalo é usado pelo componente Explorar para atualizar suas contagens de Lista relacionada para cada tempo de intervalo configurado.

Habilitar playbooks para seleção do analista

Adicione novos playbooks à lista de seleção de playbooks.

Você pode selecionar um playbook apropriado para investigar incidentes de segurança no Espaço do analista de segurança (Gerenciar ameaças à segurança usando o Espaço do analista de segurança). A opção de seleção de playbook é compatível somente com os playbooks projetados usando o Flow Designer.



Depois de criar um playbook usando o Flow Designer, siga estas etapas para incluí-lo na lista de seleção Playbook selecionado:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegue até a tabela *sys_hub_flow*.
2. Pesquise o novo playbook que você criou usando o Flow Designer.
3. Adicione o marcador **sir_playbook** aos playbooks que você deseja incluir na lista de seleção Playbook selecionado.

Nota:
Se você tiver playbooks antigos que não foram migrados de fluxos de trabalho para o Flow Designer, eles não serão exibidos na lista. Mas, se um playbook criado usando fluxos de trabalho for atribuído a um incidente de segurança por uma condição do gatilho ou por seleção manual (usando a opção **Executar Orquestração** no ambiente clássico), esse playbook será iniciado quando você abrir o incidente de segurança no Espaço do analista de segurança.

Solução de problemas do Security Incident Response

Esta seção aborda dicas importantes de solução de problemas e perguntas frequentes relacionadas ao Security Incident Response.

Problemas com as regras de controle de acesso

As Regras de controle de acesso permitem o acesso ao recurso especificado se todas as três condições a seguir forem atendidas:

- O usuário tem uma das funções especificadas na lista **Função** ou a lista está vazia.
- As condições no campo **Condição** são avaliadas como verdadeiras ou as condições estão vazias.
- O script no campo **Script** (avançado) é avaliado como verdadeiro ou define a **resposta** da variável como verdadeira ou está vazio.

Para obter mais informações sobre as Regras de controle de acesso, consulte Exploring Access Control Lists.

Importante:
Se a opção de **substituições do administrador** estiver desmarcada para uma tabela de incidentes de segurança e se o administrador puder acessar a tabela de incidentes de segurança, consulte KB1444673.

Security Incident Response Soluções Análise da plataforma

As Soluções Análise da plataforma contêm painéis pré-configurados. Os painéis apresentam métricas importantes para analisar seu processo Security Incident Response, como novos incidentes de segurança ou a idade média dos incidentes de segurança em aberto.

Use os widgets Platform Analytics no painel para visualizar dados ao longo do tempo, analisar seus processos de negócios e identificar áreas de melhoria. Com o Soluções Análise da plataforma, você pode obter valor do Performance Analytics para seu aplicativo com o mínimo de configuração. Você sempre pode criar seus próprios objetos.

Importante:
Configure e teste Soluções Análise da plataforma em uma instância de não produção antes de habilitá-los na produção.

A Solução Security Incident Response Performance Analytics está disponível no ServiceNow Store. Para obter informações sobre como baixar e instalar esse aplicativo, consulte Security Operations e a ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Para avaliar a funcionalidade, você pode ativar as soluções de Performance Analytics e a análise no formulário em instâncias que não tenham o Performance Analytics licenciado. No entanto, você tem as seguintes limitações:

- Você não pode criar novos indicadores.
- Você não pode coletar dados com mais de 180 dias.

Para obter a funcionalidade completa, licencie o Performance Analytics. Para obter mais informações, consulte Ativar assinatura do Performance Analytics .

Importante:
Por padrão, o limite de coleta de dados para a propriedade *(com.snc.pa.dc.max_records)* no Performance Analytics é definido como 5.000 registros. Mas você pode aumentar esse limite de acordo com seus requisitos, como 50.000 registros. No entanto, aumentar esse limite pode afetar o desempenho durante a coleta de dados ou ao executar operações na tabela de snapshot. Para saber mais sobre as propriedades do Performance Analytics, consulte Performance Analytics properties .

Tópicos relacionados

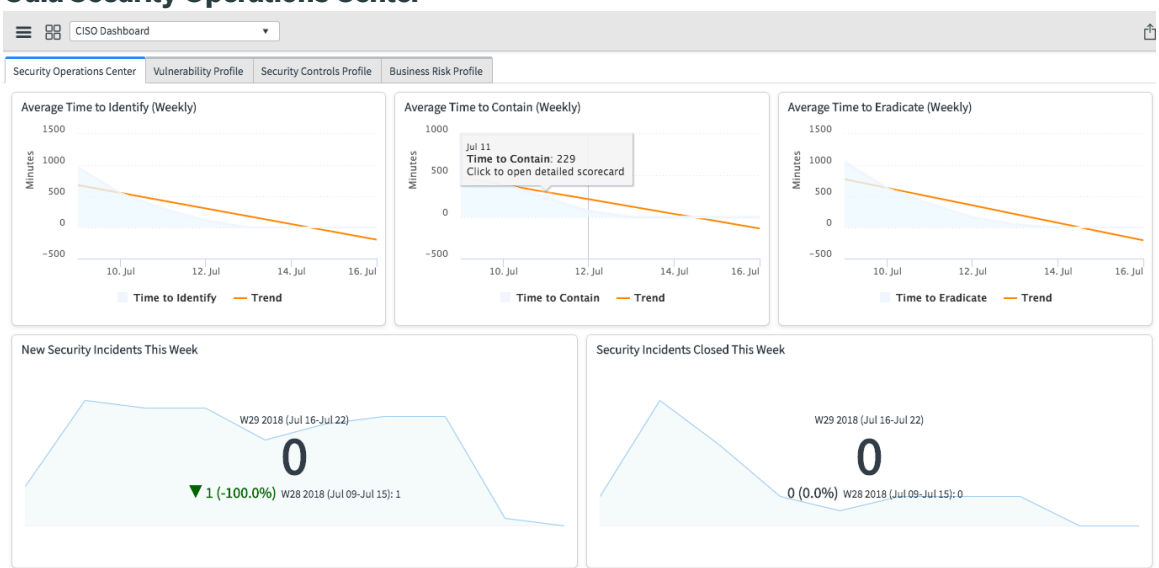
Soluções Análise da plataforma

Ative sua assinatura do Performance Analytics

Painel do CISO

Este painel revela a postura geral de segurança da sua organização, incluindo vulnerabilidades e incidentes de segurança.

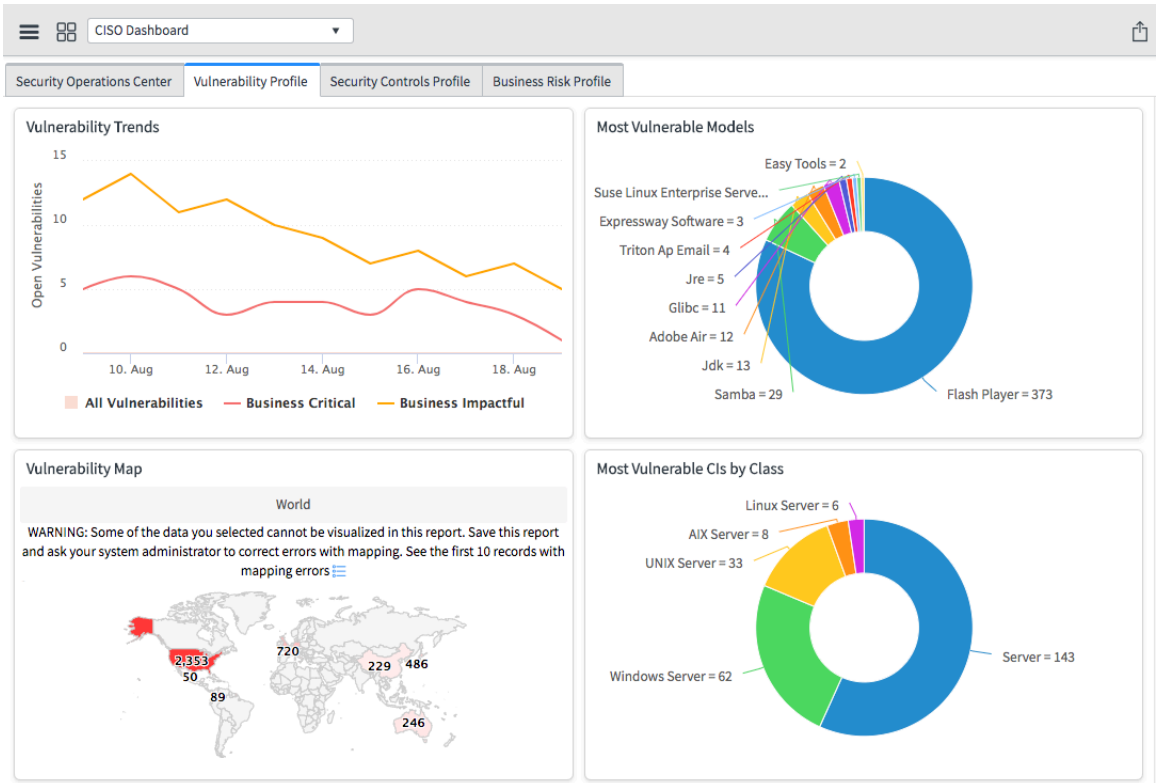
Guia Security Operations Center



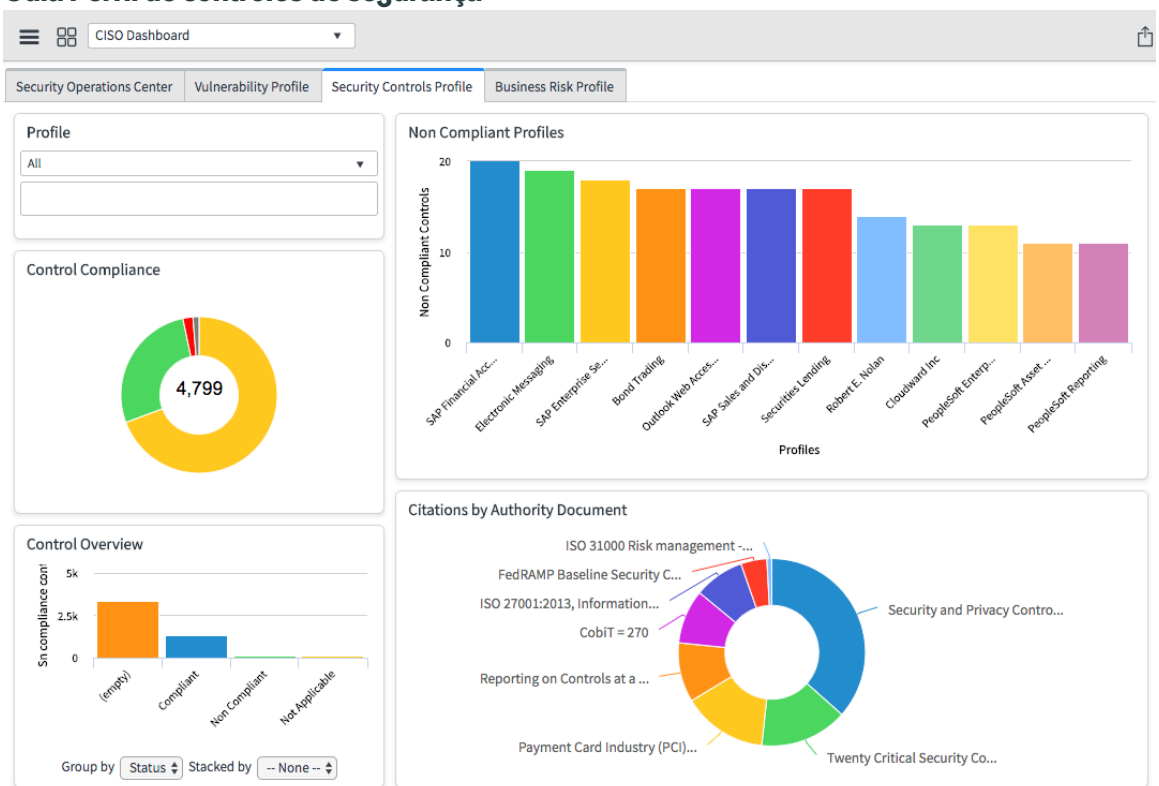
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Perfil de vulnerabilidade



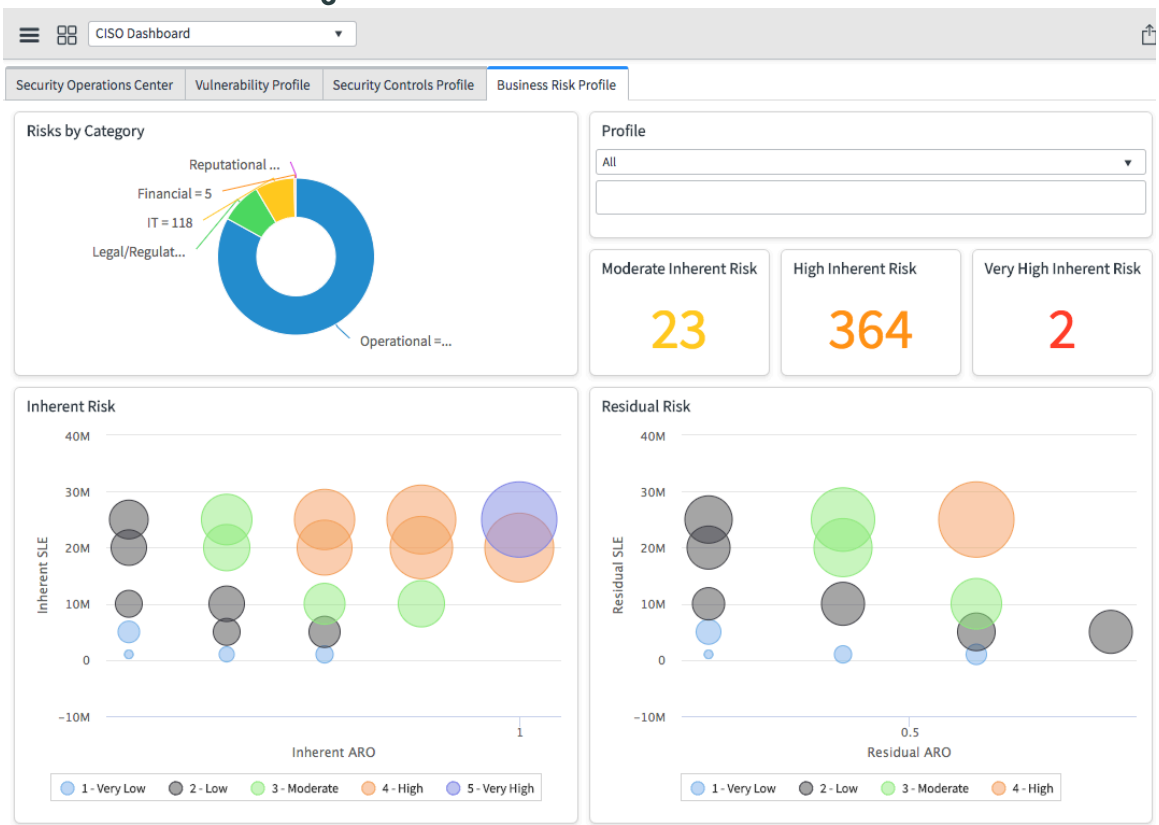
Guia Perfil de controles de segurança



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Perfil de risco de negócios



Funções e usuário finais

Usuário final e objetivo	Função necessária
CISO: precisa de visibilidade clara sobre a postura de segurança atual da organização em geral	sn_si.ciso

Indicadores do painel do CISO

O painel do CISO apresenta os seguintes indicadores-chave de desempenho:

Incidente de segurança: tempo médio de identificação

Uma média de 7 dias do tempo em minutos necessário para identificar um incidente de segurança, calculada diariamente.

Tempo médio de contenção

Uma média de 7 dias do tempo em minutos necessário para conter um incidente de segurança, calculada diariamente.

Tempo médio para eliminar

Uma média de 7 dias do tempo em minutos necessários para erradicar um incidente de segurança, calculada diariamente. O tempo médio para conter e o tempo médio para erradicar são baseados no indicador SI: tempo médio de duração dividido por estado do incidente de segurança.

Novos Incidentes de segurança nesta semana

A soma semanal da pontuação do indicador diário de Número de novos incidentes de segurança.

Incidentes de segurança encerrados (semanalmente)

A soma de 7 dias de execução do indicador diário de Número de incidentes de segurança encerrados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Novos incidentes de segurança por prioridade

Detalhamento diário do indicador Número de novos incidentes de segurança por Prioridade.

Volume de incidentes de segurança novos versus encerrados (semanalmente)

A série temporal de soma de 7 dias consecutivos do indicador Número de novos incidentes representada graficamente em relação à série temporal de soma de 7 dias consecutivos do indicador Número de incidentes encerrados.

Mapa térmico de incidente de segurança

Um mapa global que mostra o número de incidentes de segurança em aberto em cada país.

Mapa de Árvore de Incidentes de Segurança

Um mapa de árvore interativo em que você pode selecionar para ver:

- Incidentes de segurança por serviço de negócios, divididos por criticalidade dos negócios
- Incidentes de segurança divididos por categoria ou subcategoria de incidente
- Incidentes de segurança por grupo de atribuição ou por designado
- "Estatísticas de vítima" de incidente de segurança por recurso afetado ou usuário afetado

Detalhamentos

Os seguintes detalhamentos se aplicam aos indicadores no painel:

- Criticalidade dos negócios
- Grupo de Segurança
- Idade do Incidente de segurança
- Categoria de Incidente de segurança
- Código de fechamento de incidentes de segurança
- Prioridade de Incidente de segurança
- Estado do Incidente de segurança
- SI - Serviço de negócios
- Vulnerabilidade

Visualizações de dados

O painel inclui as seguintes visualizações:

Título	Tipo	Descrição
Incidentes de segurança em aberto por mais de 30 dias por grupo de atribuição e estado	Mapa térmico	Exibe modelos com os itens mais vulneráveis.
Risco por categoria	Donut de Donut	Lista a idade dos itens vulneráveis reabertos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título	Tipo	Descrição
Citações por documento de autoridade	Donut de Donut	Número de vulnerabilidades ativas
Incidentes de segurança com o designado que não está ativo	Mapa térmico	Exibe o número de itens vulneráveis em aberto associados a vulnerabilidades (registros de enumeração de vulnerabilidade comum (CVE)), do maior para o menor.
Incidentes de segurança não atualizados há mais de 30 dias por grupo de atribuição e estado	Mapa térmico	Exibe fornecedores com os itens mais vulneráveis.
Mapa de Vulnerabilidades	Mapa	Um mapa-múndi mostrando vulnerabilidades por local
Modelos mais vulneráveis	Donut de Donut	As aplicações que contêm mais vulnerabilidades
ICs mais vulneráveis por classe	Donut de Donut	ICs por tipo de servidor
Serviços com vulnerabilidades críticas significativas	Lista	
Perfis fora de conformidade	Barra de barra	Controles fora de conformidade por perfil
Visão geral de controle	Barra de barra	Número de controles em conformidade e fora de conformidade
Exceções da Política	Lista	Exceções de política com prioridade, proprietário e descrição resumida
Risco por categoria	Donut de Donut	O número de riscos em cada categoria de risco
Risco inerente	Bolha de bolha	SLE inerente versus ARO inerente
Risco residual	Bolha de bolha	SLE residual versus ARO residual
Riscos moderados, altos e muito altos	Pontuações	Os números de riscos moderados, altos e muito altos, respectivamente
Risco por perfil	Barra Barra empilhada	Contagem de risco em que você pode selecionar o que agrupar e o que empilhar

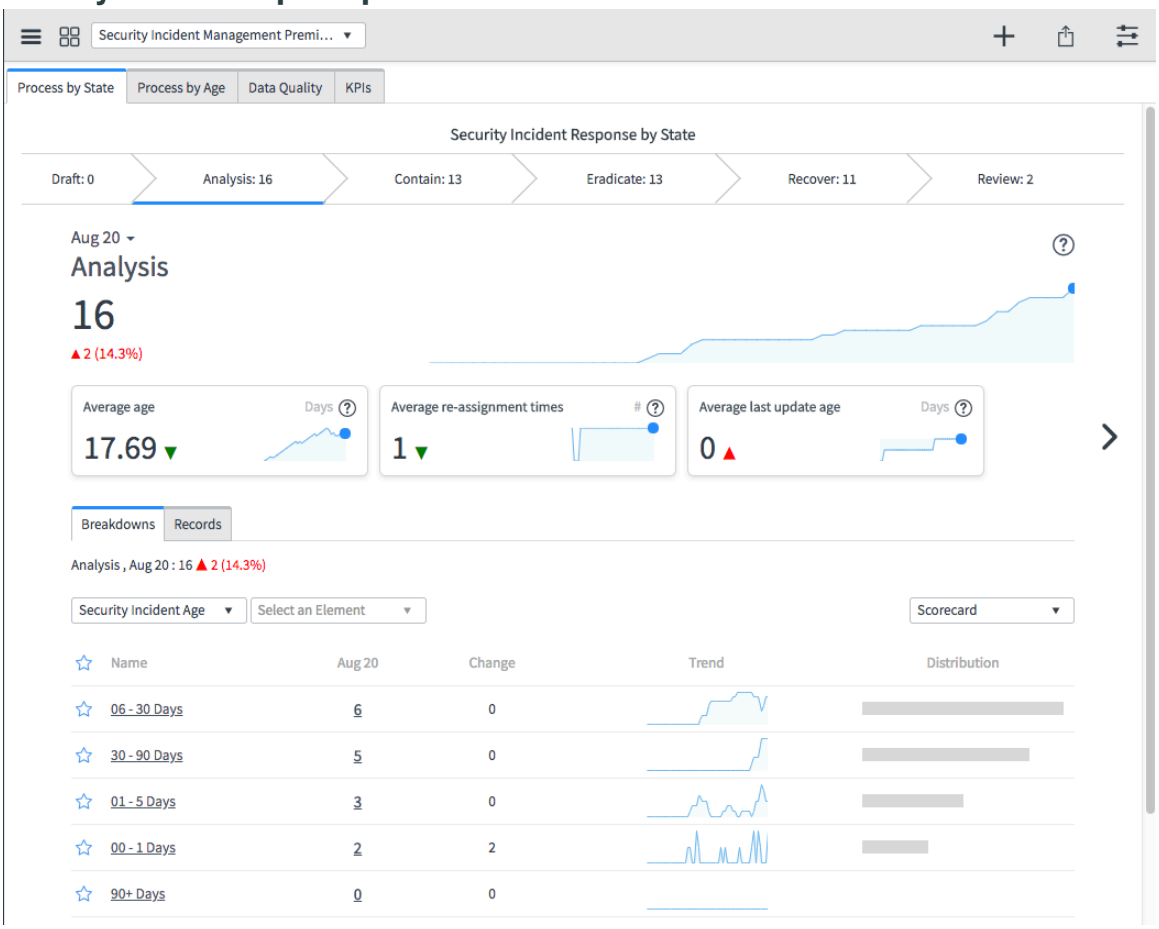
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painel do Security Incident Management Premium

Este painel usa visualizações avançadas Platform Analytics para ajudar os gerentes de segurança a rastrear o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação. A versão licenciada de Performance Analytics é, portanto, necessária.

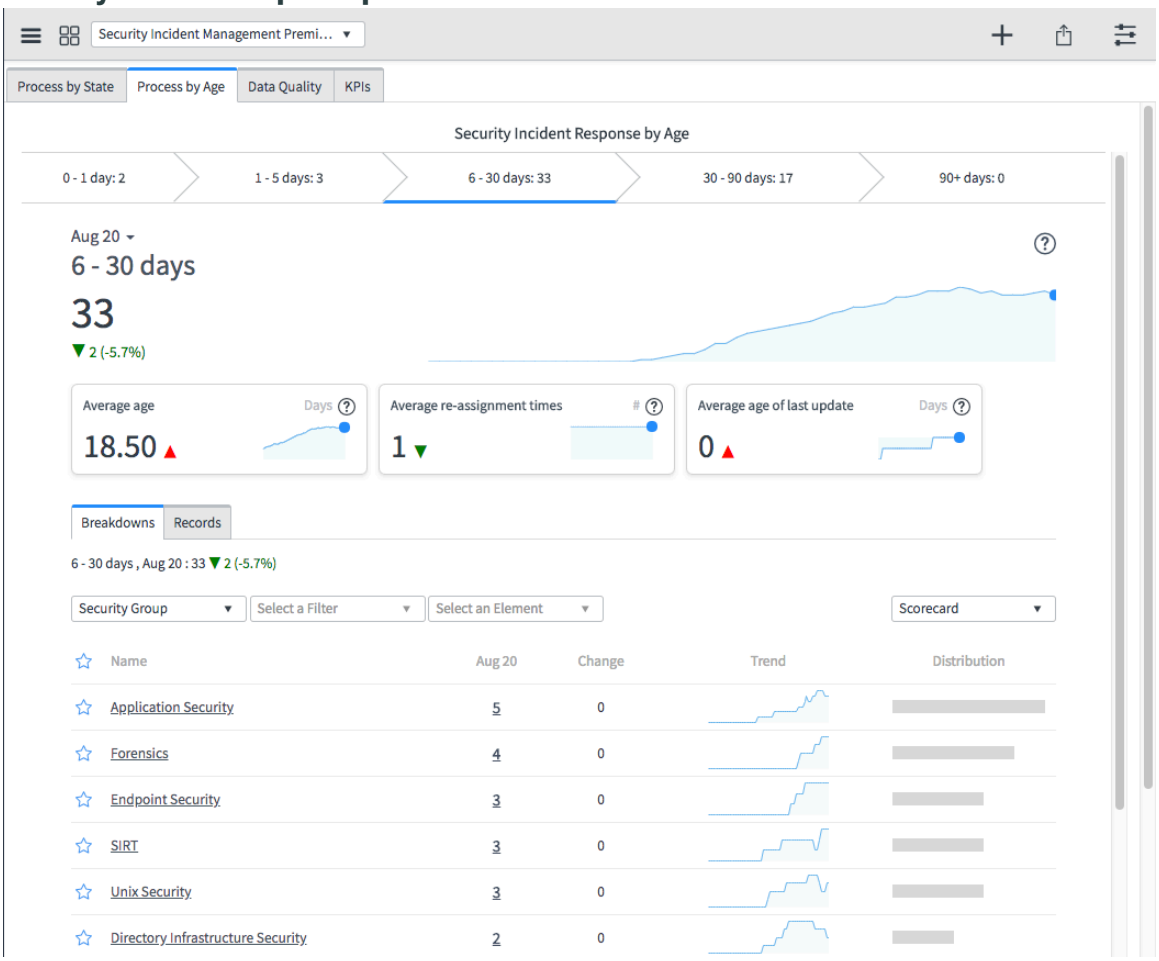
Security Incident Response por estado



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Security Incident Response por idade



Funções e usuário finais

Usuário final e objetivo	Função necessária	Benefícios
Security Response Manager: precisa de visibilidade clara do estado geral e do volume de incidentes de segurança associados a aplicações e serviços.	sn_si.manager	Pode revisar a postura geral de segurança com a capacidade de ajustar os membros dos grupos de atribuição.
Administrador do Security Response: precisa identificar áreas de interesse rapidamente e ter controle total sobre todos os dados do Security Incident Response ao administrar territórios e habilidades, conforme necessário.	sn_si.admin	Pode ajustar os parâmetros de cálculo de risco para garantir que os itens vulneráveis mais pertinentes à organização sejam tratados primeiro.
Analistas do Security Response: precisam priorizar rapidamente em quais vulnerabilidades se concentrar com base na criticidade para a organização.	sn_si.analyst	Os analistas de segurança de nível 1 e 2 trabalham em incidentes de segurança. Eles podem criar e atualizar incidentes de segurança, solicitações e tarefas, bem como problemas, mudanças e indisponibilidades relacionadas aos seus incidentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicadores do Security Incident Management Premium

As guias Processo por estado e Processo por idade contêm widgets de workbench com os seguintes indicadores:

Idade média

O indicador Idade média dos incidentes de segurança em aberto usa a fórmula [[Idade somada dos incidentes de segurança em aberto]] / [[Número de incidentes de segurança em aberto]] / 24 para fornecer um resultado em dias.

Tempos médios de reatribuição

O indicador Reatribuição média de incidentes de segurança em aberto usa a fórmula Reatribuição somada de incidentes de segurança em aberto / Número de incidentes de segurança em aberto.

Idade média do último upgrade

O indicador Idade média da última atualização dos incidentes de segurança em aberto usa a fórmula Soma da idade da última atualização dos incidentes de segurança em aberto / Número de incidentes de segurança em aberto / 24 para fornecer um resultado em dias.

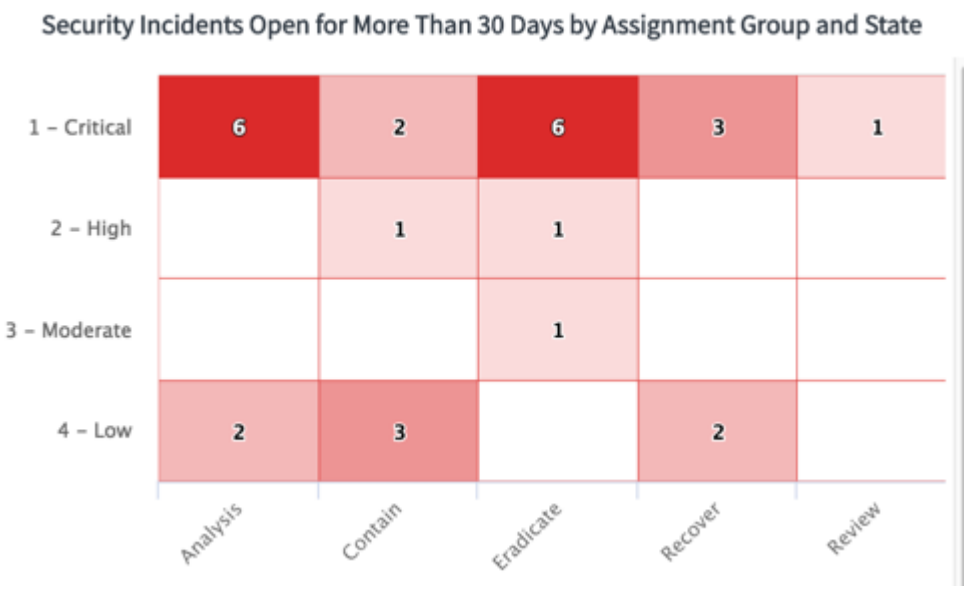
% não atualizada em 5 dias

O indicador Percentual de incidentes de segurança em aberto não atualizados nos últimos 5 dias usa a fórmula ([[Número de incidentes de segurança em aberto não atualizados nos últimos 5 dias]] / [[Número de incidentes de segurança em aberto]]) * 100.

A guia Qualidade de dados tem filtros interativos para a Categoria do incidente de segurança e os níveis de Risco, Prioridade e Severidade. Esses filtros são aplicados simultaneamente aos seguintes indicadores:

Incidentes de segurança em aberto por mais de 30 dias por grupo de atribuição e estado

O número de incidentes de segurança em aberto filtrados por uma idade de 30 dias e divididos por grupo de atribuição e estado.



Incidentes de segurança com o designado que não está ativo

O número de incidentes de segurança em aberto sem nenhum designado ou um designado que não está ativo.

Incidentes de segurança em aberto por mais de 30 dias por grupo de atribuição e estado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O indicador Número de incidentes de segurança em aberto não atualizados nos últimos 30 dias dividido por Grupo de atribuição e Estado.

A guia KPI tem os seguintes indicadores adicionais:

- Percentual de novos incidentes de segurança críticos
- Idade média dos incidentes de segurança em aberto
- Tempo médio de encerramento dos incidentes de segurança
- Percentual de incidentes de segurança que foram reatribuídos
- Percentual de incidentes de segurança encerrados na primeira atribuição
- Percentual de incidentes de segurança encerrados por autoatendimento
- Percentual de incidentes de segurança não resolvidos
- Tempo médio de encerramento das tarefas de incidente de segurança

Detalhamentos

Os seguintes detalhamentos se aplicam aos indicadores no painel:

- Grupo de Segurança
- Idade do Incidente de segurança
- Categoria de Incidente de segurança
- Prioridade de Incidente de segurança
- Estado do Incidente de segurança

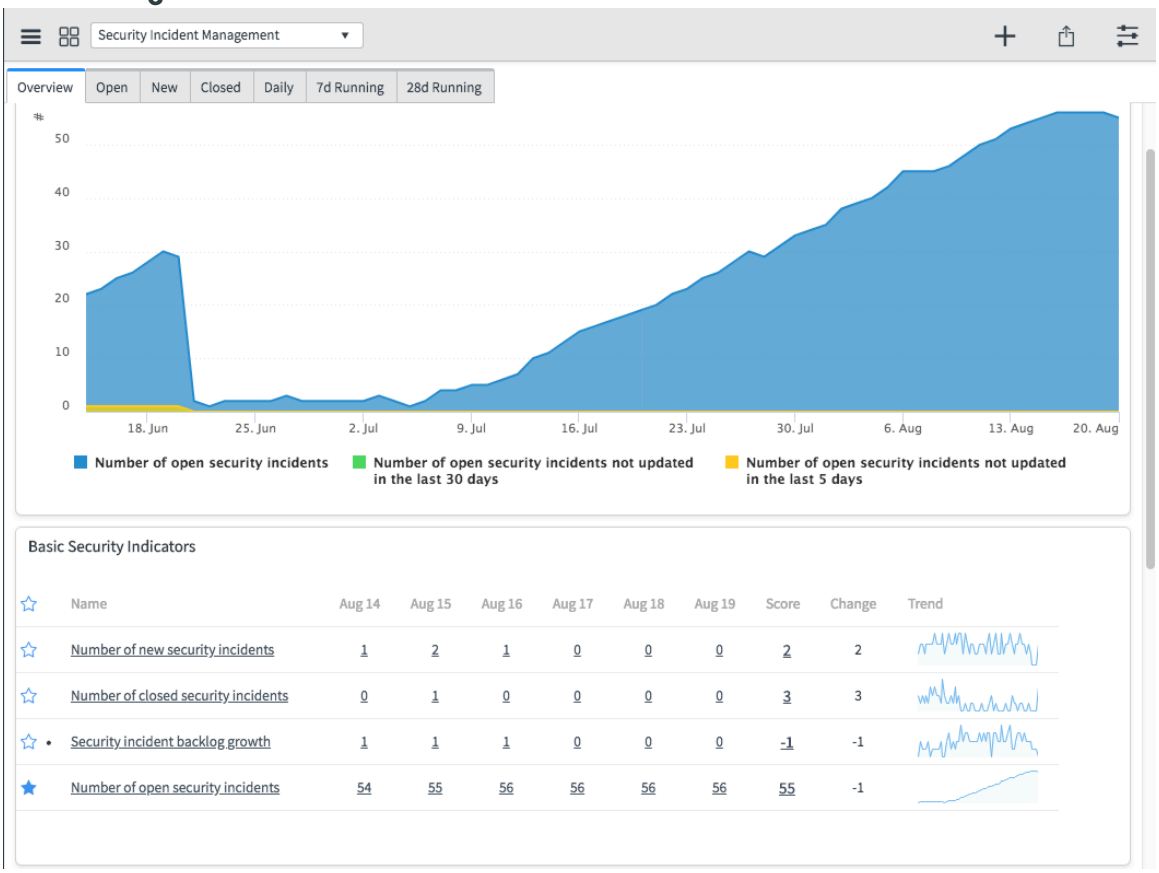
Painel do Security Incident Management

Com este painel, os gerentes de segurança podem rastrear facilmente o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação.

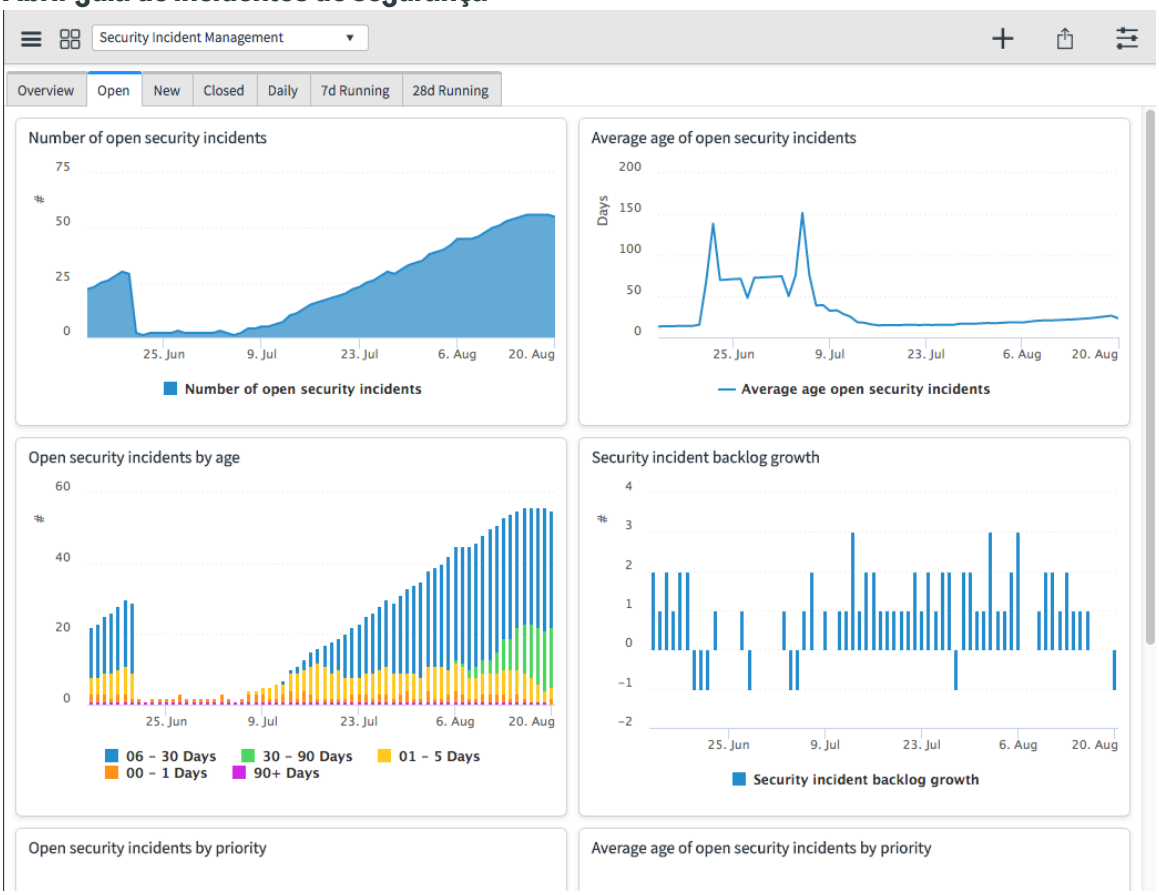
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral



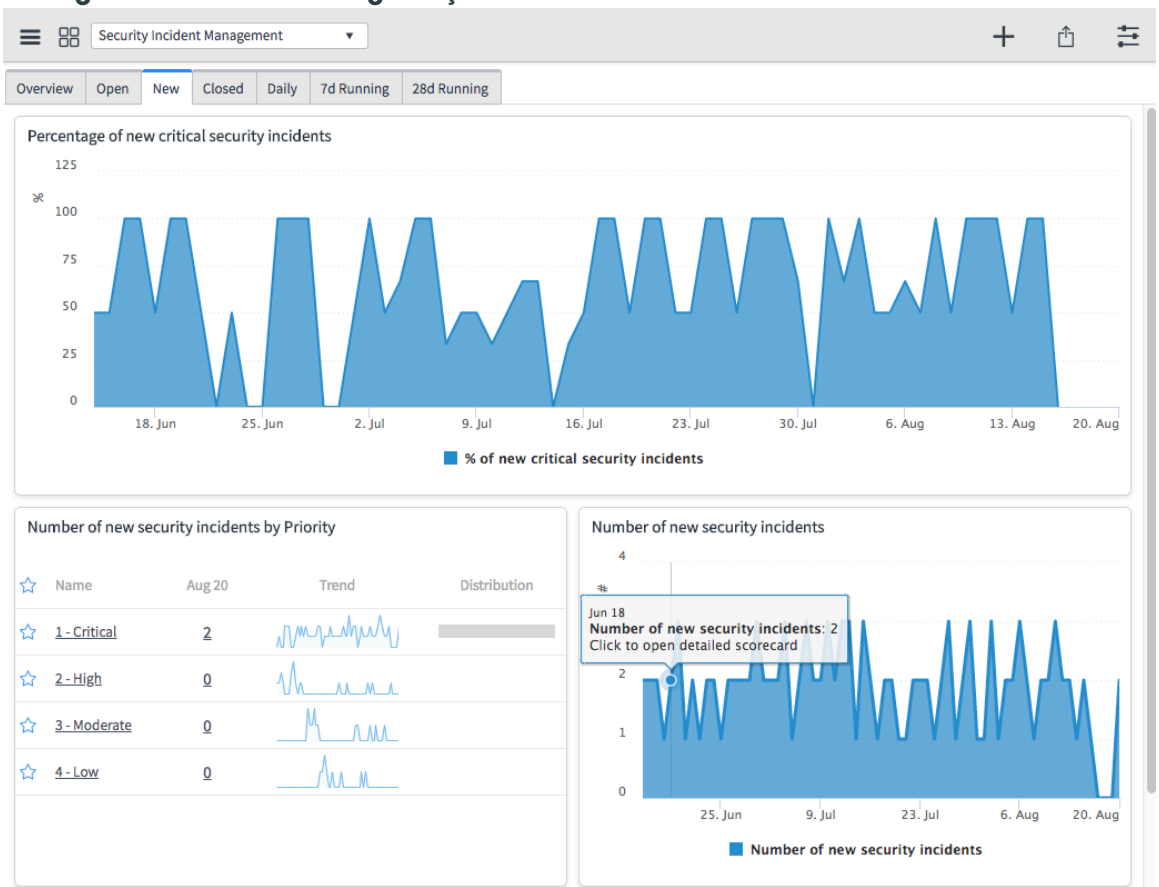
Abrir guia de incidentes de segurança



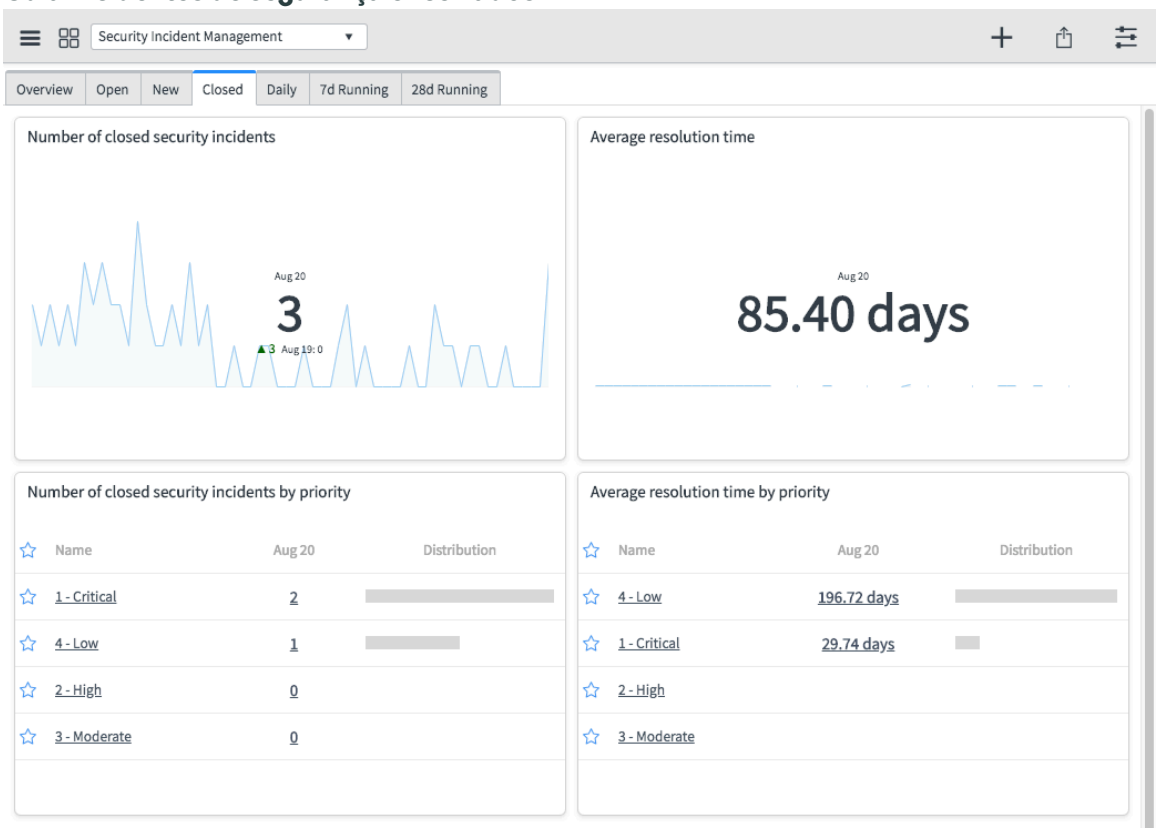
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nova guia de incidente de segurança



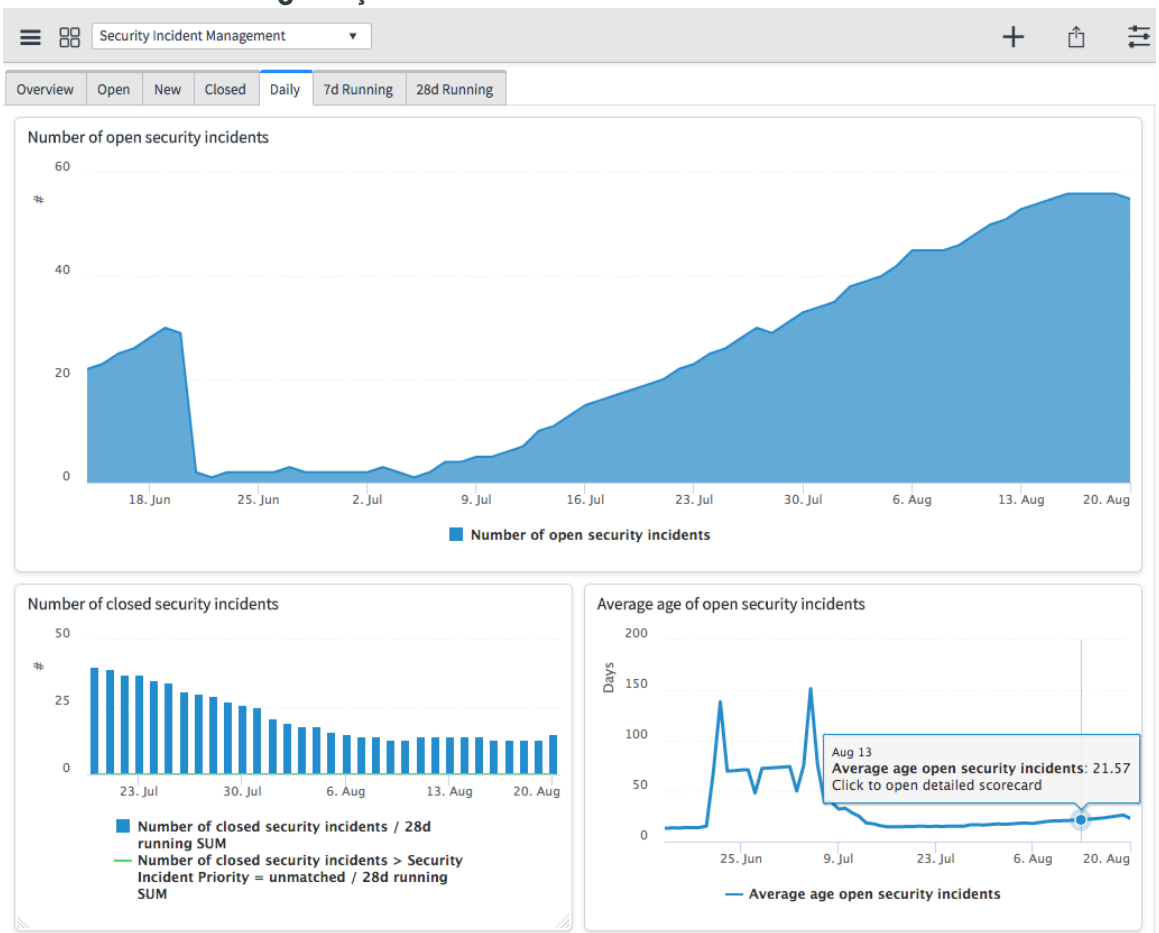
Guia Incidentes de segurança encerrados



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Incidentes de segurança diários



As guias **Execução** de 7 dias e **Execução** de 28 dias seguem o formato da guia **Diariamente**.

Funções e usuário finais

Usuário final e objetivo	Função necessária	Benefícios
Security Response Manager: precisa de visibilidade clara do estado geral e do volume de incidentes de segurança associados a aplicações e serviços.	sn_si.manager	Pode revisar a postura geral de segurança com a capacidade de ajustar os membros dos grupos de atribuição.
Administrador do Security Response: precisa identificar áreas de interesse rapidamente e ter controle total sobre todos os dados do Security Incident Response ao administrar territórios e habilidades, conforme necessário.	sn_si.admin	Pode ajustar os parâmetros de cálculo de risco para garantir que os itens vulneráveis mais pertinentes à organização sejam tratados primeiro.
Analistas do Security Response: precisam priorizar rapidamente em quais vulnerabilidades se concentrar com base na criticidade para a organização.	sn_si.analyst	Os analistas de segurança de nível 1 e 2 trabalham em incidentes de segurança. Eles podem criar e atualizar incidentes de segurança, solicitações e tarefas, bem como problemas, mudanças e

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuário final e objetivo	Função necessária	Benefícios
		indisponibilidades relacionadas aos seus incidentes.

Indicadores do Security Incident Management

O painel do Security Incident Management apresenta os seguintes indicadores-chave de desempenho:

Novos incidentes de segurança

Um gráfico do número de novos incidentes de segurança.

Incidentes de segurança em aberto

Um gráfico em que você pode comparar o número de incidentes de segurança em aberto, o número de incidentes de segurança em aberto não atualizados nos últimos 30 dias e o número de incidentes de segurança em aberto não atualizados nos últimos 5 dias.

Indicadores básicos de segurança

Os últimos 6 dias de pontuações do número de novos incidentes de segurança, o número de incidentes de segurança encerrados, o crescimento do backlog de incidentes de segurança e o número de indicadores de incidentes de segurança em aberto.

Novos incidentes de segurança por prioridade

O número de novos incidentes de segurança divididos por prioridade.

Detalhamentos

Os seguintes detalhamentos se aplicam aos indicadores no painel:

- Grupo de Segurança
- Idade do Incidente de segurança
- Categoria de Incidente de segurança
- Prioridade de Incidente de segurança
- Estado do Incidente de segurança

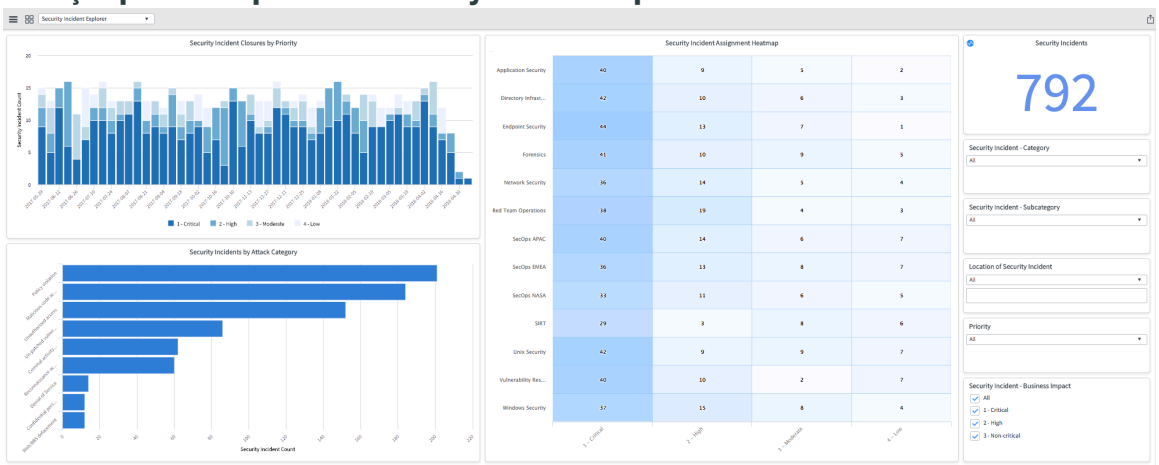
Painel do Security Incident Explorer

Com este painel, os gerentes de segurança podem exibir os incidentes de segurança resumidos e agrupados por categoria, subcategoria, local, prioridade e impacto nos negócios. Essas exibições permitem que os gerentes obtenham informações rapidamente sobre a frequência com que os ataques estão ocorrendo e quais serviços de negócios são afetados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição parcial do painel do Security Incident Explorer



Funções e usuário finais

Usuário final e objetivo	Função necessária	Benefícios
Security Response Manager: precisa de visibilidade clara do estado geral e do volume de incidentes de segurança associados a aplicações e serviços.	sn_si.manager	Pode revisar a postura geral de segurança com a capacidade de ajustar os membros dos grupos de atribuição.
Administrador do Security Response: precisa identificar áreas de interesse rapidamente e ter controle total sobre todos os dados do Security Incident Response ao administrar territórios e habilidades, conforme necessário.	sn_si.admin	Pode ajustar os parâmetros de cálculo de risco para garantir que os itens vulneráveis mais pertinentes à organização sejam tratados primeiro.
Analista do Security Response: é necessário priorizar rapidamente em quais vulnerabilidades se concentrar com base na criticidade para a organização.	sn_si.analyst	Os analistas de segurança de nível 1 e 2 trabalham em incidentes de segurança. Eles podem criar e atualizar incidentes de segurança, solicitações e tarefas, bem como problemas, mudanças e indisponibilidades relacionadas aos seus incidentes.

Indicadores do Security Incident Explorer

O painel do Security Incident Explorer apresenta os seguintes indicadores-chave de desempenho:

Incidentes de segurança

O volume total de incidentes de segurança abertos e pendentes.

Encerramentos de incidente de segurança por prioridade

O número de incidentes de segurança encerrados divididos por prioridade.

Incidentes de segurança por categoria de ataque

O número de incidentes de segurança em aberto dividido por categoria.

Mapa térmico de atribuição de incidente de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um detalhamento em dois níveis do número de incidentes de segurança em aberto por grupo de atribuição e prioridade.

Mapa térmico de incidente de segurança

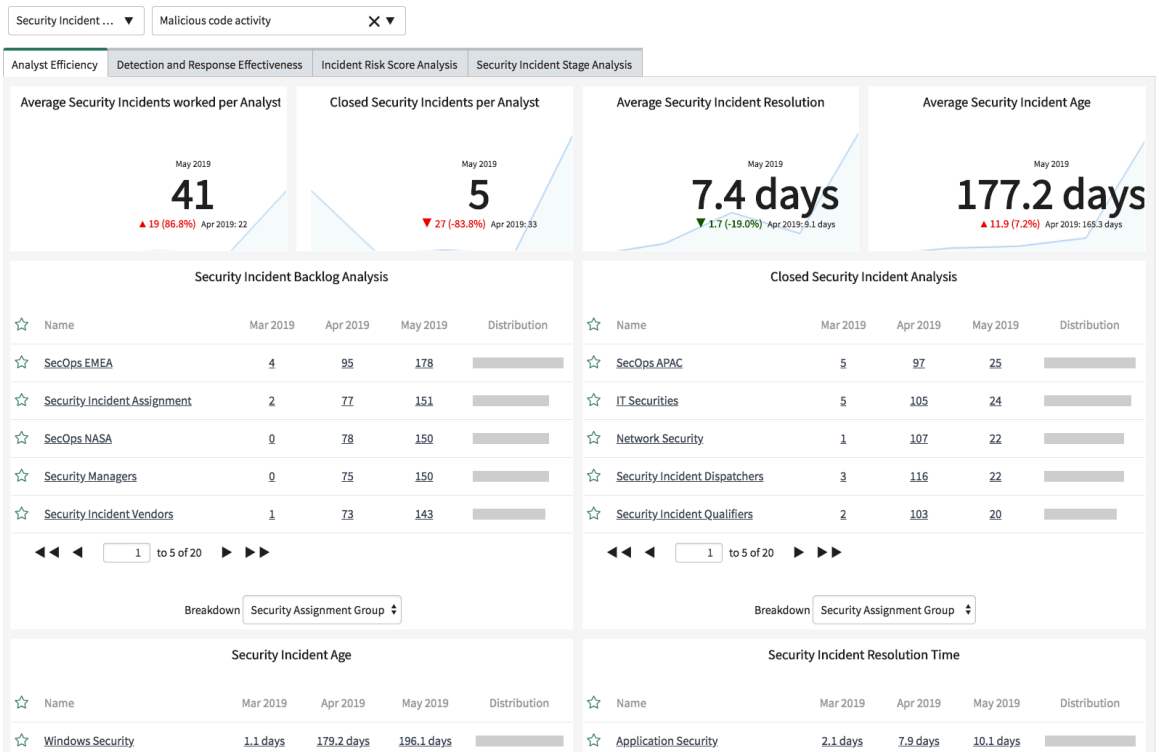
Um mapa global que mostra o número de incidentes de segurança em aberto em cada país.

Painel do Security Operations Efficiency

Os gerentes do centro de operações de segurança (SOC) podem exibir as métricas gerais de eficiência e medir o desempenho individual dos membros da equipe do SOC na organização.

O gerente do SOC pode usar o painel Performance Analytics para melhorar a eficiência e desenvolver uma imagem de como o SOC está se saindo em áreas gerais e específicas ao longo do tempo.

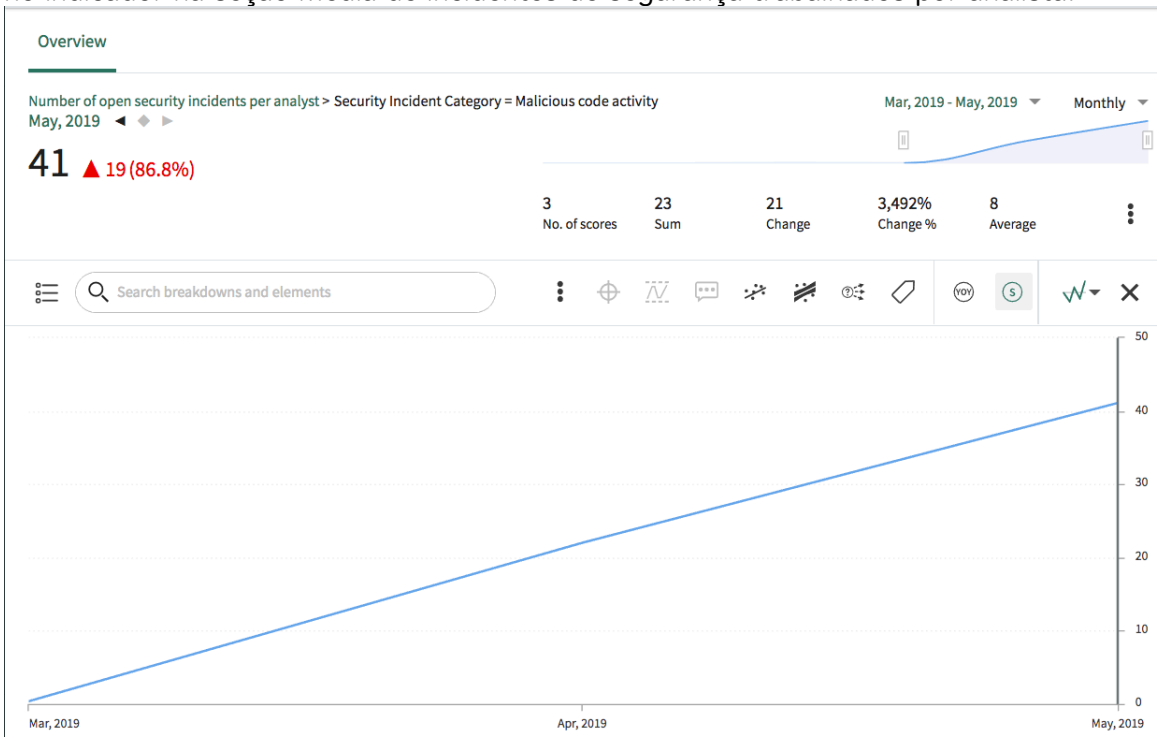
Guia Eficiência do analista



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Clique em qualquer um dos indicadores para obter mais detalhes. Por exemplo, clique no indicador na seção Média de incidentes de segurança trabalhados por analista.



O gráfico mostra que o número de incidentes de segurança em aberto aumentou de 0 em março para mais de 40 em maio. Observe os dados exibidos no cabeçalho:

- Indicador de tendência: mostra a mudança no número de incidentes em aberto no período mais recente para o qual os dados foram coletados. Este gráfico mostra dados para o período de março de 2019 a maio de 2019, e o número de incidentes em aberto aumentou em 19 no mês de maio. A eficiência do analista será melhor se o número de incidentes em aberto tiver diminuído ao longo de um período.
- Nº de pontuações: o período para o qual os dados foram coletados (março a maio de 2019).
- Soma: o número de novos incidentes em aberto para o período entre março e maio.
- Mudança: o número de novos incidentes em aberto entre março e abril.
- Média: o número médio de incidentes em aberto por analista para o período selecionado.

Guia Eficiência do analista

Indicador	Descrição
Média de incidentes de segurança trabalhados por analista	Número médio de incidentes de segurança em aberto por analista no período especificado. A fórmula usada é [[Número de incidentes de segurança em aberto / Por mês MÉDIA +]]/[[Número de agentes de segurança]]
Incidentes de segurança encerrados por analista	O número total de incidentes encerrados por cada analista na categoria selecionada no período especificado. A fórmula usada é [Número de incidentes de segurança encerrados > Categoria do incidente de segurança =<category_name> / Por SOMA de meses +]]/[[Número de agentes de segurança / Por MÉDIA de meses +]]
Média de resolução de incidente de segurança	O tempo médio gasto por cada analista para fechar incidentes de segurança no período especificado. A fórmula usada para mostrar o resultado em dias

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

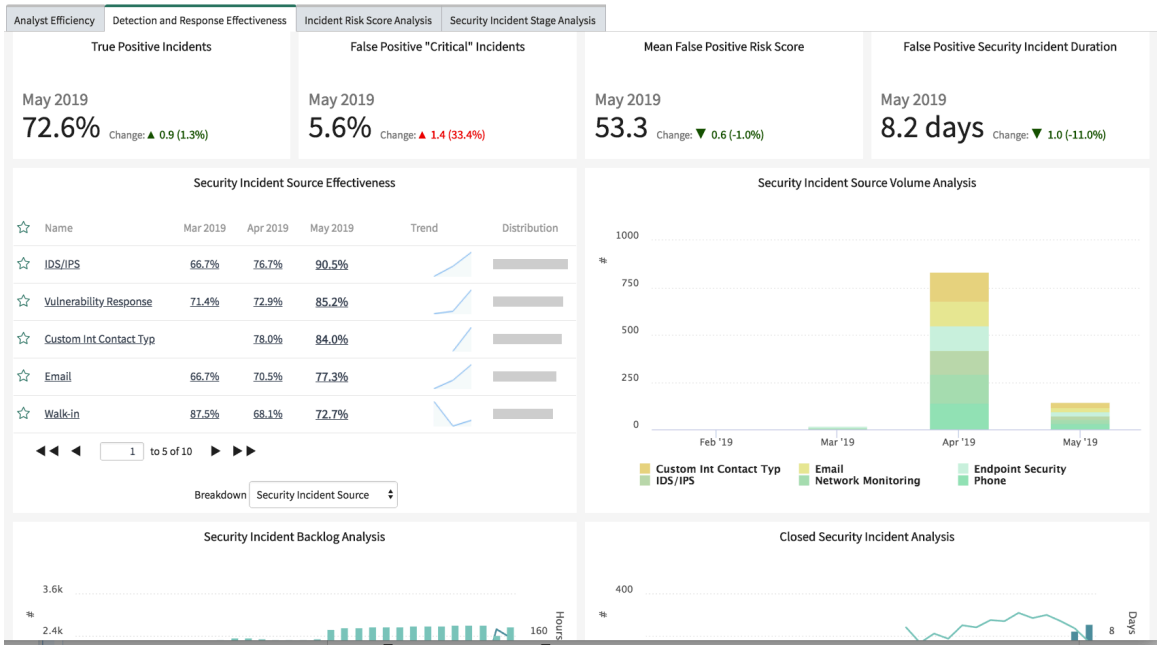
Guia Eficiência do analista

Indicador	Descrição
	é ([[Soma da duração dos incidentes de segurança encerrados > Categoria do incidente de segurança =<category_name> / MÉDIA por mês +]] / [[Número de incidentes de segurança encerrados > Categoria do incidente de segurança = / MÉDIA por mês +]]) / 24
Idade média do incidente de segurança	O número médio de dias pelos quais os incidentes de segurança permanecem abertos para cada analista. A fórmula usada para mostrar o resultado em dias é ([[Soma da idade dos incidentes de segurança em aberto > Categoria do incidente de segurança =<category_name> / Por mês MÉDIA +]]/ [[Número de incidentes de segurança em aberto > Categoria do incidente de segurança = / MÉDIA por mês +]]) / 24
Análise de backlog de incidentes de segurança	O número total de incidentes de segurança em aberto no período especificado. Selecione uma opção na lista Detalhamento para exibir o backlog de cada analista, grupo de segurança, prioridade e assim por diante. Você também pode comparar o número de incidentes de segurança em aberto entre dois meses selecionados.
Análise de incidente de segurança encerrado	O número total de incidentes de segurança encerrados no período especificado. Selecione uma opção na lista Detalhamento para exibir a contagem de cada analista, grupo de segurança, prioridade e assim por diante. Você também pode comparar o número de incidentes de segurança que foram encerrados entre dois meses selecionados.
Idade do incidente de segurança	O número médio de dias que os incidentes de segurança permanecem abertos no período especificado. Selecione uma opção na lista Detalhamento para exibir a idade do incidente de segurança para cada analista, grupo de segurança, prioridade e assim por diante. A fórmula usada para mostrar o resultado em dias é ([[Soma da idade dos incidentes de segurança em aberto > Categoria do incidente de segurança =<category_name> > Grupo de atribuição de segurança =<group_name> / Por mês MÉDIA +]]/ [[Número de incidentes de segurança em aberto > Categoria do incidente de segurança = > Grupo de atribuição de segurança = / MÉDIA por mês +]]) / 24
Tempo de resolução do incidente de segurança	O número médio de dias necessários para resolver incidentes de segurança durante o período especificado. Selecione uma opção na lista Detalhamento para exibir o tempo de resolução do incidente de segurança para cada analista, grupo de segurança, prioridade e assim por diante. A fórmula usada para mostrar o resultado em dias é ([[Duração somada dos incidentes de segurança encerrados > Categoria do incidente de segurança = Atividade de código mal-intencionado > Segurança atribuída a = John Asby / Por MÉDIA de meses +]] / [[Número de incidentes de segurança encerrados > Categoria do incidente de segurança = Atividade de código malicioso > Segurança atribuída a = John Asby / Por MÉDIA de meses +]]) / 24

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Eficácia da detecção e da resposta



Guia Eficácia da detecção e da resposta

Indicador	Descrição
Incidentes verdadeiro positivo	Percentual de incidentes de segurança considerados verdadeiros positivos na categoria selecionada para o período especificado. A fórmula usada é (1-([[Número de incidentes de segurança falso-positivos > Categoria do incidente de segurança = Atividade de código malicioso / Por mês SOMA +]] / [[Número de incidentes de segurança encerrados > Categoria de incidente de segurança = Atividade de código malicioso / Por mês SOMA +]])) * 100
Incidentes críticos falso-positivos	Percentual de incidentes de segurança críticos falso-positivos na categoria selecionada para o período especificado. A fórmula usada é ([[Número de incidentes de segurança falso-positivos > Pontuação de risco do incidente de segurança = Risco crítico > Categoria do incidente de segurança = Atividade de código mal-intencionado / Por SOMA de meses +]] / [[Número de incidentes de segurança encerrados > Categoria do incidente de segurança = Mal-intencionado atividade de código / por mês SOMA +]]) * 100

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Eficácia da detecção e da resposta

Indicador	Descrição
	Nota: Qualquer incidente de segurança em que o código Encerrado = Vulnerabilidade inválida ou Falso positivo é tratado como um incidente falso positivo
Pontuação média de risco falso-positivo	Pontuação de risco média mensal de incidentes de segurança encerrados que foram identificados como incidentes falso-positivos. Uma pontuação de risco mais baixa indica que os analistas de segurança gastaram menos tempo analisando incidentes falso-positivos. A fórmula usada é ([[Número de incidentes de segurança falso-positivos > Pontuação de risco do incidente de segurança = Risco crítico > Categoria do incidente de segurança = Atividade de código mal-intencionado / Por SOMA de meses +]] / [[Número de incidentes de segurança encerrados > Categoria do incidente de segurança = Mal-intencionado atividade de código / por mês SOMA +]]) * 100
Duração do incidente de segurança falso-positivo	Número médio de dias que os analistas de segurança gastaram na investigação de incidentes falso-positivos. A fórmula usada é ([[Duração somada de incidentes de segurança falso-positivos]] / [[Número de incidentes de segurança falso-positivos]]) / 24
Eficácia da origem do incidente de segurança	Percentual de incidentes de segurança considerados verdadeiros positivos identificados por uma origem específica para o período especificado. A origem pode ser e-mail, atividade de rede, suporte ao cliente e assim por diante. Esses dados ajudam a medir a eficácia da origem do incidente de segurança. A fórmula usada é (1-([[Número de incidentes de segurança falso-positivos > Categoria do incidente de segurança = Atividade de código mal-intencionado > Origem do incidente de segurança = IDS/IPS / Por SOMA de meses +]] / [[Número de incidentes de segurança encerrados > Incidente de segurança Categoria = Atividade de código malicioso > Origem do incidente de segurança = IDS/IPS / Por mês SOMA +]])) * 100
Análise de volume de origem de incidente de segurança	Número de incidentes de segurança encerrados no mês atual para cada origem de incidente de segurança. Você também pode comparar o número de incidentes de segurança para cada tipo de origem entre dois meses selecionados.

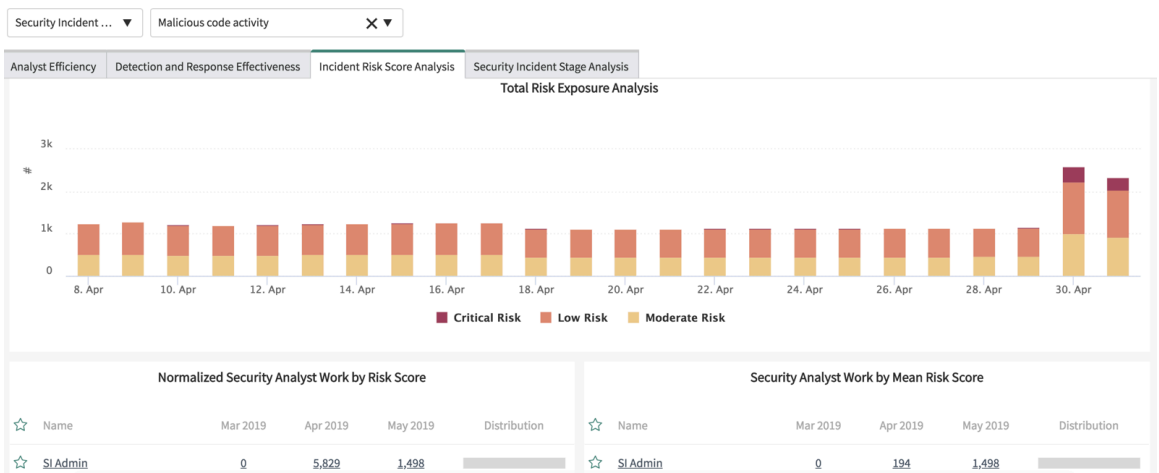
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Eficácia da detecção e da resposta

Indicador	Descrição
Análise de backlog de incidentes de segurança	O número total de incidentes de segurança em aberto no período especificado e o número médio de dias pelos quais os incidentes permanecem abertos. Você também pode comparar o número de incidentes de segurança em aberto entre dois meses selecionados. A fórmula usada para calcular o período médio do backlog é ([[Soma da idade dos incidentes de segurança em aberto > Categoria do incidente de segurança = Atividade de código mal-intencionado]]/[[Número de incidentes de segurança em aberto > Categoria do incidente de segurança = Atividade de código mal-intencionado]]) /24
Análise de incidente de segurança encerrado	O número total de incidentes de segurança encerrados no período especificado e o tempo médio de resolução desses incidentes. A fórmula usada para calcular o tempo médio de resolução é ([[Soma da duração dos incidentes de segurança encerrados > Categoria do incidente de segurança = Atividade de código malicioso]] / [[Número de incidentes de segurança encerrados > Categoria do incidente de segurança = Atividade de código malicioso]]) / 24

Guia Análise de pontuação de risco de incidente



Guia Análise de pontuação de risco de incidente

Indicador	Descrição
Análise de exposição de risco total	Número total de incidentes em aberto em cada categoria de risco (baixo, moderado e crítico) no período especificado. Você também pode comparar o número de incidentes nas diferentes categorias de risco entre dois meses.

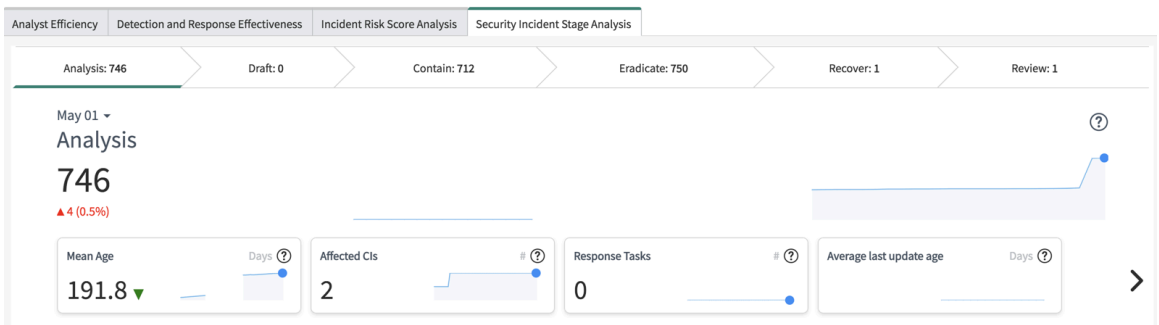
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Análise de pontuação de risco de incidente

Indicador	Descrição
Trabalho de analista de segurança normalizado por pontuação de risco	A pontuação de risco total de cada analista de segurança para o período especificado. Isso é calculado com base no número de incidentes de segurança positivos verdadeiros que o analista de segurança encerrou. A fórmula usada é [[Soma da pontuação de risco de incidentes de segurança encerrados > Categoria de incidente de segurança = Atividade de código mal-intencionado > Segurança atribuída a = Administrador de SI/por SOMA de meses +]] - [[Soma da pontuação de risco de incidentes de segurança falso-positivos> Categoria de incidente de segurança = Atividade de código malicioso > Segurança atribuída a = Administrador de SI / Por SOMA de meses +]]
Trabalho do analista de segurança por pontuação média de risco	A pontuação de risco médio de cada analista de segurança para o período especificado. A fórmula usada é [[Soma da pontuação de risco de incidentes de segurança encerrados > Categoria de incidente de segurança = Atividade de código mal-intencionado > Segurança atribuída a = Administrador de SI / Por mês MÉDIA +]] - [[Soma da pontuação de risco de incidentes de segurança falso-positivos> Categoria de incidente de segurança = Atividade de código malicioso > Segurança atribuída a = Administrador de SI / Por MÉDIA de meses +]]

Guia Análise da fase do incidente de segurança



Você pode ver o número de incidentes abertos em um dia específico e o status (análise, rascunho, contenção, erradicação, recuperação ou revisão) desses incidentes. Em cada fase, você pode exibir a idade média, os ICs afetados, as tarefas de resposta e assim por diante. Clique em um link para exibir detalhes adicionais ou o detalhamento desses incidentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Espaço de resposta a incidentes de segurança

O ServiceNow® Espaço de resposta a incidentes de segurança é uma interface recriada que fornece uma experiência de usuário de última geração para os analistas de segurança e gerentes de SOC. Usando isso, os analistas de segurança podem gerenciar o ciclo de vida dos incidentes de segurança, desde uma análise inicial até a contenção, erradicação e recuperação.

Para começar com SIR Workspace

Selecione um bloco para começar.

Explorar espaço Conheça os conceitos e recursos do espaço de SIR	**Administradores usando o espaço** Configurar espaço e recursos de SIR
Analistas usando o espaço Saiba como os analistas usam o espaço de SIR	**Exibir Painéis de SIR** Exibir painéis do espaço de SIR

Solicitar apps na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Instalar Espaço de resposta a incidentes de segurança (sn_si_aw) instalará automaticamente todas as aplicações dependentes de ServiceNow Store. Mais detalhes sobre as aplicações dependentes são informados na seção SIR Workspace plug-ins e funções.

Mais recursos

Visite o Security Incident Response fórum no ServiceNow Community.

Explorar o SIR Workspace

Explore Espaço de resposta a incidentes de segurança para entender como os analistas e gerentes de segurança executam suas operações diárias com uma experiência do usuário aprimorada, fazem uma investigação de incidente completa e obtêm uma visão geral dos incidentes de segurança, tarefas de resposta e ANS atribuídos ao analista de segurança e equipe.

Esta seção descreve o seguinte:

- SIR Workspace plug-ins e funções necessárias.
- Recursos da chave SIR Workspace.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

SIR Workspace plug-ins e funções

A seguir estão as aplicações necessárias para trabalhar com o plug-in Espaço de resposta a incidentes de segurança (sn_si_aw).

Candidaturas

- Enterprise Security Case Management PAD Commons [sn_escm_pad_cmn]
- Espaço comum do Security Operations [sn_escm_ws_cmn]
- Componente do cartão de IU de incidente de segurança [sn_sirw_evam]
- Spoke do Security Operations [sn_sec_spoke]
- Security Incident Response [sn_si]

O Enterprise Security Case Management PAD Commons requer o plug-in Playbook Experience [playbook_experience].

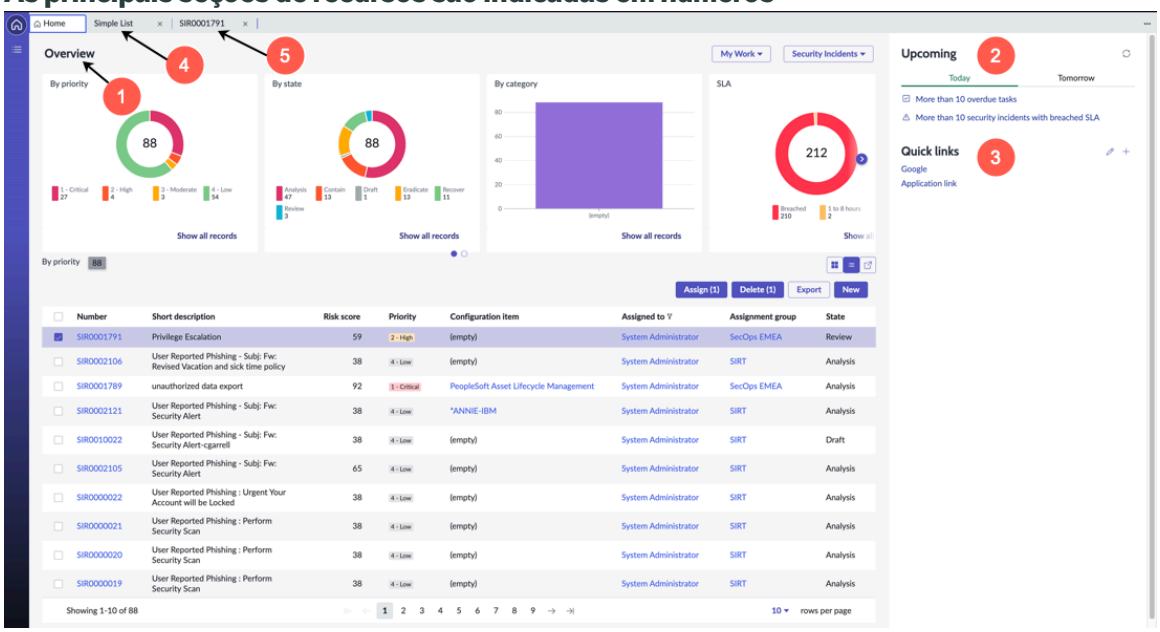
Para obter informações sobre Security Incident Response funções, tabelas, propriedades e trabalhos programados, consulte Componentes instalados com Security Incident Response

Recursos do espaço de SIR

O Espaço de resposta a incidentes de segurança consiste nos seguintes recursos principais.

1. Seção Visão geral
2. Seção A seguir
3. Links Rápidos
4. Exibição em lista
5. Interface de várias guias que oferece suporte à abertura de vários incidentes de incidente de segurança

As principais seções de recursos são indicadas em números



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

SIR Workspace visão geral da interface

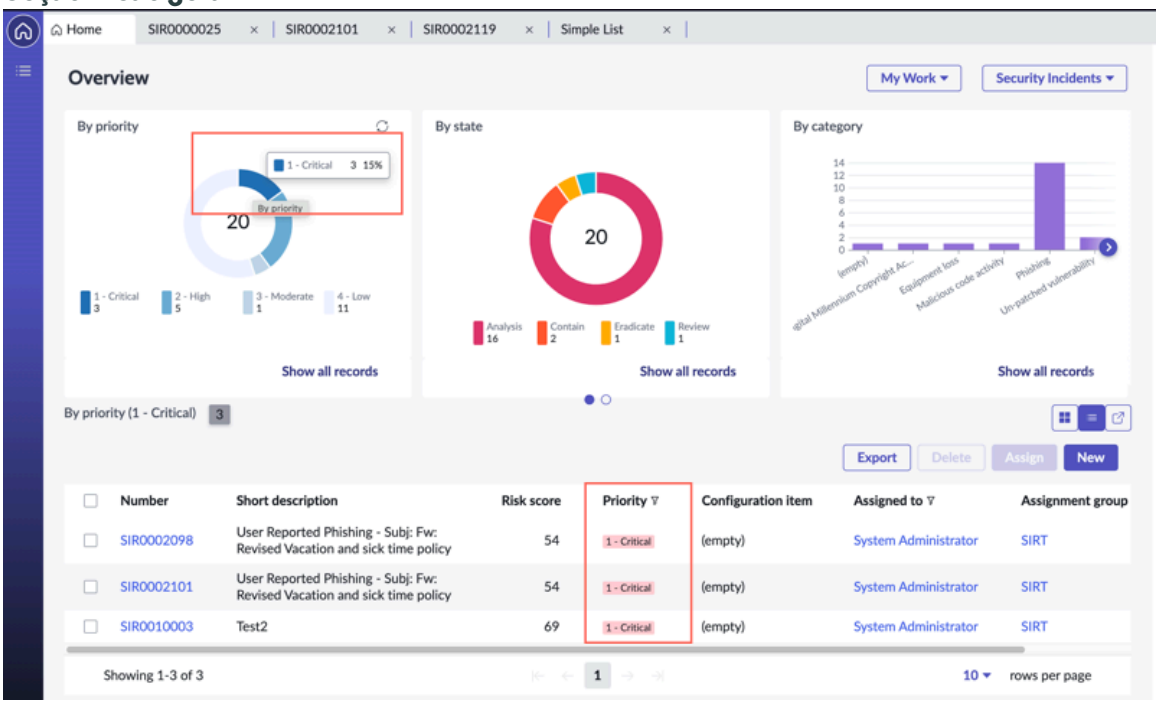
A página SIR Workspace Visão geral consiste nos detalhes dos incidentes de segurança e das tarefas de resposta que estão sob os analistas de segurança e sua equipe.

Existem vários widgets presentes em cada filtro agrupado por prioridade, categoria, estado e ANS, que estão nas filas dos analistas de segurança e na fila da equipe de analistas de segurança.

Quando os filtros são aplicados aos widgets, a metade inferior da página de visão geral é preenchida com os incidentes de segurança correspondentes ou tarefas de resposta apresentados como cartões ou itens de lista. O analista pode alternar entre a exibição de cartão ou a exibição de lista, conforme desejado.

Por exemplo, no widget **Prioridade**, se você quiser selecionar todos os incidentes críticos ou tarefas de resposta, clique no segmento **Crítico** (exemplo de captura de tela abaixo) do widget e os incidentes ou tarefas de resposta que são críticos serão exibidos na lista ou no cartão exibição.

Seção Visão geral

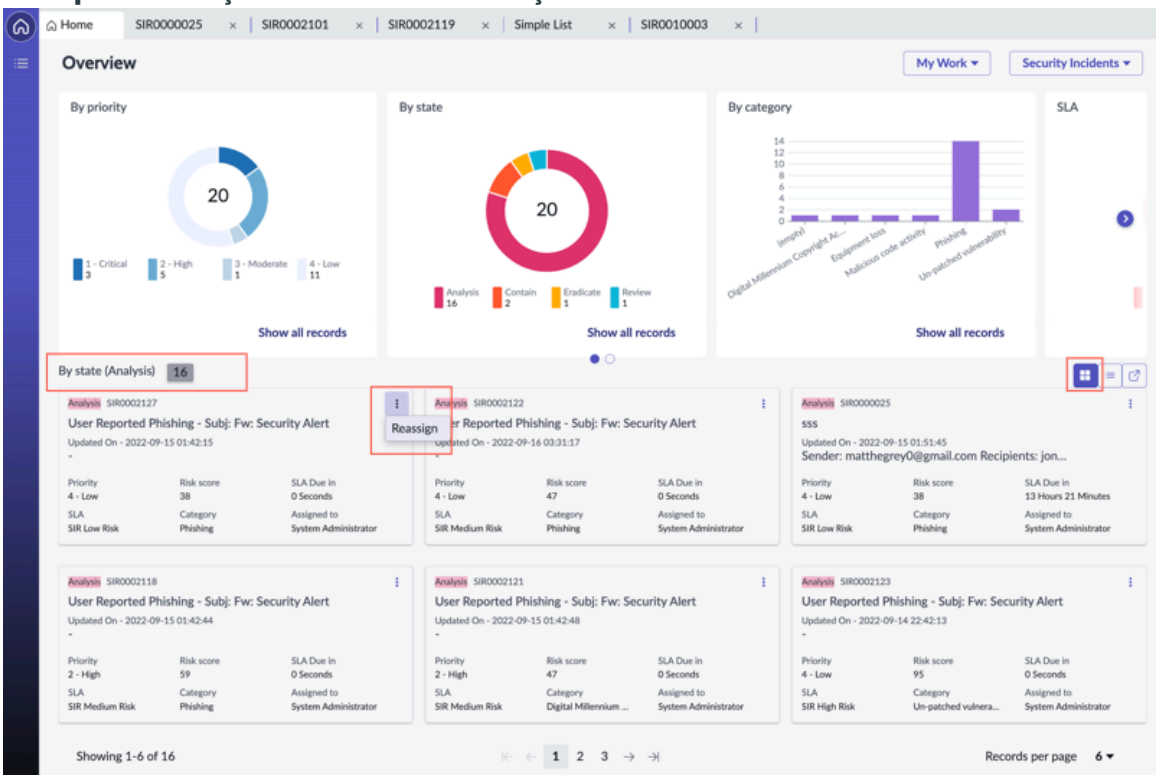


Você pode atribuir ou reatribuir os incidentes de segurança ou tarefas de resposta diretamente desta exibição, clicando no ícone de elipse e selecionando **Atribuir** (opção na exibição de cartão) ou diretamente o botão **Atribuir** (opção na exibição de lista) de acordo para atribuir um incidente.

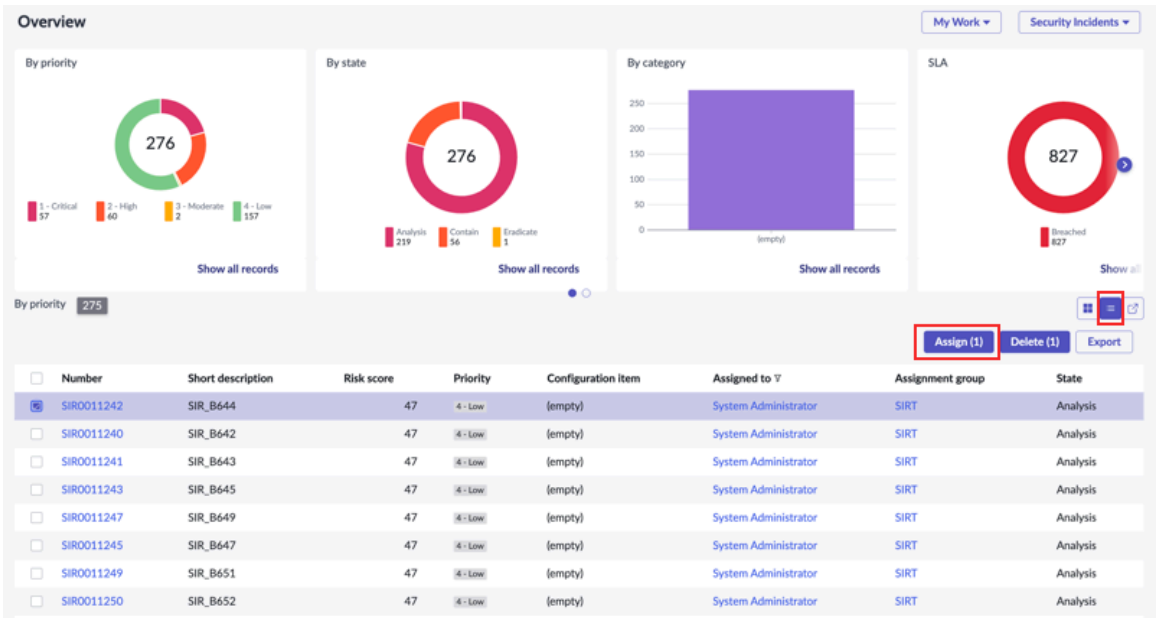
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de exibição de cartão e reatribuição



Atribuir incidente

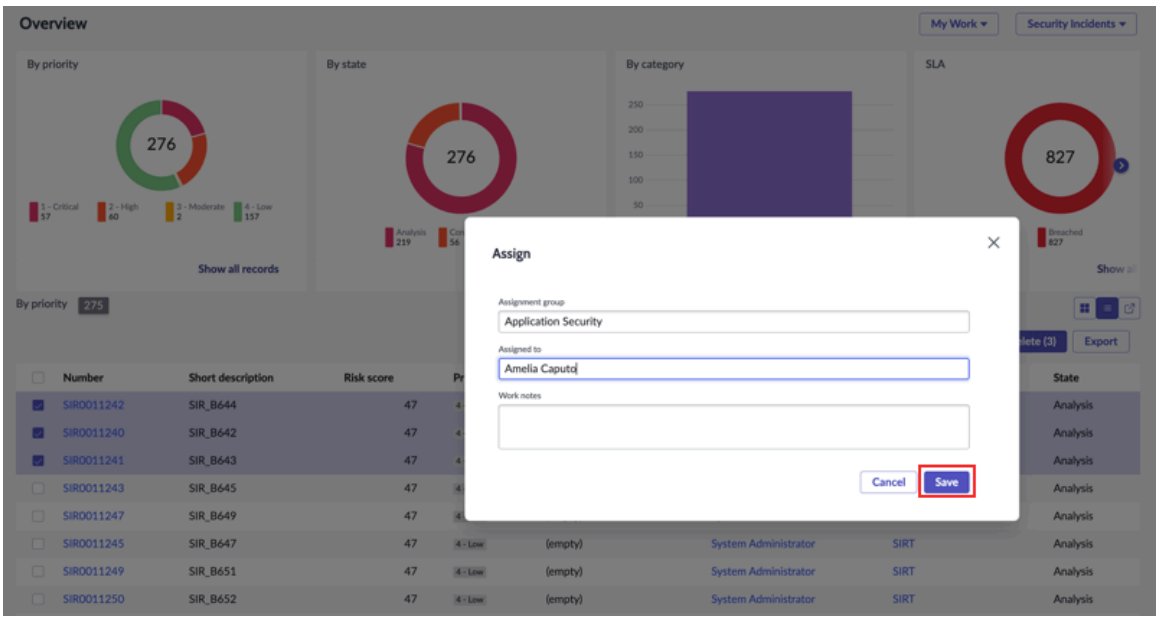


Aqui está um exemplo da exibição de lista. O usuário também pode atribuir incidentes na exibição de lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribuir incidente



Adicione ou modifique os detalhes do designado, como Grupo de atribuição e Atribuído a, adicione anotações de trabalho, se necessário.

Nota:
Você pode atribuir um ou mais incidentes de segurança ou tarefas de resposta aos grupos de atribuição. O número selecionado é exibido no botão **Atribuir**.

O usuário pode excluir incidentes de segurança desta exibição. Clique no botão **Excluir** para excluir o incidente de segurança. O registro será excluído da exibição de lista.

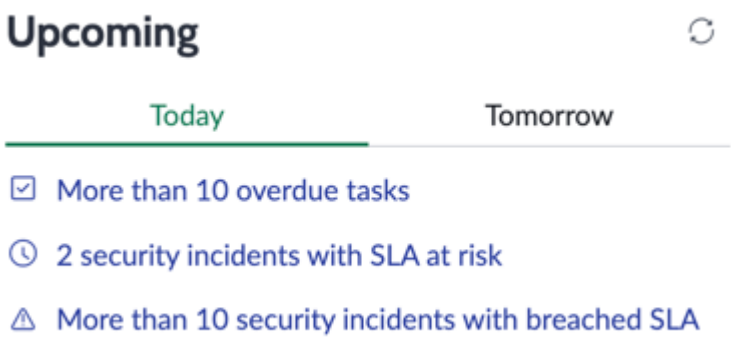
O usuário também pode exportar o conteúdo da lista. Clique no botão **Exportar** para exportar a lista no formato desejado.

Seção A seguir

Esta seção exibe as próximas tarefas, como os incidentes de segurança e as tarefas de resposta que vencem no mesmo dia e no dia seguinte.

A lista de incidentes de segurança e tarefas de resposta exibida é baseada no campo de data de vencimento e na definição do ANS definida para esses registros.

Se esta seção contiver mais de um incidente de segurança ou tarefa de resposta, o incidente ou os registros abrirão todos esses registros em uma nova guia.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

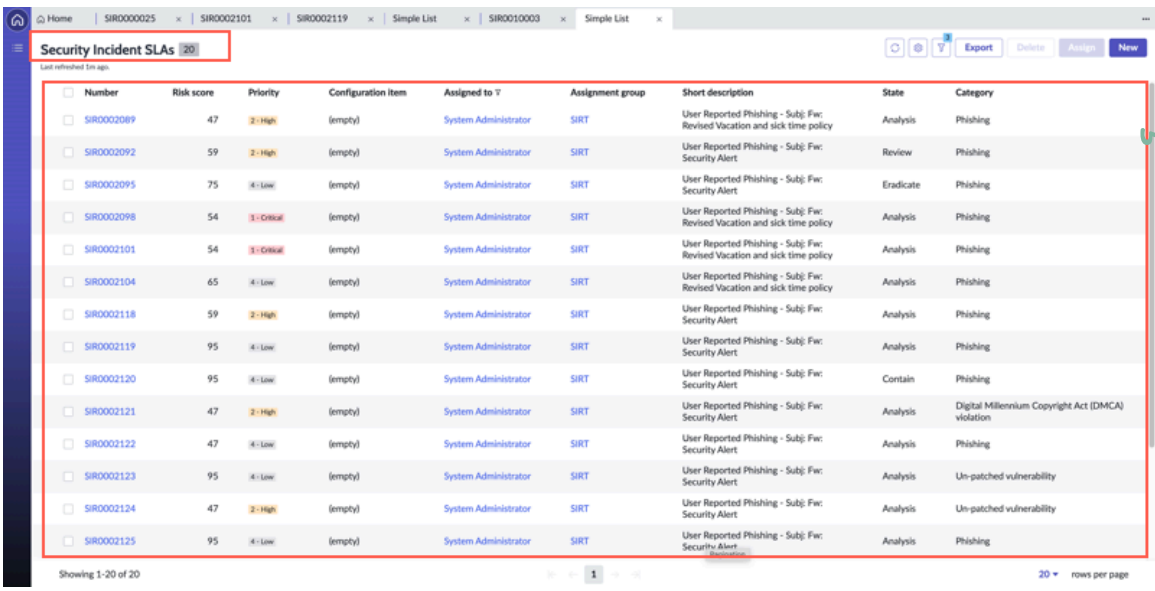
Exibir tarefas futuras

O analista de segurança pode exibir as próximas tarefas relacionadas aos incidentes de segurança e às tarefas de resposta que estão vencidas, atrasadas ou violaram o ANS definido.

Antes de Iniciar
Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Futuros**.
2. Clique na guia **Hoje** para exibir as tarefas que vencem no mesmo dia.
3. Selecione a guia **Amanhã** para exibir as tarefas que estão atrasadas para o dia seguinte.
   A próxima seção lista os incidentes de segurança ou tarefas de resposta que estão atrasados com base na data de vencimento e que violaram a definição do ANS.
4. Clique no ícone **Atualizar** para atualizar a lista da próxima seção.
   Por exemplo, se você clicar no link **Mais de 10 incidentes de segurança com ANS violado**, a lista de incidentes de ANS violados será exibida em uma nova guia no espaço.



Nota:
Você pode executar as operações Novo, Atribuir, Exportar e Excluir em qualquer exibição de lista.

Seção de links rápidos

Links rápidos funcionam como links de marcador. Você pode adicionar URLs externos e acessá-los rapidamente de dentro do espaço.

Como trabalhar com links rápidos

Adicione links rápidos para facilitar a referência.

Antes de Iniciar
Função necessária: sn_si.analyst

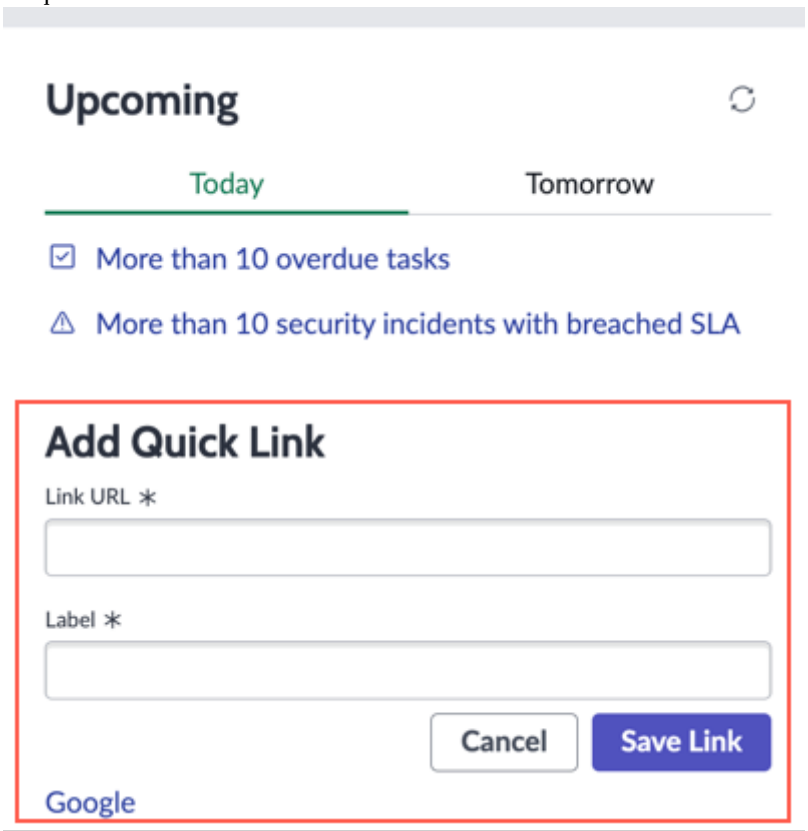
Por Que e Quando Desempenhar Esta Tarefa
Você pode adicionar e modificar links rápidos úteis e marcá-los como favoritos para ajudar na resolução do incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Links rápidos**.
2. Clique no ícone **Adicionar link rápido** para adicionar os links.
3. Insira o link para a URL e o rótulo.
4. Clique **em Salvar link**.



O novo link é adicionado abaixo da seção de links rápidos.

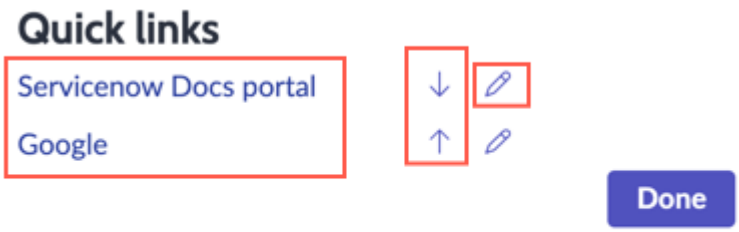
5. **Para modificar ou excluir os links:**

   a. Clique no ícone **Editar link**.

   b. Modifique o link desejado ou exiba o texto que é o rótulo do URL.

   c. Clique em **Salvar**.

   d. Clique em **Concluído**.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e. Use as setas para cima e para baixo para mover a posição dos links.

f. Clique em **Excluir** para excluir os links marcados durante a edição.

Exibição de lista no SIR Workspace

A exibição de lista consiste em incidentes de segurança, tarefas de resposta, e-mails de phishing e avaliações.

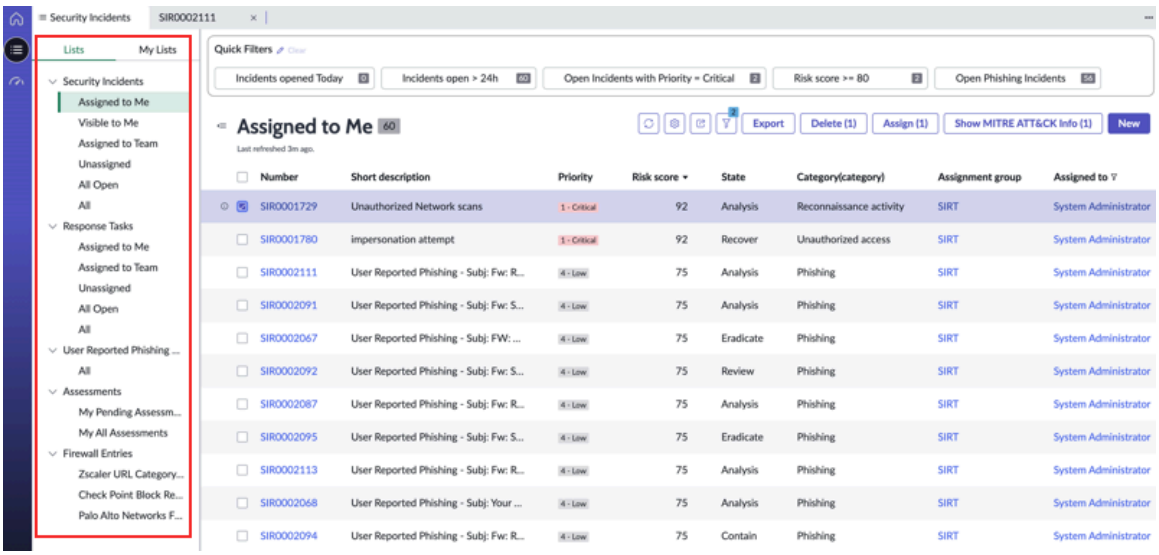
A exibição de lista tem filtros pré-aplicados, como Atribuído a Mim, Atribuído à Equipe, Não Atribuído, Todos em Aberto, Todos e assim por diante.

Usando essas categorias de lista e listas filtradas, os analistas podem encontrar rapidamente os incidentes de segurança e os registros de tarefas de resposta nos quais precisam trabalhar.

Para acessar a exibição de lista, clique no ícone de lista (de lista). Quando você clica em um registro em uma exibição de lista, o registro é aberto em uma nova guia.

Tipos de listas

Veja a seguir um exemplo de exibição das listas.



O painel de lista contém as seguintes seções:

Listas

Item de lista	Descrição	Capacidade
Incidentes de segurança	Exiba a lista de incidentes de segurança e navegue até o incidente desejado para começar a trabalhar. As seguintes listas estão disponíveis: • **Visível para mim**: incidentes de segurança que são visíveis para o usuário conectado.	• Na exibição de lista, o analista pode configurar a lista de colunas clicando no ícone de engrenagem que está disponível acima das colunas de incidentes. • O analista pode selecionar um ou mais incidentes de segurança e atribuir

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Capacidade
	• **Atribuído a mim**: incidentes de segurança que são atribuídos ao analista. • **Atribuído à equipe**: incidentes de segurança que são atribuídos a todas as equipes às quais os analistas pertencem. • **Não atribuídos**: lista de incidentes de segurança não atribuídos. • **Todos em aberto**: lista de todos os incidentes de segurança em aberto. • **Todos**: lista de todos os incidentes de segurança.	esses incidentes a outros usuários. • O analista pode excluir os incidentes de segurança. • O analista pode criar um novo incidente de segurança. • O analista pode aplicar os filtros rápidos. Aplique os filtros clicando na opção **Filtros rápidos** em vez de usar a opção de **filtro** avançada. Usando os filtros rápidos, você pode filtrar rapidamente a lista de incidentes de segurança que precisam de atenção imediata. Para obter mais informações, consulte Como trabalhar com filtros rápidos. • Os analistas podem atualizar a lista de incidentes. • O analista pode exportar a exibição de lista para os formatos Excel, CSV, JSON e PDF.
Tarefas de resposta	Exiba a lista de tarefas de resposta e navegue até a tarefa de resposta desejada para começar a trabalhar. A exibição de lista contém: • **Atribuído a mim**: tarefas de resposta que são atribuídas ao analista. • **Atribuído à equipe**: tarefas de resposta que são atribuídas às equipes às quais os analistas pertencem. • **Não atribuídas**: lista de tarefas de resposta não atribuídas.	• Na exibição de lista, o analista pode configurar a lista de colunas clicando no ícone de engrenagem que está disponível acima das colunas de incidentes. • O analista pode selecionar uma ou mais tarefas de resposta e atribuir essas tarefas a outros usuários. • O analista pode criar uma nova tarefa de resposta. • O analista pode aplicar os filtros rápidos. Aplique os filtros clicando na opção **Filtros rápidos** em vez de usar a opção de **filtro** avançada. Usando os

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas

Item de lista	Descrição	Capacidade
	• **Todas em aberto**: lista de todas as tarefas de resposta em aberto. • **Todos**: lista de todas as tarefas de resposta.	filtros rápidos, você pode filtrar rapidamente a lista de tarefas de resposta que precisam de atenção imediata. • Os analistas podem atualizar a lista de tarefas de resposta. • O analista pode exportar a exibição de lista para os formatos Excel, CSV, JSON e PDF. Para obter mais informações, consulte Exportar incidentes de segurança ou tarefas de resposta.
E-mails de Phishing	Exibir a lista de todos os e-mails de phishing. A exibição de lista será classificada com base na última atualização.	• Denunciar e-mail de phishing. Para obter mais informações, consulte Relatar E-mail de Phishing sobre como relatar um e-mail de phishing. • Excluir e-mails de phishing. • Exporte a exibição da lista de e-mails de phishing para os formatos Excel, CSV, JSON e PDF.
Avaliações	Exiba a lista de avaliações necessárias para executar a revisão pós-incidente. • **Minhas avaliações pendentes**: lista de avaliações pendentes. • **Todas as minhas avaliações**: lista de todas as avaliações.	Fazer avaliações.

Personalizar uma lista

Os analistas ou gerentes de segurança podem personalizar os incidentes de segurança ou as tarefas de resposta ou a exibição de lista personalizada de e-mails de phishing com base em suas preferências individuais.

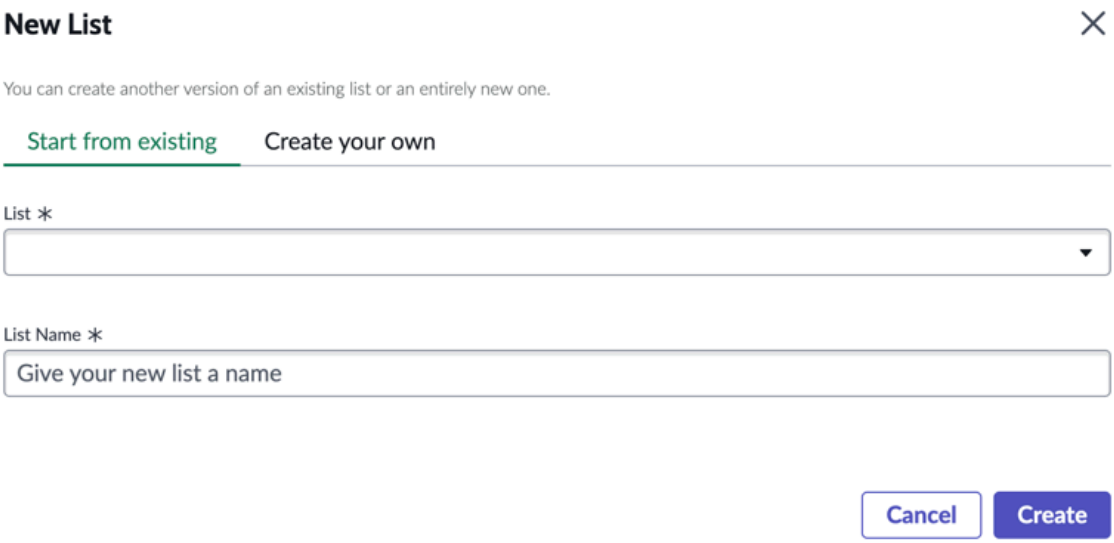
Antes de Iniciar
Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique **em Exibição de lista**.
3. Clicar **Minhas listas**.
4. Clique em **Adicionar nova lista**, disponível na parte inferior da exibição **Minhas listas**.



Os analistas de segurança podem criar outra versão de uma lista existente ou uma lista personalizada totalmente nova.

5. **Para criar a partir de uma exibição de lista existente:**

   a. Clique em **Iniciar a partir do link existente**.

   b. Selecione a **Lista** na lista suspensa.

   Nota:
   Qualquer que seja a lista selecionada na lista suspensa, o nome da lista será a cópia da sua lista principal. Por exemplo, se você selecionar **Atribuído a mim** na seção de incidentes de segurança, o nome da lista será **Atribuído a mim Cópia** da seção de incidentes de segurança.

   c. Selecione as colunas a serem personalizadas e adicione filtros.
   Crie um filtro adicionando condições que contenham um campo, operador e valor(es).

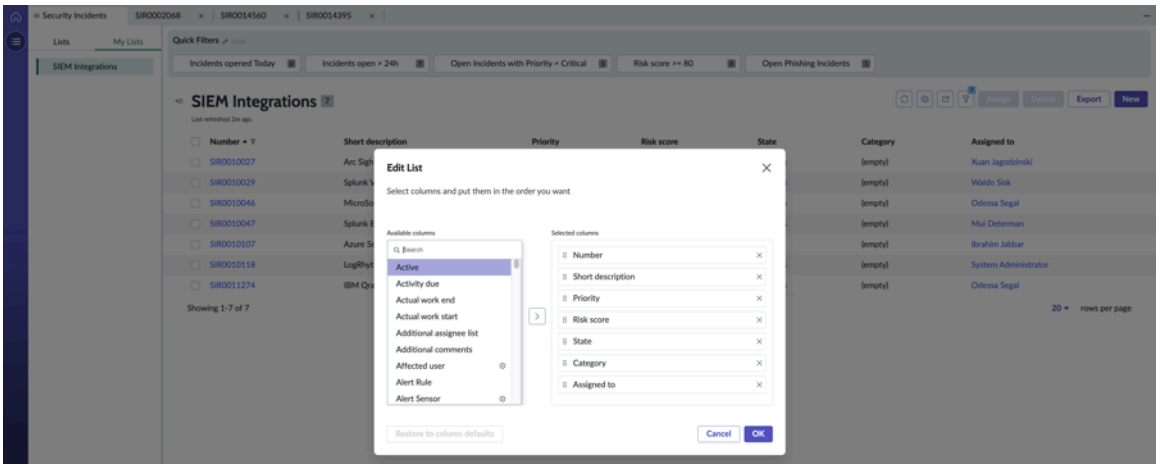
   d. Clique em **Criar**.

   Nota:
   Para personalizar sua própria exibição de lista, você pode adicionar colunas personalizadas, filtros, definir condições e classificar pela ordem conforme necessário.

   e. Depois que uma exibição de lista personalizada for criada, clique no ícone de engrenagem e personalize as colunas da lista escolhendo a opção **Editar colunas** para editar as colunas e colocá-las na ordem que você preferir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você também pode:

- **Renomeie** a exibição de lista personalizada.
- **Exclua** a exibição de lista personalizada.
- Salve a exibição de lista personalizada conforme desejado usando a opção **Salvar como**.
- **Redefina a largura** da exibição de lista.

Nota:
Você também pode executar diretamente essas operações usando os outros botões de ações da lista, como atribuir, excluir e exportar a exibição de lista que são fornecidos.

6. Para criar sua própria lista:

a. Clique em **Criar seu próprio** link.

b. Forneça um **Nome de lista**.

c. Selecione **Origem** e **Colunas**.

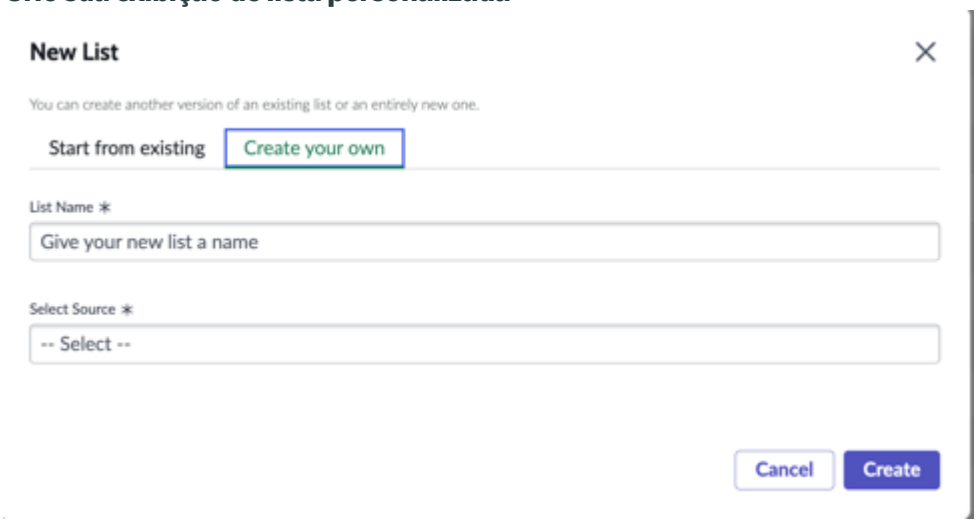
d. Adicionar filtros.
Crie um filtro adicionando condições e fornecendo a ordem na qual a lista deve ser exibida.

e. Clique em **Criar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Crie sua exibição de lista personalizada



Uma nova lista será criada conforme definido e personalizada por você na seção **Minhas listas**.

Nota:
você pode **Reordenar** sua exibição personalizada movendo suas posições.

Atribuir incidentes de segurança

Atribua incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

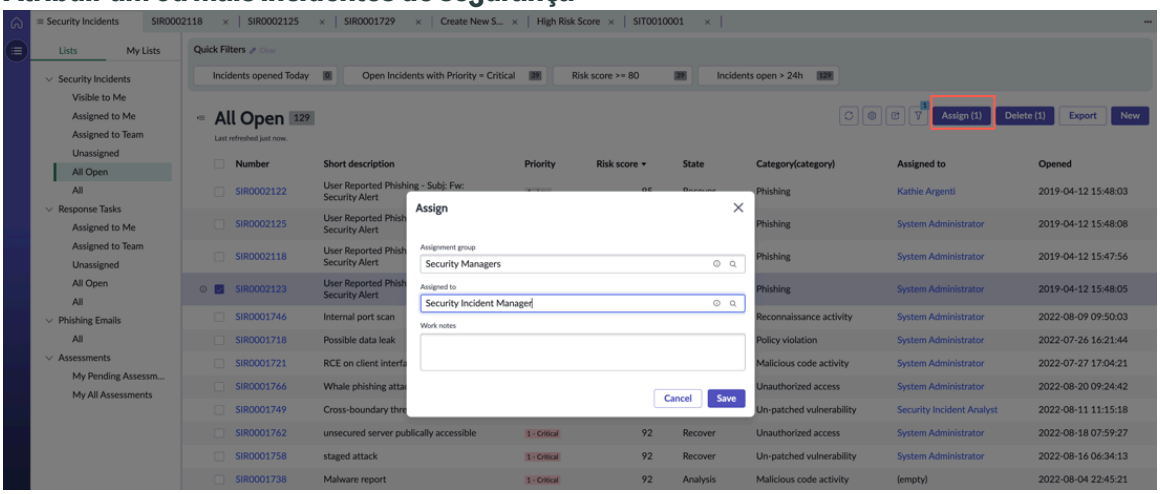
1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique no ícone de de lista).
3. Clique **em Listas**.
4. Por exemplo, vá para **Incidentes de segurança** > **Todos em aberto**.
5. Selecione um ou mais incidentes de segurança.
6. Clique **em Atribuir**.
7. Preencha os detalhes, como Grupo de atribuição, Atribuído a, e adicione Anotações de trabalho, se necessário.
   O incidente será atribuído ao usuário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Clique em **Salvar**.

Atribuir um ou mais incidentes de segurança



Atribuir tarefas de resposta

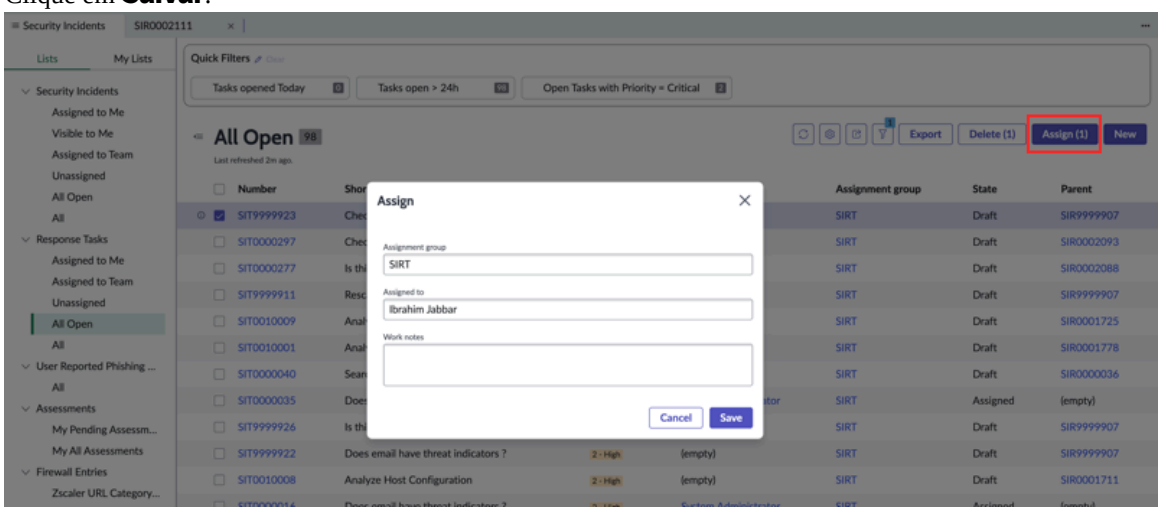
Atribua tarefas de resposta para um problema de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique no ícone de de lista).
3. Clique **em Listas**.
   Por exemplo, vá para **Tarefas de resposta** > **Todos em aberto**.
4. Selecione uma ou mais tarefas de resposta.
5. Clique **em Atribuir**.
6. Preencha os detalhes, como Grupo de atribuição, Atribuído a, e adicione Anotações de trabalho, se necessário.
   O incidente será atribuído ao usuário.
7. Clique em **Salvar**.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatar E-mail de Phishing

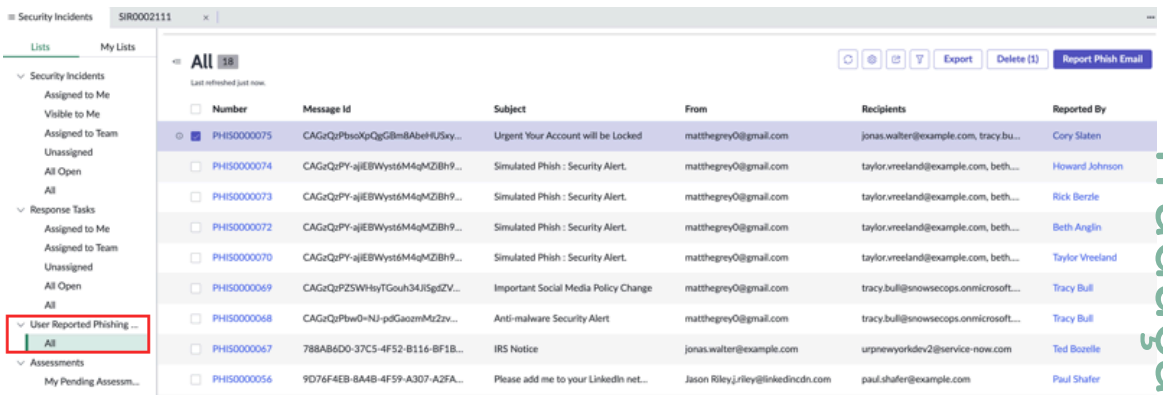
Relate e-mails de phishing na exibição de listas.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique no ícone de de lista).
3. Ir para **E-mails de phishing relatados por usuário** > **Todos**.
   A lista de e-mails de phishing relatados pelo usuário é exibida.



4. Clique no botão **Relatar e-mail de phishing**.
   Relate um e-mail de phishing carregando-o.
5. Clique em **Adicionar arquivo** para adicionar anexos.
6. Clique em **Carregar**.

> **Nota:**
> Relate um e-mail de phishing carregando os anexos. Você pode carregar apenas um e-mail de phishing de cada vez e deve estar no formato .eml.

7. Clique em **Enviar**.
   O e-mail de phishing para registrar um incidente de segurança é criado.

Como trabalhar com filtros rápidos

Filtros rápidos são filtros de fácil acesso que estão disponíveis em, incidentes de segurança e listas de tarefas de resposta.

Antes de Iniciar

Função necessária: sn_si.admin

O SIR Workspace fornece o recurso de filtros rápidos que permite filtrar a lista de incidentes de segurança ou tarefas de resposta com facilidade.

Você pode usar filtros rápidos para configurar novos filtros ou modificar os filtros existentes que aparecem nessas listas. O sistema básico fornece os seguintes filtros rápidos para cada incidente de segurança:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Incidentes abertos hoje**
- **Incidentes em aberto > 24 horas**
- **Incidentes em aberto com Prioridade= Crítica**
- **Risco >= 80**
- **Incidentes de phishing em aberto**

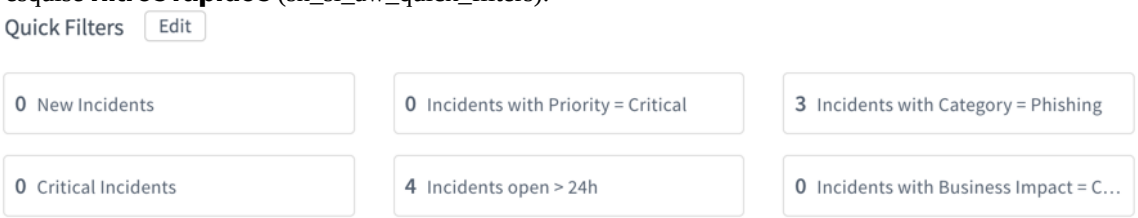
O sistema de base fornece os seguintes filtros rápidos para cada tarefa de resposta:

- **Tarefas em aberto > 24h**
- **Tarefas em Aberto com Prioridade = Crítica**

Nota:
Um administrador pode configurar a lista necessária de filtros rápidos de acordo com a necessidade da organização.

Procedimento

1. Navegar até **Definição do Sistema** > **Tabelas**.
2. Pesquise **filtros rápidos** (sn_si_aw_quick_filters).



3. Ir para **Links relacionados** > **Mostrar lista** seção.
   A página da lista **Filtros rápidos** é exibida. OOTB. A seguir está a lista de filtros rápidos enviados com a aplicação.

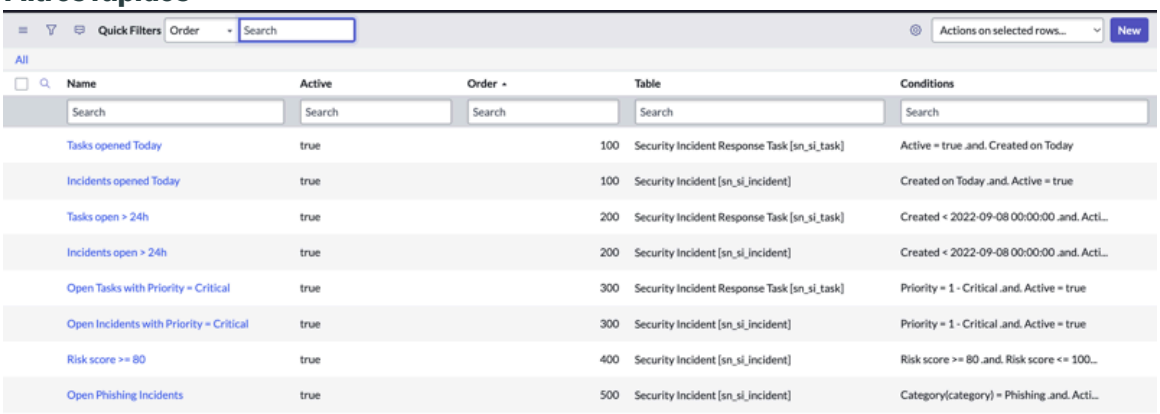
Nome	Tabela	Valor
Tarefas abertas hoje	Tarefa de incidente de segurança [sn_si_task]	Verdadeiro
Incidentes abertos hoje	Incidente de segurança [sn_si_incident]	Verdadeiro
Tarefas em aberto > 24h	Tarefa do Security Incident Response [sn_si_task]	Verdadeiro
Incidentes em aberto > 24h	Incidente de segurança [sn_si_incident]	Verdadeiro
Tarefas em Aberto com Prioridade = Crítica	Tarefa do Security Incident Response [sn_si_incident]	Verdadeiro
Incidentes em Aberto com Prioridade = Crítica	Incidente de segurança [sn_si_incident]	Verdadeiro
Pontuação de risco >= 80	Incidente de segurança [sn_si_incident]	Verdadeiro
Incidentes de phishing em aberto	Incidente de segurança [sn_si_incident]	Verdadeiro

Tradução automática

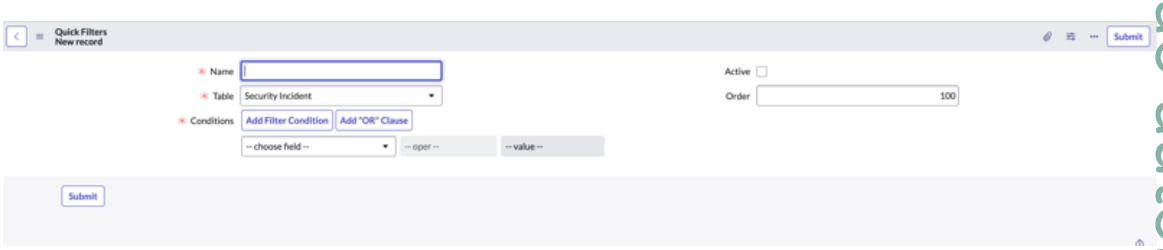
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
O administrador de segurança pode prosseguir e configurar esses filtros rápidos. De acordo com a necessidade do negócio, o administrador pode modificar o valor existente para falso e criar um novo filtro rápido.

Filtros rápidos



4. Clique em **Novo** para criar um novo filtro.
5. Insira um nome para o filtro, selecione a Tabela e especifique a condição do filtro.
6. Clique em **Enviar** para retornar à página da lista anterior.
   Você verá o filtro recém-adicionado listado na página.



Nota:

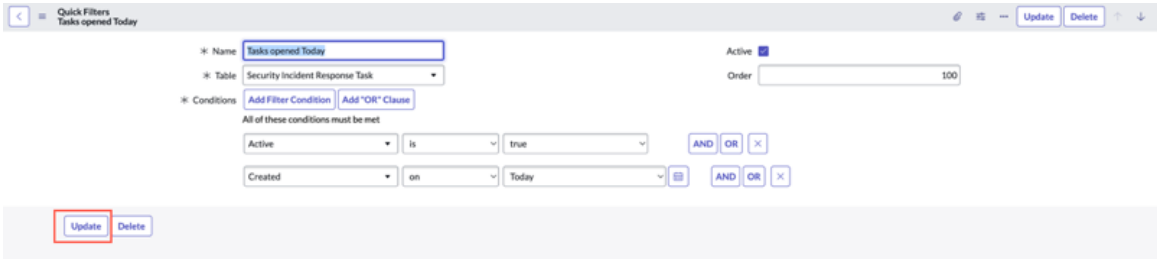
- O filtro rápido será aplicável somente se a caixa de seleção **Ativo** estiver marcada.
- No espaço, qualquer usuário conectado pode personalizar os filtros rápidos ativos que estão disponíveis na aplicação. Os usuários podem ocultar ou exibir os filtros rápidos recém-criados. Este recurso é baseado na preferência do usuário.
- Se um usuário tiver modificado as preferências de filtros rápidos e um novo filtro rápido for criado depois disso, se o filtro rápido estiver definido como ativo, ele não se aplicará à preferência do usuário. O usuário precisa alterar manualmente as preferências na exibição personalizada.

7. Selecione qualquer registro de filtro existente para modificar os filtros rápidos existentes.
8. Modifique o nome e a condição do filtro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Clique em **Atualizar**.



Adicionar ou modificar filtros rápidos

Adicione ou modifique filtros rápidos para incidentes de segurança ou tarefas de resposta na exibição de lista.

Antes de Iniciar

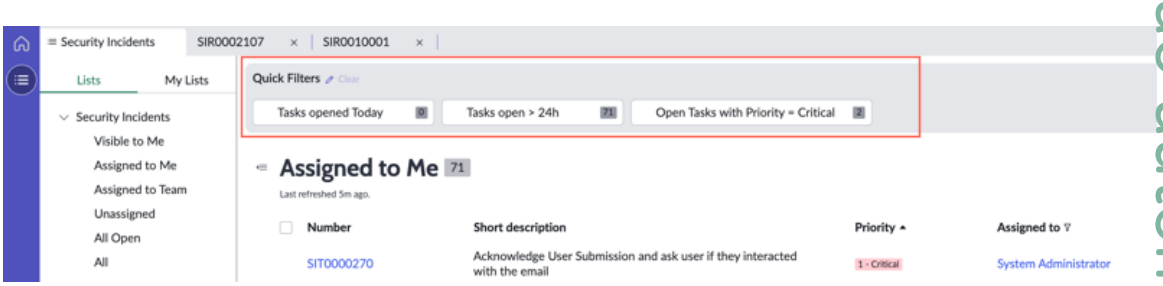
Função necessária: sn_si.basic

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.

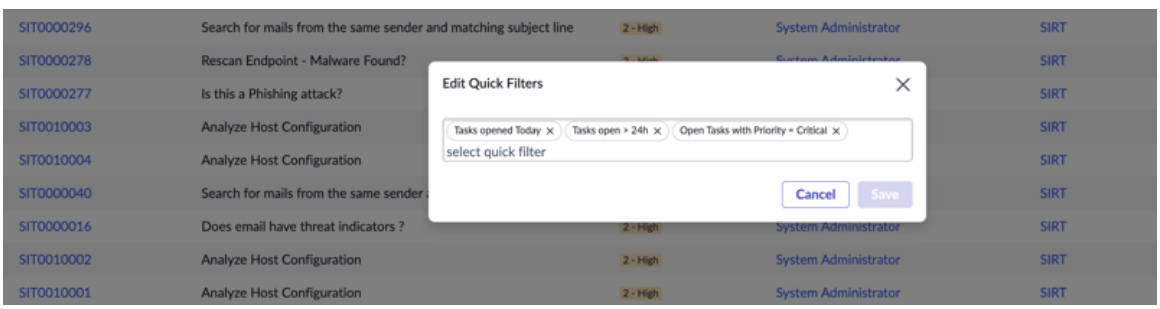
2. Clique no ícone de de lista).

3. Por exemplo, vá para **Listas** > **Incidentes de segurança** > **Filtros rápidos** seção.



4. Clique no ícone **Editar** para fazer as mudanças.

Nota:
A mudança que você fizer será mantida e, quando o usuário retornar a esta página na próxima vez, a preferência persistente será exibida.



5. Clique em **Salvar**.

Exportar incidentes de segurança ou tarefas de resposta

Exporte os incidentes de segurança ou as tarefas de resposta da exibição de lista.

Tradução automática

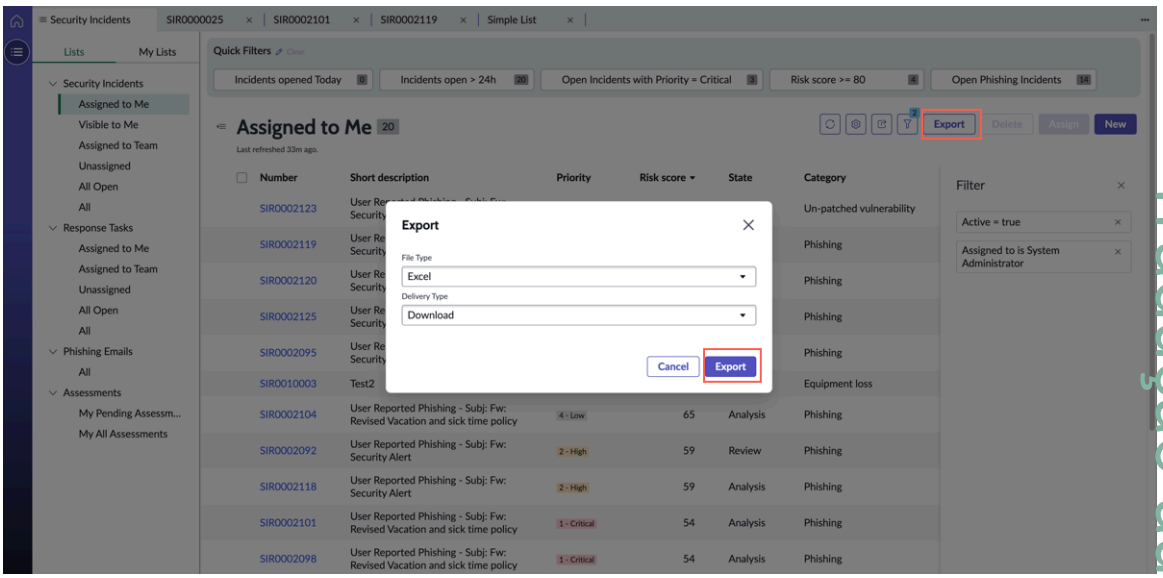
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique no ícone de lista .
3. Clique **em Listas**.
4. Ir para **Incidentes de segurança ou tarefas de resposta** > **Todos em aberto**.
5. Exiba a lista e clique em **Exportar**.



6. Selecione o Tipo de **arquivo e o Tipo** de **entrega**.
   Por exemplo, **Excel** e **download** ou e- **mail** da lista.
7. Clique em **Exportar**.
   O arquivo será baixado ou enviado por e-mail de acordo com a opção escolhida.

Configuração do SIR Workspace

Esta seção descreve as configurações necessárias para trabalhar com o Espaço de resposta a incidentes de segurança.

Configurar exibição de registros de SIR

Esta seção descreve como as listas relacionadas são agrupadas e apresentadas na guia Registros relacionados ao SIR para facilitar a navegação.

Os usuários do espaço também podem pesquisar facilmente a lista relacionada por nome.

Configurar investigação de tempo de design de SI

Use esta seção para configurar a página de investigação de tempo de design do incidente de segurança para adicionar vários pontos de entrada e seus registros associados no Espaço de resposta a incidentes de segurança.

Função necessária: sn_si.admin.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seguir, detalhamos as etapas envolvidas na configuração da página de investigação no Espaço de resposta a incidentes de segurança.

- Criando exibição para tabelas de informações associadas
- Como adicionar uma lista de ponto de entrada
- Exibição de mapeamento das informações associadas à lista de ponto de entrada
- Configure cada lista associada da exibição para processar a renderização de dados em tempo de execução

Tópicos relacionados

Explorar tela de investigação

Criando exibição para tabelas de informações associadas

A tela de investigação aproveita as exibições de lista relacionada criadas no incidente de segurança para configurar as listas associadas.

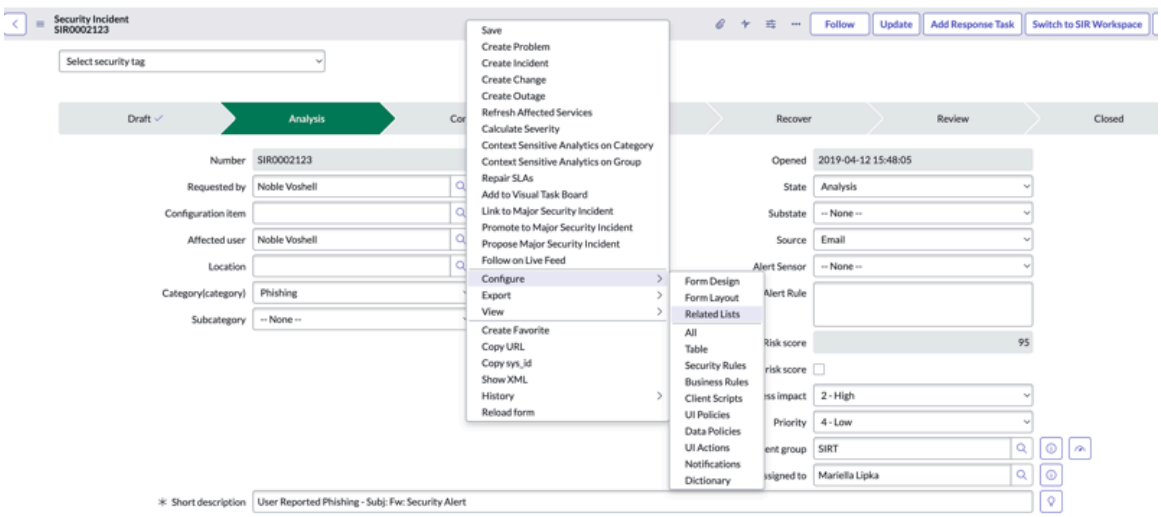
Antes de Iniciar

Função necessária: sn_si.admin

A seguir está um procedimento para criar uma exibição e adicionar listas relacionadas a ela.

Procedimento

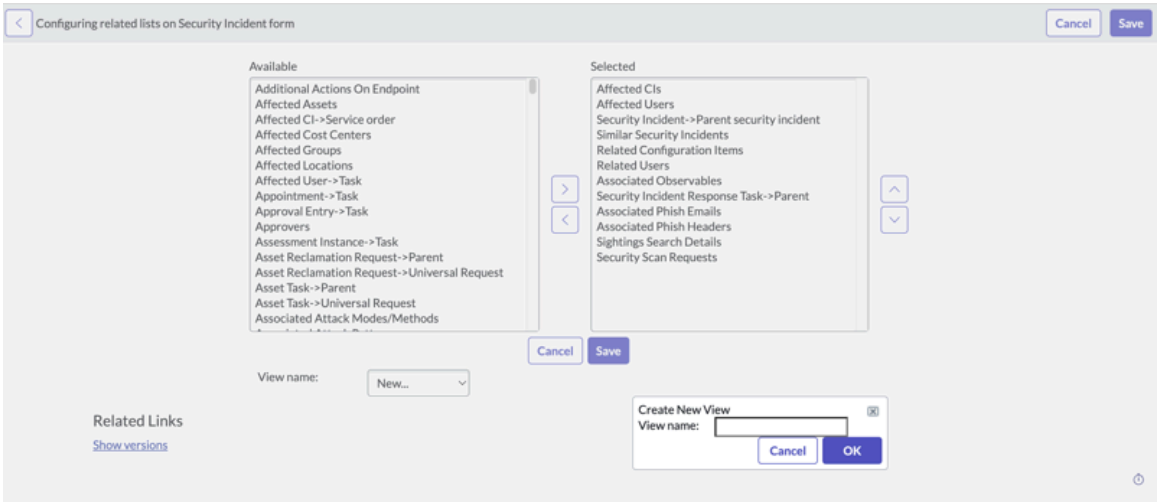
1. Navegue até a lista de **incidentes de segurança**.
2. Abra qualquer incidente de segurança na IU clássica.
3. No menu de contexto do formulário, navegue até **Configurar** > **Listas relacionadas**.
   A janela de bucket de caixa de listagem dupla é exibida.



4. Vá para a lista suspensa **Exibir nome** e clique em **Novo** para criar uma nova exibição.
   Você deve adicionar um nome à exibição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Adicione as listas relacionadas desejadas ao bucket direito na exibição recém-criada e salve a exibição.
   Esta exibição será usada para renderizar as informações associadas na guia Investigação.

Como adicionar uma lista de ponto de entrada

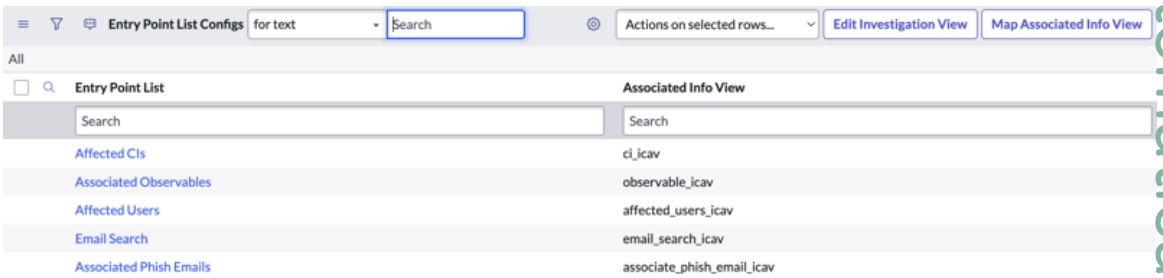
Configure a nova lista de ponto de entrada para adicioná-la à página de investigação.

Antes de Iniciar

Função necessária: administrador

Procedimento

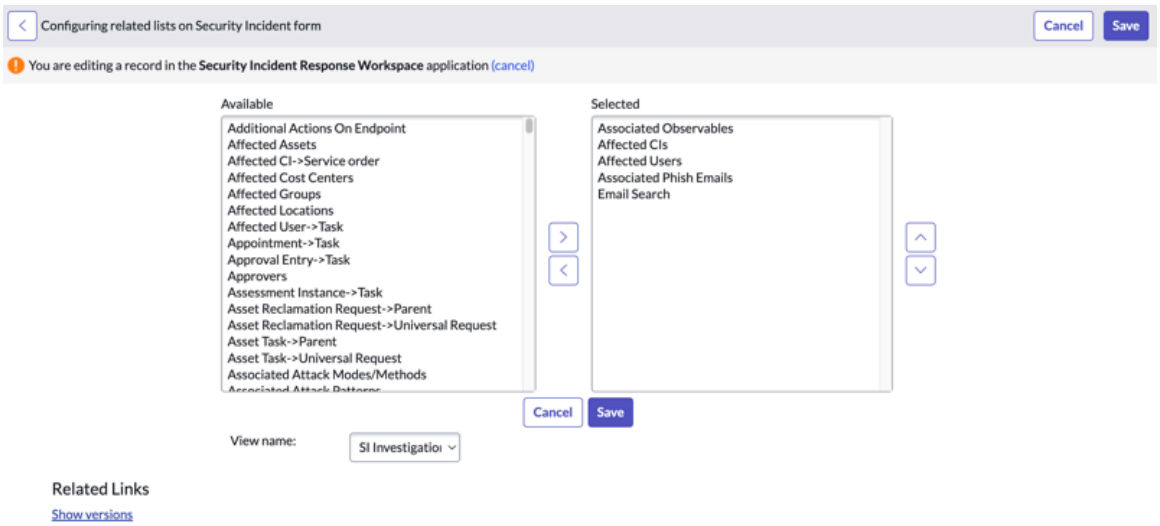
1. Navegar até **sn_si_aw_entry_point_config.list**.
   A página **Configurações de listas de ponto de entrada** é exibida.



2. Clique no botão **Editar exibição de investigação** para adicionar uma lista de pontos de entrada à tela de investigação.
   O **formulário Configurar listas relacionadas no incidente de segurança** é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Adicione ou remova a lista de pontos de entrada da exibição do bucket de caixa de listagem dupla.
4. Clique em **Salvar**.

Nota:
A exibição correspondente à tela Investigação que contém as listas de ponto de entrada é chamada **de Exibição de investigação de SI** e é selecionada por padrão quando você navega para a página **Editar exibição de investigação**.

A ordem na qual as listas de ponto de entrada são exibidas na tela de investigação é determinada pela ordem na exibição selecionada do slush bucket.

Exibição de mapeamento das informações associadas à lista de ponto de entrada

Mapeie a exibição de informações associada à lista de ponto de entrada recém-adicionada usando a ação Mapear Exibição de Informações Associadas.

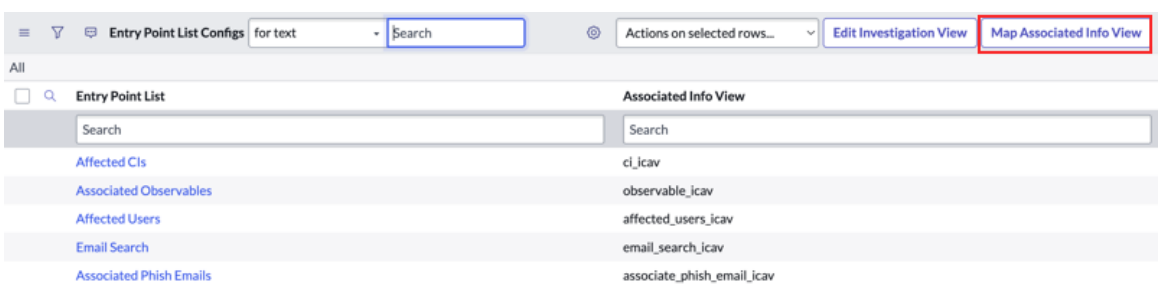
Antes de Iniciar

Nota:
Esta etapa é necessária para que a lista de pontos de entrada fique visível na página Investigação. Mesmo se você não quiser que nenhuma lista de informações associada seja mostrada em um ponto de entrada, ainda será necessário criar uma exibição fictícia e mapeá-la.

Função necessária: administrador

Procedimento

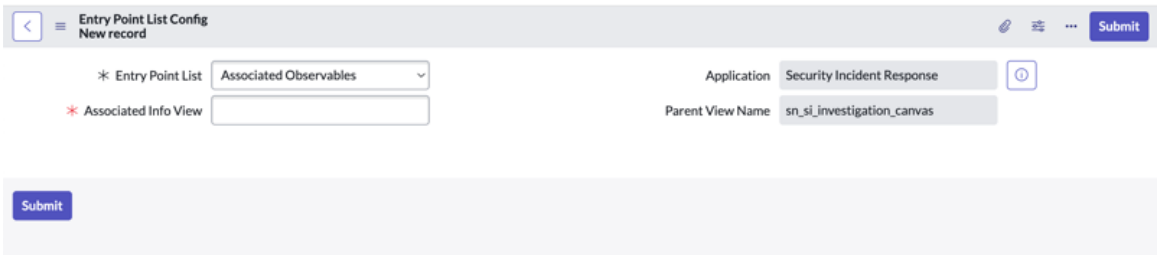
1. Clique no botão **Exibir informações associadas do mapa** na página **Configurações do ponto de entrada**.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Selecione a lista de ponto de entrada recém-adicionada na **lista suspensa Lista de Pontos** de Entrada.
3. Insira o nome da exibição que contém as listas relacionadas às informações associadas no campo **Exibição** de informações associadas.
   Para obter informações sobre como criar uma exibição para as listas relacionadas de informações associadas, consulte Criando exibição para tabelas de informações associadas.



4. **Salve** o formulário.
5. Além disso, se necessário, você pode adicionar ou remover mais listas associadas usando a **exibição Editar informações associadas**.
   Você também pode configurar o layout da lista de ponto de entrada usando a ação **Editar** layout da lista de ponto de entrada. Adicione ou remova colunas do slush bucket conforme desejado e salve o formulário.

Configure cada lista associada da exibição para processar a renderização de dados em tempo de execução

Configure cada lista associada da exibição para lidar com a renderização de dados de tempo de execução.

Antes de Iniciar

Nota:
Esta etapa é obrigatória para cada lista associada configurada na exibição de informações associada. Caso contrário, a lista associada não estará disponível na página de investigação.

Cada uma das listas associadas adicionadas (ao mapear uma exibição de informações associada a uma lista de ponto de entrada) Exibição de mapeamento das informações associadas à lista de ponto de entrada (ou da exibição diretamente) precisa de uma configuração adicional para filtrar os dados em relação à seleção de registro de tempo de execução e seleção de filtros.

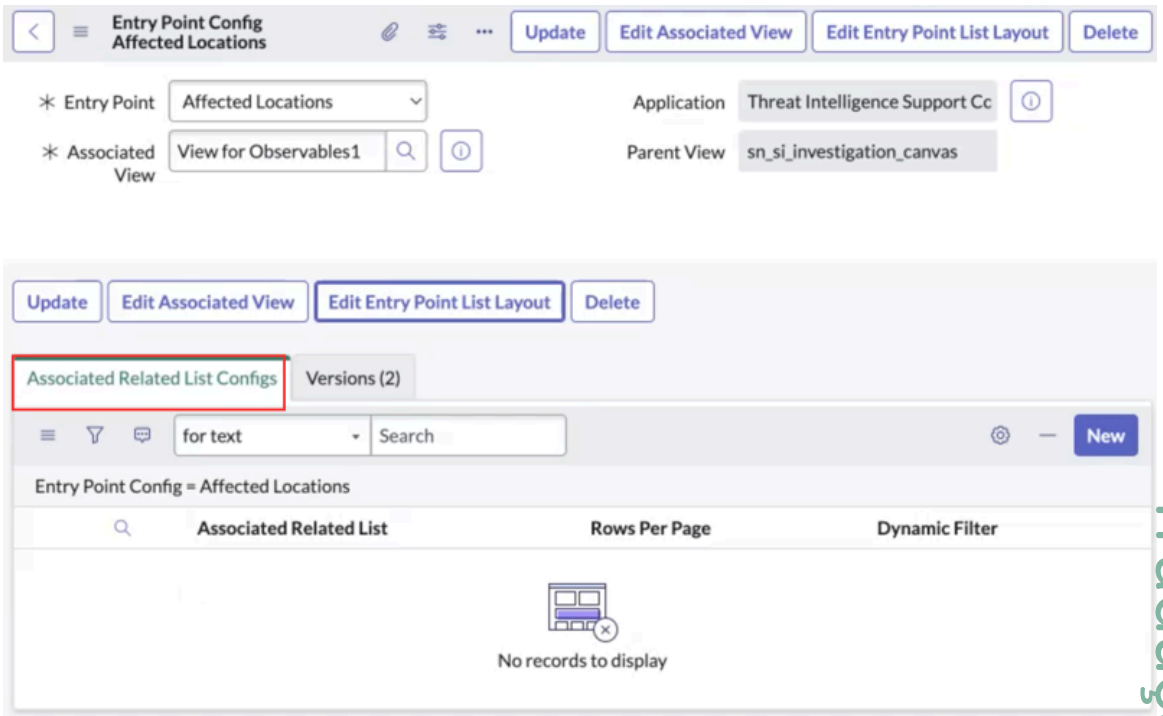
Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

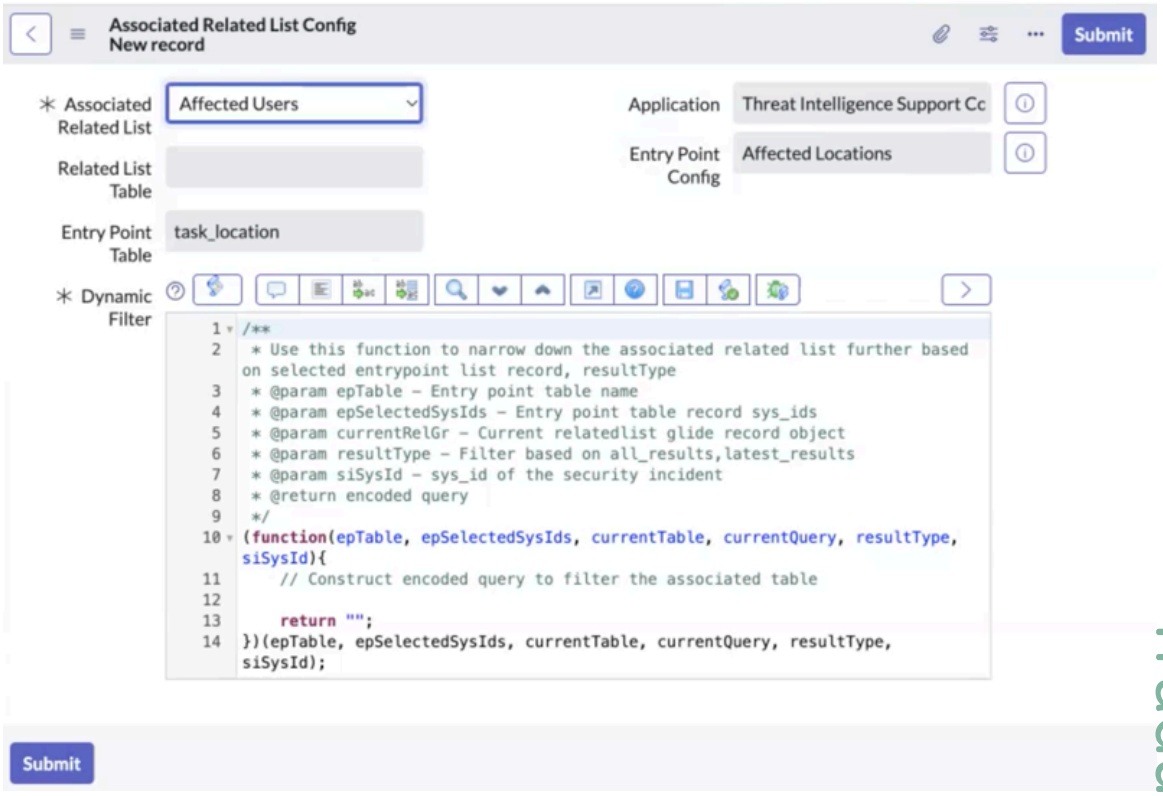
1. Clique em **Novo** em **Configs. da lista associada**.



2. Selecione o valor do campo **Lista associada**.
3. Use a coluna **Filtro dinâmico** para filtrar ainda mais a lista associada com base nos registros da lista de ponto de entrada selecionados e no tipo de resultado (resultados mais recentes de cada implementação do fornecedor, todos os resultados).
   Consulte os exemplos existentes que são enviados com o produto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Além disso, você pode configurar o layout da lista associada usando a ação **Editar** layout da lista associada. Na janela do slush bucket, adicione ou remova colunas conforme necessário.

SIR Workspace Registros relacionados

Esta seção consiste nos itens de listas relacionadas que são agrupados em seções, como observáveis associados e itens de configuração.

Os grupos de listas relacionadas a seguir que estão disponíveis como parte do sistema de base. Você pode modificar esses grupos ou criar grupos na aplicação e suas respectivas ações.

Você pode modificar esses grupos ou criar novos grupos. Para obter mais informações, consulte Configurar lista relacionada de incidentes de segurança sobre como configurar e agrupar a lista relacionada para incidentes de segurança e tarefas de resposta. Cada lista relacionada é totalmente funcional no SIR Workspace.

Lista relacionada	Item agrupado
Impacto nos negócios	• Itens de configuração • Usuários afetados • Itens de Configuração Relacionados • Usuários relacionados • Serviços afetados

Tradução automática

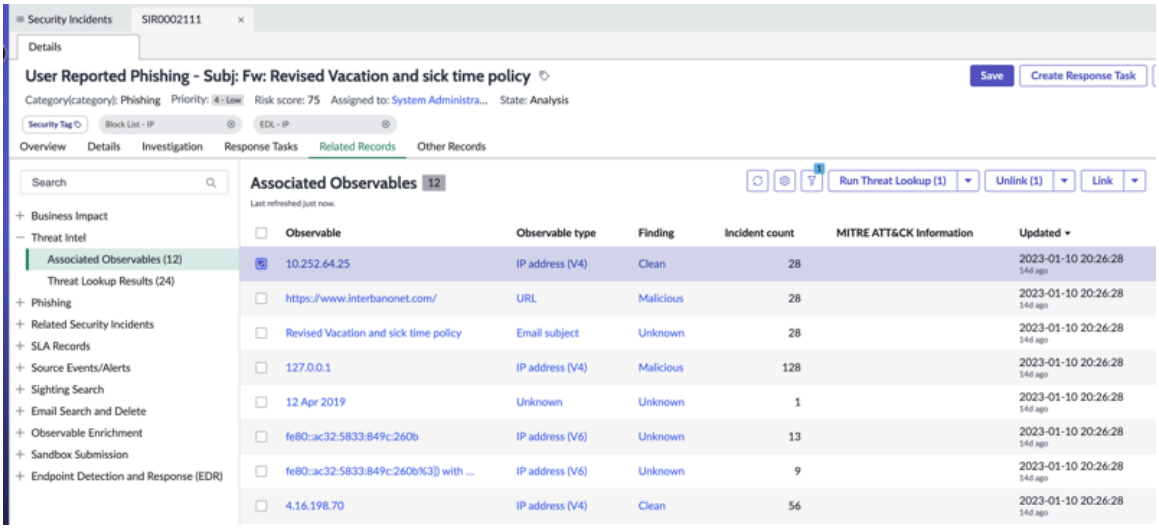
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Item agrupado
Inteligência sobre ameaça	• Observáveis Associados • Resultados da Pesquisa de ameaças
Phishing	• E-mails de Phishing Associados • Cabeçalhos de Phishing Associados
Incidentes de segurança relacionados	• Incidente primário de segurança • Incidente secundário de segurança • Incidente de segurança semelhante
Registro de ANS	ANSs de tarefas
Eventos/alertas de origem	Os eventos ou alertas de origem são a lista relacionada à integração de SIEM habilitada, como e-mail de origem, logs de detalhamento do LogRhythm, eventos do LogRhythm, infração agregada do IBM QRadar e assim por diante. **Nota:** Esta lista depende totalmente da integração que você tem em sua instância. Para exibir a lista relacionada à integração SIEM relevante, você deve instalar a versão mais recente.
Pesquisa de Vistas	• Resultados da pesquisa de detecções • Detalhes de Pesquisa de detecções • Vista
Aprimoramento de Observável	• Resultados de aprimoramento observável • Eventos de MISP associados • Resultados do aprimoramento de MISP
Detecção e resposta de endpoint (EDR)	• Detalhes do host • Processos em execução • Serviços em execução • Usuários Conectados • Estatísticas de Rede • Obter arquivo • Isolar Entradas de Host

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Item agrupado
	• Ações adicionais no endpoint • Detalhes do Microsoft Defender para máquinas relacionadas ao endpoint



Nota:
Em geral, você poderá criar novos registros, vincular ou desvincular registros existentes ou novos registros em relação ao grupo de lista relacionada, conforme aplicável.

Tópicos relacionados

Configurar lista relacionada de incidentes de segurança

Configurar lista relacionada de incidentes de segurança

Você pode adicionar novas listas relacionadas ou novos grupos de listas relacionadas e modificar grupos existentes ou listas relacionadas que aparecem no SIR Workspace.

Antes de Iniciar

A lista relacionada de incidentes de segurança é agrupada e exibida como itens de lista relacionada de grupo na guia **Registros relacionados** no espaço de trabalho.

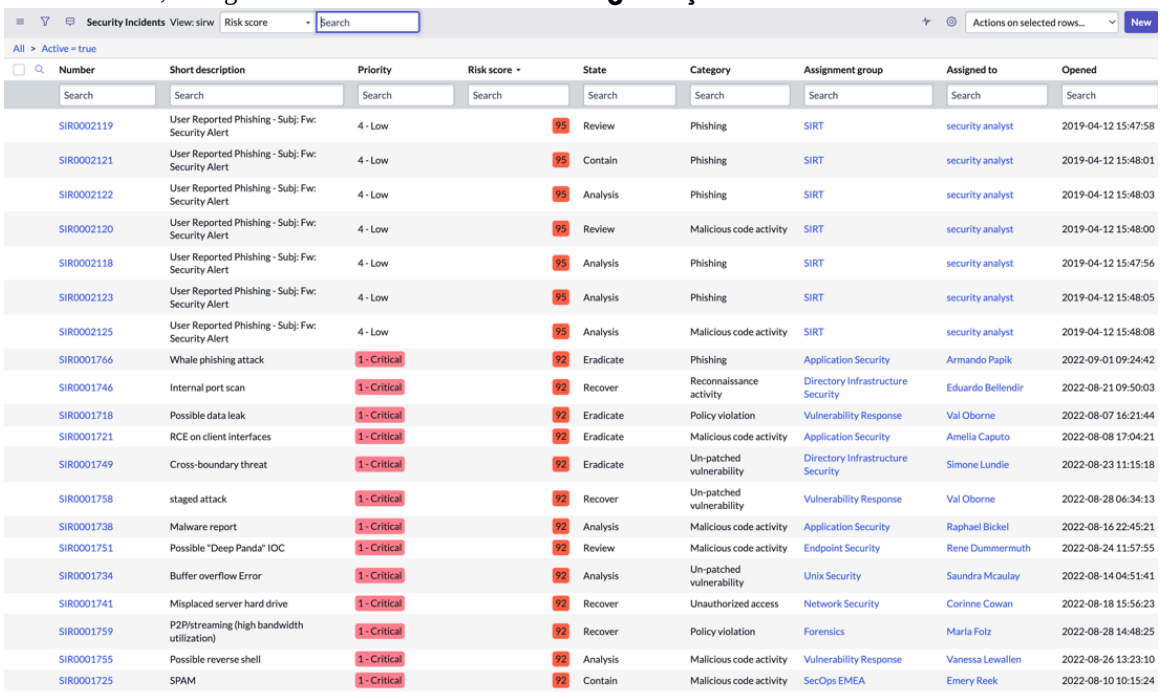
Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Na IU clássica, navegue até **Todos** > **Incidente de segurança** > **Mostrar incidentes em aberto**.

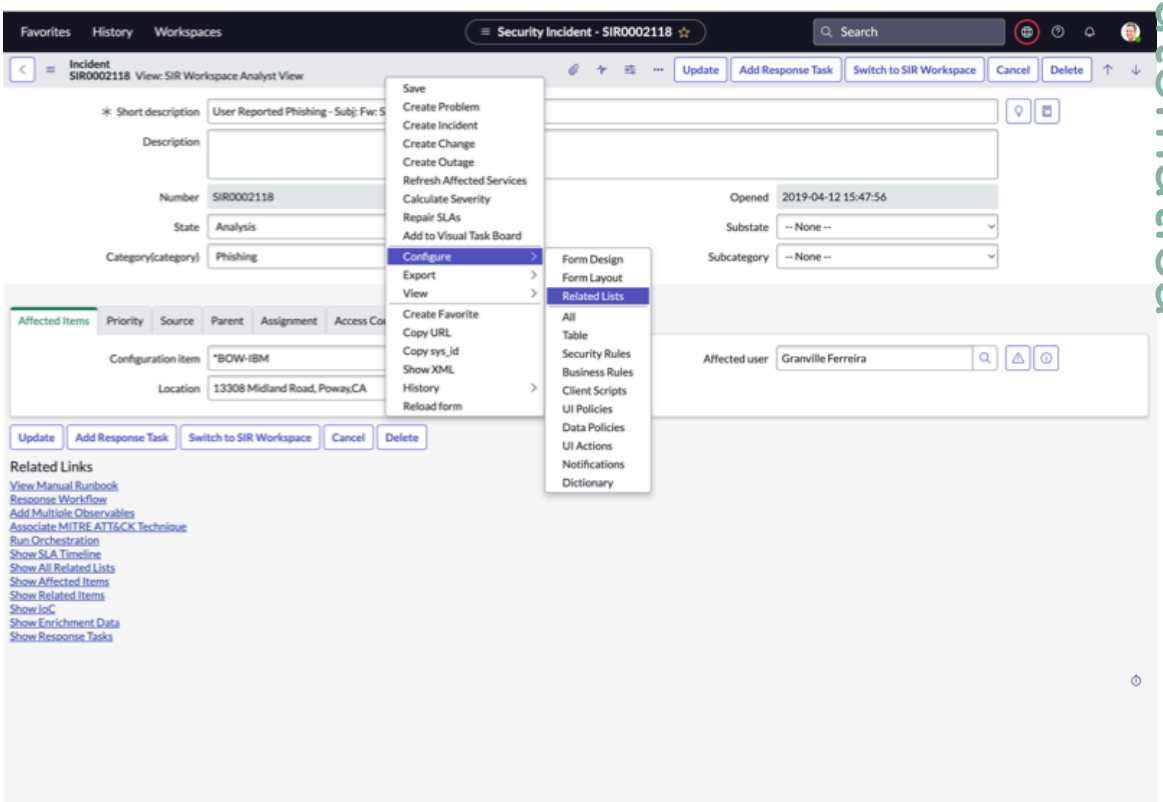


Security Incidents View: sirw | Risk score | Search | Actions on selected rows... | New

All > Active = true

Number	Short description	Priority	Risk score	State	Category	Assignment group	Assigned to	Opened
SIR0002119	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Phishing	SIRT	security analyst	2019-04-12 15:47:58
SIR0002121	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Contain	Phishing	SIRT	security analyst	2019-04-12 15:48:01
SIR0002122	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:03
SIR0002120	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:00
SIR0002118	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:47:56
SIR0002123	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:05
SIR0002125	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:08
SIR0001766	Whale phishing attack	1 - Critical	92	Eradicate	Phishing	Application Security	Armando Papik	2022-09-01 09:24:42
SIR0001746	Internal port scan	1 - Critical	92	Recover	Reconnaissance activity	Directory Infrastructure Security	Eduardo Bellendir	2022-08-21 09:50:03
SIR0001718	Possible data leak	1 - Critical	92	Eradicate	Policy violation	Vulnerability Response	Val Oborne	2022-08-07 16:21:44
SIR0001721	RCE on client interfaces	1 - Critical	92	Eradicate	Malicious code activity	Application Security	Amelia Caputo	2022-08-08 17:04:21
SIR0001749	Cross-boundary threat	1 - Critical	92	Eradicate	Un-patched vulnerability	Directory Infrastructure Security	Simone Lundie	2022-08-23 11:15:18
SIR0001758	staged attack	1 - Critical	92	Recover	Un-patched vulnerability	Vulnerability Response	Val Oborne	2022-08-28 06:34:13
SIR0001738	Malware report	1 - Critical	92	Analysis	Malicious code activity	Application Security	Raphael Bickel	2022-08-16 22:45:21
SIR0001751	Possible "Deep Panda" IOC	1 - Critical	92	Review	Malicious code activity	Endpoint Security	Rene Dummermuth	2022-08-24 11:57:55
SIR0001734	Buffer overflow Error	1 - Critical	92	Analysis	Un-patched vulnerability	Unix Security	Saundra Mcaulay	2022-08-14 04:51:41
SIR0001741	Misplaced server hard drive	1 - Critical	92	Recover	Unauthorized access	Network Security	Corinne Cowan	2022-08-18 15:56:23
SIR0001759	P2P/streaming (high bandwidth utilization)	1 - Critical	92	Recover	Policy violation	Forensics	Marla Folz	2022-08-28 14:48:25
SIR0001755	Possible reverse shell	1 - Critical	92	Analysis	Malicious code activity	Vulnerability Response	Vanessa Lewallen	2022-08-26 13:23:10
SIR0001725	SPAM	1 - Critical	92	Contain	Malicious code activity	SecOps EMEA	Emery Reek	2022-08-10 10:15:24

2. Selecione qualquer registro de incidente.
3. Clique com o botão direito do mouse no menu de contexto do incidente.
4. Ir para **Configurar** > **Lista relacionada**.



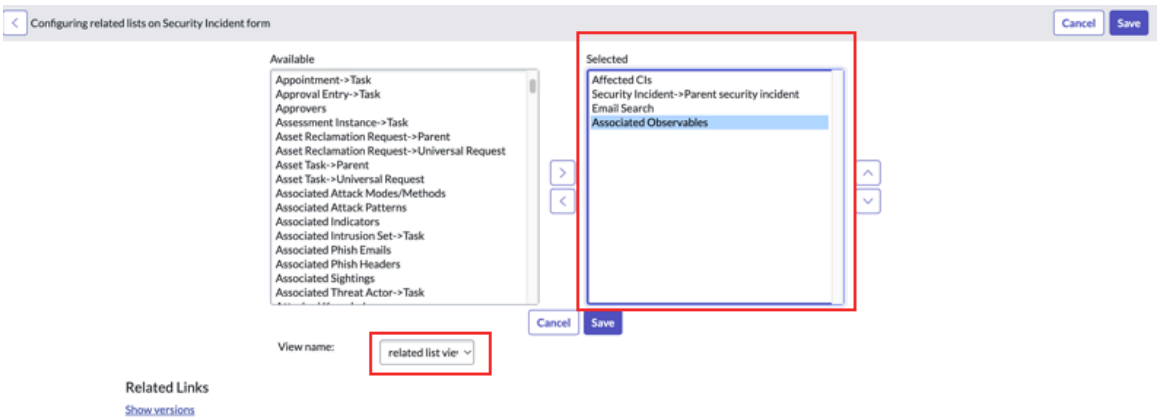
O **formulário Configurar listas relacionadas no incidente de segurança** é exibido.

5. Vá para **Exibir nome** e selecione **Novo**.

Tradução automática

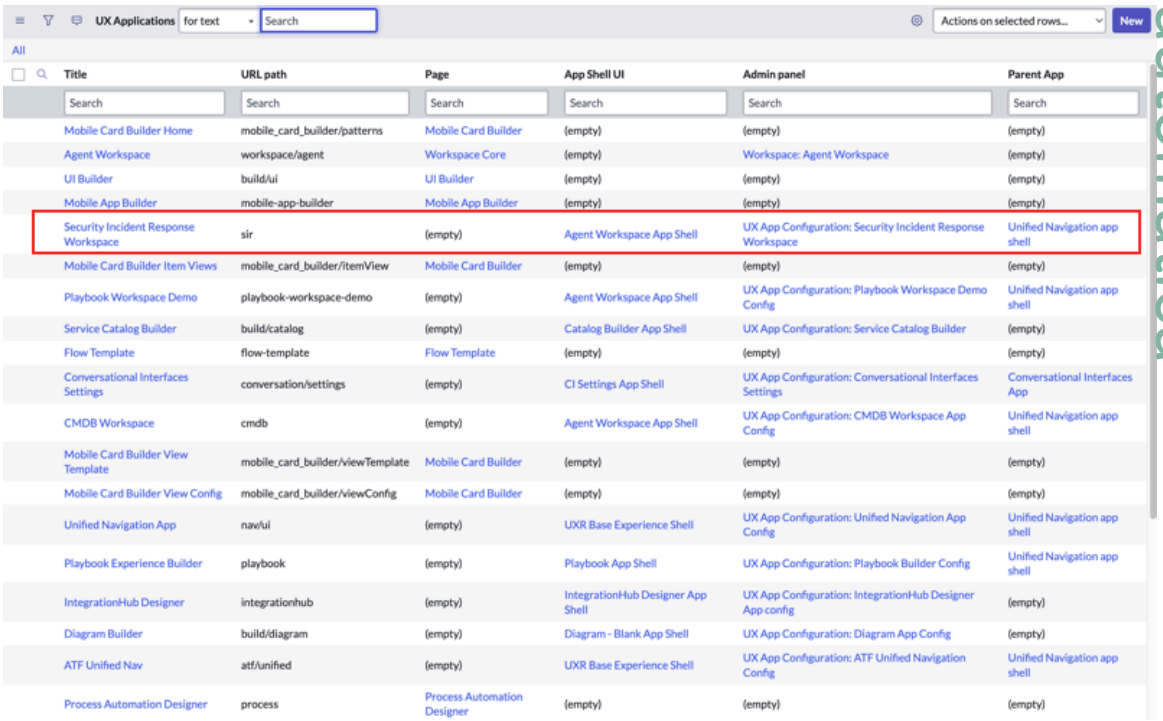
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Insira um nome para a exibição.
7. Selecione a exibição recém-criada.
   Depois de selecionar a exibição, escolha os campos de lista relacionados necessários no bucket de caixa de listagem dupla.



Nota:
Se você quiser modificar alguma coisa, selecione a exibição e remova ou adicione os itens.

8. Clique em **Salvar**.
9. Na navegação à esquerda, navegue até **Todos** > **Estrutura do Now Experience** > **Experiências**.
10. Selecione **Espaço do Security Incident Response**.

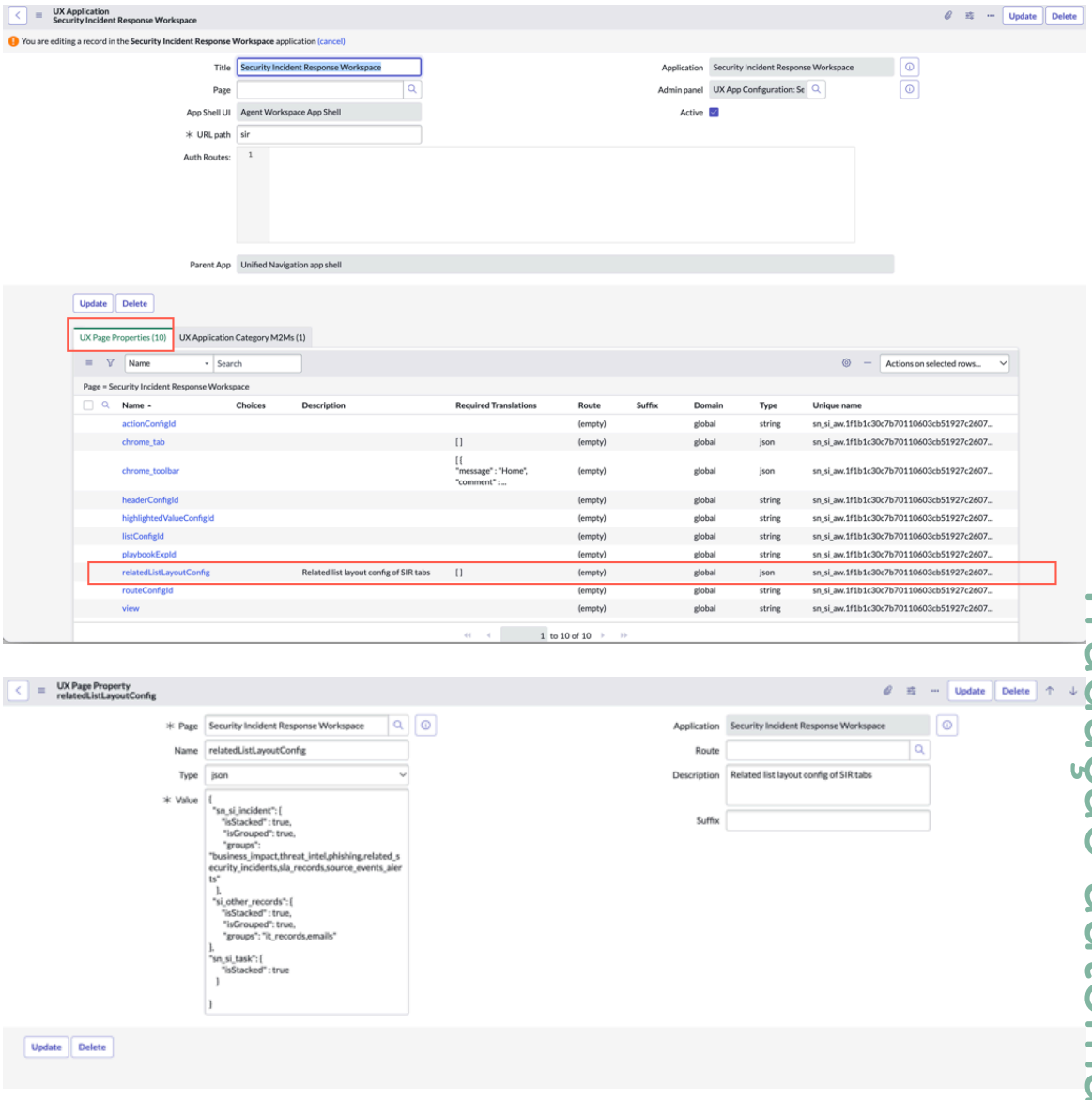


A página **Espaço do Security Incident Response da aplicação de UX** é exibida.

11. Vá para a guia **Propriedades da página de UX** e selecione a opção **relatedListLayoutConfig** na exibição de lista.

Tradução automática

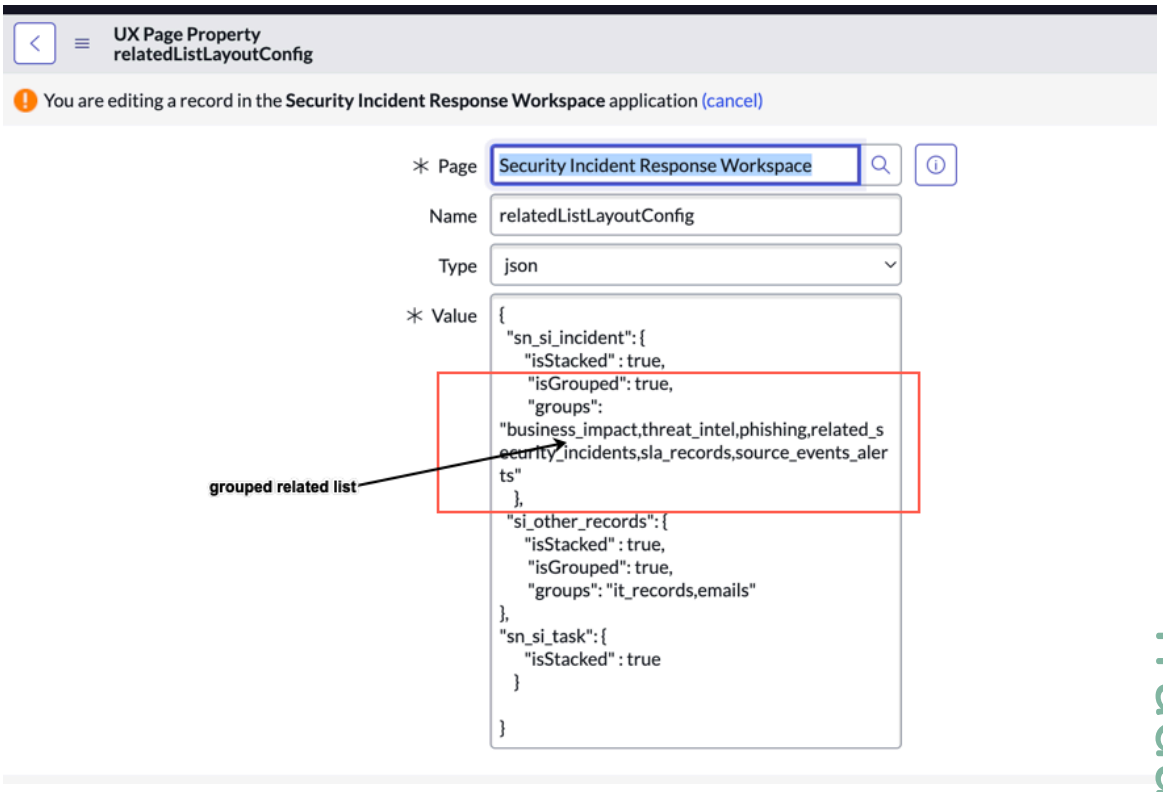
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



12. Adicione o nome de exibição recém-criado separado por uma vírgula a uma lista já existente de valores na caixa de texto **Valor** no campo **sn_si_incident.viewsUsedForGrouping**.
Por exemplo, se você tiver criado um novo nome de exibição como **Impacto nos negócios**, na caixa de texto **Valor**, deverá especificá-lo como **business_impact** (que é separado por sublinhado no nome da exibição e separado por uma vírgula após um valor existente) em sn_si_incident :campo de grupos.

Tradução automática

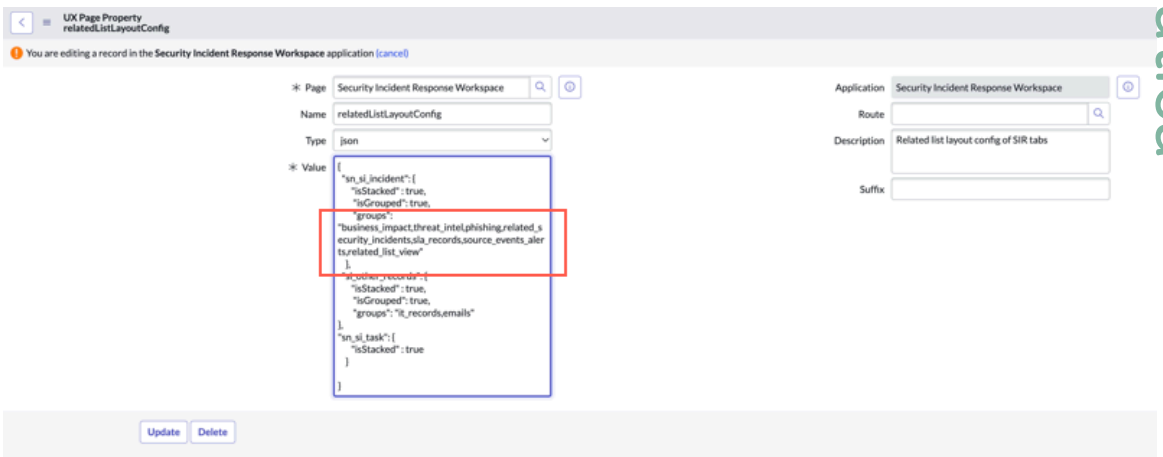
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:
Se você adicionar o novo nome de exibição no campo **sn_si_incident.viewsUsedForGrouping**, a entrada será criada na guia **Registros relacionados** do espaço.

Se você atualizar a entrada do nome da exibição em **si_other_records.viewsUsedForGrouping**, o grupo da lista relacionada será adicionado à guia **Outros registros** do espaço.

Abaixo está um exemplo de exibição que mostra as exibições recém-criadas adicionadas.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
obrigatórioRolesForGrouping contém nomes de registro sys_user_role separados por vírgula. O usuário do espaço de SIR deve ter pelo menos uma dessas funções para usar as listas relacionadas agrupadas. Quando um usuário não tem nenhuma dessas funções, a exibição de listas relacionadas configurada para a função do usuário atual usando a configuração de regra de exibição será representada verticalmente sem agrupamento. Esta propriedade é ignorada quando a propriedade **isGrouped** é definida como falsa. Se esta propriedade estiver vazia, qualquer usuário poderá acessar as listas relacionadas agrupadas.

13. Clique em **Salvar**.
14. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
15. Selecione qualquer incidente de segurança específico.
16. Vá para a guia **Registros relacionados** do espaço.
    As listas relacionadas agrupadas são exibidas.

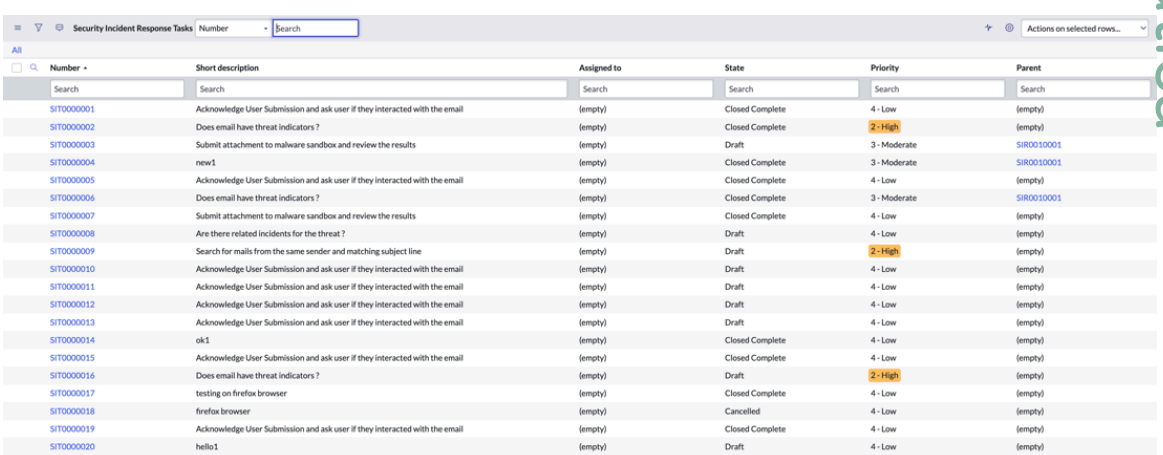
Configurar lista relacionada de tarefa de resposta

Use esta seção para configurar as novas listas relacionadas de tarefas de resposta que aparecem na aplicação Security Incident Response.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
A lista relacionada de tarefas de resposta não é agrupada, mas exibida como itens de lista relacionada individuais, pois há algumas listas padrão. Exiba os itens relacionados às tarefas de **resposta na guia Tarefas** de resposta do registro de incidente de segurança do espaço.

Procedimento
1. Navegar até **Todos** > **Incidente de segurança** > **Tarefas de resposta** > **Mostrar Todas as Tarefas**.



Number	Short description	Assigned to	State	Priority	Parent
SIT0000001	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000002	Does email have threat indicators ?	(empty)	Closed Complete	2 - High	(empty)
SIT0000003	Submit attachment to malware sandbox and review the results	(empty)	Draft	3 - Moderate	SIR0010001
SIT0000004	new1	(empty)	Closed Complete	3 - Moderate	SIR0010001
SIT0000005	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000006	Does email have threat indicators ?	(empty)	Closed Complete	3 - Moderate	SIR0010001
SIT0000007	Submit attachment to malware sandbox and review the results	(empty)	Closed Complete	4 - Low	(empty)
SIT0000008	Are there related incidents for the threat ?	(empty)	Draft	4 - Low	(empty)
SIT0000009	Search for mails from the same sender and matching subject line	(empty)	Draft	2 - High	(empty)
SIT0000010	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000011	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000012	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000013	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Draft	4 - Low	(empty)
SIT0000014	ok1	(empty)	Closed Complete	4 - Low	(empty)
SIT0000015	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000016	Does email have threat indicators ?	(empty)	Draft	2 - High	(empty)
SIT0000017	testing on firefox browser	(empty)	Closed Complete	4 - Low	(empty)
SIT0000018	firefox browser	(empty)	Cancelled	4 - Low	(empty)
SIT0000019	Acknowledge User Submission and ask user if they interacted with the email	(empty)	Closed Complete	4 - Low	(empty)
SIT0000020	hello1	(empty)	Draft	4 - Low	(empty)

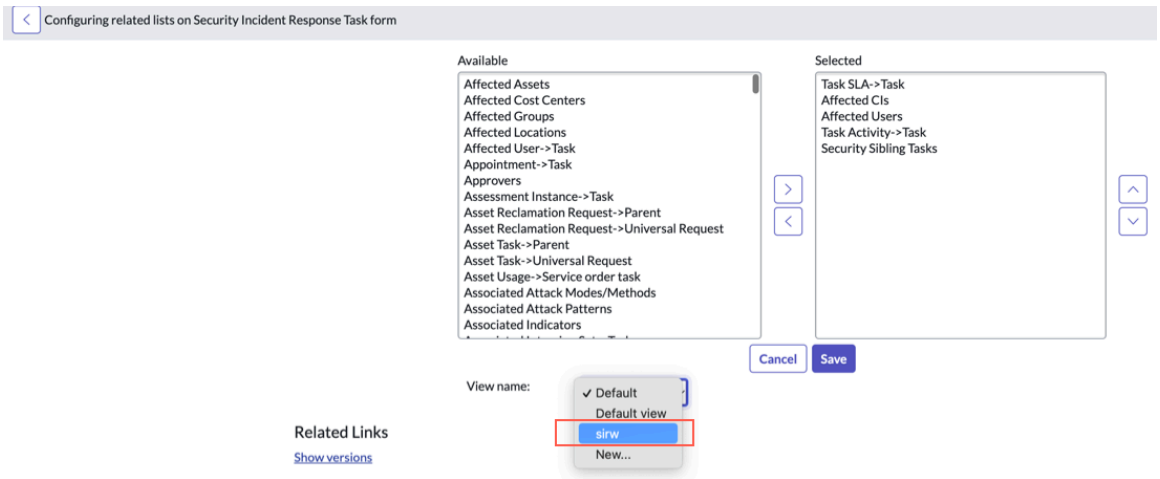
2. Selecione qualquer registro de tarefa de resposta.
3. Clique com o botão direito do mouse no menu de contexto Tarefa do Security Incident Response.
4. Navegar até **Configurar** > **Lista relacionada**.

Tradução automática

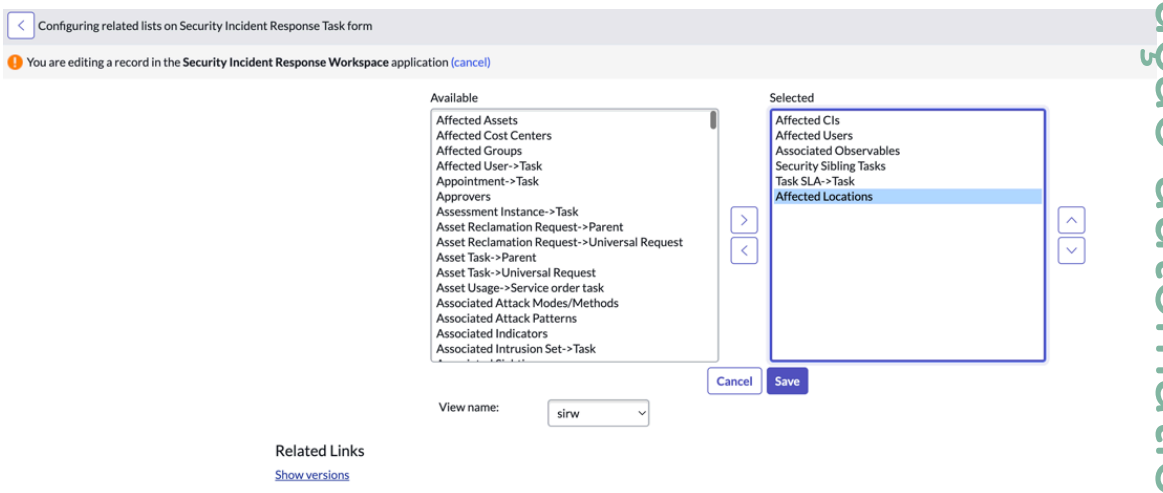
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O **formulário Configurar listas relacionadas no Security Response no formulário de tarefa do Security Response** é exibido.

5. Vá para **Exibir nome** e selecione a exibição **sirw**.



6. Selecione os campos de lista relacionados desejados no slush bucket.
Por exemplo, Locais afetados.



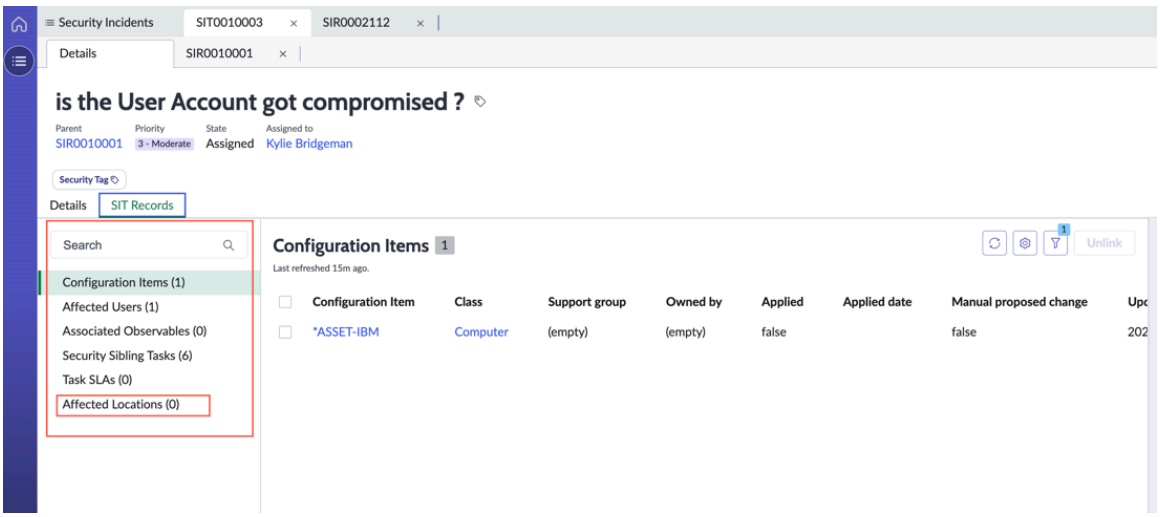
7. Clique em **Salvar**.

8. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança** > **Tarefas de resposta** > **Registros de SIT**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As listas relacionadas configuradas (por exemplo, Locais afetados conforme selecionado) são listadas na lista de registros SIT.



Como usar SIR Workspace

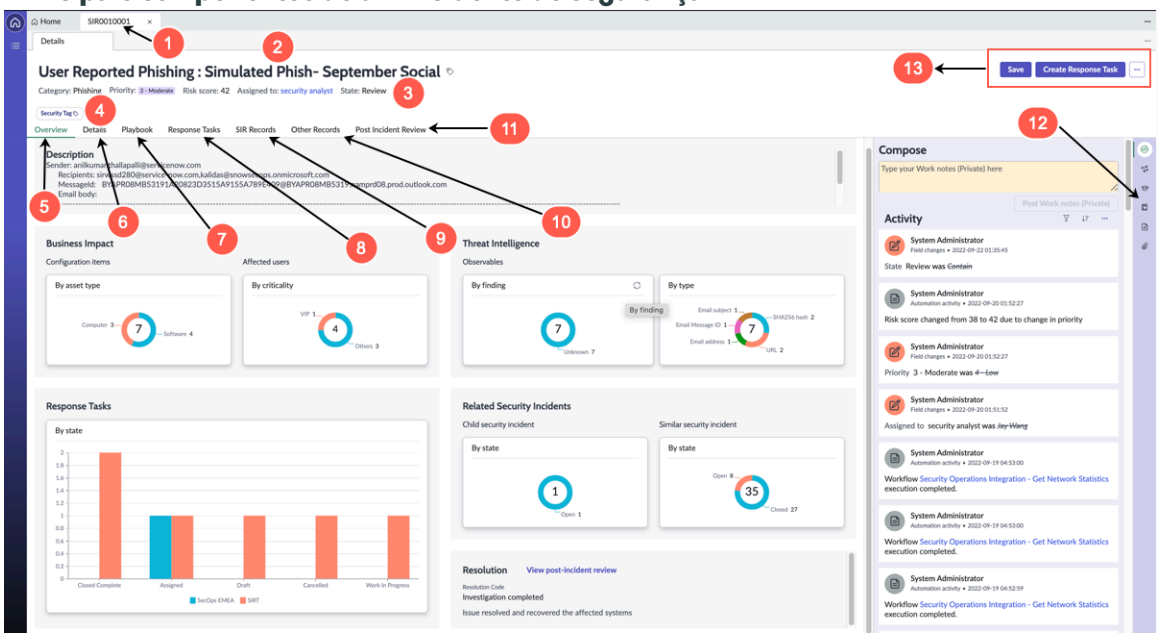
Analistas e gerentes de segurança usam SIR Workspace para executar operações diárias com uma experiência do usuário aprimorada, concluir a investigação de incidentes e obter uma visão geral.

Como trabalhar com registros de incidentes de segurança

O registro de incidente de segurança consiste no seguinte.

Principais componentes disponíveis em um registro de incidente de segurança:

Principais componentes de um incidente de segurança



Número	Nome	Descrição
1	Número do incidente de segurança	O número do incidente de segurança está disponível no nome da guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Número	Nome	Descrição
2	Descrição resumida	Descrição resumida do incidente de segurança que é exibido acima da faixa do formulário.
3	Faixa de formulário	Esta é uma seção somente leitura que contém os campos-chave, como Categoria, Prioridade, Pontuação de risco, Estado e os detalhes de atribuição do incidente. **Nota:** Os marcadores de plataforma regulares também podem ser aplicados aqui.
4	Marcadores de segurança	Exibe os marcadores de segurança associados a um incidente de segurança.
5	Visão geral	Fornece uma visão geral do snapshot do incidente de segurança, como Descrição, Impacto nos negócios, composto por detalhes do ativo por tipo, usuários afetados por criticidade, Itens de inteligência contra ameaças, compostos por observáveis por descoberta e por tipo, Tarefas de resposta, Incidentes de segurança relacionados, compostos por incidentes de segurança secundários e incidentes de segurança semelhantes.
6	Detalhes	A guia de detalhes exibe o formulário de incidente de segurança.
7	Investigação	A guia Investigação exibe a experiência de investigação de incidentes.
8	Playbook	O Playbook é acionado por meio do Designer de automação de processos (PAD). Se um processo for criado e se uma condição do gatilho for definida para acionar o playbook para um incidente de segurança. Em seguida, um playbook é exibido.
9	Tarefas de resposta	As Tarefas de resposta capturam todas as tarefas de resposta associadas a um incidente de segurança.
10	Registros relacionados	A guia Registros relacionados consiste em todas as listas relacionadas da IU clássica nesta seção. As listas relacionadas são agrupadas em várias seções, como impacto nos negócios, informações sobre ameaças e assim por diante, para facilitar a navegação.
11	Outros registros	A guia Outros registros consiste em registros de TI, como solicitações de mudanças, incidentes e e-mails agrupados e exibidos nesta seção.
12	Guia Análise pós-incidente	Conforme o incidente de segurança progride para o estado Revisão, a guia Revisão pós-incidente é exibida com as avaliações e relatórios pós-incidente na guia.
13	Menu contextual	Fornece acesso fácil às ações rápidas e está disponível em todas as guias para o analista acessar sempre que necessário. O menu contextual fornece navegação fácil para vários recursos, como:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Número	Nome	Descrição
		1. Fluxo de atividades **2.** Playbook **3.** Assistência de Analista **4.** Runbook **5.** Modelos **6.** Anexos
14	Ações de IU de formulário	As várias ações de IU do formulário de incidente de segurança são exibidas na parte superior direita do formulário de incidente. As ações de IU de formulário disponíveis são: • Salvar • Criar Tarefa de Resposta • Compor E-mail • Adicionar Playbook • Abrir fluxo ou fluxos de trabalho associados • Incidente de Creta • Criar problema • Criar solicitação de mudança • Criar indisponibilidade • Calcular Gravidade • Link para Incidente de segurança grave • Propor como Incidente de segurança grave • Promover a Incidente de segurança grave • Executar ações adicionais no endpoint • Associar técnica do MITRE ATT&CK • Alternar para a IU Clássica • Adicionar ao Caso de Segurança • Deletar Para obter mais informações, consulte Como trabalhar com ações de IU de formulário.

Seção Visão geral do incidente de segurança

A seção Visão geral no espaço apresenta as principais informações associadas ao incidente de segurança.

Os gráficos de donut são desabilitados quando um analista clica em qualquer item do gráfico e leva você até o respectivo registro com uma exibição de lista filtrada de itens na guia correspondente. Por exemplo, se **Observáveis maliciosos** for clicado, você será direcionado para os observáveis com uma exibição de lista filtrada de observáveis maliciosos na guia **Registros relacionados**.

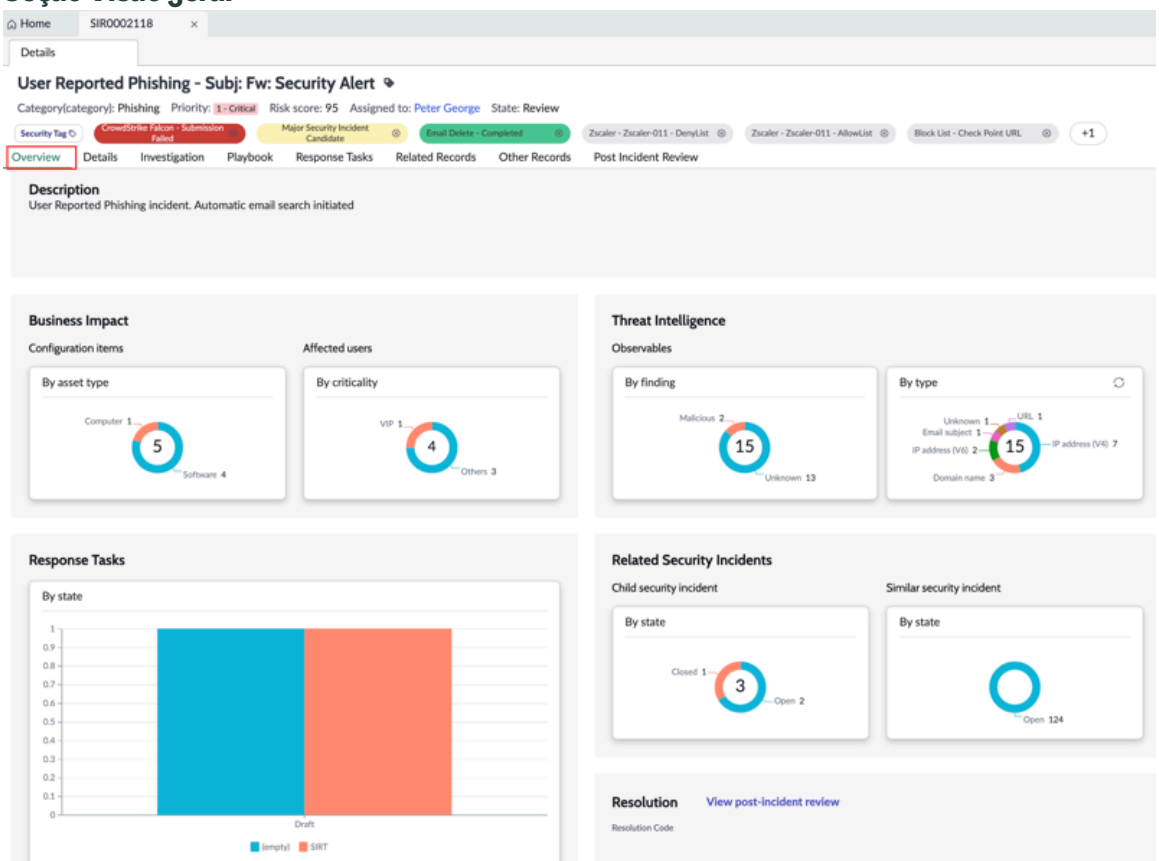
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seção Visão geral exibe o seguinte:

- Descrição do incidente de segurança.
- Detalhes do impacto nos negócios, como itens de configuração por tipo de ativo e usuários afetados por criticidade, sejam eles usuários VIP ou outros usuários.
- Itens de inteligência contra ameaças, como observáveis por descoberta - se os observáveis são maliciosos ou desconhecidos e por tipo.
- Tarefas de resposta por estado e grupo de atribuição.
- Incidentes de segurança relacionados que consistem em incidentes de segurança secundários por estado (abertos ou encerrados) e incidentes de segurança semelhantes por estado (abertos ou encerrados).
- A seção de resolução é exibida quando um incidente passa para o estado Revisão e, em seguida, a seção de resolução é exibida na seção **Visão geral** com uma capacidade de exibir a revisão pós-incidente.
- Resolução - exibir revisão pós-incidente: clique no link para navegar até a página de **revisão pós-incidente**.
- Depois que o incidente é encerrado, a seção Resolução exibe o Código de resolução, as Anotações de resolução e Resolvido por (usuário) são exibidos junto com os detalhes da análise pós-incidente.

Seção Visão geral



Incidente de segurança Seção de detalhes

Esta seção exibe os campos de formulário de incidente de segurança que são renderizados a partir da IU clássica de incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

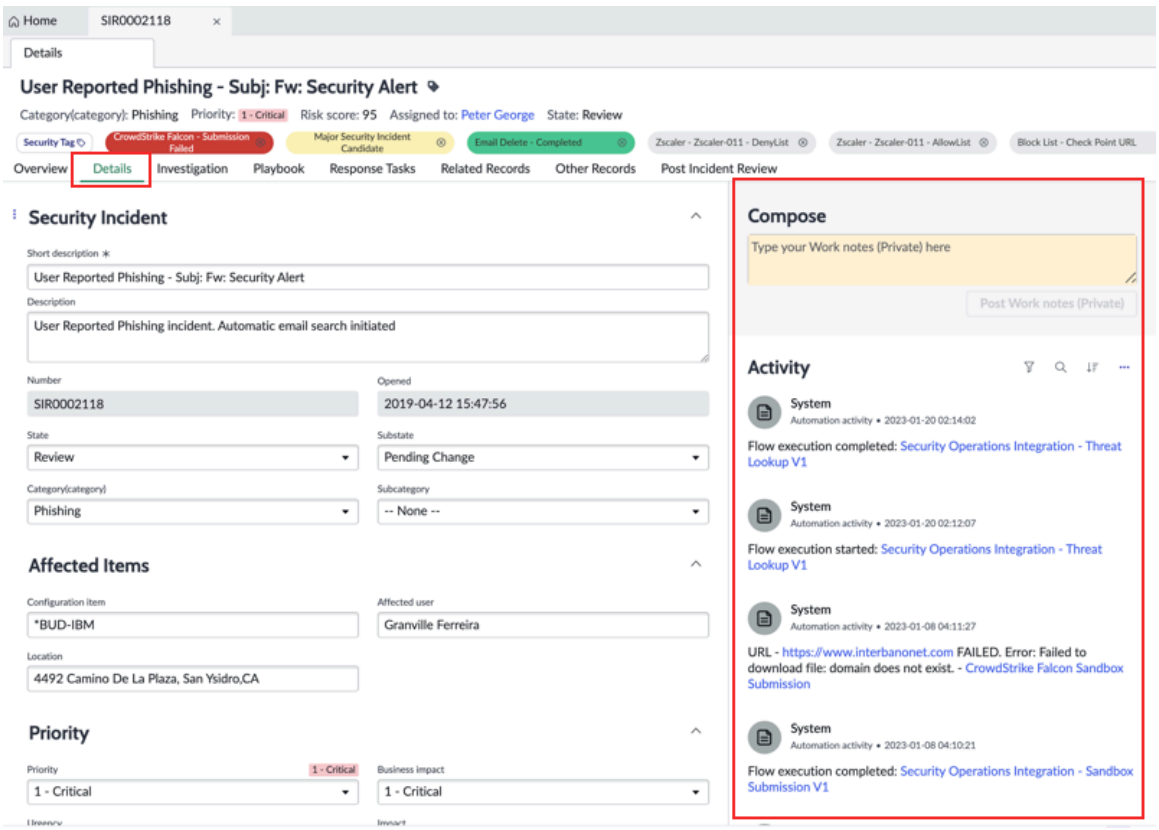
A IU clássica tem uma exibição chamada Exibição de **SIRW** criada. Esta exibição é mapeada para a guia **Detalhes** no novo espaço. Todas as personalizações necessárias precisam ser implementadas nesta exibição.

Os campos de formulário são agrupados nas seguintes seções e exibidos na exibição de formulário da guia Detalhes. Clique em qualquer seção ou pule para a respectiva seção no formulário:

- Incidente de segurança
- Prioridade
- Origem
- Primário
- Atribuição
- Controles de acesso
- Itens afetados
- Resolução

A guia **Detalhes** contém a seção Fluxo de **atividades** no próprio formulário de detalhes para um acesso rápido aos analistas de segurança para adicionar comentários e publicá-los.

Guia Detalhes e Fluxo de atividades



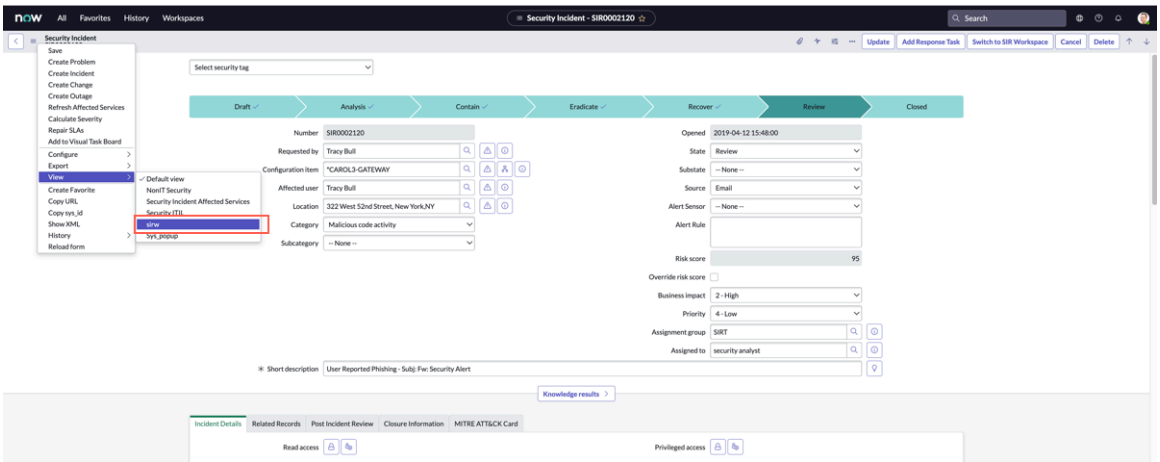
Veja a exibição Espaço do analista de SIR:

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar incidentes em aberto**.
2. Selecione qualquer registro de incidente de segurança.
3. Clique no menu de contexto e selecione **Exibição** > **SIRW**.

Tradução automática

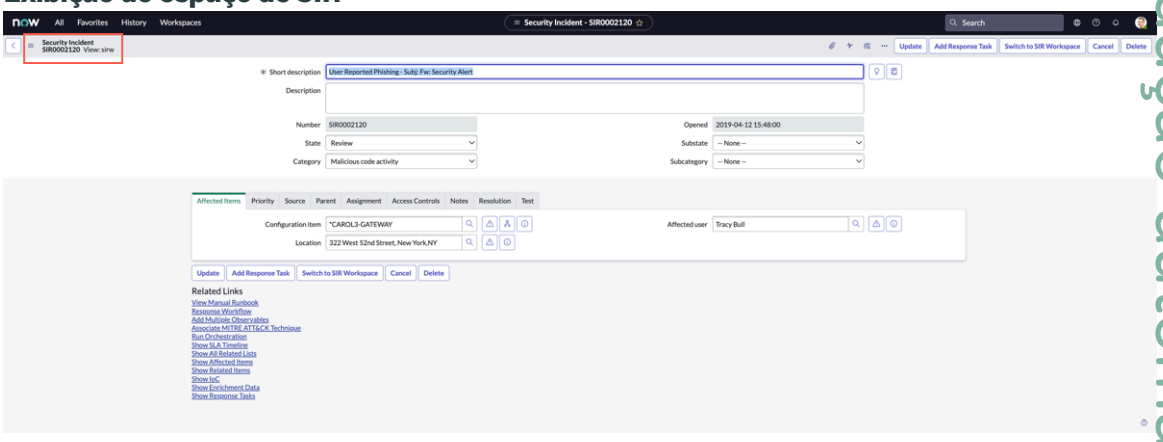
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Você pode personalizar usando a exibição do espaço da **sirw** no formulário de IU clássico.



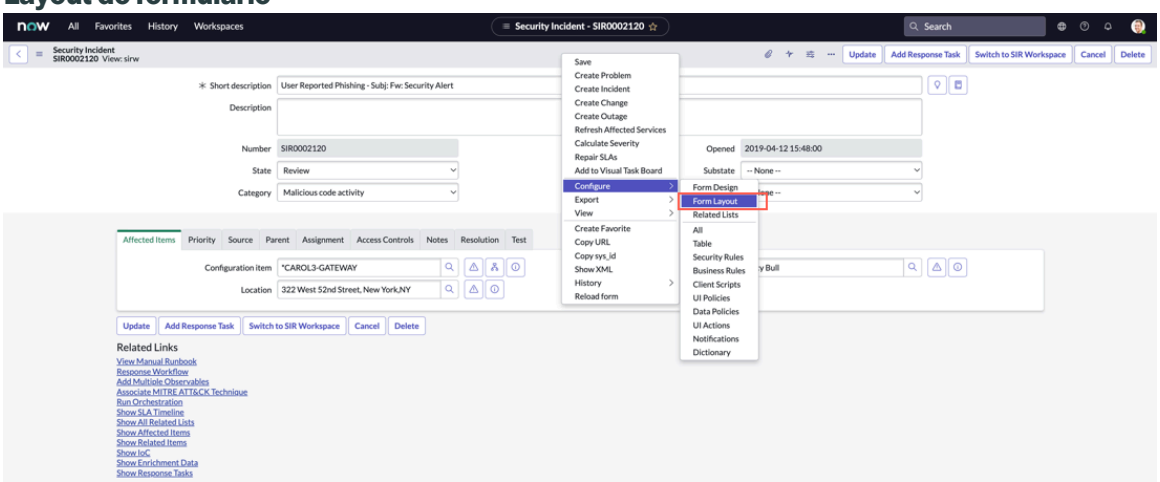
4. A exibição do espaço de trabalho de incidente de segurança é renderizada conforme mostrado abaixo.

Exibição do espaço de SIR



5. No registro de Incidente de segurança, clique com o botão direito do mouse e vá para **Configurar** > **Layout do formulário**.

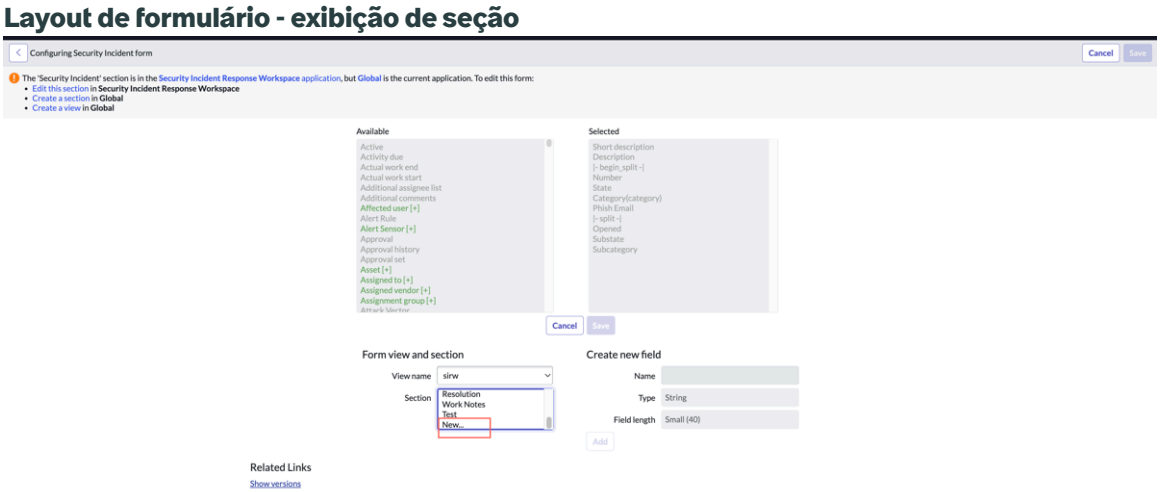
Layout do formulário



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

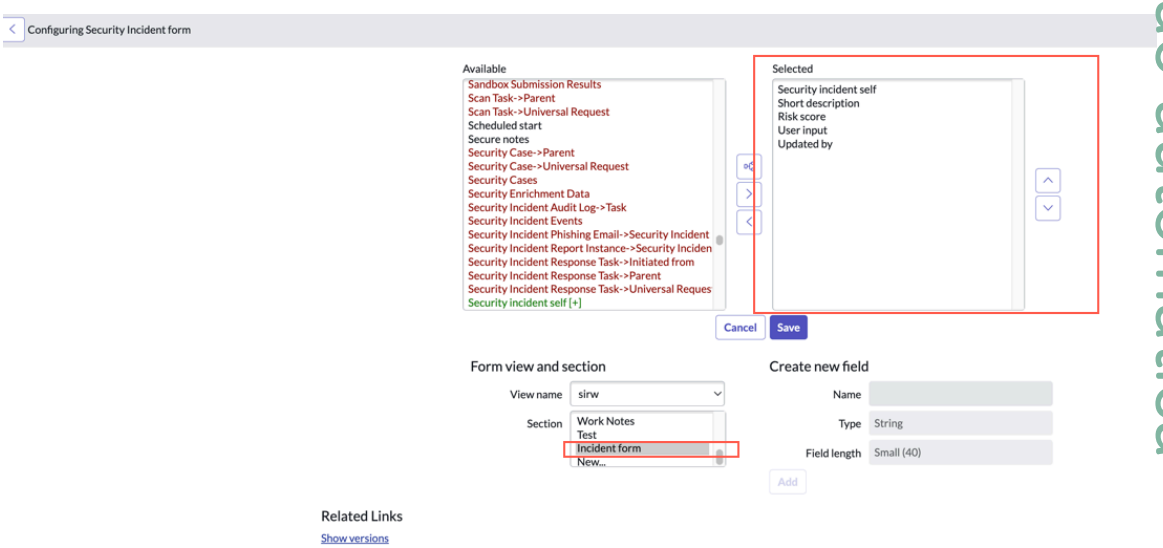
6. Faça uma busca detalhada na **exibição e na seção Formulário** e selecione **Novo** da **seção** para criar uma nova seção.



7. Forneça o novo nome da seção e clique em **OK**.

   Por exemplo, formulário Incidente.

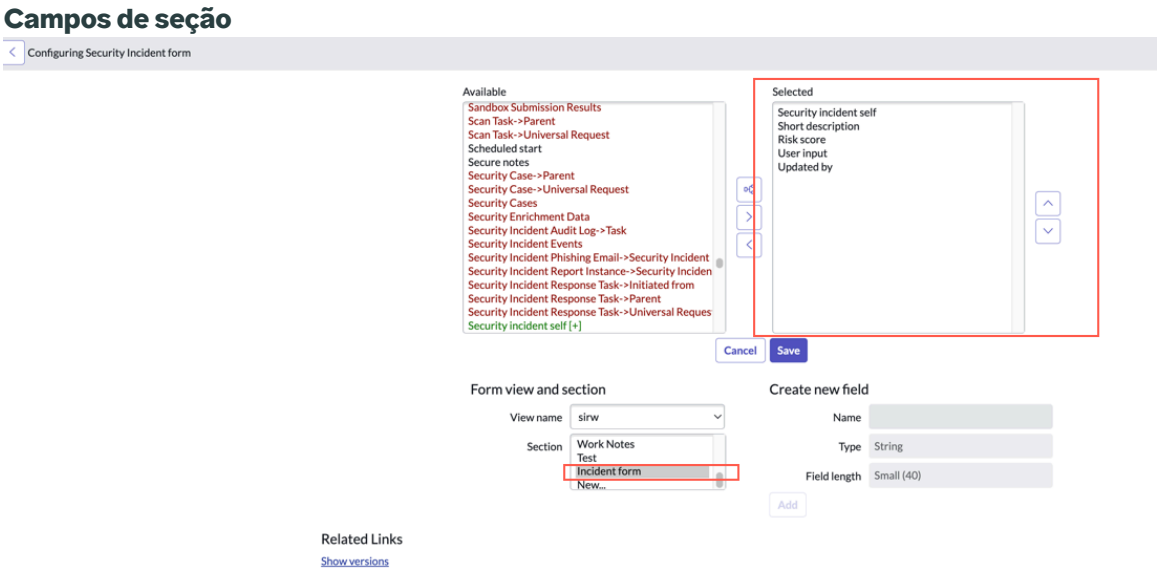
8. A nova seção é criada e adicionada à **Seção**.



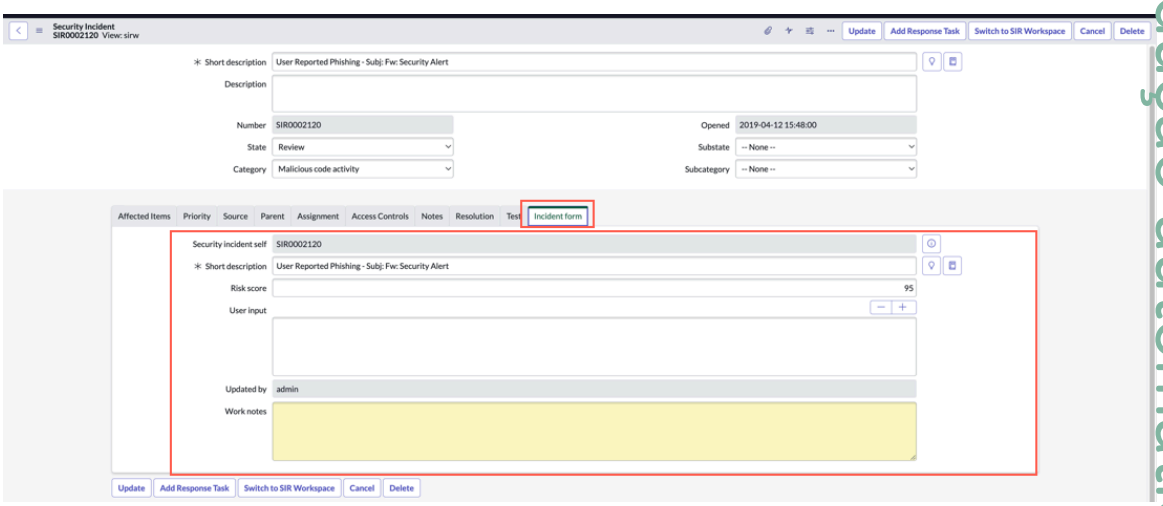
9. Selecione sua nova seção, adicione os campos de seção necessários ao slush bucket e clique em **Salvar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



10. A seção recém-adicionada é exibida junto com o layout da seção existente no formulário de incidente de segurança.



11. Agora, clique em **Alternar para espaço de SIR** para ir para o formulário de incidente de segurança e a seção personalizada na guia **Detalhes** do espaço de trabalho.

SIR Workspace Orquestração

Espaço de resposta a incidentes de segurança As atividades de orquestração ajudarão os analistas de segurança a exibir a tela de investigação e executar várias ações aplicáveis.

SIR Workspace Tela de investigação

Espaço de resposta a incidentes de segurança O permite que os analistas de segurança exibam as principais informações associadas ao incidente de segurança durante o processo de correção do incidente. As informações principais também incluem as listas relacionadas, como Observáveis, Resultados de pesquisa de ameaças, Pesquisa de detecções, Aprimoramento de observável e assim por diante.

Na IU clássica, a maioria das ações de orquestração associadas às integrações prontas para uso está disponível nas listas relacionadas. Por exemplo, Executar pesquisa de ameaças, Executar aprimoramento de observável etc. estão presentes na lista relacionada

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de Observáveis associados. Da mesma forma, Obter detalhes do host, Obter estatísticas de rede e assim por diante estão disponíveis na lista relacionada de Itens de configuração.

Quando um analista de segurança executa essas ações, os resultados são preenchidos em uma lista relacionada diferente. Por exemplo, quando um usuário executa a Pesquisa de ameaças de execução, os resultados ficam disponíveis na tabela Resultados da pesquisa de ameaças. Às vezes, os resultados estão disponíveis em várias tabelas diferentes. Durante esse processo, os analistas de segurança têm uma experiência do usuário desconectada e desorganizada ao correlacionar as informações de vários locais.

No novo SIR Workspacerecriado, a tela **Investigação** (guia) fornece todas as informações necessárias agrupadas logicamente em um só lugar para o Analista realizar a investigação.

Explorar tela de investigação

O objetivo primário da tela de investigação é apresentar os dados de incidentes de segurança necessários em um local comum.

No SIR Workspace, a investigação de incidentes de segurança gira principalmente em torno de alguns pontos de entrada principais.

A seguir estão alguns pontos de entrada principais que são provisionados para os analistas de segurança no sistema de base:

- Observáveis Associados
- Itens de configuração
- Usuários afetados
- E-mails de Phishing Associados
- Pesquisa de e-mail

Você também pode configurar os pontos de entrada acima adicionando, modificando ou removendo os pontos de entrada, conforme aplicável. Para obter mais informações, consulte Configurar investigação de tempo de design de SI.

Na guia **Investigação**, a tabela de ponto de entrada atua como a tabela primária. Todas as tabelas que contêm os resultados de uma ação de orquestração realizada na tabela primária são apresentadas como tabela secundária no ponto de entrada.

Por exemplo, para o ponto de entrada de **Observáveisassociados, a tabela Observáveis associados** é a tabela primária e outras tabelas, como Resultados de pesquisa de ameaças, Resultados de envio da área restrita e assim por diante, são a tabela secundária.

O analista de segurança pode executar todas as ações de orquestração na tabela Observáveis associados e exibir todas as informações associadas na mesma página, sem a necessidade de navegar por vários locais.

Nota:
Quando um usuário clica nos gráficos interativos na página **Visão geral**, como observáveis maliciosos, o usuário será direcionado para a exibição filtrada de observáveis maliciosos na tela de investigação. Como alternativa, o usuário pode iniciar a investigação diretamente navegando até a tela de investigação que terá todos os dados.

A lista de tabelas secundárias em um ponto de entrada também é configurável. Para obter mais informações, consulte Configurar investigação de tempo de design de SI.

A seguir está um exemplo detalhado de um ponto de entrada (observável associado) que é configurado e provisionado no sistema de base:

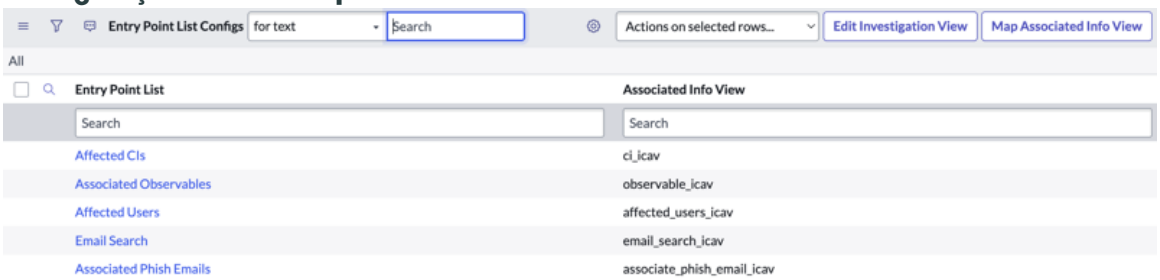
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Selecione o ponto de entrada **Observáveis associados** na lista suspensa.

   Aqui, a tabela primária também é **Observável associado**.

Configurações de lista de ponto de entrada



2. Selecione um ou mais observáveis da tabela primária.
3. Execute a funcionalidade desejada.

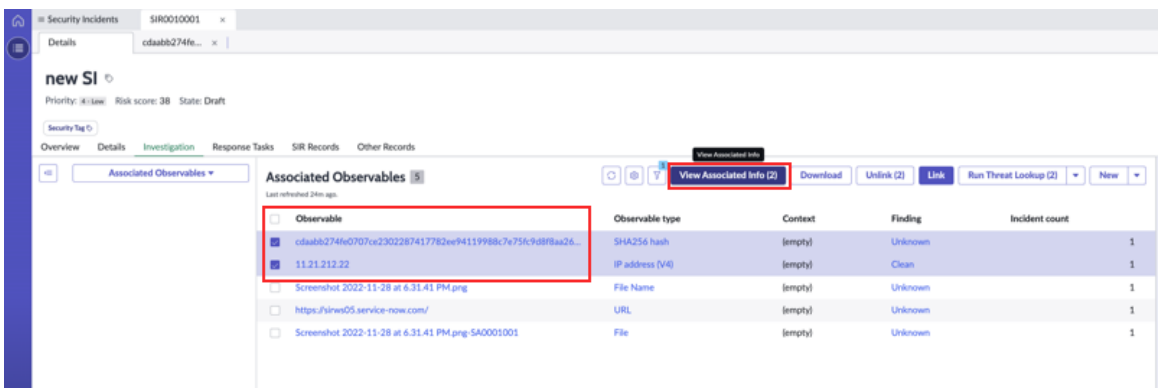
   Por exemplo, selecione **Executar pesquisa de ameaças** para buscar os resultados da pesquisa de ameaças para um observável selecionado.

> **Nota:**
> Quando uma ação observável correspondente é executada, o processo é executado no back-end e os resultados são exibidos abaixo da lista Observáveis.

4. Clique em **Exibir informações associadas** para exibir os resultados dos observáveis. Os resultados são exibidos na mesma página.

> **Nota:**
> Você pode exibir os resultados usando filtros por resultados, selecione **Todos os resultados** ou **Resultados mais recentes**, qualquer que seja a exibição desejada. Por padrão, os resultados mais recentes são exibidos. Se houver várias implementações (de integrações), os resultados mais recentes por implementação serão mostrados.

Além disso, você pode filtrar os resultados **por listas relacionadas associadas,** que são os resultados da tabela secundária. Por padrão, todas as listas relacionadas à tabela secundária configurada são exibidas. Para obter mais informações, consulte Configurar investigação de tempo de design de SI. No entanto, você pode optar por selecionar somente as tabelas secundárias necessárias.



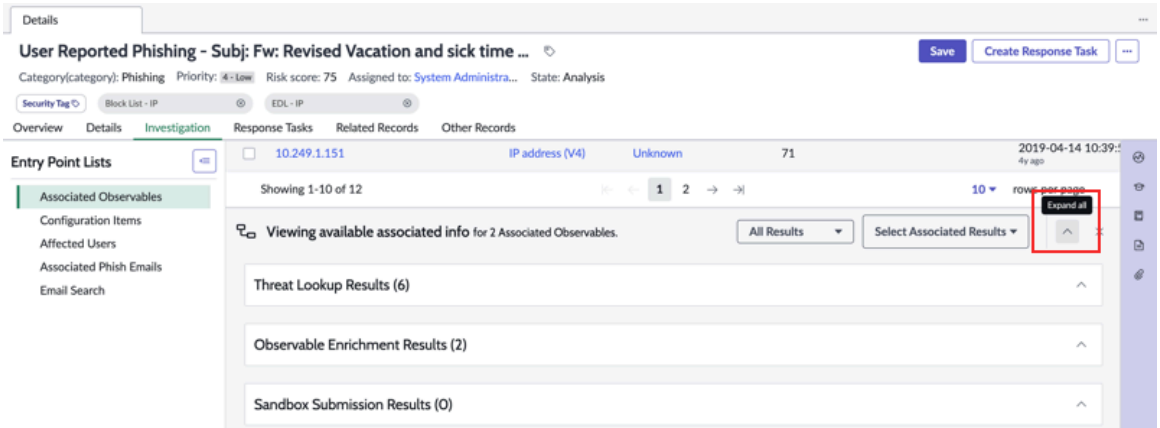
5. Ao clicar em **Exibir informações associadas,** você pode exibir todos os dados da tabela secundária associada em um só lugar. No entanto, você pode fechar a exibição de listas

Tradução automática

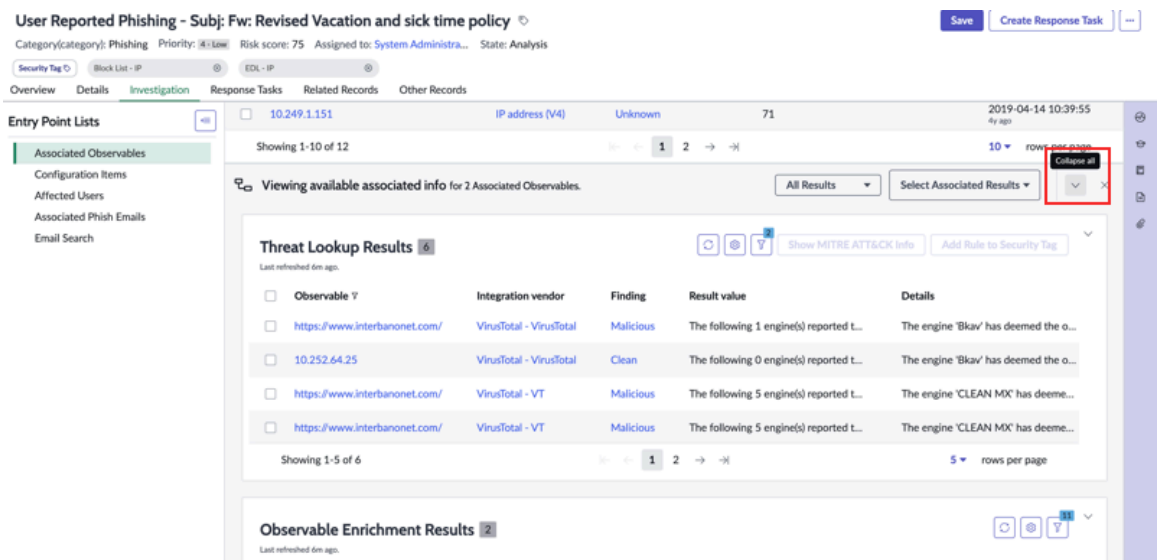
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

relacionadas selecionando o botão **Fechar exibição**. Depois de fechar a exibição, você só poderá ver a tabela primária de observáveis como antes.

6. Clique no ícone **Expandir tudo** na direção ascendente na tabela **Exibição de resultados de informações associadas disponíveis** para expandir todos os dados da tabela secundária de todas as listas relacionadas.



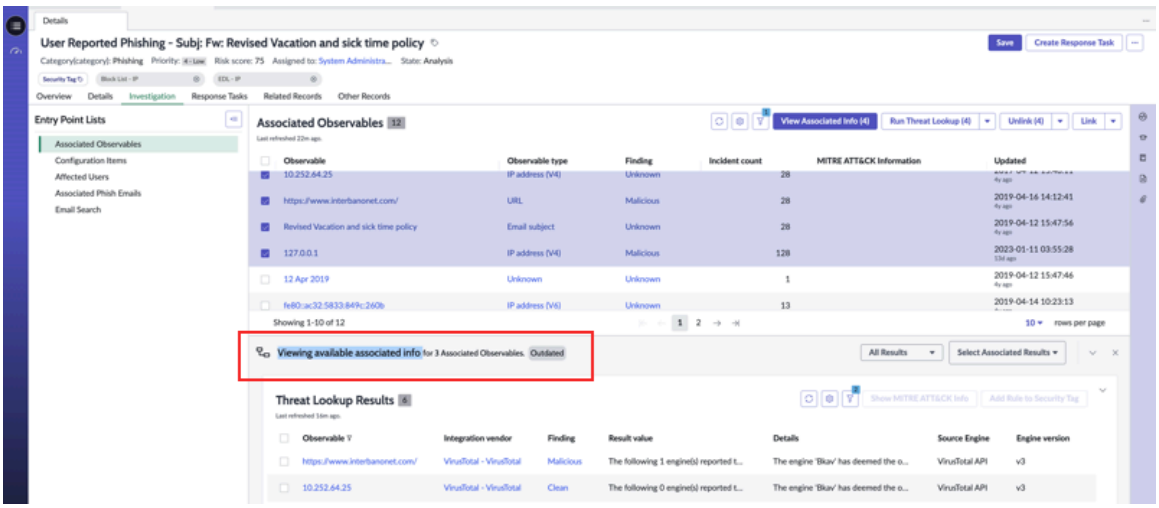
7. Clique em **Recolher tudo** ícone de direção descendente para recolher todos os dados da tabela secundária das listas relacionadas.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A faixa na parte superior da seção de informações associada que contém todos os dados da tabela secundária mostra quantas informações relacionadas ao observável estão sendo apresentadas ao usuário. Por exemplo, inicialmente, se você selecionar dois observáveis e clicar em **Exibir informações associadas**, a faixa mostrará **Exibindo informações associadas disponíveis para 2 observáveis associados.**. Se você selecionar, por exemplo, outro observável, a faixa informará que as informações estão desatualizadas (captura de tela abaixo). Você precisará clicar em **Exibir informações associadas** novamente para obter os dados mais recentes.



Além da exibição abrangente acima das informações associadas aos observáveis, se você quiser exibir mais informações sobre um registro na tabela primária, clique no observável e o formulário de registro da tabela primária será aberto em uma guia diferente com uma exibição mais detalhada do registro selecionado. Todos os dados da tabela secundária associados desse registro selecionado específico também são apresentados na seção **Informações associadas**.

No entanto, a seção de informações associada exibe somente os resultados mais recentes da tabela secundária, conforme visto na tela de investigação, no modo somente leitura. Nenhuma ação é possível nesta exibição. A página de formulário da tabela secundária pode ser aberta em uma nova guia que renderizará a página totalmente funcional com quaisquer ações, se houver.

Você pode alternar entre as diferentes tabelas usando a lista suspensa. Você também pode expandir ou recolher cada formulário na seção de informações associada.

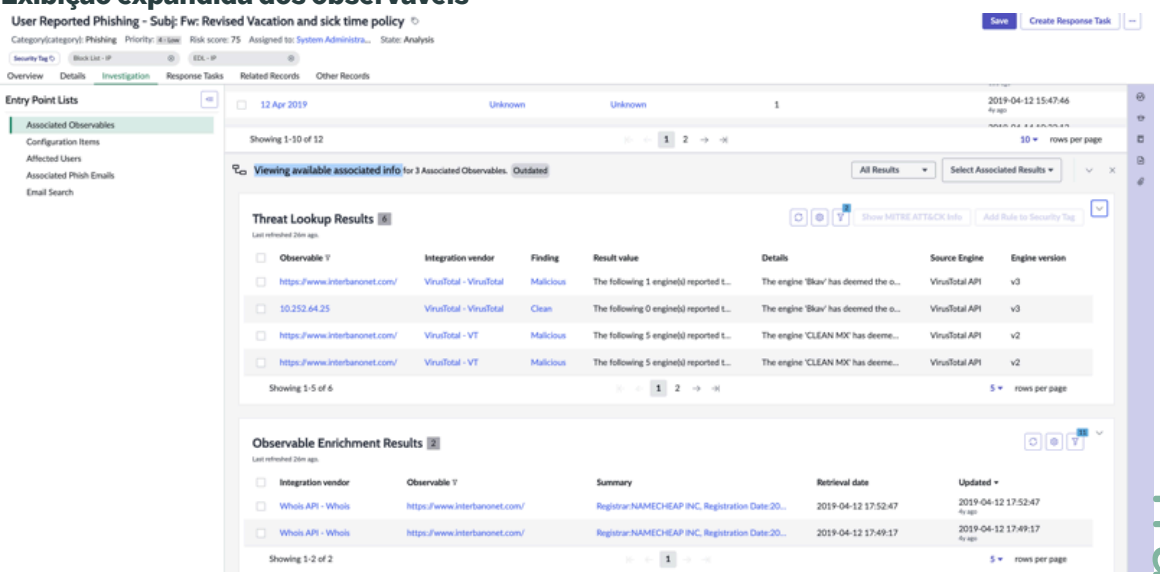
Na página de formulário do **Observável** (página de formulário de registro da tabela primária), você pode executar determinadas ações conforme disponíveis. Sempre que você executar uma ação, poderá clicar em Atualizar na faixa de informações associada para atualizar os dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Clique em **Expandir tudo** para expandir todas as tabelas secundárias de listas relacionadas. Por padrão, todos os secundários são expandidos.

Exibição expandida dos observáveis



Tópicos relacionados

Configurar investigação de tempo de design de SI

Estrutura de experiência unificada para integrações com tecnologia do Capability Framework

Na IU clássica, a experiência é desconectada ao executar atividades de orquestração, como executar a aparência de ameaça, executar a pesquisa de vista e assim por diante. Cada recurso tem sua própria experiência ao executá-lo. No novo espaço, há uma experiência unificada em todos os recursos.

A experiência unificada é aplicável somente para as integrações e atividades de orquestração que se enquadram na estrutura de recursos. Pode haver ações específicas para a integração, por exemplo, Criar indicadores no Microsoft Defender. Essas ações terão sua própria experiência, conforme exigido pelo caso de uso.

A nova estrutura consiste em telas modais com três etapas, conforme explicado abaixo.

1. **Implementações**: a primeira etapa envolve a seleção de uma ou mais implementações que estão presentes em relação ao recurso selecionado.

   Por exemplo, quando o analista clicar em **Executar pesquisa de ameaças**, ele poderá selecionar uma ou mais implementações presentes para a **capacidade Executar pesquisa de ameaças**.

   Cada implementação terá os detalhes da origem da integração. Consulte a tabela abaixo. Informações adicionais também são apresentadas em relação a cada implementação.

   As informações adicionais podem incluir, por exemplo, informações sobre filtros, tipos de observáveis compatíveis etc. As informações adicionais podem ser configuradas conforme desejado. Para obter mais informações, consulte o procedimento de configuração técnica da estrutura de UX.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

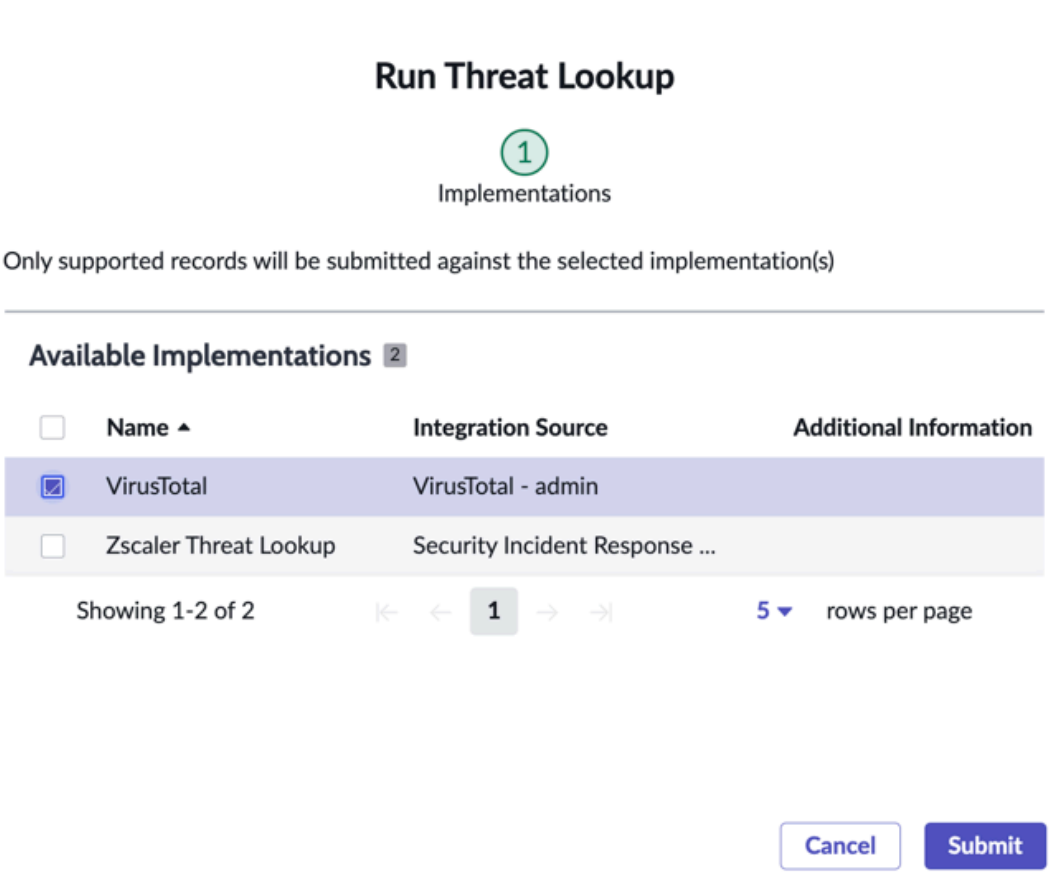
Modal da Estrutura de implementação unificada

Implementação	Descrição
Nome	Nome da implementação.
Origem da Integração	A origem da implementação, como a configuração que está sendo usada.
Informação adicional	Esta coluna captura as informações estáticas que adicionam mais contexto ao analista de segurança em relação às implementações selecionadas para prosseguir com uma ação. Por exemplo, suporte ou informações filtradas. Além disso, se uma implementação oferecer suporte a apenas determinados tipos de observáveis, como domínio ou URL, você poderá adicionar essas informações adicionais aqui nesta coluna para fornecer o contexto ao usuário. **Nota:** A estrutura de IU basicamente permitiria a seleção de qualquer tipo de implementação e qualquer tipo de observável. Durante o envio, as integrações do sistema de base existentes que são enviadas cuidarão da filtragem no back-end e enviarão somente o tipo compatível de observáveis. O restante dos registros que não correspondem à suporte será ignorado. Portanto, uma mensagem de informação de IU é exibida ao selecionar o recurso: **Somente registros compatíveis serão enviados em relação às implementações selecionadas.**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tela 1: Implementações

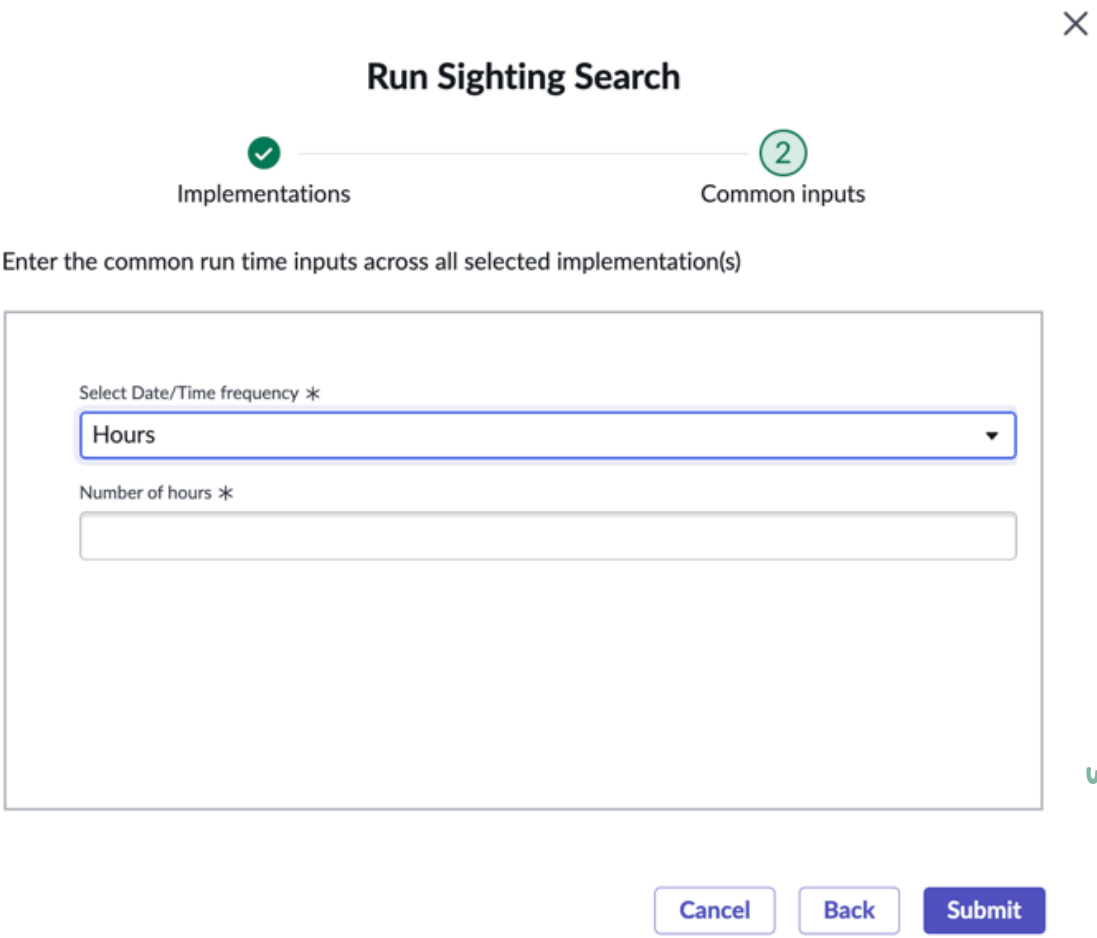


2. **Entradas comuns**: adicione entradas comuns para as implementações selecionadas ou para todas as implementações aplicáveis selecionadas. Esta é a tela 2 da sua implementação. Por exemplo, a partir de agora, somente a **Pesquisa de detecções** tem a tela de entradas comuns. Esta implementação é uma combinação da tela 1 (implementações) e da tela 2 (entradas comuns).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tela 1 + Tela 2



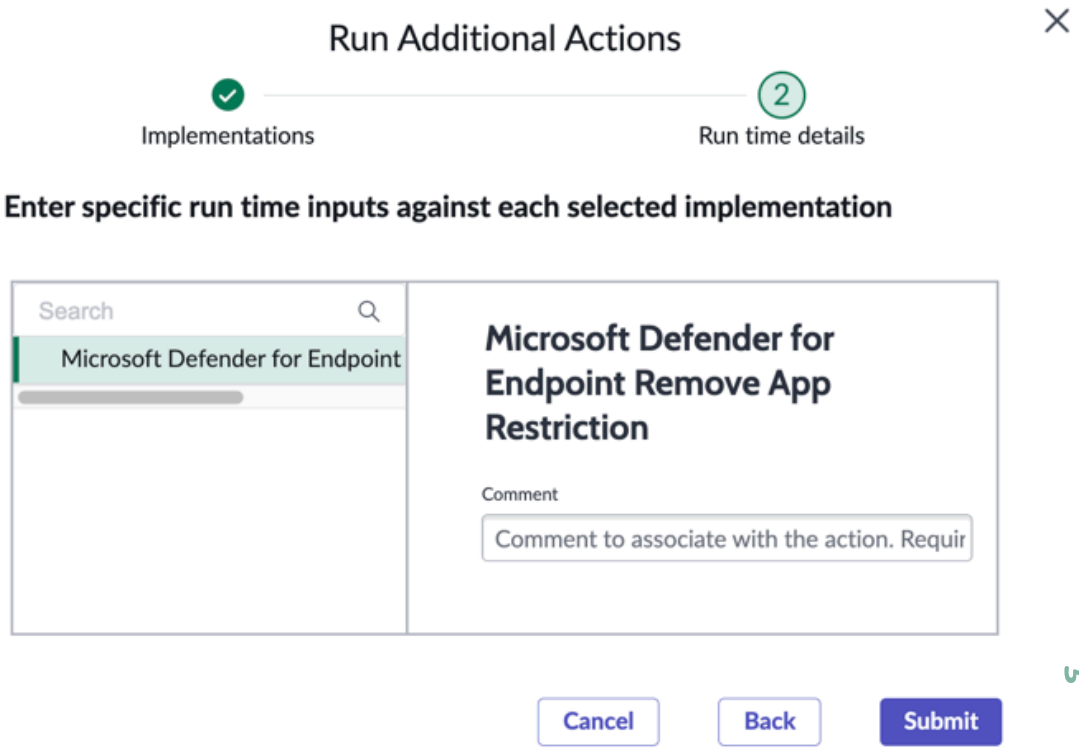
3. **Detalhes do tempo de execução**: adicione entradas de tempo de execução específicas para as implementações selecionadas que são diferentes umas das outras implementações. Esta é a tela 3 da sua implementação. Esta implementação é uma

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

combinação da tela 1 (implementações) e da tela 3 (entradas de tempo de execução específicas).

Entradas específicas



Nota:
Nem todas as três etapas são sempre necessárias. Dependendo da capacidade e do tipo de entradas necessárias, a etapa de detalhes do tempo de execução e a etapa de entradas comuns ficarão visíveis.

Capacidades de experiência unificada e telas de modal

A tabela a seguir abaixo descreve os recursos e as telas aplicáveis.

Exemplo de experiência unificada

Este exemplo demonstra os recursos da estrutura de experiência unificada.

Exemplo 1: selecionar implementações: pesquisa de ameaças

O exemplo abaixo demonstra as implementações.

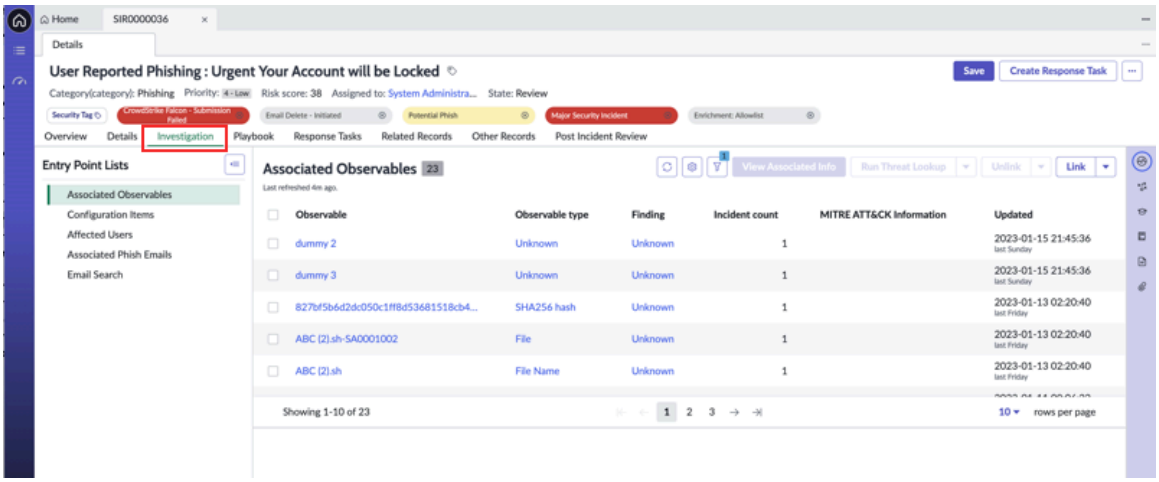
Exemplo 1: somente tela 1: pesquisa de ameaças

Você pode executar a ação **Executar recursos de integração relacionados à pesquisa de ameaças** usando a guia **Investigação** do SIR Workspace.

1. Na guia **Investigação**, navegue até a seção **Listas de pontos de entrada** exibida no lado esquerdo da página.
2. Selecione qualquer ponto de entrada e execute a ação de recurso de integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:
Você também pode navegar até a guia **Registros relacionados** no espaço de trabalho para executar a ação de recursos de integrações.

A**pesquisa de ameaças** é um dos exemplos que são descritos em detalhes sobre como executar as integrações.

Selecionar implementações

Selecione uma ou mais implementações, conforme aplicável.

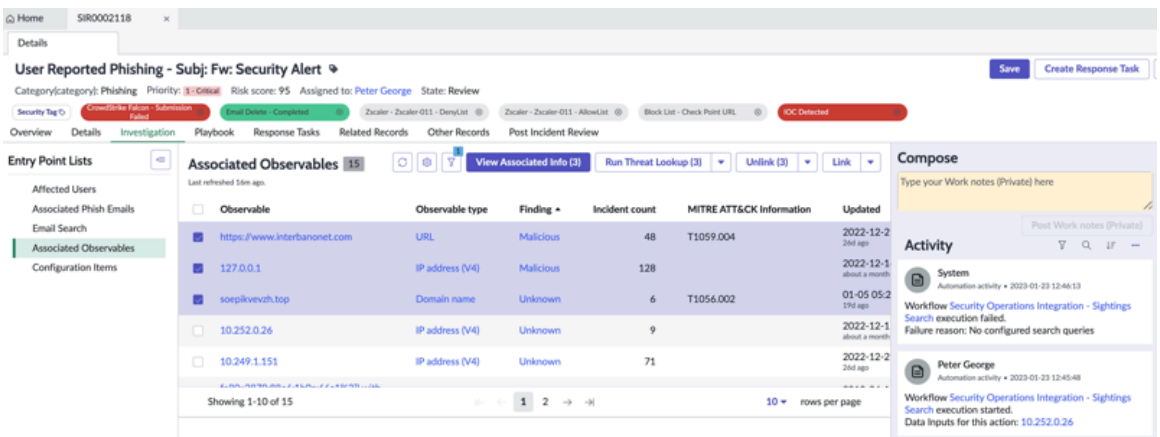
Antes de Iniciar

Função necessária: sn_si.analyst

As implementações disponíveis são listadas. Selecione as implementações. Depois de selecioná-las, somente os registros compatíveis serão enviados em relação a cada implementação selecionada.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Vá para a guia **Investigação** do espaço.
   A guia de investigação com as listas de pontos de entrada é exibida.



4. Selecione o observável associado nas listas de ponto de entrada.

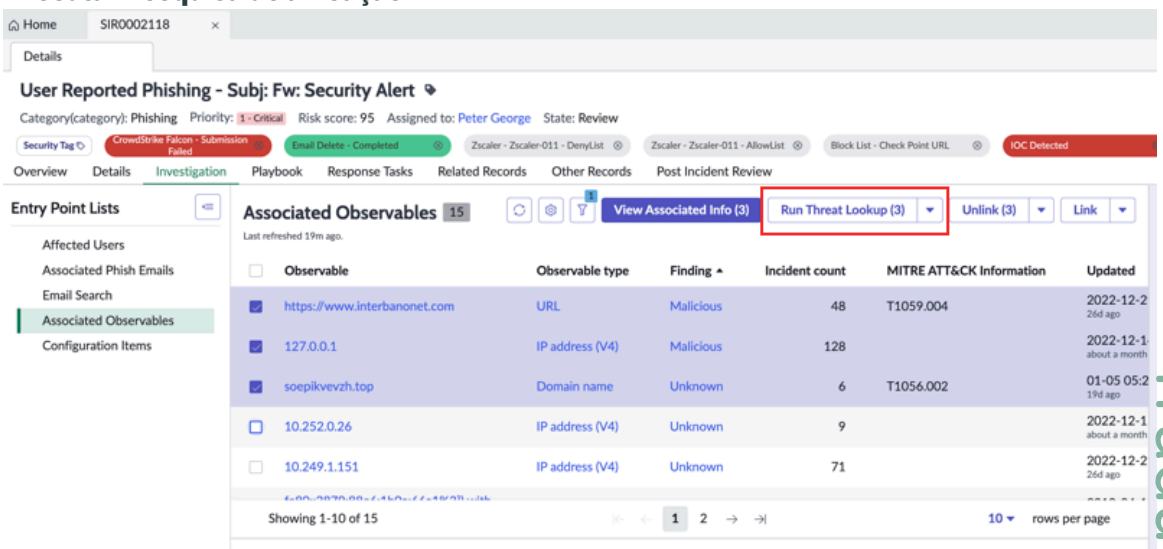
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, selecione **Observáveis Associados** lista relacionada. Os registros de observáveis correspondentes são exibidos.

Nota:
Você pode selecionar uma implementação para executar uma pesquisa nos observáveis selecionados ou pode executar a pesquisa selecionando todas as implementações.

Executar Pesquisa de ameaças



5. Marque a caixa de seleção de qualquer observável que você deseja executar a pesquisa de ameaças.
6. Navegue até o menu suspenso de ações das listas relacionadas que é exibido na parte superior da página de listas relacionadas.
7. Selecione **Executar pesquisa de ameaças** para executar a ação de recursos de integração relacionada às informações de ameaça.

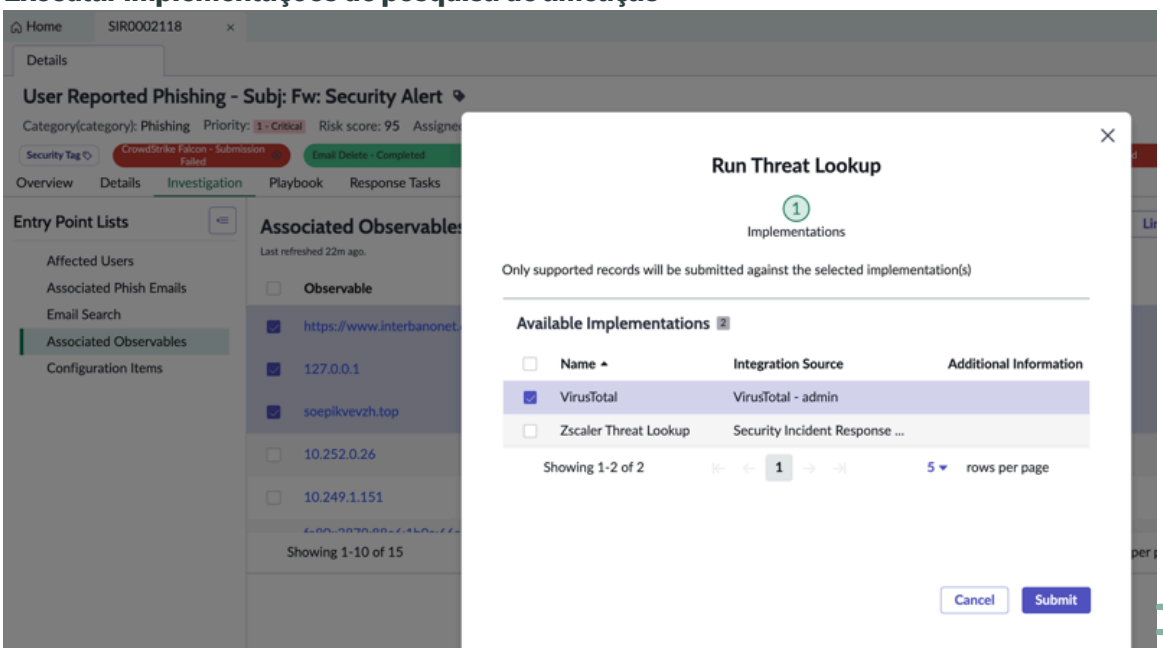
Nota:
A funcionalidade Executar pesquisas de ameaças realiza pesquisas de inteligência contra ameaças para determinar se um ou mais observáveis estão associados a ameaças de segurança conhecidas.

A tela do modal **Executar implementações de pesquisa de ameaças** é exibida.

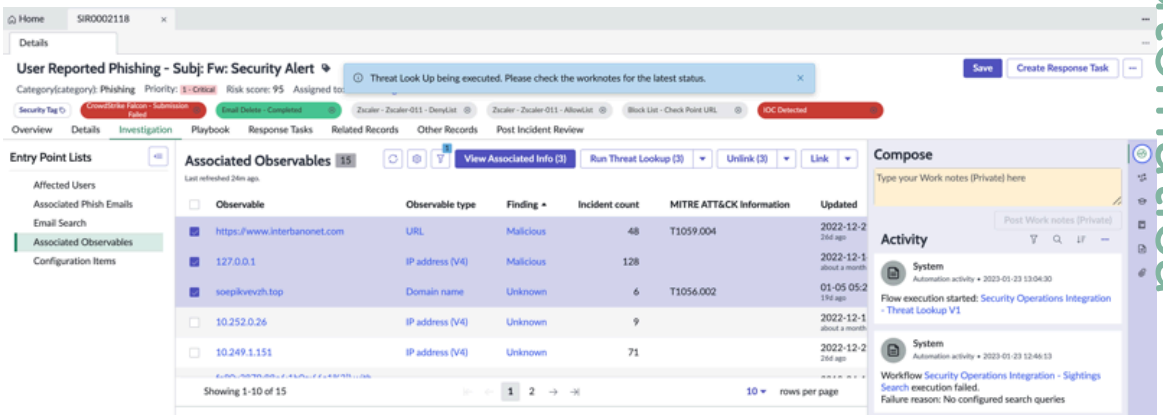
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Executar implementações de pesquisa de ameaças



8. Selecione uma ou mais implementações na lista.
9. Clique em **Enviar**.
   Depois que os registros selecionados forem enviados, será exibida uma mensagem informando que a pesquisa está sendo executada. Depois que a implementação é processada no back-end, os resultados são exibidos na seção da lista relacionada **Resultados da pesquisa de ameaças**. Além disso, a respectiva atividade de implementação é exibida na seção **Atividade**. Duas atividades são exibidas, uma é quando a execução da implementação é iniciada e a segunda é quando a execução é concluída.



Nota:
As listas relacionadas a informações sobre **ameaças**, como as listas relacionadas a observáveis associados, são exibidas na seção **Resultados da pesquisa de ameaças** e as listas relacionadas à **Pesquisa** de detecções são exibidas na seção **Resultados** da pesquisa de detecções em Registros relacionados.

Exemplo 2: entradas comuns: pesquisa de detecções

O exemplo abaixo demonstra a ação de recurso de entradas comuns.

Você pode executar a ação de recursos de integração relacionada **Executar pesquisa de detecções** usando a guia **Investigação** do SIR Workspace.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Na guia **Investigação**, navegue até a seção **Listas de pontos de entrada** exibida no lado esquerdo da página.
2. Selecione o respectivo ponto de entrada e execute a ação de recurso de integração.

Nota:
Você também pode navegar até a guia **Registros relacionados** no espaço de trabalho para executar a ação de recursos de integrações.

Adicionar entradas comuns a uma implementação

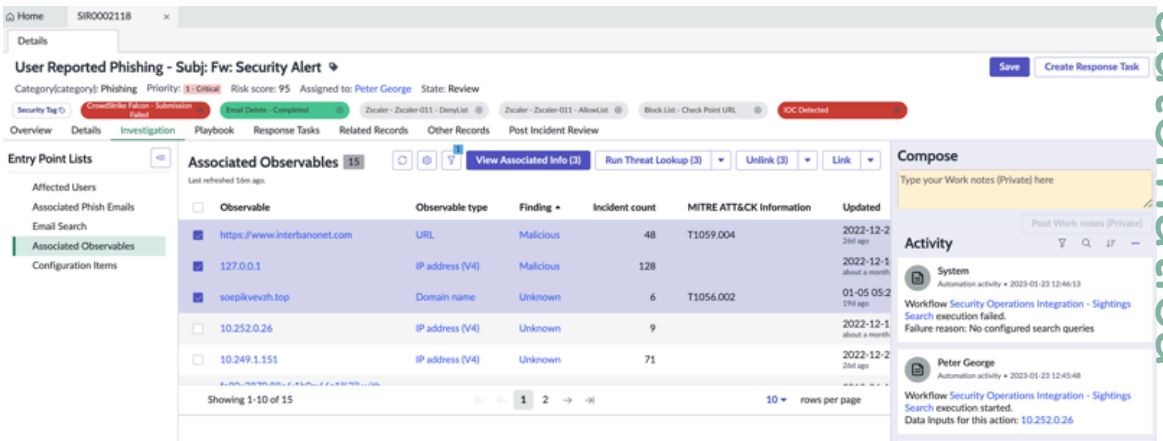
Adicione entradas de tempo de execução comuns que se apliquem a todas as implementações selecionadas, conforme aplicável.

Antes de Iniciar
Função necessária: sn_si.analyst

As implementações disponíveis são listadas. Selecione as implementações. Depois de selecioná-las, somente os registros compatíveis serão enviados em relação a cada implementação selecionada.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Vá para a guia **Investigação** do espaço.
   A guia de investigação com as listas de pontos de entrada é exibida.



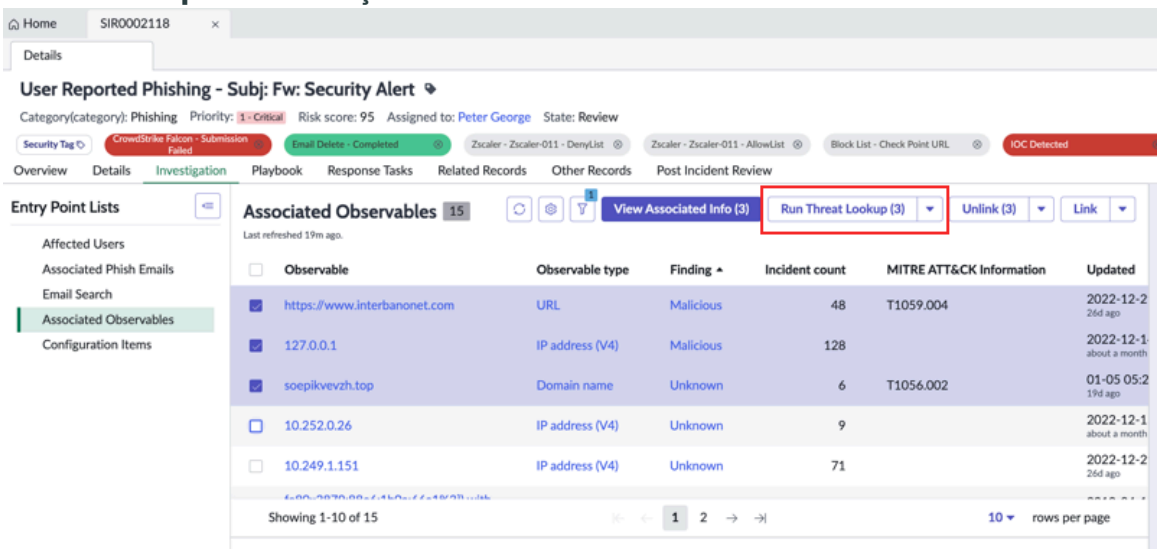
4. Selecione o observável associado nas listas de ponto de entrada.
   Por exemplo, selecione **Observáveis Associados** lista relacionada. Os registros de observáveis correspondentes são exibidos.

Nota:
Você pode selecionar uma implementação para executar uma pesquisa de vista para os observáveis selecionados ou selecionar várias implementações.

Tradução automática

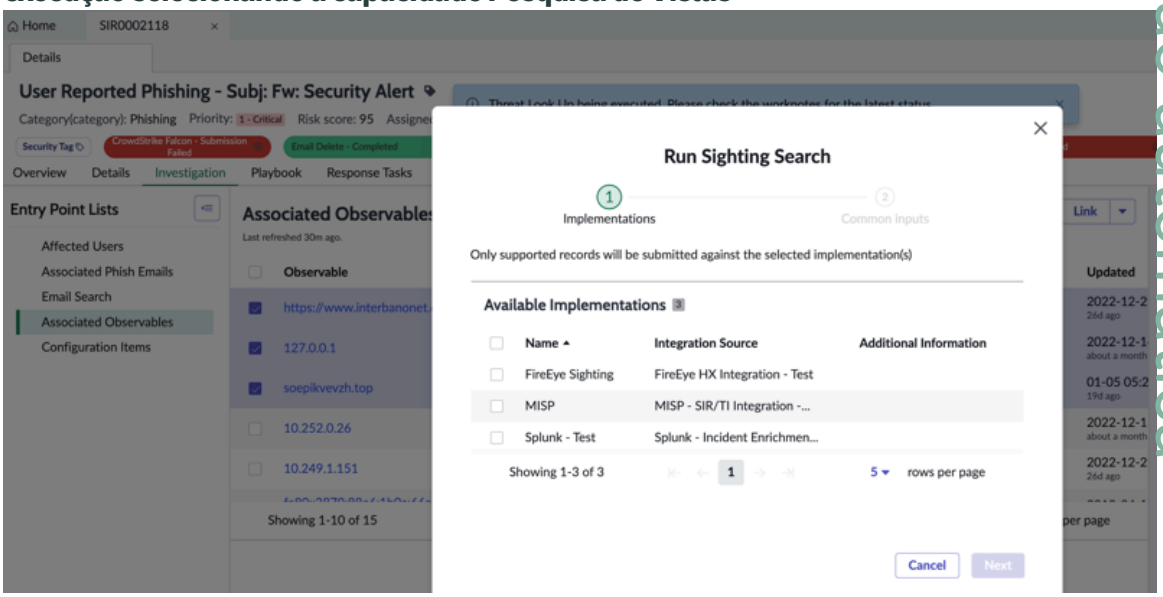
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Executar Pesquisa de ameaças



5. Marque a caixa de seleção de qualquer observável que você deseja executar a pesquisa de ameaças.
6. Selecione **Executar pesquisa de detecções** para realizar a pesquisa de e-mail.
   A caixa de diálogo modal Executar implementações de pesquisa de detecções é exibida.

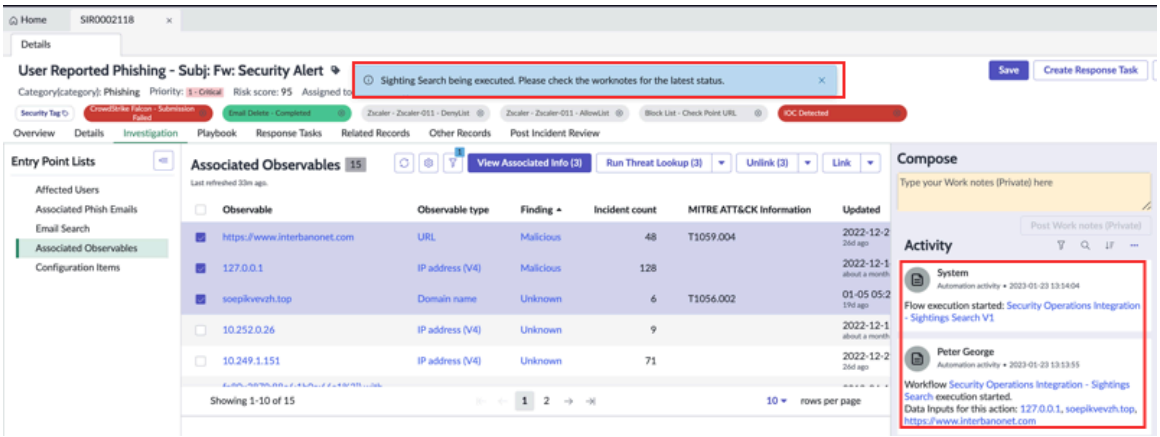
Um exemplo que mostra como adicionar entradas comuns de tempo de execução selecionando a capacidade Pesquisa de Vistas



7. Selecione uma ou mais implementações na lista.
8. Clique em **Avançar**.
   Depois que os registros selecionados forem enviados, será exibida uma mensagem informando que a pesquisa de vista está sendo solicitada. Depois que a implementação é processada no back-end, os resultados são exibidos na seção da lista relacionada **Pesquisa de detecções**. Além disso, a respectiva atividade de implementação é exibida na seção Atividade. Duas atividades são exibidas, uma é quando a execução da implementação é iniciada e a segunda é quando a execução é concluída.
9. Selecione o valor de entrada de tempo de execução comum.
10. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Depois que os registros selecionados forem enviados, será exibida uma mensagem informando que a pesquisa de vista está sendo solicitada. Depois que a implementação é processada no back-end, os resultados são exibidos na seção da lista relacionada **Resultados** da pesquisa de vistas. Além disso, o respectivo status de processamento da atividade de implementação é exibido na seção **Atividade**.

Exemplo 3: adicionar entradas de detalhes de tempo de execução específicas a uma implementação: Executar ações adicionais

Adicione entradas de detalhes de tempo de execução específicas a uma implementação, Executar ações adicionais.

Você pode executar a ação **Executar ações adicionais** relacionadas às capacidades de integração usando a guia **Investigação** do SIR Workspace.

1. Na guia **Investigação**, navegue até a seção **Listas de pontos de entrada** exibida no lado esquerdo da página.
2. Selecione o respectivo ponto de entrada e execute a ação de recurso de integração.

Nota:
Você também pode navegar até a guia **Registros relacionados** no espaço de trabalho para executar a ação de recursos de integrações.

Adicionar entradas específicas a uma implementação

Adicione entradas de tempo de execução específicas para cada implementação selecionada, conforme aplicável.

Antes de Iniciar
Função necessária: sn_si.analyst

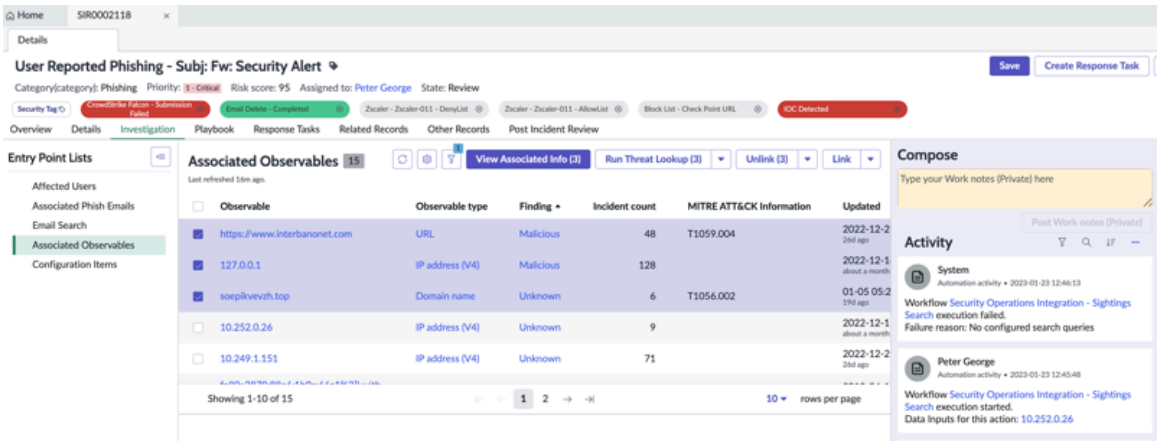
As implementações disponíveis são listadas. Selecione as implementações. Depois de selecioná-las, somente os registros compatíveis serão enviados em relação a cada implementação selecionada.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Vá para a guia **Investigação** do espaço.
   A guia de investigação com as listas de pontos de entrada é exibida.

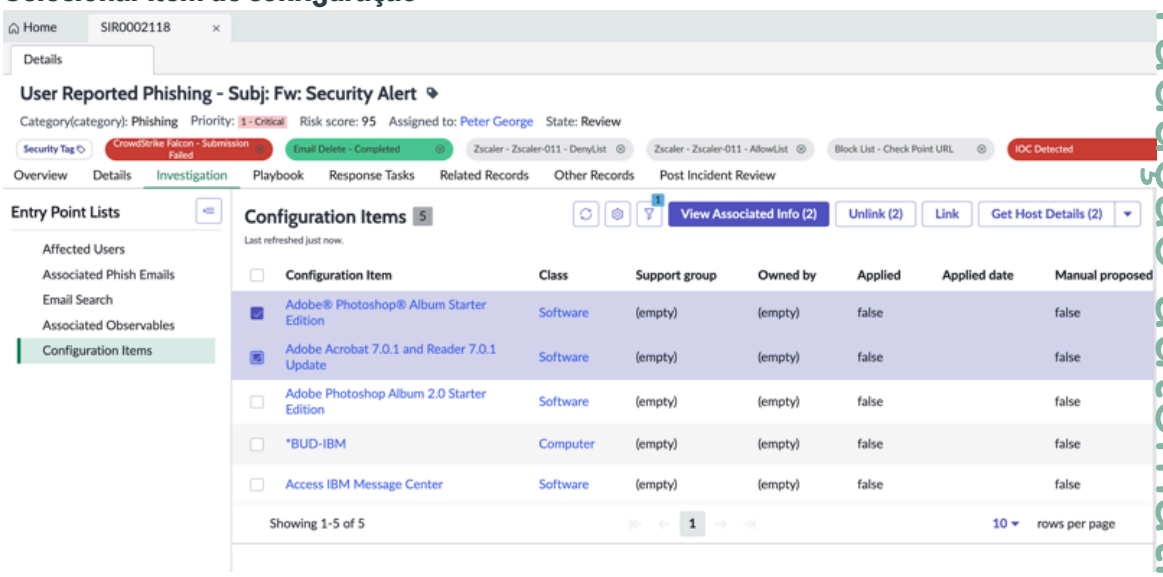
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Selecione o item de configuração na lista de ponto de entrada.
   Por exemplo, selecione a lista de ponto de entrada **do item de configuração**. Os registros de itens de configuração correspondentes são exibidos.

Selecionar item de configuração



5. Selecione qualquer **Item de configuração**.

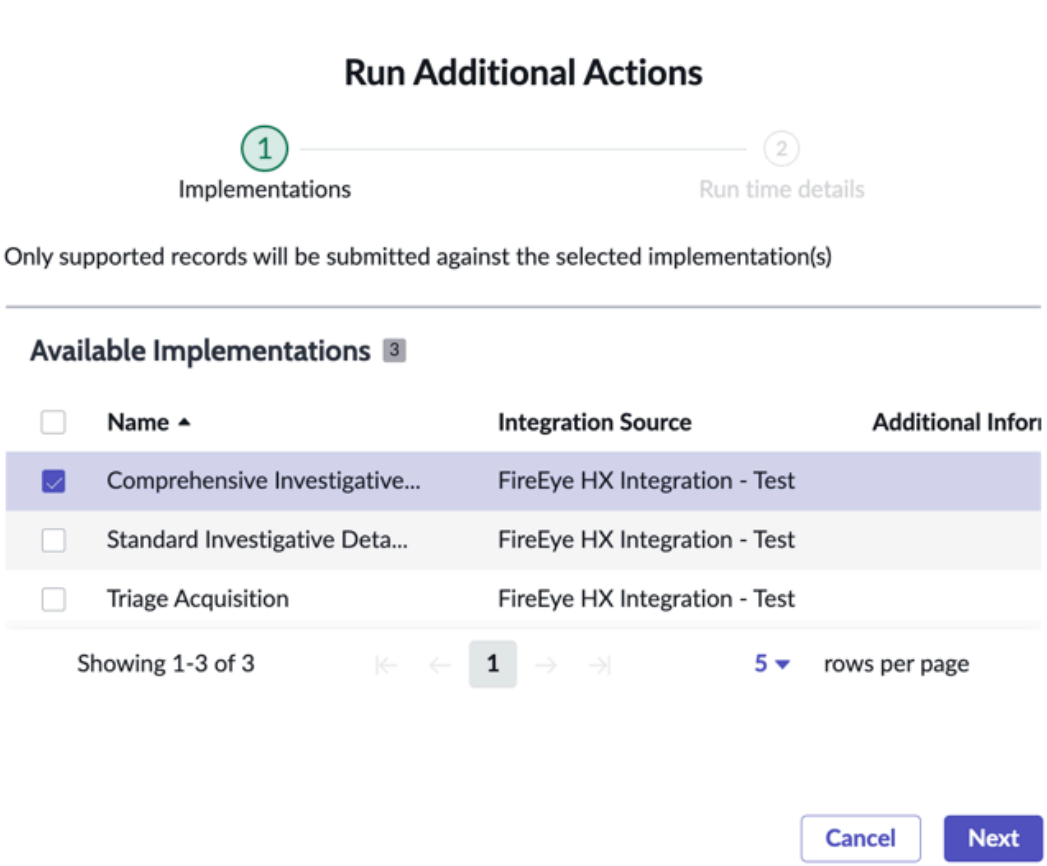
6. Navegue até as listas suspensas relacionadas exibidas na parte superior da página.
   Para o item de configuração (IC) de incidente de segurança, as listas suspensas contêm a seguinte lista de ações de recursos. As ações de IC listadas coletam os resultados e os armazenam como dados de aprimoramento em um incidente de segurança:
   - Obter arquivo: esta capacidade executa a ação para obter arquivos com um valor de hash específico ou um nome de arquivo.
   - Isolar host: esta capacidade restringe as conexões do sistema a outros dispositivos.
   - Obter detalhes do host: esta capacidade recupera os detalhes do host, detalhes de usuários conectados e outros recursos de aprimoramento.
   - Executar ações adicionais: esta capacidade executa as ações adicionais além das ações padrão.
   - Obter estatísticas de rede: esta capacidade recupera as estatísticas de rede de um recurso afetado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Obter processo em execução: esta capacidade recupera uma lista de processos em execução em um item de configuração (IC) de um host.
- Obter usuários conectados: esta capacidade reúne os dados de usuários conectados e os relaciona ao incidente de segurança.

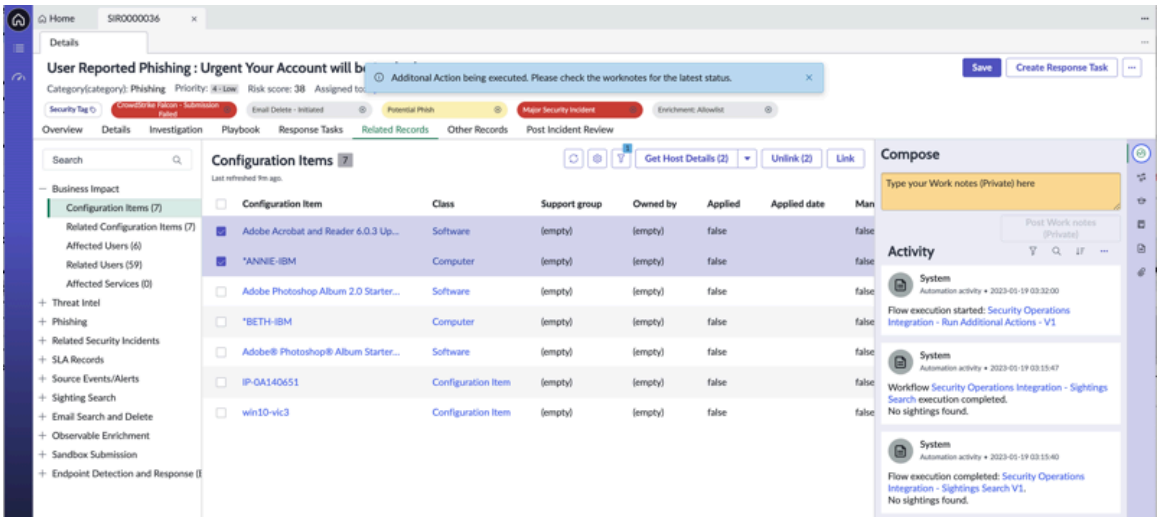
7. Selecione **Executar ações adicionais** para executar a ação de recursos de integração relacionados a informações de ameaça.
   A caixa de diálogo modal Executar implementações adicionais é exibida.
8. Selecione uma ou mais implementações na lista.



9. Clique em **Avançar**.
   Agora você será movido para a próxima etapa para adicionar os detalhes do tempo de execução.
10. Insira um comentário para associar à ação.
11. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Depois que os registros selecionados forem enviados, será exibida uma mensagem informando que a solicitação de ação adicional está sendo executada. Além disso, o respectivo andamento da ação de implementação é exibido na seção **Atividade**.

12. Exiba os resultados da seção da lista relacionada de EDR.

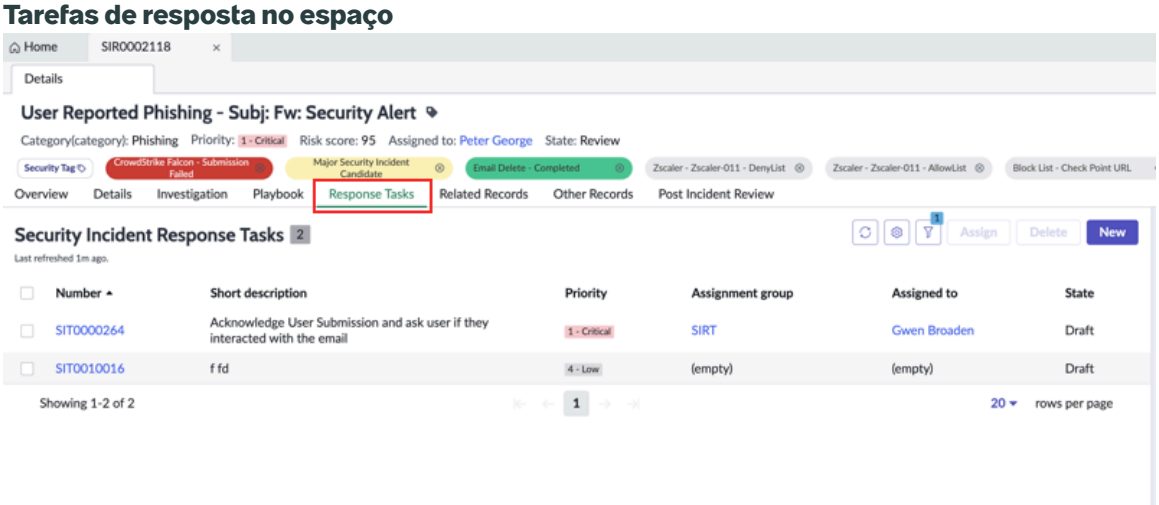
Tarefas do Security Incident Response

Todas as tarefas de resposta associadas a um incidente de segurança são exibidas na seção Tarefas de resposta.

O analista será capaz de:

- criar uma nova tarefa de resposta
- atribuir tarefas de resposta a si mesmo ou a outras pessoas
- excluir tarefas de resposta

Tarefas de resposta no espaço



Nota:
Para fazer edições rápidas nas tarefas de resposta. Selecione a tarefa de resposta e uma lista de tarefas de resposta será exibida, selecione o registro, faça mudanças e salve a tarefa de resposta.

Criar uma tarefa de resposta

Crie tarefas de resposta para rastrear ações separadas a serem executadas para responder ao problema de segurança.

Tradução automática

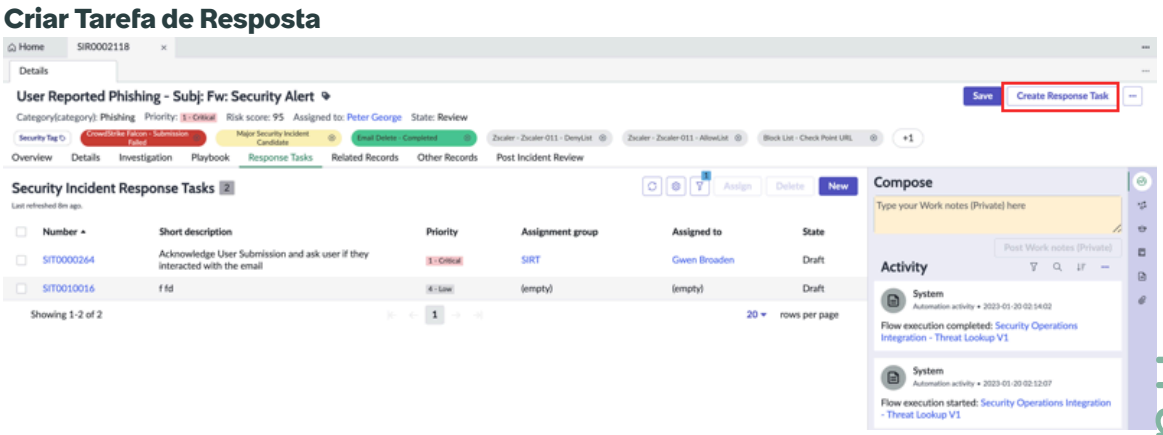
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Clique em **Criar tarefa de resposta** nas ações de IU.



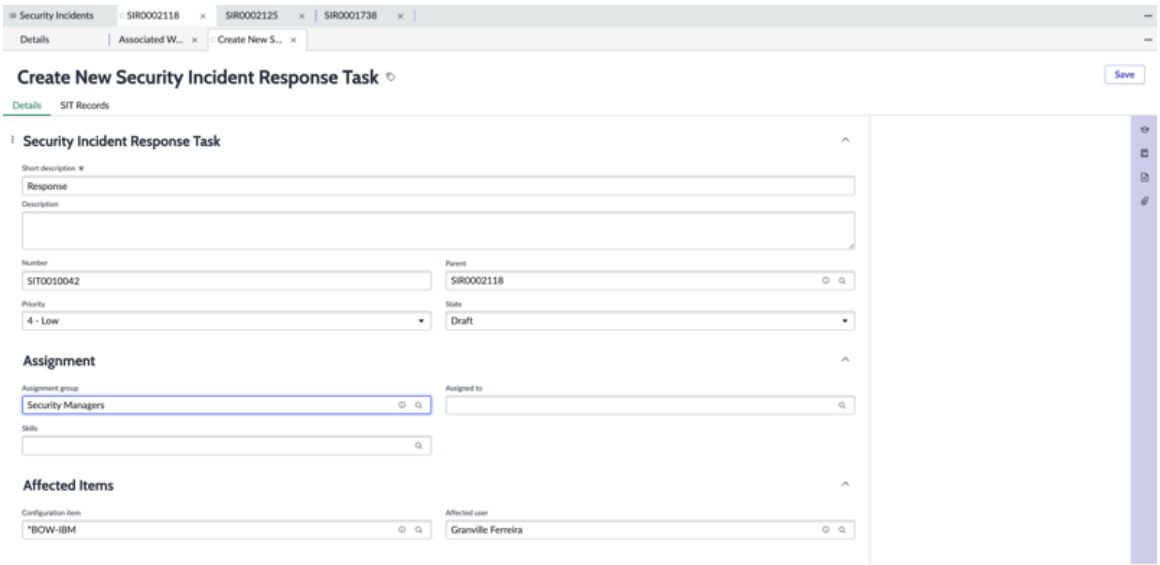
3. Preencha os campos no formulário, conforme apropriado.

Incidente de segurança

Campo	Descrição
Descrição resumida	Uma descrição da tarefa Security Incident Response.
Descrição	Uma descrição para a tarefa selecionada.
Número	Número exclusivo que é gerado automaticamente para um incidente de segurança.
Primário	O número do incidente de segurança relacionado.
Prioridade	A prioridade usada para determinar quando esta tarefa será realizada.
Estado	O estado atual da tarefa de resposta de segurança. Por padrão, o estado inicial é **Rascunho**.
Grupo de atribuição	O grupo de atribuição do qual o trabalhador atribuído é selecionado.
Atribuído a	O indivíduo atribuído para executar a tarefa.
Habilidades	A habilidade necessária para executar esta tarefa. Pesquise na pesquisa e selecione a habilidade necessária.
Itens afetados	Os itens afetados pelo problema de segurança.
Item de Configuração	O item de configuração afetado pelo problema de segurança.
Usuário afetado	A pessoa afetada pelo problema de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



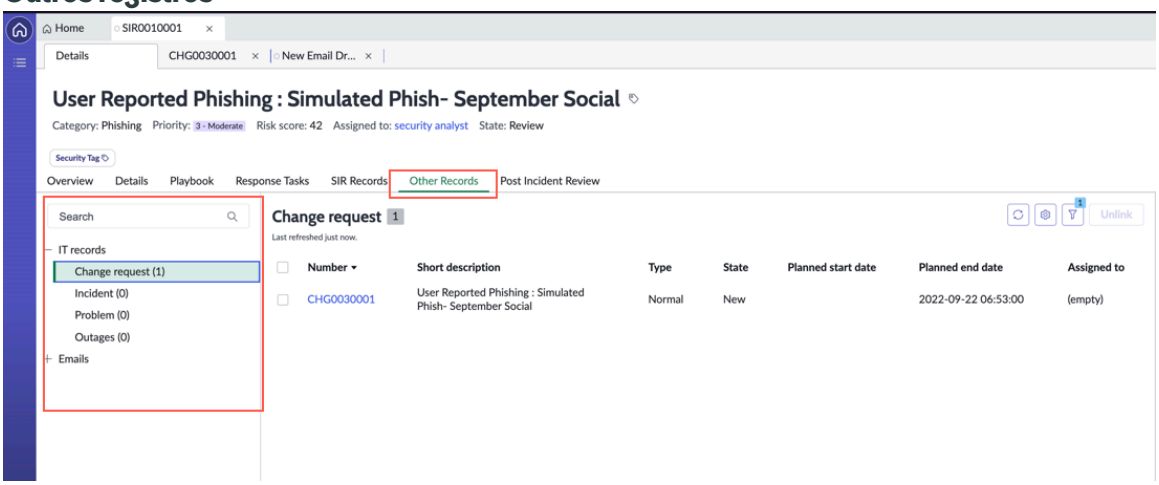
4. Clique em **Salvar**.
   A nova tarefa de resposta (SIT) é criada.

Outros registros do Security Incident Response

Esta seção exibe os outros registros, como registros relacionados a TI e registros de e-mail. Em registros de TI, são exibidos Incidente, Solicitação de mudança, Problema e Indisponibilidades.

Em E-mail, são exibidos Rascunho, E-mails enviados e E-mails recebidos.

Outros registros



Criar um incidente

Crie um incidente em um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst.

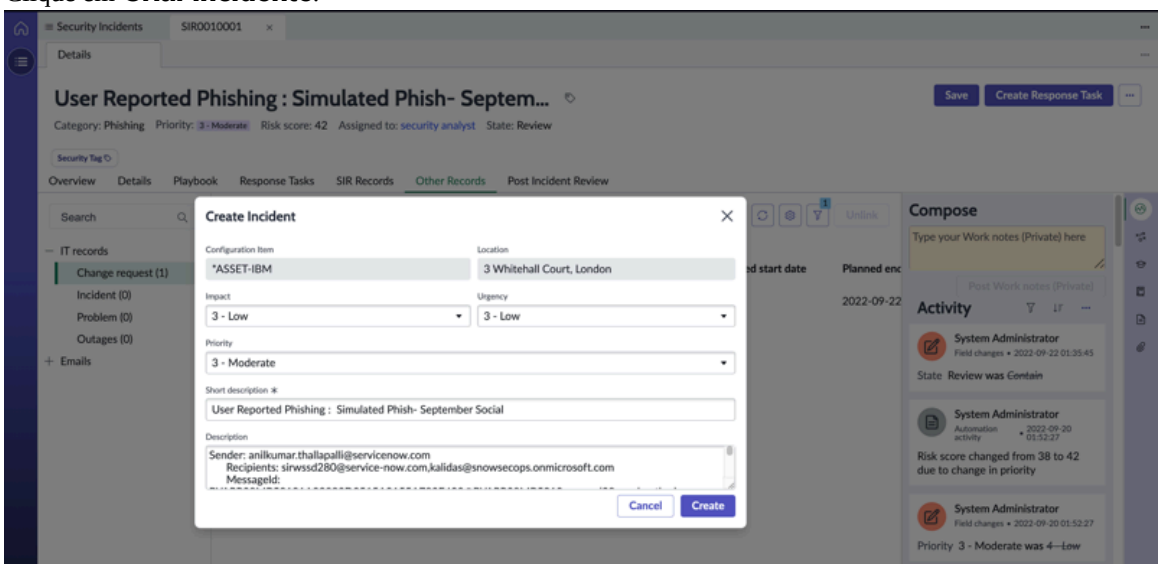
Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um registro de incidente.

Tradução automática

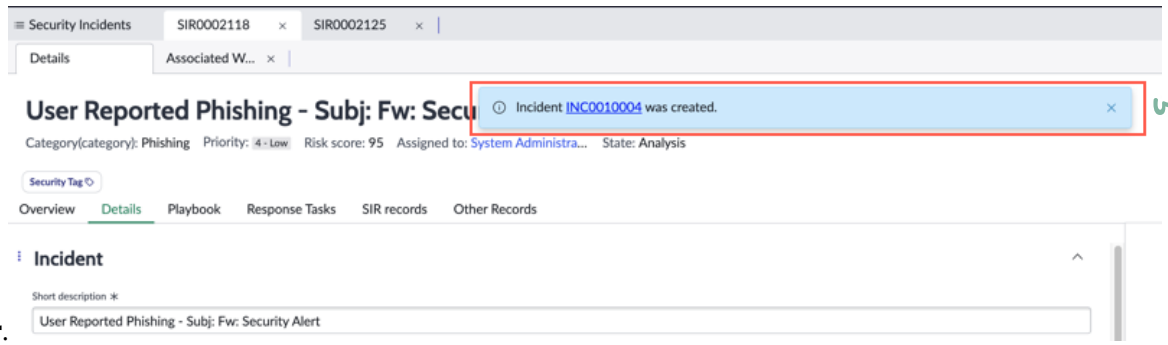
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique em **Criar incidente**.



4. Insira os detalhes como Item de configuração, Impacto, Urgência, Local, Prioridade e Descrição resumida.

5. Clique em **Criar**.



6. Um incidente é criado.

Como criar tarefa de problema

Crie uma tarefa de problema.

Antes de Iniciar

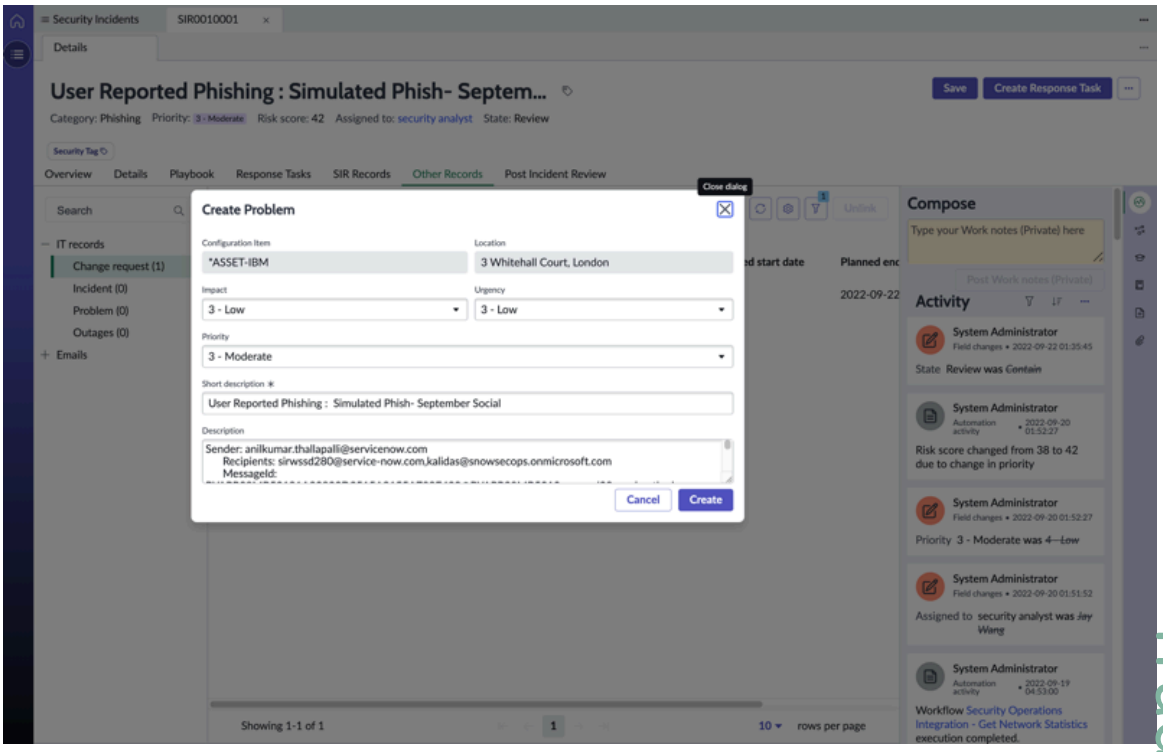
Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um registro de incidente.
3. Clique **em Criar problema**.

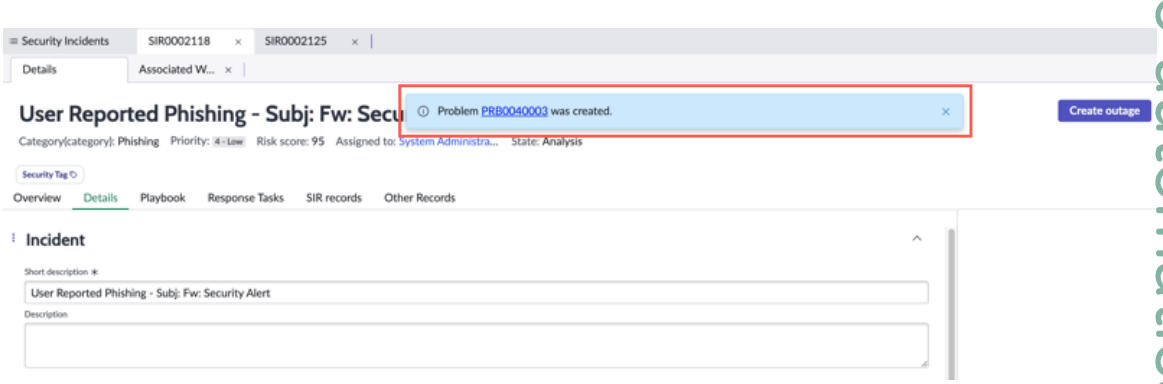
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Preencha os detalhes como Item de configuração, Local, Impacto, Urgência, Prioridade e Descrição resumida.

5. Clique em **Criar**.



6. Uma tarefa de problema é criada.

Criar uma solicitação de mudança

Crie uma solicitação de mudança.

Antes de Iniciar

Função necessária: sn_si.analyst.

Procedimento

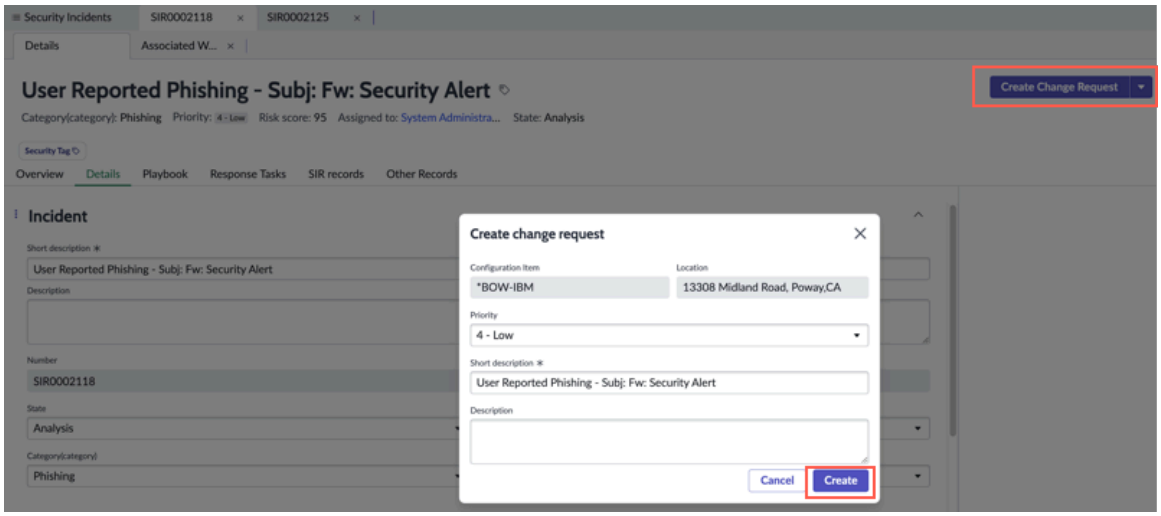
1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.

2. Abra um registro de incidente.

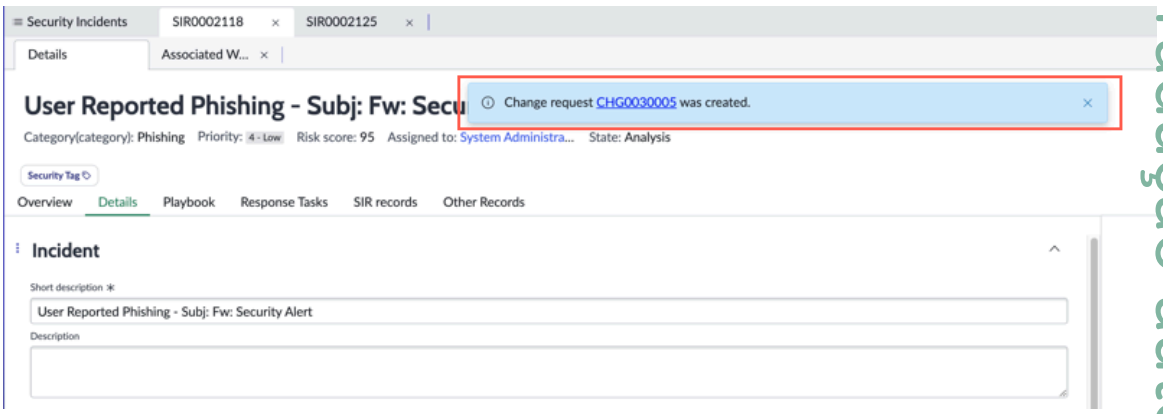
3. Clique **em Criar solicitação de mudança**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Insira os detalhes como Item de configuração, Local, Prioridade e Descrição resumida.
5. Clique em **Criar**.



6. Uma solicitação de mudança é criada.

Criar indisponibilidade

Crie uma indisponibilidade a partir de um incidente para rastrear o tempo de inatividade de um item de configuração.

Antes de Iniciar

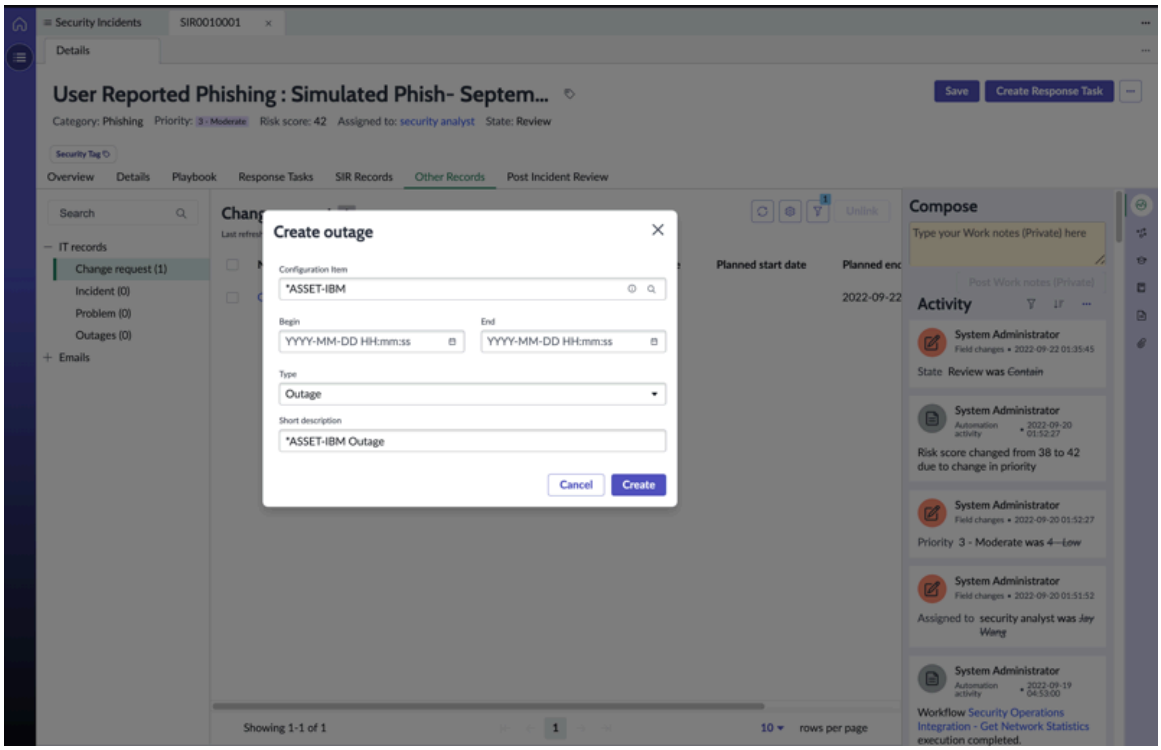
Função necessária: sn_si.analyst

Procedimento

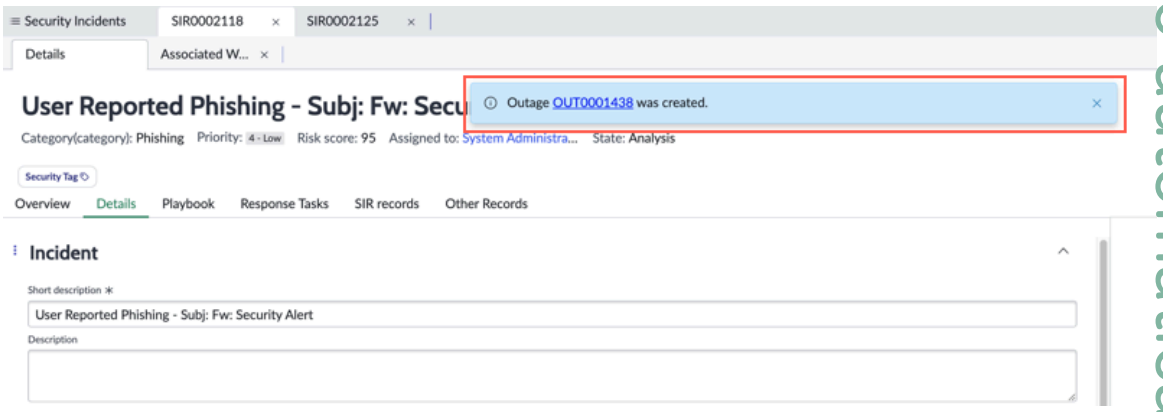
1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra um registro de incidente.
3. Clique **em Criar indisponibilidade**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Insira os detalhes, como Item de configuração, Data de início, Data de término, Tipo e Descrição resumida.
5. Clique em **Criar**.



Tradução automática

Compor e-mails

Como analista, você pode compor e-mails diretamente de incidentes de segurança.

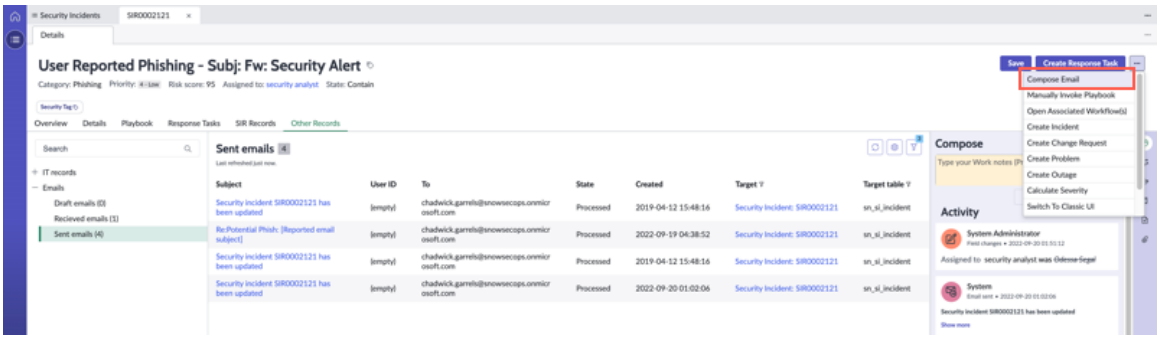
Antes de Iniciar

Função necessária: sn_si.analyst

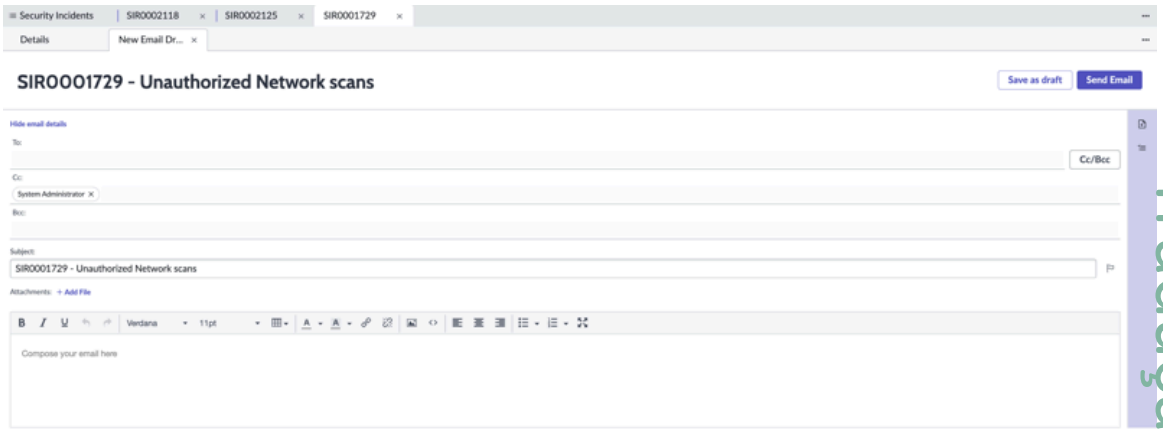
Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Selecione e abra o incidente para o qual você deseja compor um e-mail.
3. Clique no estouro e selecione **Compor e-mail**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

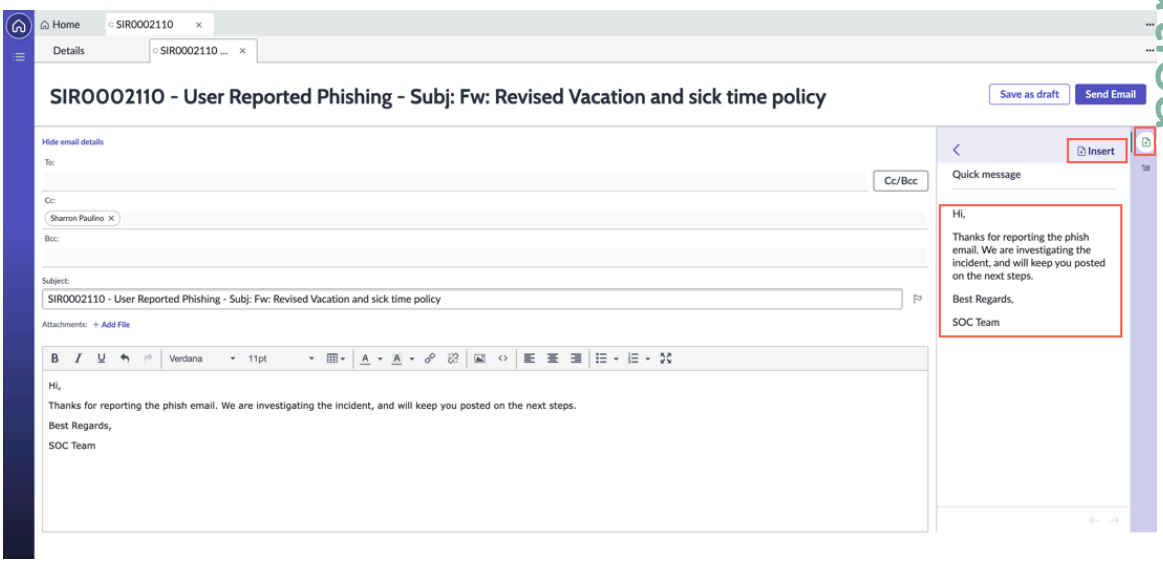


4. Insira o campo **Para** e **CC**.



5. **Adicione** anexos, se houver.

6. No formulário de e-mail, clique em **Mensagens rápidas** para exibir as mensagens rápidas exibidas no lado direito da seção **Compor e-mails**.
   As mensagens rápidas disponíveis são exibidas. Selecione a mensagem e clique em **Inserir**. As mensagens são inseridas no corpo do e-mail.



7. Componha seu e-mail e clique em **Enviar e-mail**.

Tradução automática

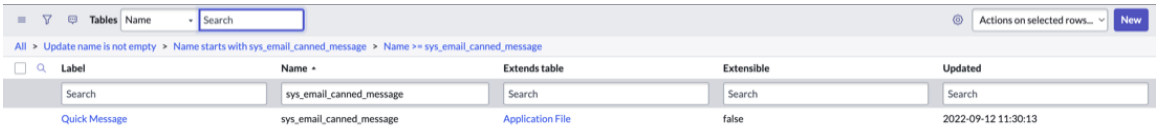
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Você pode salvar um e-mail como rascunho. Esses e-mails de rascunho estarão disponíveis na guia Outros registros.

Como configurar Mensagens Rápidas:

a. Navegar até **Definições do sistema** > **Tabelas**.

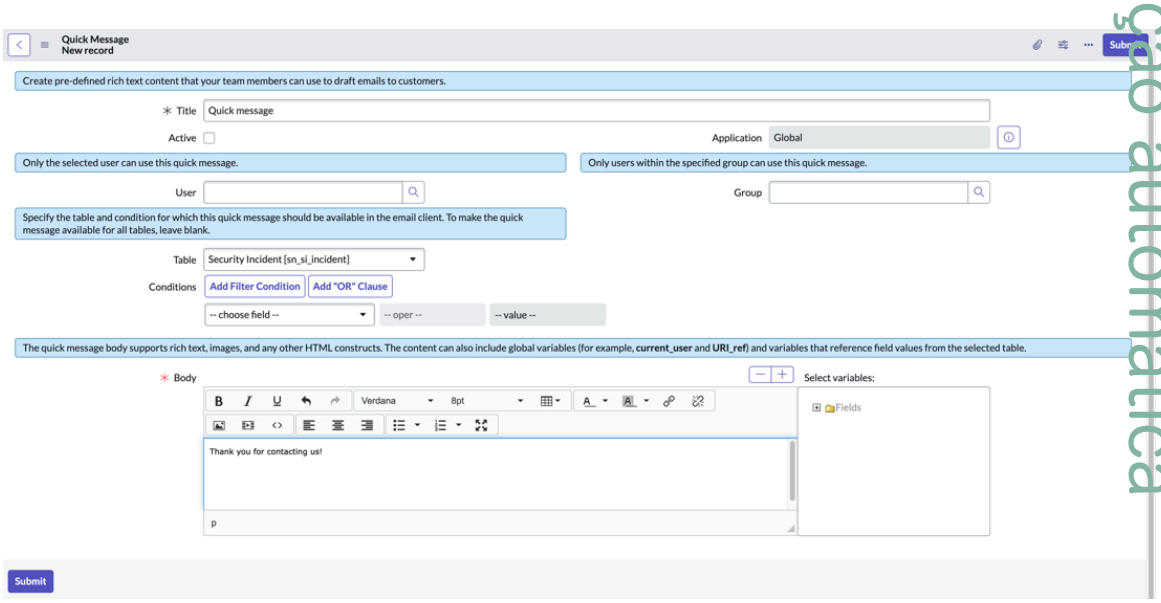
b. Pesquise a tabela **Mensagem rápida (sys_email_canned_message)**.



c. Ir para **Links relacionados** > **Mostrar lista**.

d. Criar **novo**.

e. Insira o **Título**, **o corpo da mensagem**, marque a **Tabela: Incidente de segurança (sn_si_incident)** e a caixa de seleção **Ativa**.



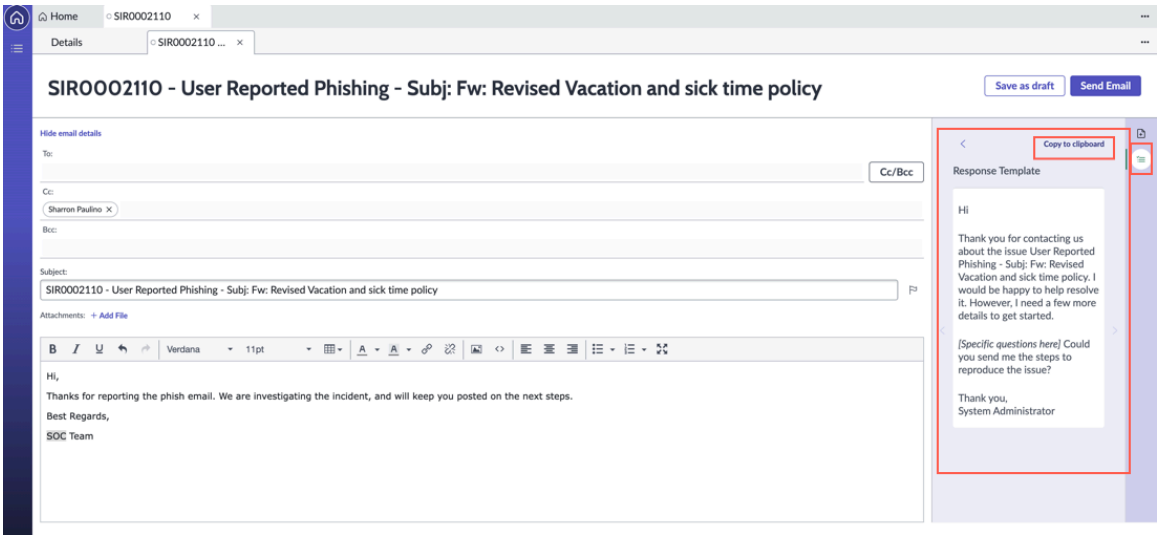
f. Clique em **Enviar**.
Depois que uma nova entrada é criada na tabela, a mensagem rápida aparece no menu contextual.

8. Clique em **Modelos** para adicionar qualquer modelo, se necessário.

9. Selecione o **Modelo de resposta**, clique em **Copiar para a área de transferência** e aplique o modelo, se necessário.

Tradução automática

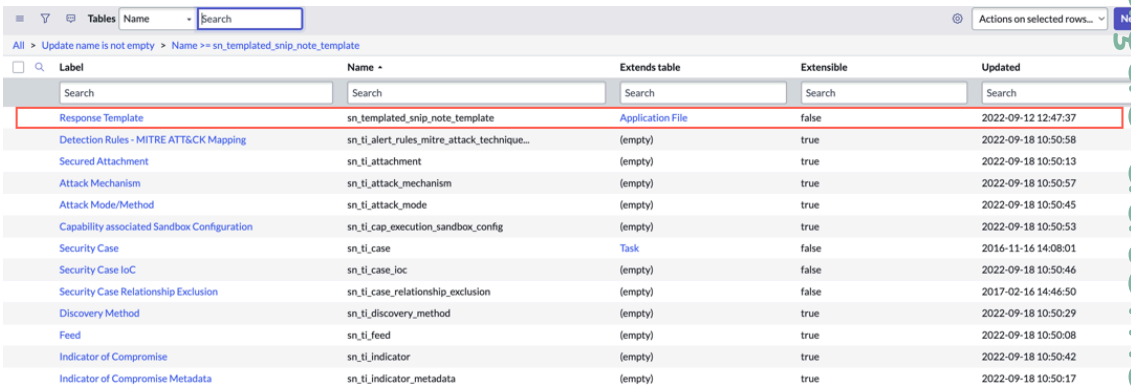
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Como configurar modelos de resposta:

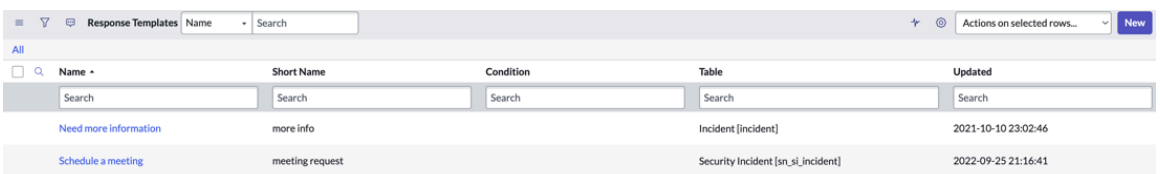
a. Navegar até **Definições do sistema** > **Tabelas**.

b. Pesquise a tabela **Modelo de resposta (sn_templated_snip_note_template)**.



c. Ir para **Links relacionados** > **Mostrar lista**.

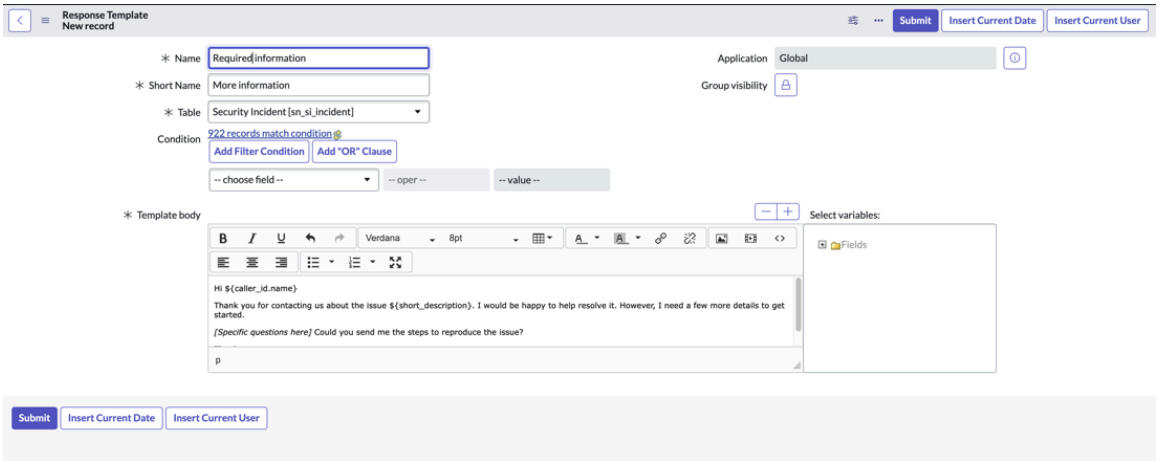
d. Criar **novo**.



e. Insira o **Nome**, **Nome Curto**, selecione a **Tabela: Incidente de segurança (sn_si_incident)** e **Corpo do modelo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



f. Clique em **Enviar**.
Depois que uma nova entrada é criada na tabela, o novo modelo aparece no menu contextual.

Análise pós-incidente do Security Incident Response

A revisão pós-incidente aparece quando um incidente é movido para um estado de revisão.

Para obter informações mais detalhadas sobre a realização das atividades pós-incidente, consulte Relatório de análise pós-incidente

A análise pós-incidente consiste nas seguintes seções:

1. Avaliações
2. Relatórios

No espaço do Security Incident Response, você poderá solicitar e fazer avaliações usando essas duas novas ações de IU.

Nome	Descrição
Avaliações	Avaliação exibe todas as avaliações associadas a outras avaliações de incidente de segurança. O analista poderá fazer avaliações e solicitar avaliações. • **Fazer avaliações**: clique em **Fazer avaliações** para fazer as avaliações (se aplicável) e concluir a avaliação. Antes de concluir a avaliação, o estado do incidente de segurança é Pronto para realizar e a data de vencimento do incidente é indicada em vermelho. • Solicitar avaliações: clique em **Solicitar avaliação** para obter avaliações adicionais

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	e adicionar os novos usuários que você deseja solicitar. **Nota:** Usuários que já solicitaram não aparecerão nesta seção. Qualquer avaliação para este incidente foi configurada com base nas condições definidas na análise pós-incidente, seja obrigatória ou opcional.
Relatórios	Modifique as configurações de tempo de execução e gere o relatório. Selecione a Instância de relatório, modifique os filtros e salve o relatório. O analista pode visualizar e baixar o relatório PIR.

Playbook de incidente de segurança

Invoque o fluxo do playbook de incidente de segurança automaticamente ou manualmente.

Um Playbook ficará visível somente se pelo menos um playbook estiver associado a um incidente de segurança. O componente do playbook funciona somente para os processos criados pelo Designer de automação de processos (PAD) e não para os fluxos criados pelo Flow Designer. Para os fluxos habilitados para o Flow Designer existentes, ele continuará a funcionar e as atividades continuarão a ser renderizadas como tarefas de resposta.

Existem duas maneiras de associar o playbook ao incidente de segurança:

- Invocar playbook automaticamente
- Adicionar playbook manualmente

Invocar playbook automaticamente

Para que um Playbook seja invocado automaticamente, um processo precisa ser definido usando o **Designer de automação de processos (PAD)**e, quando a condição do gatilho for atendida, automaticamente a guia do playbook será renderizada com as atividades do playbook sendo exibidas.

Adicionar playbook manualmente

Para que um Playbook seja invocado manualmente, navegue até a ação de IU Formulário e selecione **Adicionar Playbook**. Para obter mais informações, consulte, Adicionar Playbook

Nota:
Se já houver um playbook disponível, os novos playbooks adicionados serão executados em paralelo aos playbooks existentes.

- No playbook, o analista pode filtrar os cartões do playbook por status.
- O analista pode cancelar um playbook selecionando-o no ícone de elipse.

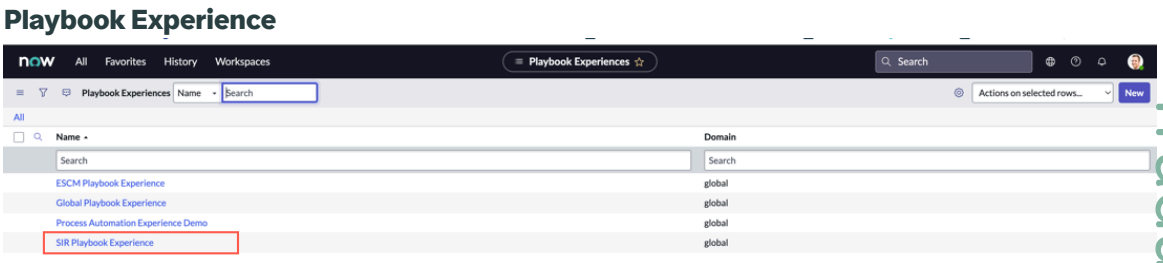
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

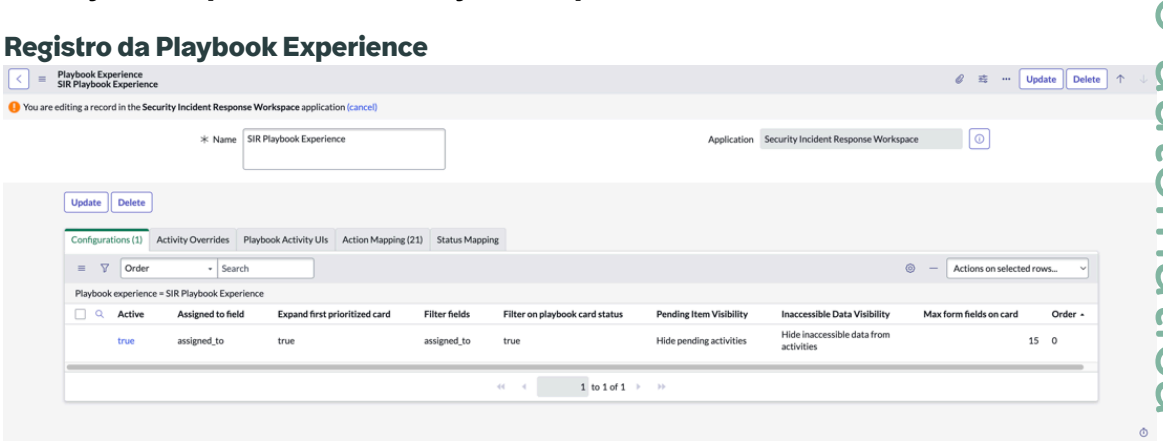
- Em cada atividade, o analista poderá executar as ações definidas nos cartões de atividade, como Ignorar, Marcar como concluído, Cancelar ou ações de Orquestração, como Enviar para área restrita, Pesquisar e-mails e assim por diante.
- Cada uma dessas ações é definida na definição de atividade, e o cartão completo visível é personalizável no momento da criação da própria definição de atividade.

Nota:
Todas as definições de atividade futuras e as próximas etapas a serem realizadas são exibidas com um ícone de cadeado e estão no modo somente leitura para o usuário. O modo de exibição do playbook é controlado por uma configuração conforme explicado abaixo.

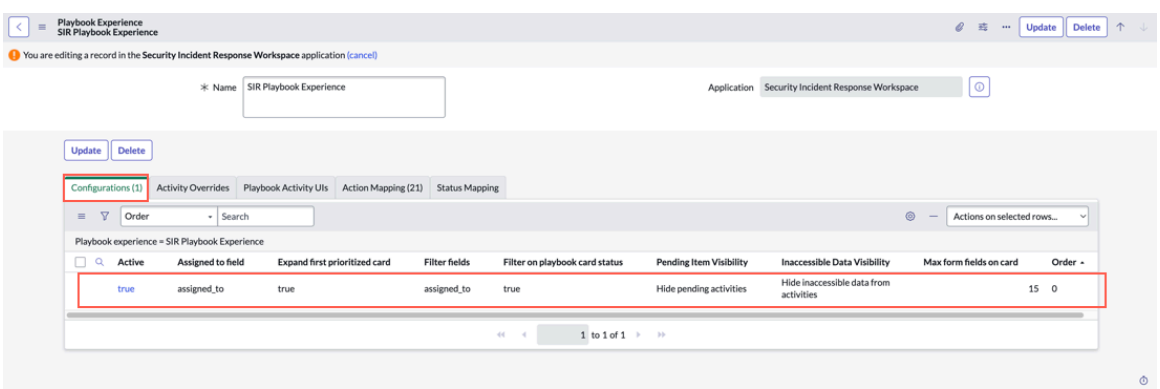
1. Navegar até **Todos** > **Playbook Experiences**.
2. Na página Playbook Experiences, selecione uma **Playbook Experience de SIR**.



A página **Playbook Experience do SIR Playbook Experience** é exibida.



3. Clique no registro de **configuração**.

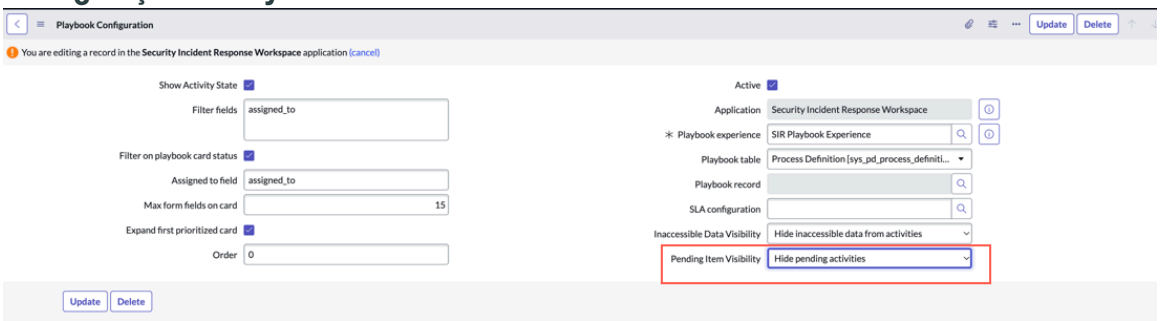


4. Na guia Configuração, clique em Configuração da Playbook Experience de SIR.

Tradução automática

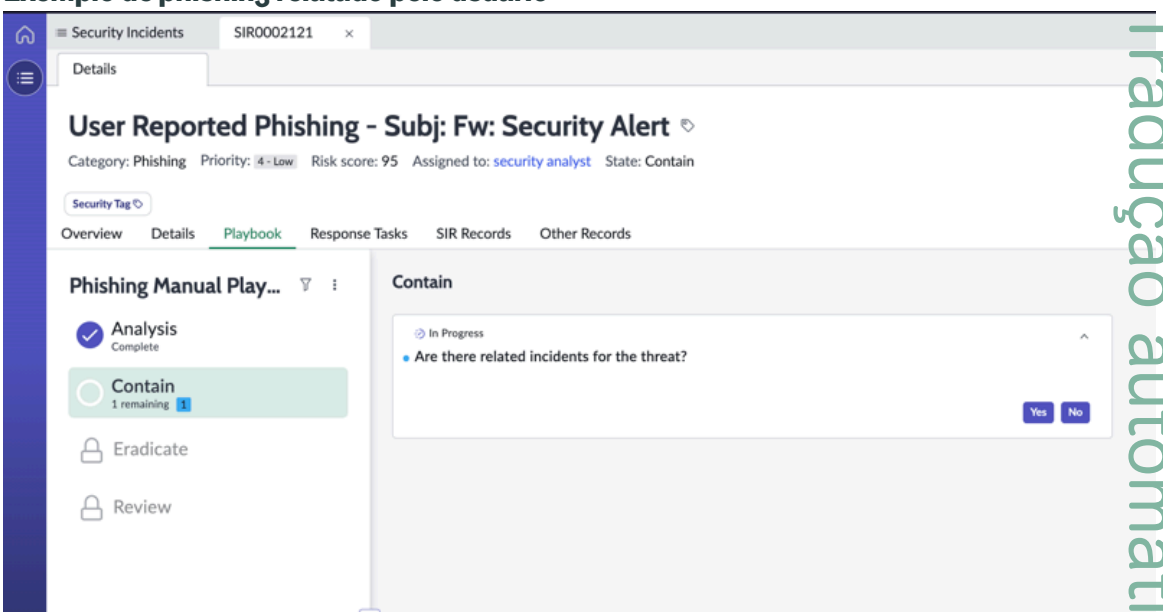
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração do Playbook



5. Navegue até a lista suspensa do campo **Visibilidade do item pendente**, selecione a opção desejada e salve o registro. Escolhas das seguintes opções:
   - **Ocultar atividades pendentes**: selecione esta opção para ocultar as atividades pendentes que você gostaria de ver na seção do playbook do espaço.

Exemplo de phishing relatado pelo usuário

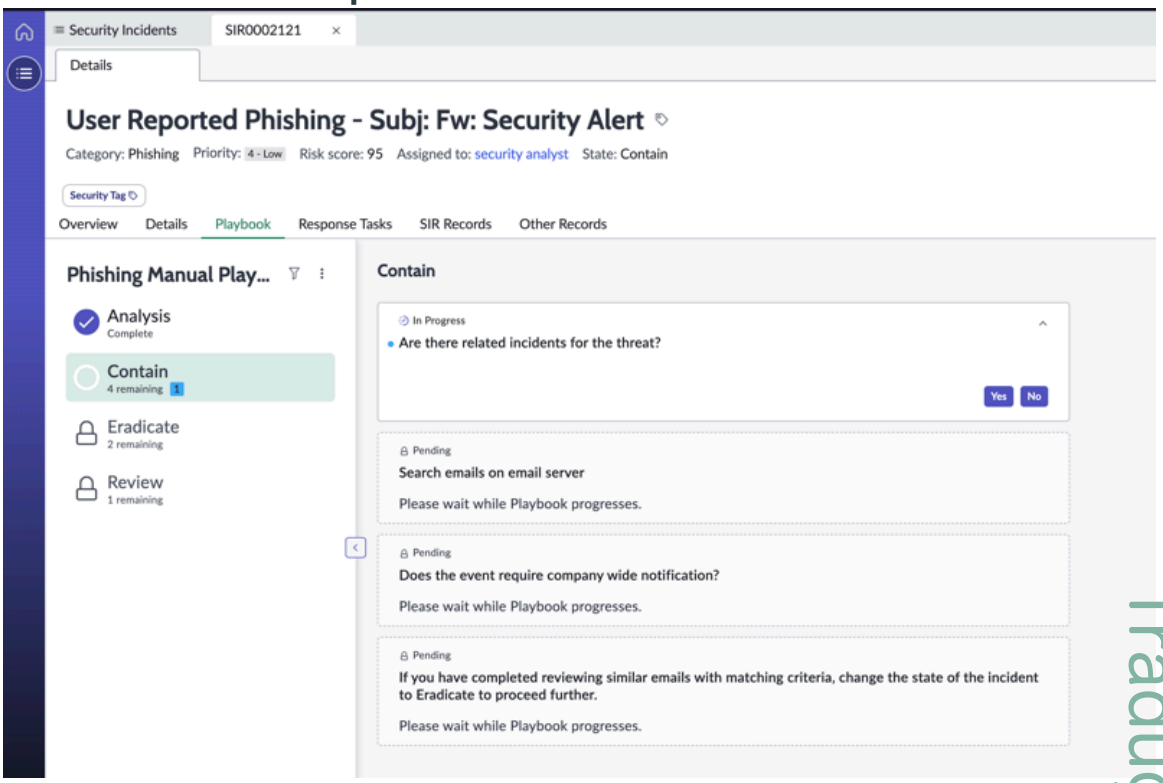


Tradução automática

   - **Mostrar fases e atividades pendentes**: selecione esta opção para mostrar fases e atividades pendentes que você gostaria de ver na seção do playbook do espaço.

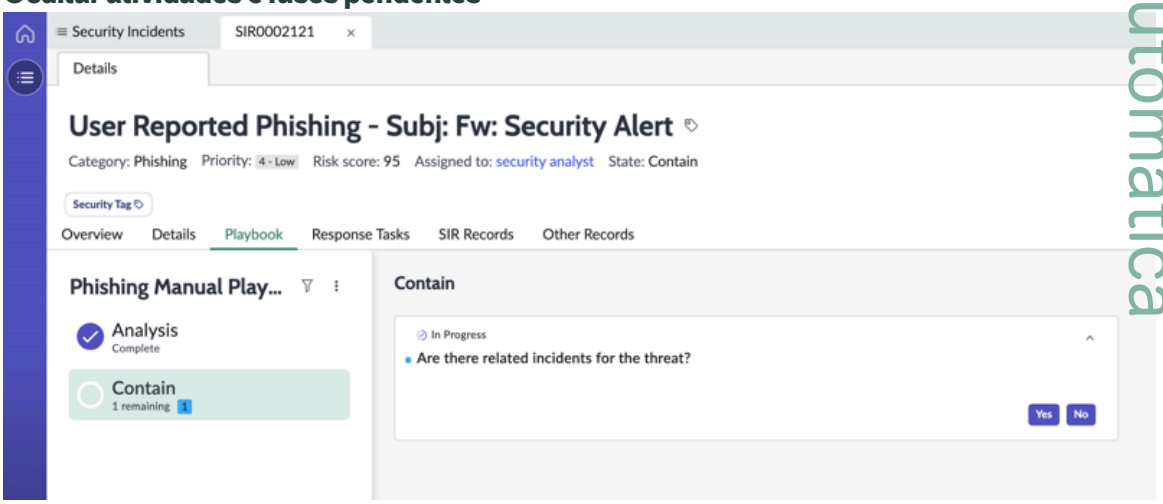
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mostrar atividades e fases pendentes



- **Ocultar atividades e fases pendentes**: selecione esta opção para ocultar as atividades e fases pendentes que você gostaria de ver na seção do playbook do espaço.

Ocultar atividades e fases pendentes

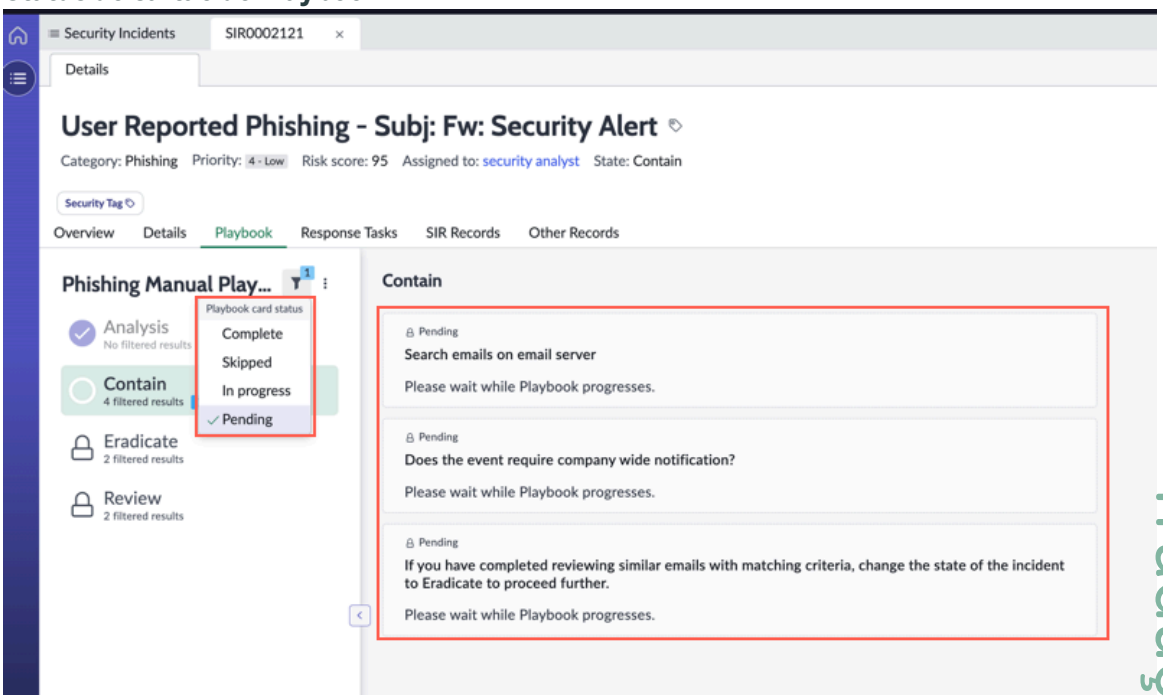


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Na seção Playbook, use a opção de filtro para filtrar as atividades por status do cartão do Playbook (definição de atividade).

Status do cartão do Playbook



Adicionar Playbook

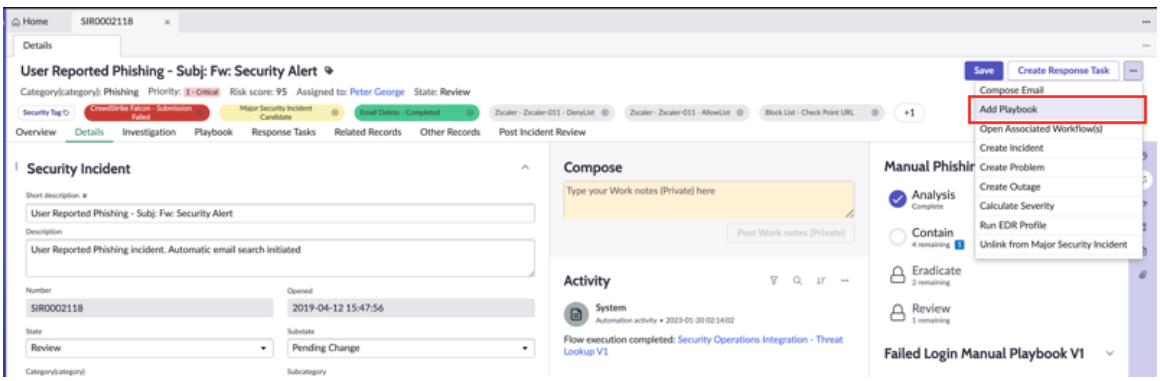
Use esta seção para adicionar o playbook manualmente.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

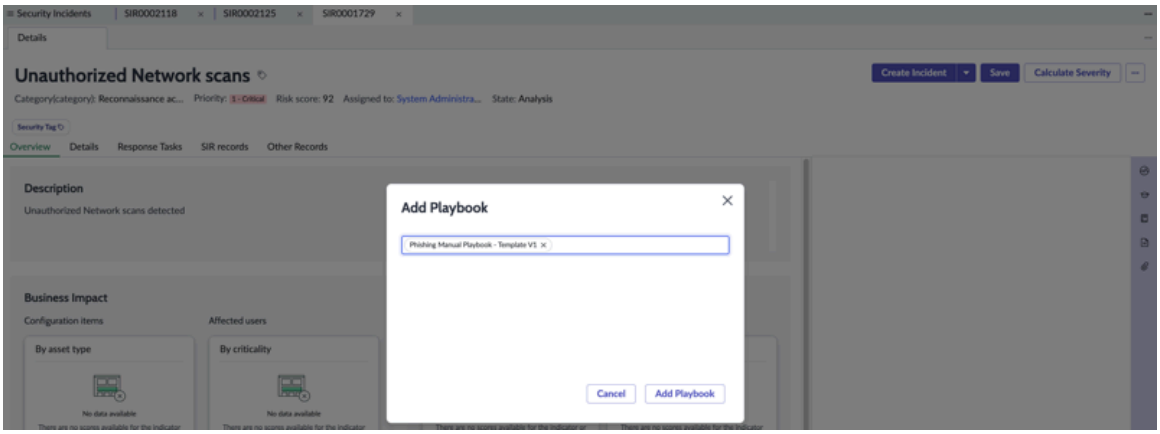
1. Navegar até **Todos** > **Incidente de segurança** > **Espaço de trabalho do analista de segurança**.
2. Abra um registro de incidentes
3. Clique **em Adicionar Playbook**.



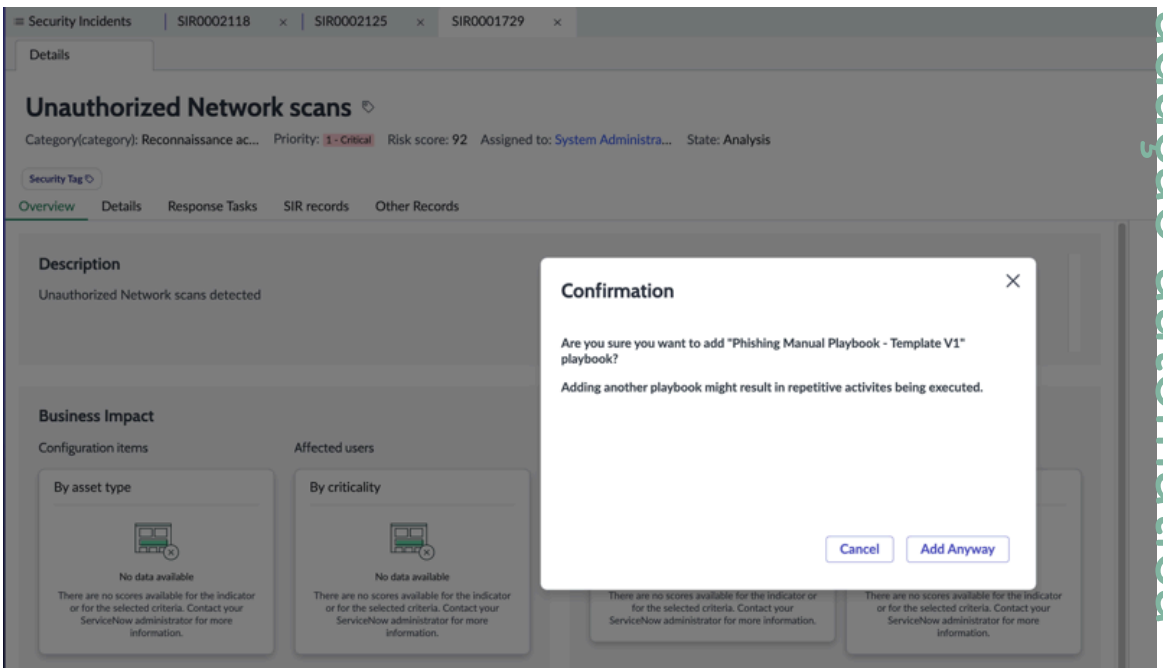
A caixa de diálogo **Adicionar Playbook** é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

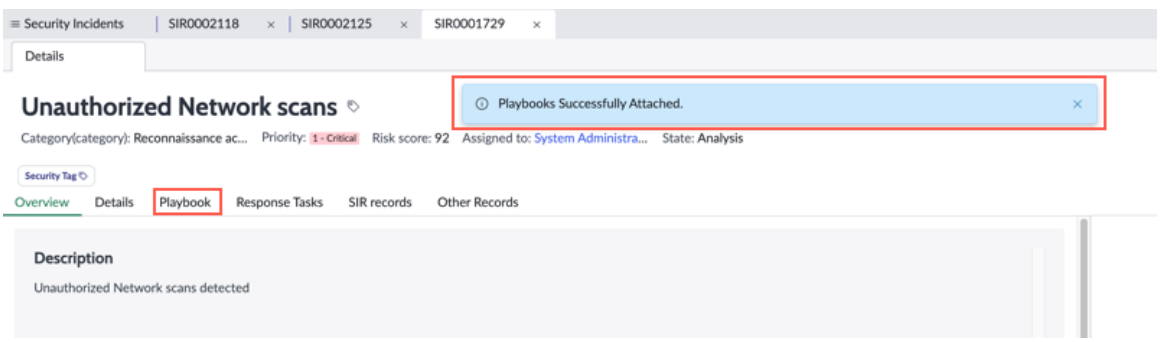


4. Selecione o modelo de playbook.
5. Clique **em Adicionar Playbook**.
   Uma caixa de diálogo de mensagem de confirmação será exibida para você confirmar.
6. Clique **em Adicionar mesmo assim**.



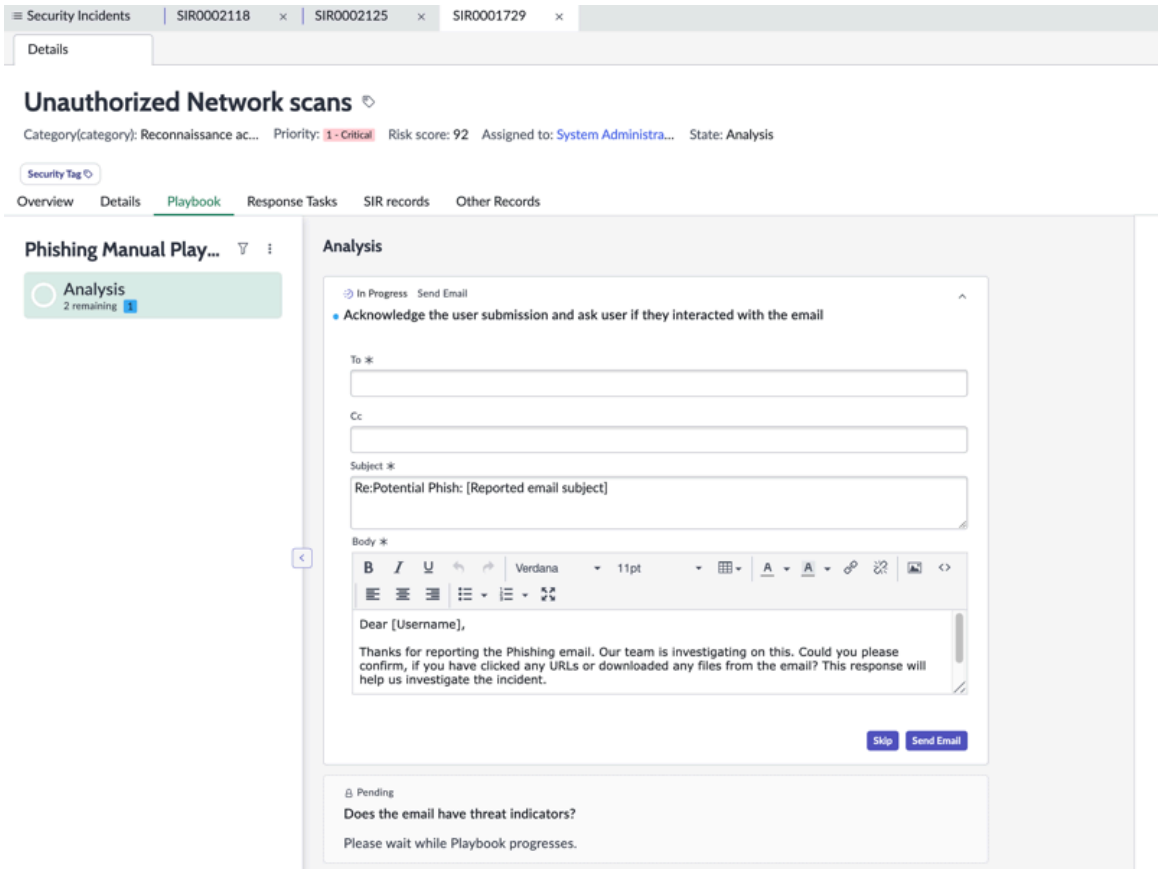
Tradução automática

7. O **Playbook** é adicionado ao lado da guia **Detalhes**.



8. Clique na guia **Playbook**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Execute a série de atividades listada para passar para o próximo nível.

> **Nota:**
> Se um incidente de segurança estiver associado a um playbook, até que o playbook associado seja fechado ou cancelado, o usuário não poderá associar novamente o mesmo playbook ao mesmo incidente de segurança.

Pré-requisitos para os Playbooks

Você precisa das funções e plug-ins a seguir para criar os Playbooks.

Função necessária: administrador

- Habilite o plug-in Process Automation Designer (PAD) [com.glide.pad.license].
- Habilite os seguintes plug-ins para uma experiência de playbook:
  - com.playbook_experience
  - now_playbook_exp
  - com.glide.playbook_experience.config
- Habilite o spoke Security Operations para acessar fluxos [com.snc.secops.spoke].
- Enterprise Security Case Management PAD Commons.

Certifique-se de ter lido a documentação da plataforma na Playbook Experience e no Designer de automação de processos (PAD) antes de iniciar este guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recriando playbooks existentes no PAD

Você não pode converter fluxos existentes diretamente em processos no PAD. Cada etapa do Flow Designer que cria uma tarefa de resposta para orientar o analista deve ser dividida em ações ou subfluxos separados.

Você não tem permissão para converter fluxos existentes diretamente em processos no PAD. Cada etapa do Flow Designer que cria uma tarefa de resposta para orientar o analista deve ser dividida em ações ou subfluxos separados. Ao usar esses subfluxos ou ações granulares, você deve criar definições de atividade. Depois de criar essas definições de atividade, elas são adicionadas como atividades em uma raia na definição do processo. Você pode reutilizar as definições de atividade em vários playbooks.

Você pode personalizar cada atividade para renderizar as ações necessárias nelas e a aparência do cartão ao criar a definição da atividade. A atividade pode mostrar clientes de e-mail, tabelas, ações, artigos da base de conhecimento, URLs e assim por diante. Você pode definir como a definição de atividade e a ação subjacente ou os subfluxos são criados.

Para obter mais informações, consulte as seções a seguir.

- Definições de atividades
- Designer de automação de processos

Definições de Atividades

O Now Platform fornece algumas definições de atividade no sistema de base. Além disso, para os playbooks do sistema de base do SIR Workspace, há algumas definições de atividade definidas no sistema de base na aplicação Enterprise Security Case Management PAD Commons.

Função necessária: sn_si.admin.

Esta é a lista de definições de atividade que fazem parte do sistema de base:

Definição de Atividade	Tabela	Descrição	Aplicação
Aguardar condição sem experiência	Global [global]	Aguardar condição sem experiência	Enterprise Security Case Management PAD Commons
Enviar para área restrita FCS X	Incidente de segurança [sn_si_incident]	Enviar para área restrita	Enterprise Security Case Management PAD Commons
Enviar e-mail	Incidente de segurança [sn_si_incident]	Atividade de envio de e-mail para playbooks de SIR.	Enterprise Security Case Management PAD Commons
Pesquisar E-mail	Incidente de segurança [sn_si_incident]	Pesquisar e-mails no servidor de e-mail	Enterprise Security Case Management PAD Commons
Atualizar estado da tarefa	Incidente de segurança [sn_si_incident]	Atualizar o estado da tarefa	Enterprise Security Case Management PAD Commons
Excluir e-mail	Incidente de segurança [sn_si_incident]	Excluir e-mails	Enterprise Security Case Management PAD Commons

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definição de Atividade	Tabela	Descrição	Aplicação
Resultado Sim Não	Tarefa [task]	Resultado esperado	Enterprise Security Case Management PAD Commons

Exemplo de definição de atividade: enviar e-mail

A seguir está um exemplo de definição de atividade de envio de e-mail.

Básico

Os detalhes básicos capturam o nome (rótulo), a aplicação, a descrição, a tabela e de todas as aplicações a partir das quais ele pode ser acessado.

Adicione o plano de automação, a experiência de atividade e envie. Após o envio, edite o documento para adicionar mais detalhes em cada guia.

Plano de Automação

O plano de automação associa a ação de back-end ou os subfluxos criados usando o Flow Designer. Este exemplo usa: **Subfluxo Enviar e-mail - Atividade ESCM**.

Este subfluxo permite o envio de um e-mail. Ele tem a lógica principal para enviar um e-mail. Ela tem todos os campos de entrada e de saída definidos.

Todos os campos de entrada são mostrados na seção do plano de automação. Cada campo de entrada pode ser habilitado para ficar visível somente para o administrador, no modal padrão, no modal padrão e no painel de configuração:

- **Somente visibilidade do administrador**: quando definida como administrador, somente o administrador pode exibi-la.
- **Incluir no modelo padrão**: quando definido para exibição no modal padrão, ele aparece somente no modal de propriedades.
- **Incluir no modelo padrão e no painel de configuração**: quando definido para exibição no modal padrão e no painel de configuração, ele aparece no painel de configuração do PAD, bem como no modal de propriedades. Para obter mais informações, consulte Definições de atividade .

Você pode definir os campos de entrada no momento da própria definição da atividade, desde que não precise alterar esses valores no momento da configuração. Isso ajuda o proprietário do processo de negócios a economizar tempo ao configurar uma atividade em um processo.

Experiência de Atividade

A guia de experiência da atividade define como o cartão de atividade é renderizado no tempo de execução. O sistema básico fornece os seguintes tipos de experiência:

- Aprovação
- Item do catálogo
- Criar Registro
- Instrucional
- Conhecimento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Lista de
- Notificação
- Registro

Com base no tipo de experiência selecionado, os outros campos são preenchidos. Para obter mais informações, consulte a documentação da Now Platform.

Neste exemplo, o tipo de **registro** está selecionado.

Nota:
Por exemplo, se você quiser renderizar uma tabela, poderá escolher lista como o tipo de experiência.

Registro Associado

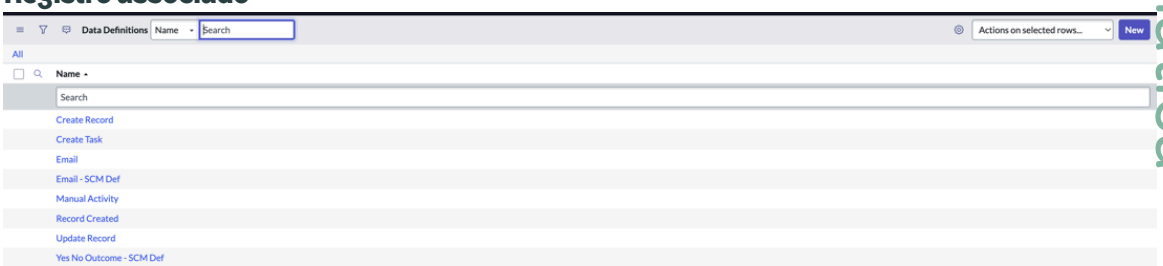
Use este registro para armazenar os dados associados pertencentes à atividade atual. Isso capturaria os dados de tempo de execução, bem como o status da experiência.

- Tabela associada: dados de fluxo
- Registro associado: VL
- Tabela de status de experiência: dados de fluxo
- Registro de status de experiência: VL

Neste exemplo, a tabela de dados de fluxo é usada para capturar os dados de tempo de execução. Os dados de tempo de execução podem variar de acordo com o caso de uso. Neste exemplo, os dados de tempo de execução são campos como Para, cc, Assunto e corpo. Para cada caso de uso, uma definição de dados de fluxo precisa ser criada para definir o tipo de dados de tempo de execução.

1. Navegue até o painel esquerdo e insira **sys_flow_data_definition.list**. Exibe a lista de definições criadas para a tabela de dados de fluxo.

Registro associado

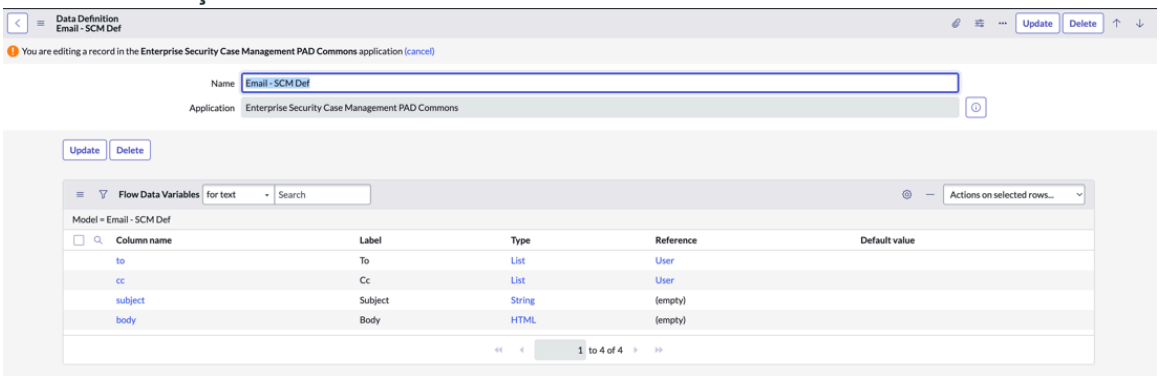


2. Abra **E-mail - Def de SCM** para exibir a definição relacionada a este exemplo.

Tradução automática

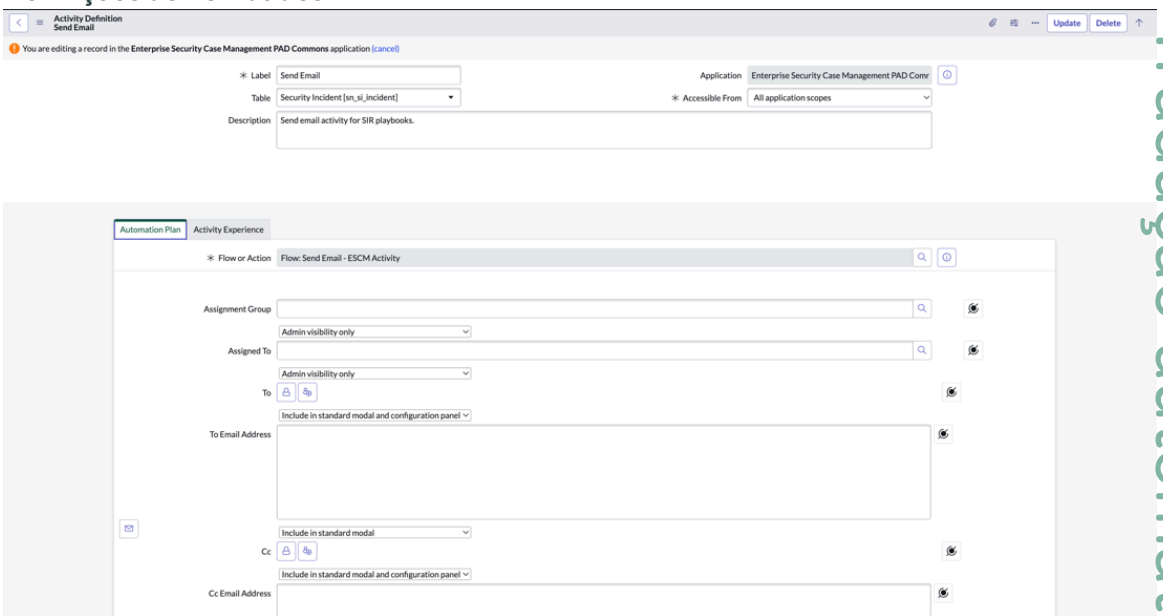
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

E-mail — Definição de SCM



Esta definição de dados de fluxo deve ser usada pelo subfluxo ou pela ação associada a esta definição de atividade (consultar plano de automação) para capturar os dados de tempo de execução.

Definições de Atividades



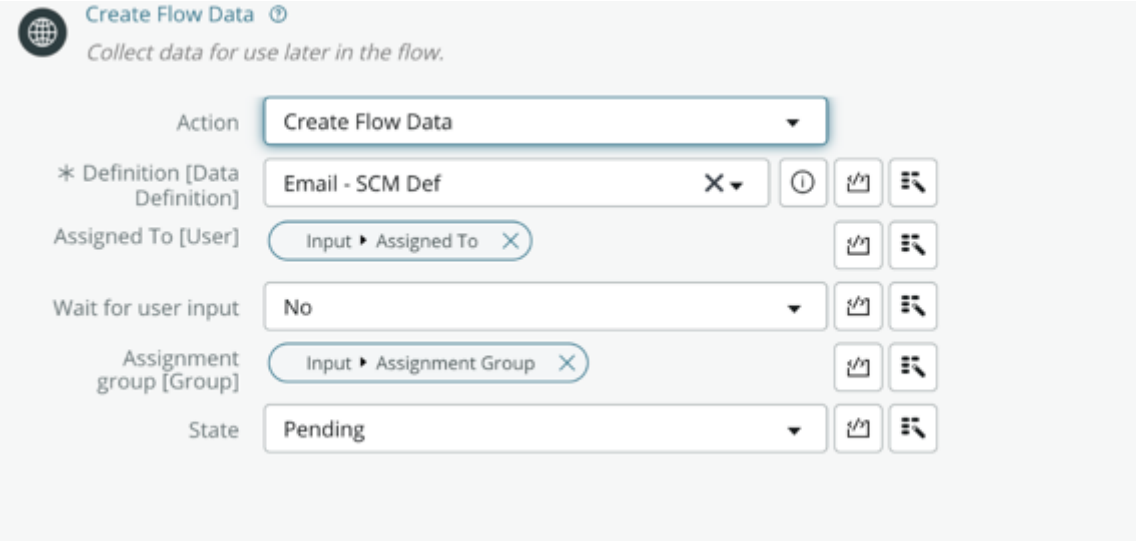
3. Neste exemplo, abra o subfluxo: **Enviar e-mail - Atividade ESCM**. Na etapa **Criar dados de fluxo**, a definição de dados de fluxo que você criou é mapeada em relação ao campo **Definição**. Este registro de dados de fluxo é usado em todo o subfluxo. Neste exemplo, o

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

status do cartão de atividade (status de experiência) é capturado na tabela de dados de fluxo.

Enviar e-mail - Atividade ESCM



Nota:

Se você quiser capturar os dados de tempo de execução em um registro de tabela diferente da tabela de dados de fluxo, digamos, por exemplo, em uma tarefa de resposta. Você pode selecionar a tabela associada como Tabela de tarefa de resposta. O registro associado deve ser definido como registro de tarefa de resposta criado pelo subfluxo.

Da mesma forma, a tabela de status de experiência captura o status do cartão de atividade. No sistema de base, o campo de estado da tabela de dados de fluxo é mapeado para o status do cartão de atividade. Portanto, quando a tabela de dados de fluxo é usada para capturar o status da experiência, ela atualiza automaticamente o status do cartão de atividade. Você também pode usar uma tabela diferente da tabela de dados de fluxo para capturar o status da experiência.

Por exemplo, se você quiser mapear o status da tarefa de resposta para o status do cartão de atividade, isso será possível. Para fazer isso:

1. Navegar até **Todos** > **Playbook Experiences**.

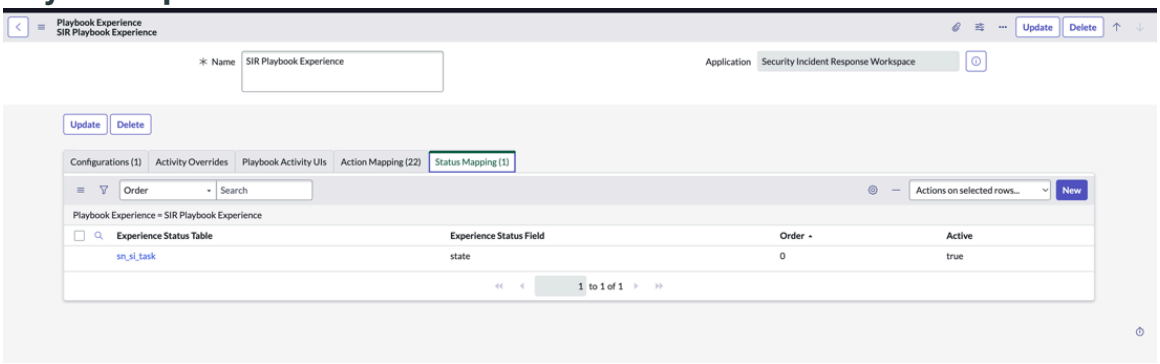
Playbook Experiences

2. Abra **a Playbook Experience de SIR**.
3. Abra a lista relacionada **de Mapeamento de status**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook Experience

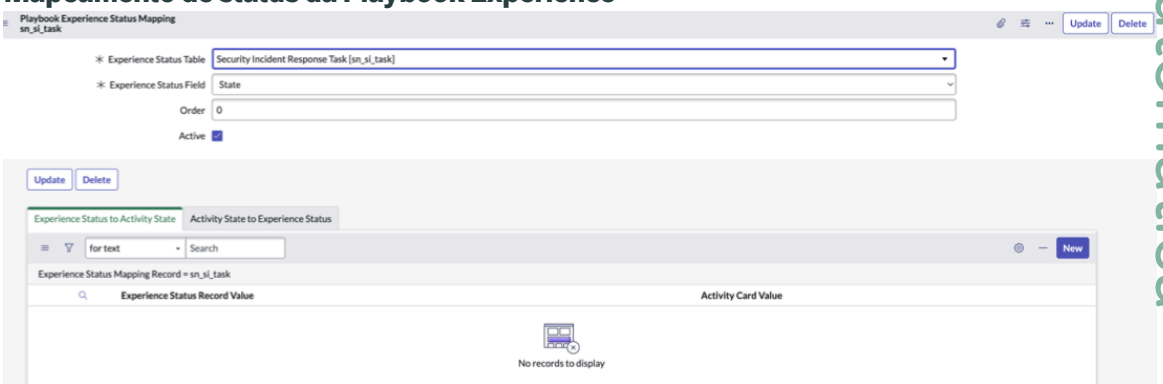


4. Insira o campo **Tarefa de resposta** em relação à tabela de status da experiência.
5. Insira o campo **Estado em** relação ao Status da experiência.

Status da experiência

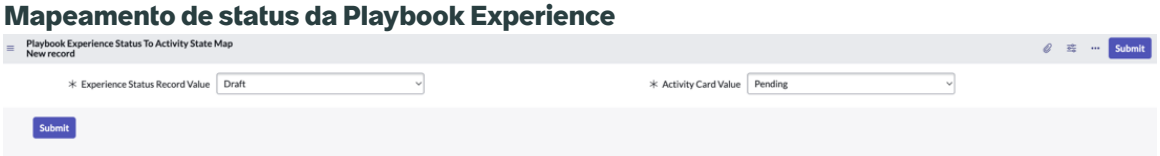
6. Clique em **Enviar**. O registro é criado.

Mapeamento de status da Playbook Experience



7. Em Status de experiência para estado de atividade, mapeie os estados da tarefa de resposta para o status do cartão de atividade.
8. O lado esquerdo mostra os estados da tarefa de resposta e o lado direito mostra o status do cartão de atividade.

Mapeamento de status da Playbook Experience



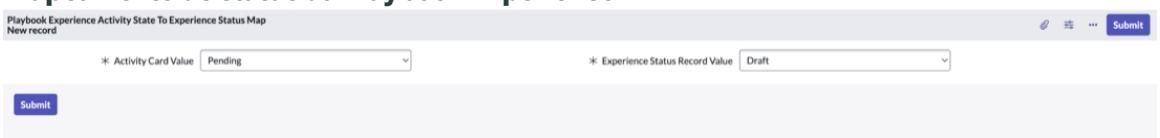
9. O mapeamento pode ser bidirecional. Na lista relacionada Estado da atividade para Experiência também, mapeie os status corretamente. Esta etapa é o inverso da etapa

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

anterior. Nesse caso, o lado esquerdo mostra o status do cartão de atividade e o lado direito mostra o status da tarefa de resposta.

Mapeamento de status da Playbook Experience



Detalhes

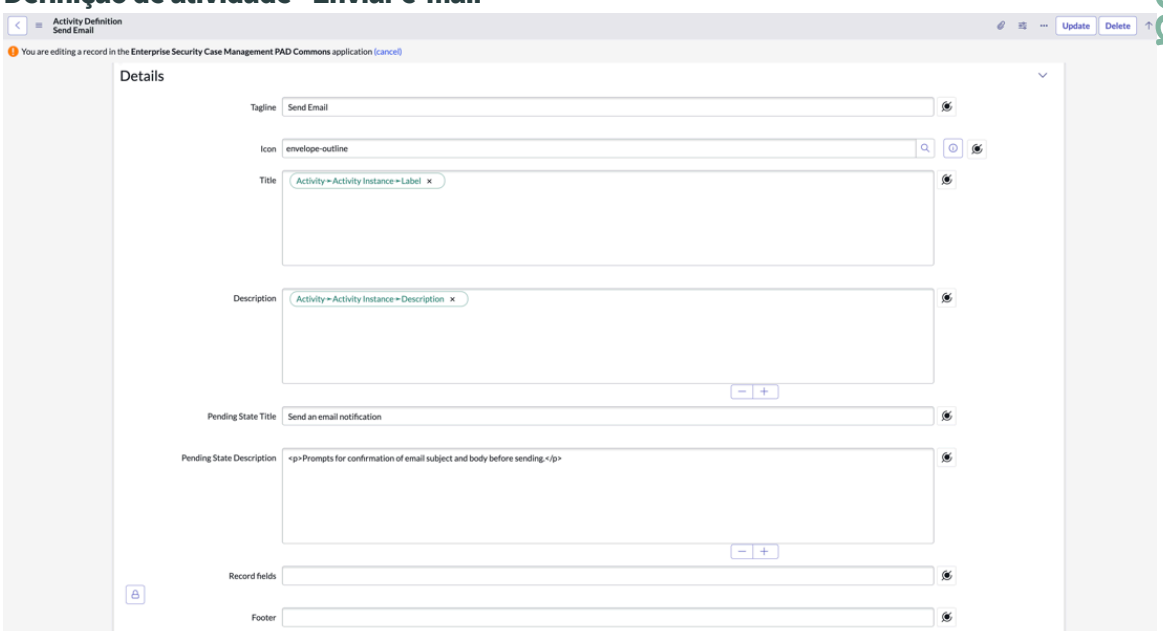
- Slogan: Enviar e-mail
- Ícone: Contorno do envelope (não mostrado na interface do usuário)
- Título: **Atividade** > **Instância de Atividade** > **Rótulo**. Aqui, selecionamos o rótulo da instância da atividade. Esta referência com pontos substituirá o valor do rótulo como título dinamicamente no tempo de execução.
- Descrição: **Atividade** > **Instância de Atividade** > **Descrição**. Aqui, selecionamos a descrição da instância da atividade. Esta referência com pontos substituirá o valor do rótulo como título dinamicamente no tempo de execução.
- Título de estado pendente: enviar uma notificação por e-mail. Este é o título quando a atividade está no status Pendente.
- Descrição do estado pendente: solicita a confirmação do assunto e do corpo do e-mail antes do envio. Esta é a descrição do cartão de atividade quando o status é pendente Campos de registro: há campos de registro selecionados neste exemplo.

  Os campos de registro são uma lista separada por vírgulas de nomes de campo a serem exibidos para o registro associado em uma lista de pares de nome-valor. Os dados são pré-buscados no servidor, a referência com pontos é compatível e as permissões **canRead ()**são avaliadas em cada campo.

- Rodapé: não há rodapé definido para este exemplo.

  Rodapé é um texto em uma área cinza do rodapé do cartão. Você pode adicionar qualquer informação significativa ao mostrado.

Definição de atividade - Enviar e-mail



Tradução automática

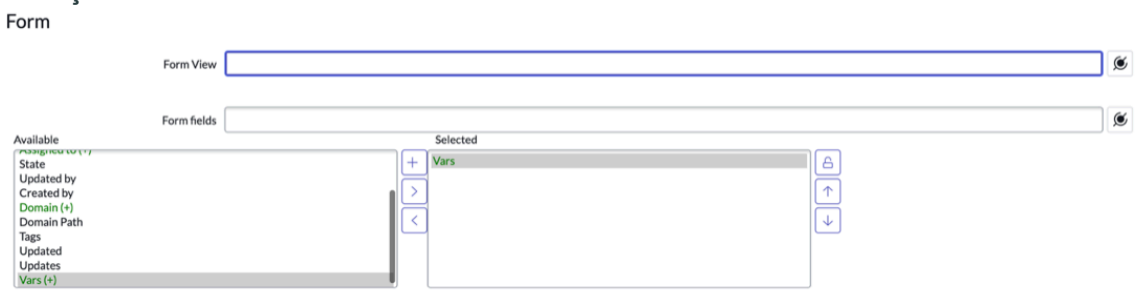
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário

- Exibição de formulário: collect_data
- Campos de formulário:

Este exemplo usa a exibição collect_data para mostrar os campos que devem ser apresentados ao usuário para inserir entradas. A exibição Collect_data é uma exibição fornecida pela plataforma que corresponde à tabela de dados de fluxo. Como alternativa, você pode deixar a Exibição de formulário em branco e selecionar Variáveis na lista de valores disponíveis em Campos de formulário. (clique no ícone de cadeado para abrir a lista de valores disponíveis).

Exibição de formulário



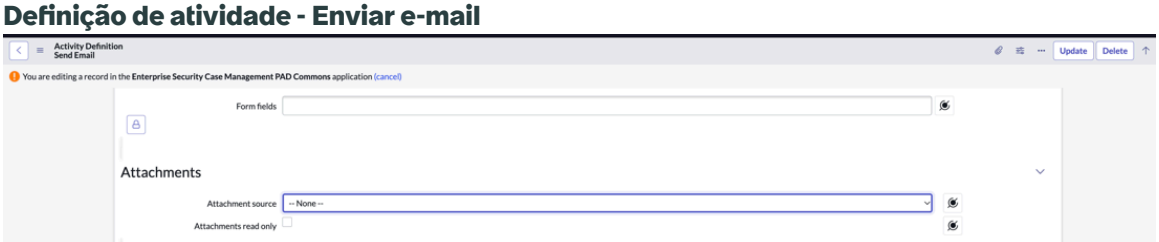
Anexos

Neste exemplo:

- A origem do anexo está vazia.
- Somente leitura de anexo não selecionado.

1. Origem do anexo - Menu suspenso. Quais anexos serão mostrados no cartão: aqueles anexados ao registro primário, ao registro associado ou a nenhum.
2. Somente leitura do anexo: verdadeiro ou falso. Impede que o usuário renomeie ou exclua os anexos existentes.

Definição de atividade - Enviar e-mail



Recursos

Neste exemplo,

- Mostrar ANS - Desmarcado
- Mostrar check-list - Desmarcada
- É Automatizado - Apagado

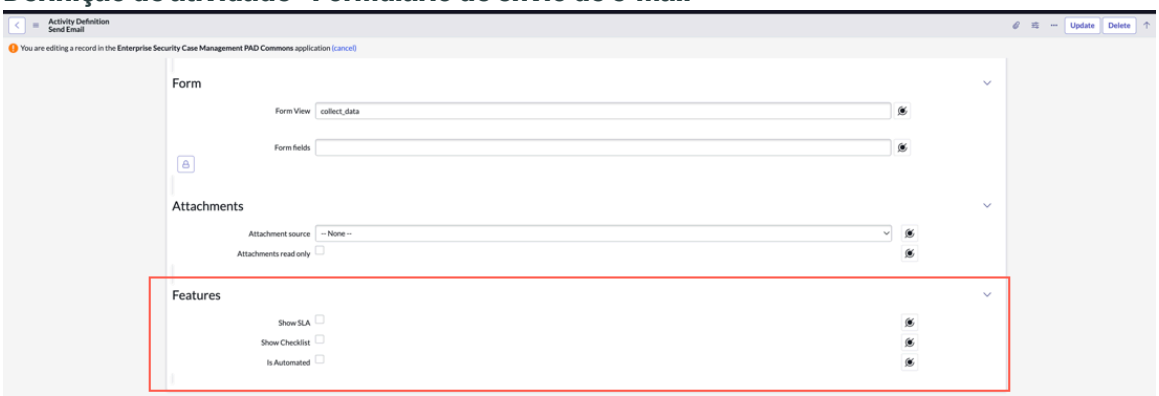
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mostrar ANS: Verdadeiro/Falso. Renderiza um temporizador de SLA no cabeçalho do cartão para o registro associado. O SLA é escolhido de acordo com o registro de configuração de SLA especificado na configuração do Playbook.

1. Mostrar check-list - Verdadeiro ou Falso. Renderiza qualquer check-list anexada ao registro associado. A check-list é editável e as mudanças são salvas sem exigir uma ação declarativa.
2. É automatizado: verdadeiro ou falso. Se verdadeiro, o **slogan**e o **ícone**serão substituídos pelo texto **Tarefa automatizada** e um ícone automatizado.

Definição de atividade - Formulário de envio de e-mail

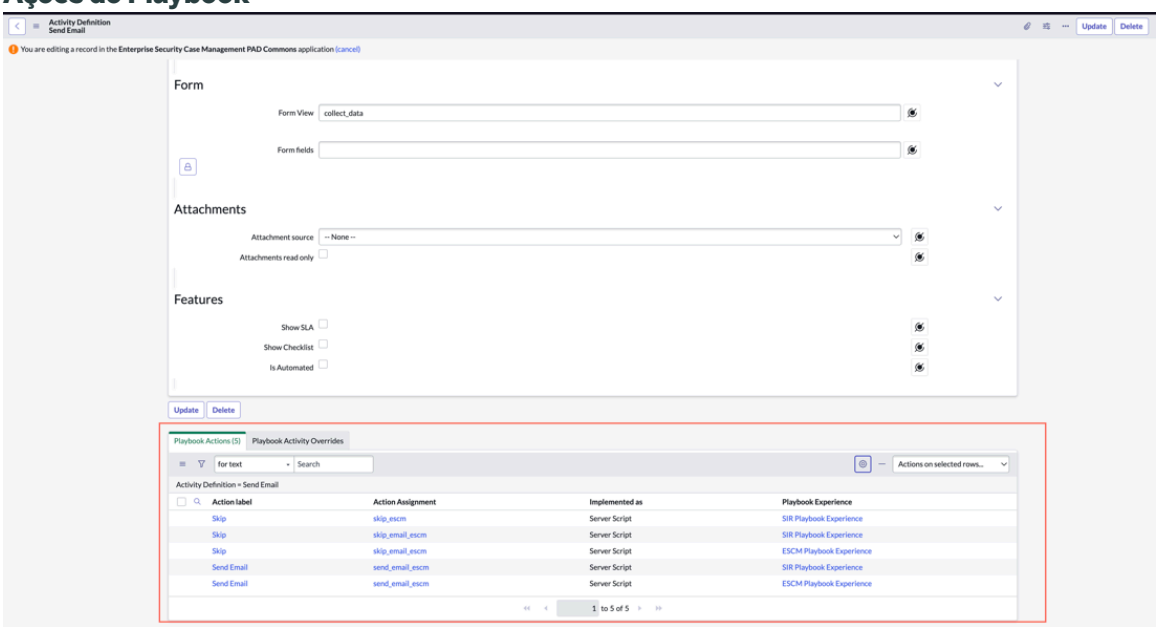


Ações do Playbook na definição de atividade

Esta seção tem as ações que serão renderizadas no cartão de atividade. Este exemplo tem as ações **Ignorar**e **Enviar e-mail**.

Para adicionar uma nova ação ao cartão de atividade, você deve criar um registro na lista relacionada **Ações do Playbook** presente na parte inferior da página.

Ações do Playbook



1. Clique em **Nova**.
2. Selecione a ação de atividade existente no campo Atribuição de ação.
3. Selecione Playbook Experience de **SIR** no campo Playbook Experience.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

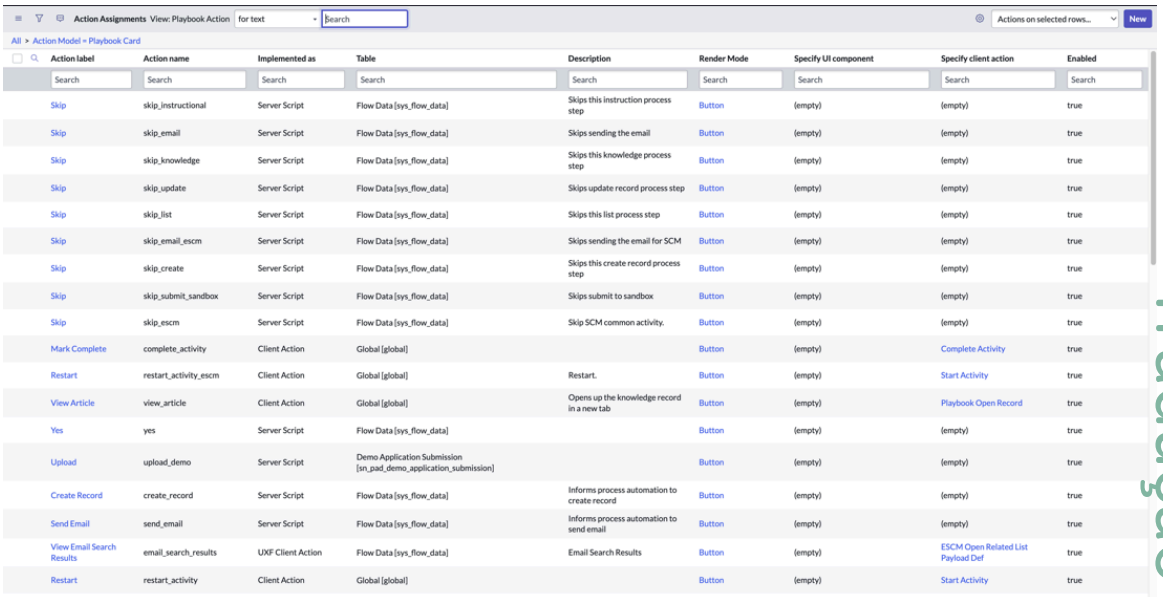
Criar uma Ação de Atividade

A seguir está o procedimento para criar uma ação de atividade.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Playbook Experiences** > **Ação/ Comportamento** > **Ações de Atividade**.



Action label	Action name	Implemented as	Table	Description	Render Mode	Specify UI component	Specify client action	Enabled
Skip	skip_instructional	Server Script	Flow Data [sys_flow_data]	Skips this instruction process step	Button	(empty)	(empty)	true
Skip	skip_email	Server Script	Flow Data [sys_flow_data]	Skips sending the email	Button	(empty)	(empty)	true
Skip	skip_knowledge	Server Script	Flow Data [sys_flow_data]	Skips this knowledge process step	Button	(empty)	(empty)	true
Skip	skip_update	Server Script	Flow Data [sys_flow_data]	Skips update record process step	Button	(empty)	(empty)	true
Skip	skip_list	Server Script	Flow Data [sys_flow_data]	Skips this list process step	Button	(empty)	(empty)	true
Skip	skip_email_escm	Server Script	Flow Data [sys_flow_data]	Skips sending the email for SCM	Button	(empty)	(empty)	true
Skip	skip_create	Server Script	Flow Data [sys_flow_data]	Skips this create record process step	Button	(empty)	(empty)	true
Skip	skip_submit_sandbox	Server Script	Flow Data [sys_flow_data]	Skips submit to sandbox	Button	(empty)	(empty)	true
Skip	skip_escm	Server Script	Flow Data [sys_flow_data]	Skip SCM common activity.	Button	(empty)	(empty)	true
Mark Complete	complete_activity	Client Action	Global [global]		Button	(empty)	Complete Activity	true
Restart	restart_activity_escm	Client Action	Global [global]	Restart.	Button	(empty)	Start Activity	true
View Article	view_article	Client Action	Global [global]	Opens up the knowledge record in a new tab	Button	(empty)	Playbook Open Record	true
Yes	yes	Server Script	Flow Data [sys_flow_data]		Button	(empty)	(empty)	true
Upload	upload_demo	Server Script	Demo Application Submission [sn_pad_demo_application_submission]		Button	(empty)	(empty)	true
Create Record	create_record	Server Script	Flow Data [sys_flow_data]	Informs process automation to create record	Button	(empty)	(empty)	true
Send Email	send_email	Server Script	Flow Data [sys_flow_data]	Informs process automation to send email	Button	(empty)	(empty)	true
View Email Search Results	email_search_results	UXF Client Action	Flow Data [sys_flow_data]	Email Search Results	Button	(empty)	ESCM Open Related List Payload Def	true
Restart	restart_activity	Client Action	Global [global]		Button	(empty)	Start Activity	true

2. Clique em **Nova**.

   Consulte a documentação da Now Platform para saber como criar essas ações. Neste exemplo, Ignorar é implementado como um script de servidor.

3. **Substituição do Playbook:**

   Se você quiser substituir o tipo de experiência de atividade existente, é possível. Para obter mais informações, consulte a documentação da Now Platform. Não há substituições de Playbook para este exemplo.

Enviar para área restrita FCS X

Enviar para FCS X Sandbox é um exemplo de um processo de definição de atividade.

Básico

Os detalhes básicos capturam o nome (rótulo), aplicação, descrição, tabela e de todas as aplicações que podem ser acessadas.

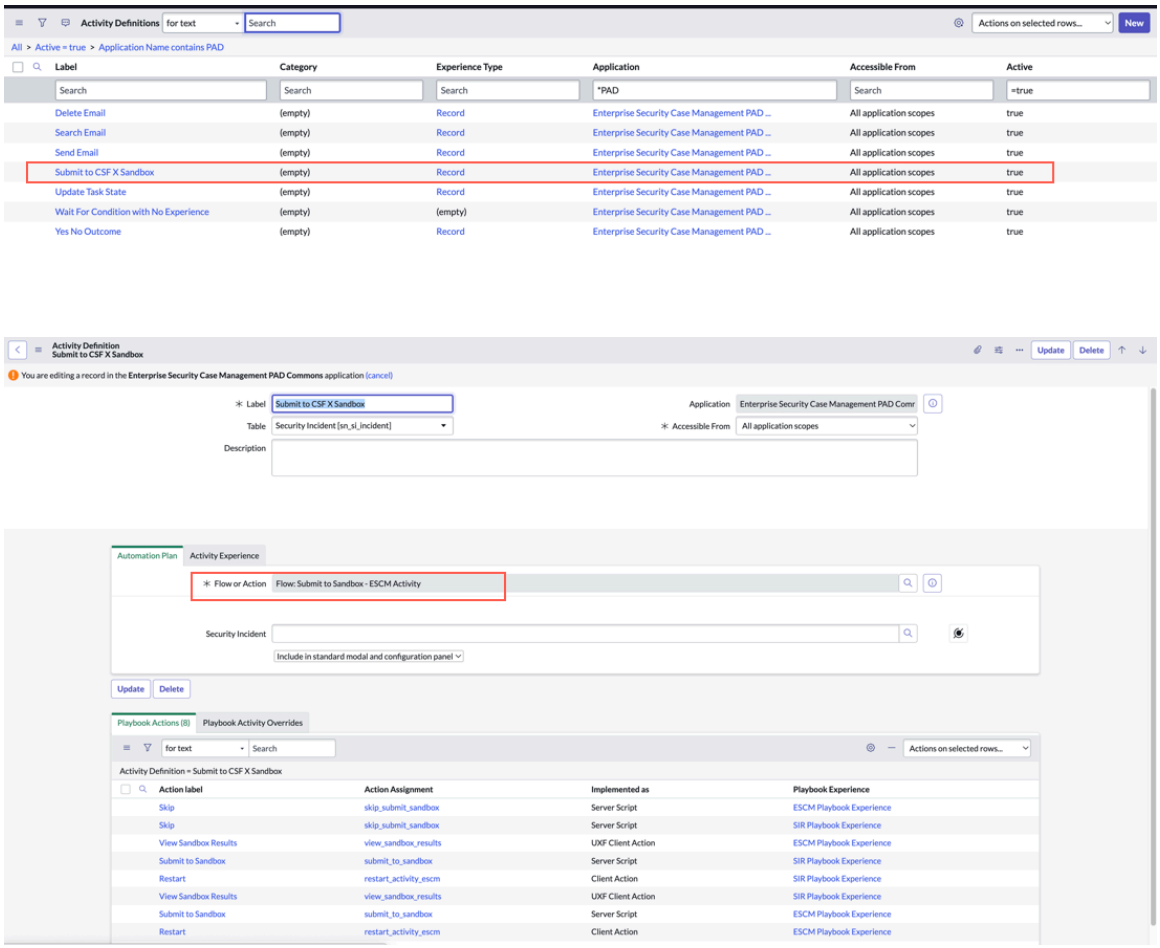
Adicione o plano de automação, a experiência de atividade e envie. Depois de enviado, edite o documento para adicionar mais detalhes em cada guia.

Plano de Automação

O plano de automação associa a ação de back-end/subfluxo criado usando o Flow Designer. Este exemplo usa **o subfluxo Enviar para área restrita - Atividade ESCM**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Este subfluxo permite enviar os observáveis maliciosos para a área restrita. Ela tem todos os campos de entrada e de saída definidos.

Incidente de segurança é o campo de entrada.

Experiência de Atividade

Neste exemplo, o tipo de **registro** está selecionado.

Registro Associado

O registro associado serve para armazenar os dados associados pertencentes à atividade atual. Isso capturaria os dados de tempo de execução, bem como o status da experiência.

- Tabela associada: dados de fluxo
- Registro associado: VL
- Tabela de status de experiência: dados de fluxo
- Registro de status de experiência: VL

Detalhes

- Slogan: Enviar e-mail
- Ícone: Contorno de envelope
- Título: **Atividade** > **Instância de Atividade** > **Rótulo**. Aqui, selecionamos o rótulo da instância da atividade. Esta referência com pontos substituirá o valor do rótulo como título dinamicamente no tempo de execução.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Descrição: VL (a saída do subfluxo é mapeada)
- Título do estado pendente: em branco
- Descrição do estado pendente: em branco
- Campos do Registro
- Rodapé

Formulário

- Exibição de formulário: em branco
- Campos de formulário: em branco

Anexos

Neste exemplo:

- Origem do anexo - Nenhuma
- Somente leitura de anexo - Não verificado

1. Origem do anexo - Este é um menu suspenso. Quais anexos serão mostrados no cartão: aqueles anexados ao Registro Primário, ao Registro Associado ou a nenhum.
2. Somente leitura de anexo - Verdadeiro/falso. Impede que o usuário renomeie ou exclua os anexos existentes.

Recursos

Neste exemplo,

- Mostrar ANS - Desmarcado
- Mostrar check-list - Não verificado
- É automatizado - desmarcado

Ações do Playbook na definição de atividade

Esta seção tem as ações que serão renderizadas no cartão de atividade.

Este exemplo tem as ações Ignorar, Exibir resultados da área restrita, Enviar para área restrita e Reiniciar.

Para adicionar uma nova ação ao cartão de atividade, você precisa criar um novo registro na lista relacionada Ações do Playbook presente na parte inferior da página.

Substituição de Playbook

Não há substituições de Playbook para este exemplo.

Playbooks de amostra para espaço de SIR

Você pode criar ou configurar playbooks para o Espaço SIR de forma rápida e fácil sem escrever código complicado. Você pode usar esses playbooks para resolver ameaças à segurança passo a passo. Você pode invocar o fluxo do playbook de incidente de segurança automaticamente ou manualmente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O Security Incident Response fornece os seguintes playbooks com o sistema de base:

- Playbook for Manual Phishing
- Playbook for Automated Phishing
- Playbook para malware manual
- Playbook for Automated Malware
- Playbook para falha de login manual

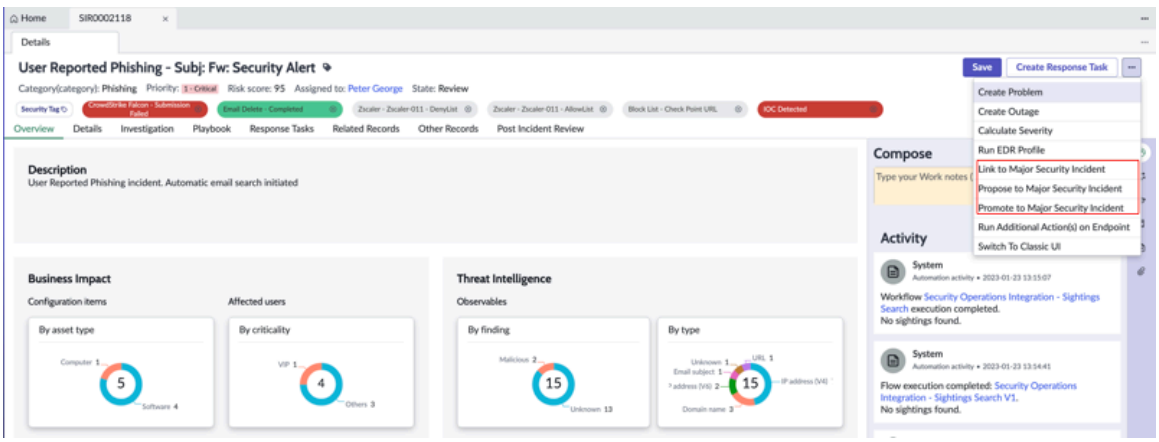
Trabalhando com registros MSI

Usando o espaço do Security Incident Response, você pode propor, promover ou vincular incidentes de segurança como incidentes de segurança graves quando os incidentes são identificados como ameaça crítica para a organização.

Depois de instalar Gestão de incidentes graves de segurança (MSIM) em sua instância Now Platform, você pode lidar com a transição de incidentes de segurança para incidentes graves.

As ações de IU Gestão de incidentes graves de segurança (MSIM) são exibidas na parte superior direita da faixa do formulário de incidente de segurança do espaço de SIR. Selecione a ação de IU conforme aplicável.

Nota:
Algumas ações são contextuais. Por exemplo, a ação Desvincular está disponível somente quando o incidente de segurança já foi proposto, promovido ou vinculado a um incidente de segurança grave.



Propor como incidente de segurança grave

Proponha um incidente de segurança como um incidente de segurança grave (MSI).

Antes de Iniciar

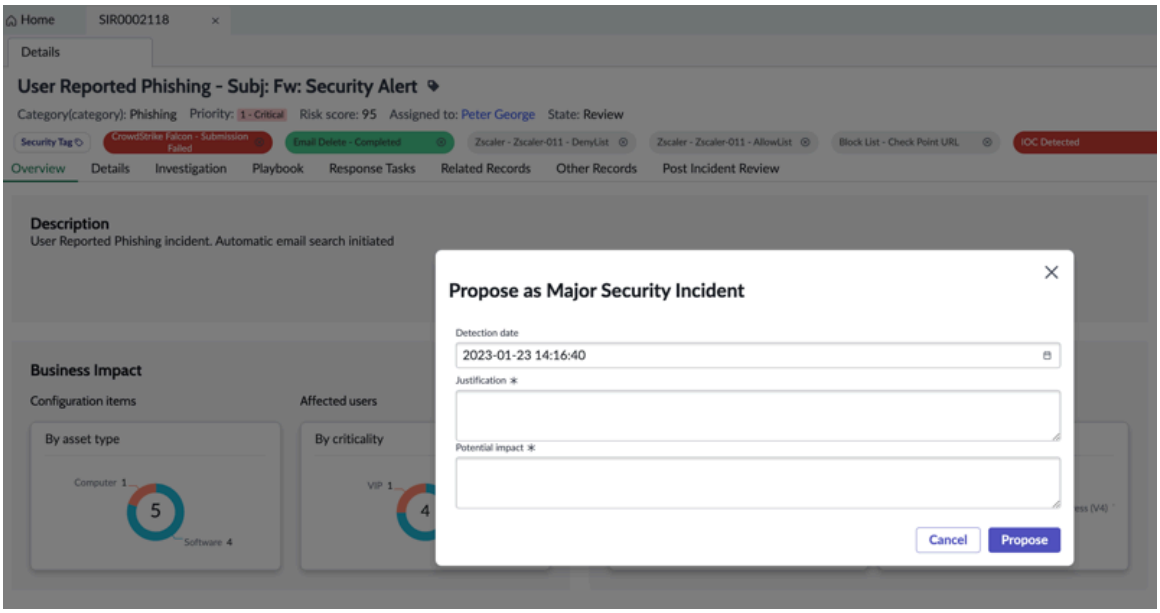
Função necessária: sn_si.analyst.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Clique **em Propor incidente de segurança grave**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No formulário, preencha os campos como Data de detecção, Justificativa e Impacto potencial.
5. Clique **em Propor**.
   O registro de incidente é proposto como um candidato a incidente de segurança grave.
   Depois que o registro de incidente é proposto como um candidato a incidente de segurança grave, o marcador **Candidato** a incidente de segurança grave é aplicado e exibido na faixa do formulário de incidente de segurança.

> **Nota:**
> Clique **em Desvincular do incidente de segurança grave** para desvincular o incidente se você não quiser propor ou não tiver nenhum impacto crítico. O incidente será desvinculado e as listas na exibição de lista para o analista de segurança para correção.

Promover a incidente de segurança grave

Promova um incidente de segurança a incidente de segurança grave.

Antes de Iniciar

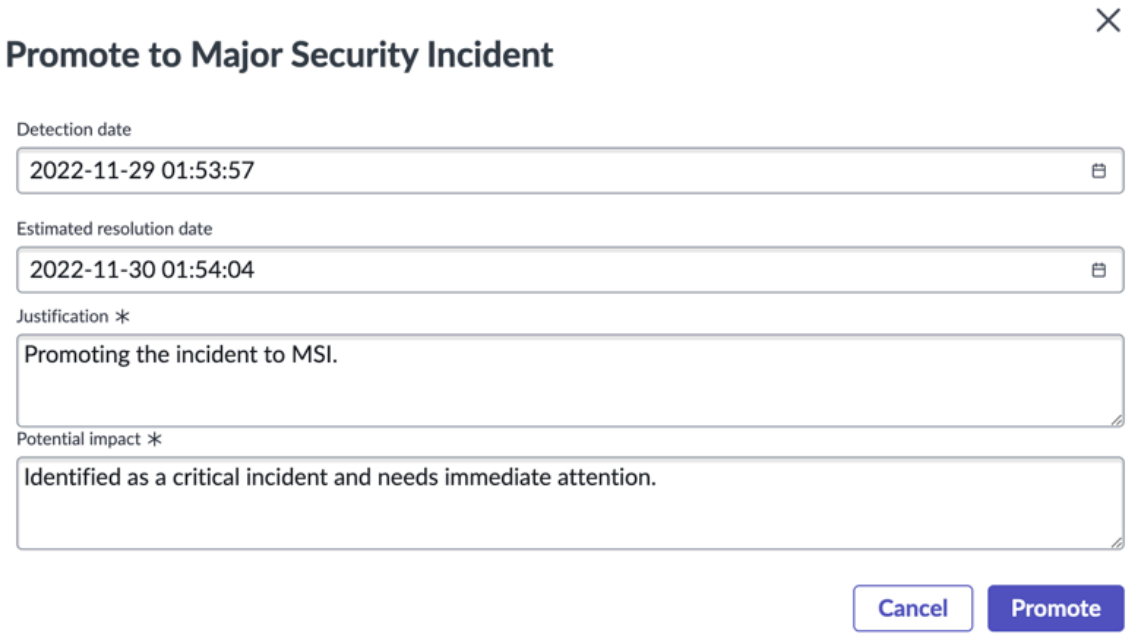
Função necessária: sn_si.analyst.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Clique **em Promover a incidente de segurança grave**.
4. No formulário, preencha os campos como Data de detecção, Data de resolução estimada, Justificativa e Impacto potencial.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique **em Promover**.
   O registro de incidente é promovido como um incidente de segurança grave.
   Depois que o registro de incidente é promovido como um incidente de segurança grave, o marcador **de incidente** de segurança grave é aplicado e exibido na faixa do formulário.

> **Nota:**
> Você também pode desvincular o incidente de segurança grave se o incidente não for crítico, o incidente será desvinculado e listado na exibição de lista para a correção do analista de segurança.

Link para o incidente de segurança grave

Vincule um incidente de segurança a um incidente de segurança grave como incidente(s) de segurança secundário(s).

Antes de Iniciar

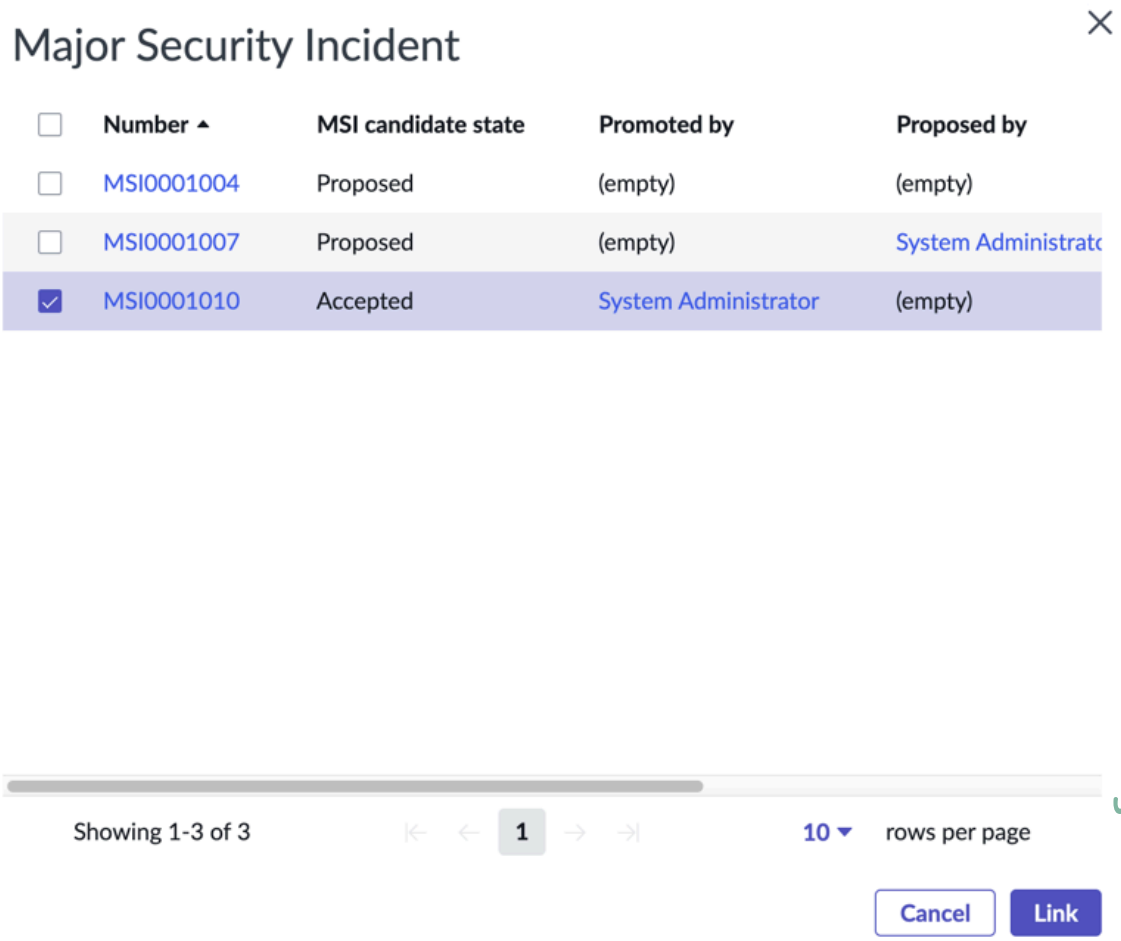
Função necessária: sn_si.analyst.

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Abra qualquer incidente de segurança.
3. Clique **em Link para incidente de segurança grave**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Selecione o(s) incidente(s) a ser(em) vinculado(s) a um incidente de segurança grave.
5. Clique em **Vincular**.
6. O registro de incidente é vinculado como um incidente secundário do incidente de segurança grave. Depois que o incidente é vinculado como um incidente secundário a um incidente de segurança grave, o marcador **Incidente** de segurança grave é aplicado e exibido na faixa do formulário.

Como trabalhar com ações de IU de formulário

A seguir estão as ações de IU que são exibidas no formulário de incidente de segurança.

Para navegar até as ações de IU do formulário:

1. Ir para **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Selecione qualquer incidente de segurança na exibição de lista.
3. Todas as ações de IU estão presentes no canto superior direito do formulário de incidente de segurança.

Ações de IU de formulário do espaço

Nome do Campo	Descrição
Salvar	Salve ou atualize o registro do Security Incident Response depois de fazer mudanças.
Criar Tarefa de Resposta	Crie uma tarefa de resposta para o incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição
Compor e-mails	Redija e-mails para o incidente de segurança.
Adicionar Playbook	Adicione o playbook manualmente para o incidente de segurança.
Criar Incidente	Crie um incidente no incidente de segurança.
Criar caso de Atendimento ao cliente	Crie um caso de atendimento ao cliente para o incidente de segurança que será rastreado pela equipe do Customer Service Management (CSM). **Nota:** Esta opção está disponível somente quando o Customer Service Management (CSM) está instalado.
Abrir fluxo(s) de trabalho associado(s)	Abra qualquer contexto de fluxo de trabalho associado ao incidente de segurança. Esta opção ficará visível somente se houver fluxos de trabalho.
Criar solicitação de mudança	Crie uma solicitação de mudança no incidente de segurança.
Criar problema	Crie um problema no incidente de segurança.
Criar indisponibilidade	Crie uma indisponibilidade no incidente de segurança.
Calcular Gravidade	Calcule a severidade de um incidente de segurança usando calculadoras predefinidas. A severidade é calculada com base nas regras predefinidas nas calculadoras. A severidade de um incidente é baseada na pontuação de risco, no impacto nos negócios e na prioridade.
Executar perfil de EDR	Selecione e execute o perfil de EDR para a integração necessária. **Nota:** Esta opção está disponível somente quando alguma integração está instalada.
Link para o incidente de segurança grave	Vincule um incidente de segurança a um incidente de segurança grave.
Relatar evento de risco	Relate este incidente de segurança como um evento de risco para a equipe de Gestão de riscos. A equipe de Gestão de riscos analisa o evento e garante que esses eventos e as perdas associadas não se repitam. **Nota:** Esta opção está disponível somente quando o Risk Management está instalado.
Desvincular de um incidente de segurança grave	Desvincular do incidente de segurança grave.
Propor como incidente de segurança grave	Propor um incidente de segurança como um incidente de segurança grave.
Promover a incidente de segurança grave	Promova um incidente de segurança como um incidente de segurança grave.
Executar ações adicionais no endpoint	Execute ações adicionais no endpoint.

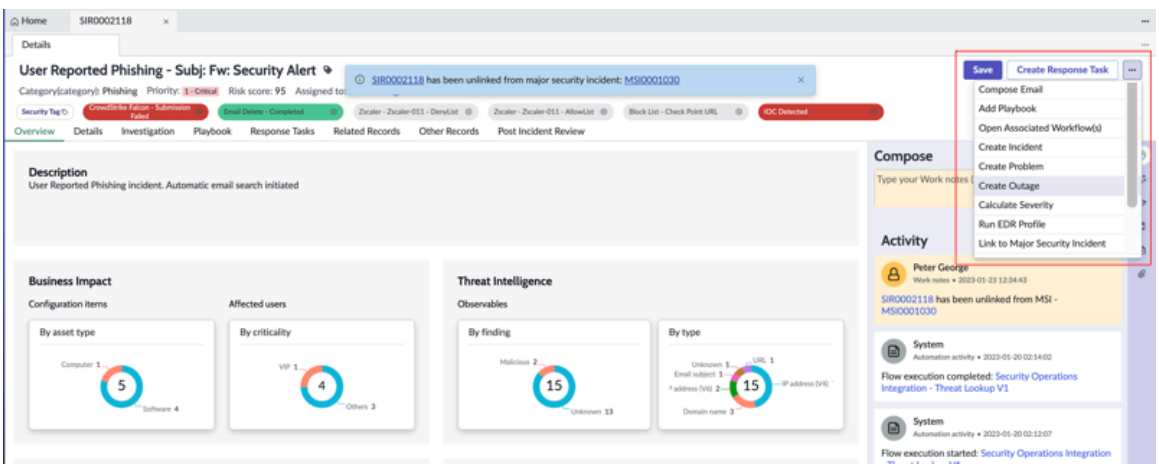
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição
	Nota: Esta opção está disponível somente quando as integrações de endpoint estão instaladas. Por exemplo: FireEye HX
Criar um novo evento no MISP	Crie e modifique eventos no MISP automaticamente ou manualmente. **Nota:** Esta opção está disponível somente quando a integração do MISP está instalada.
Associar técnica do MITRE ATT&K	Associe as técnicas do MITRE ATT&K ao incidente de segurança. **Nota:** Esta opção está disponível quando o MITRE ATT&K está instalado.
Mostrar informações do MITRE ATT&K	Mostra as informações do MITRE ATT&K associadas ao incidente de segurança. **Nota:** Esta opção está disponível quando o MITRE ATT&K está instalado.
Adicionar ao Caso de Segurança	Adicione o incidente de segurança a um caso de segurança existente ou novo. **Nota:** Esta opção está disponível quando o Threat Intel está instalado.
Alternar para a IU Clássica	Permita que o analista alterne entre a IU clássica e a nova para que o analista também possa trabalhar nas funcionalidades existentes que ainda não estão disponíveis no novo espaço.
Cancelar	Cancele um incidente de segurança. Depois de selecionar **Cancelar,** todos os registros relacionados, como tarefas de resposta e incidentes de segurança secundários, também serão cancelados.
Deletar	Exclua um registro de incidente de segurança.

Tradução automática

4. Clique em um número de incidente de segurança para exibir o registro do incidente de segurança. Você pode ver as ações de IU na parte superior da página.



© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de fechamento de incidente de segurança

Feche o incidente de segurança atualizando o estado do incidente.

Antes de Iniciar

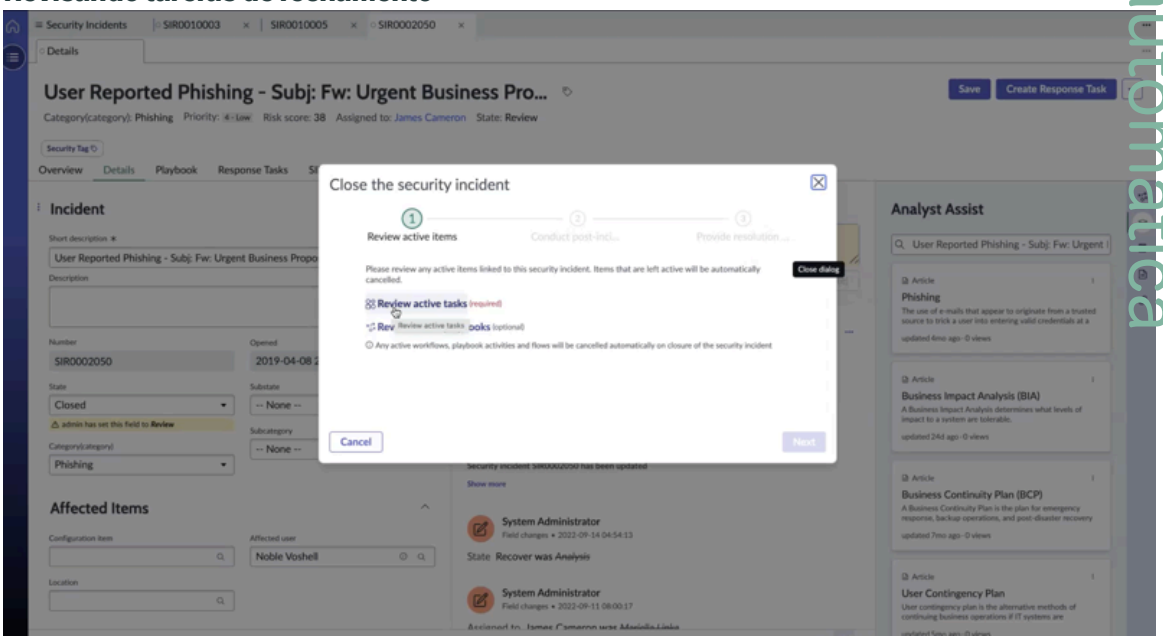
Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Espaço de resposta a incidentes de segurança**.
2. Por exemplo, vá para **Listas** > **Incidentes de segurança** > **Incidentes abertos**.
3. Abra um incidente que você deseja fechar.
4. Vá para a guia **Detalhes**.
5. Faça uma busca detalhada no estado do incidente e selecione **Fechar**.
6. Execute as atividades de encerramento.

   - Esta é uma etapa obrigatória para revisar qualquer tarefa antes de fechar um incidente de segurança. Todas as tarefas de resposta devem ser revisadas pelo analista e encerradas ou canceladas antes do encerramento como incidente de segurança. Quando o analista clica em **Revisar tarefas ativas**, o usuário é direcionado para a guia **Tarefas de resposta**. Uma mensagem de sessão será exibida, informando que você está no processo de encerrar um incidente de segurança. Clique **em continuar**.
   - Clique em **Continuar**. A primeira etapa - revisar as tarefas ativas no encerramento do incidente de segurança está concluída.

Revisando tarefas de fechamento



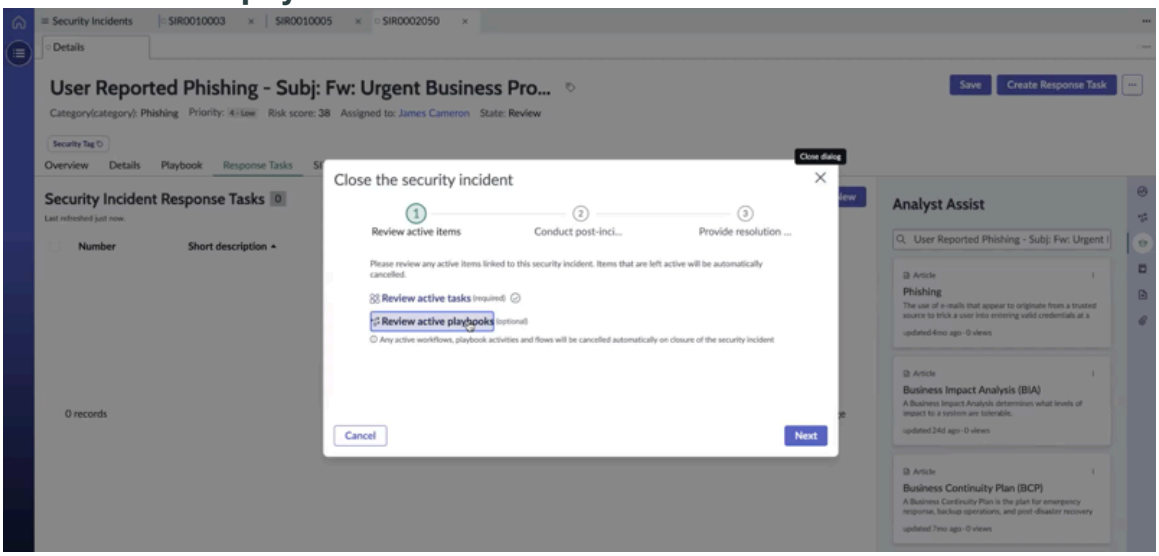
   - Avance para a próxima etapa para revisar os playbooks ativos para o analista revisar, que é uma etapa opcional. Você pode clicar no link para revisar a tarefa do playbook ativo e fechá-lo conforme necessário.

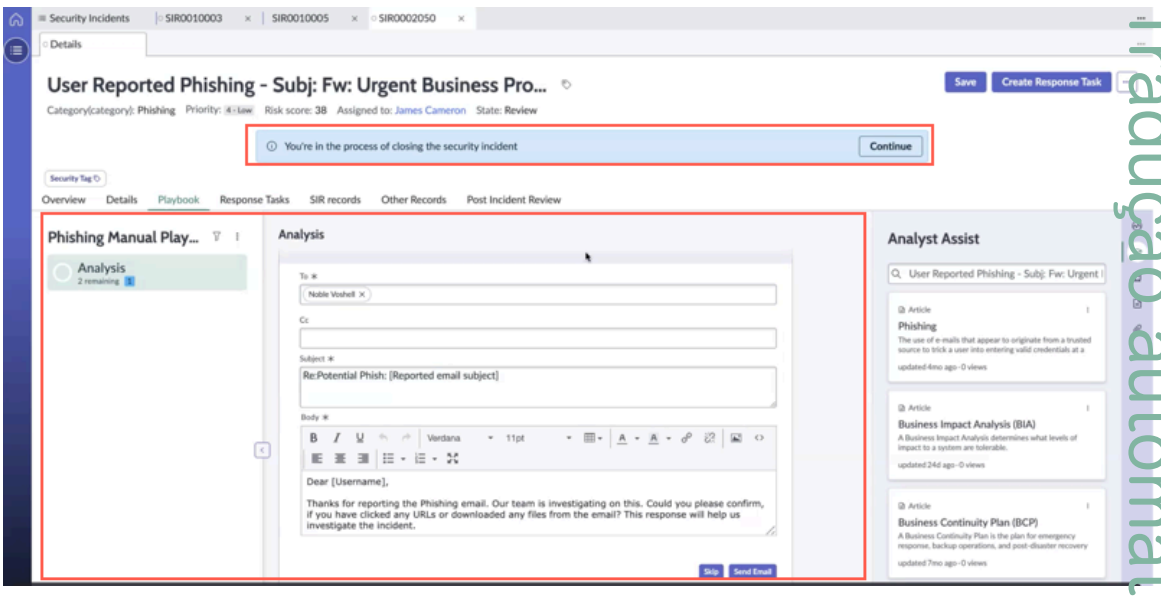
> **Nota:**
> Todos os fluxos de trabalho ativos, atividades do playbook e fluxos serão cancelados automaticamente no fechamento do incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Revisar tarefas do playbook



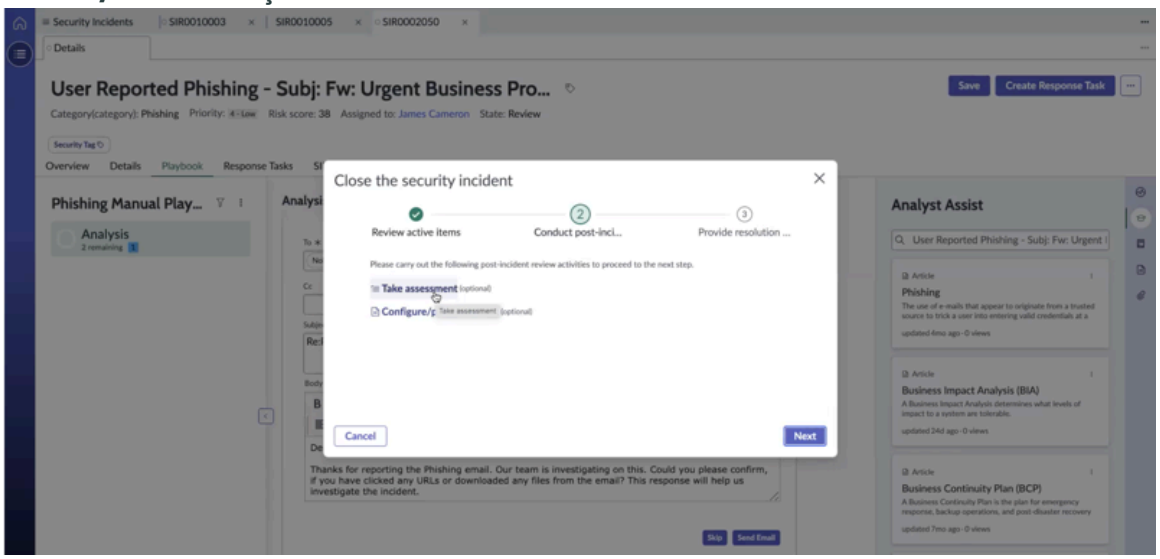


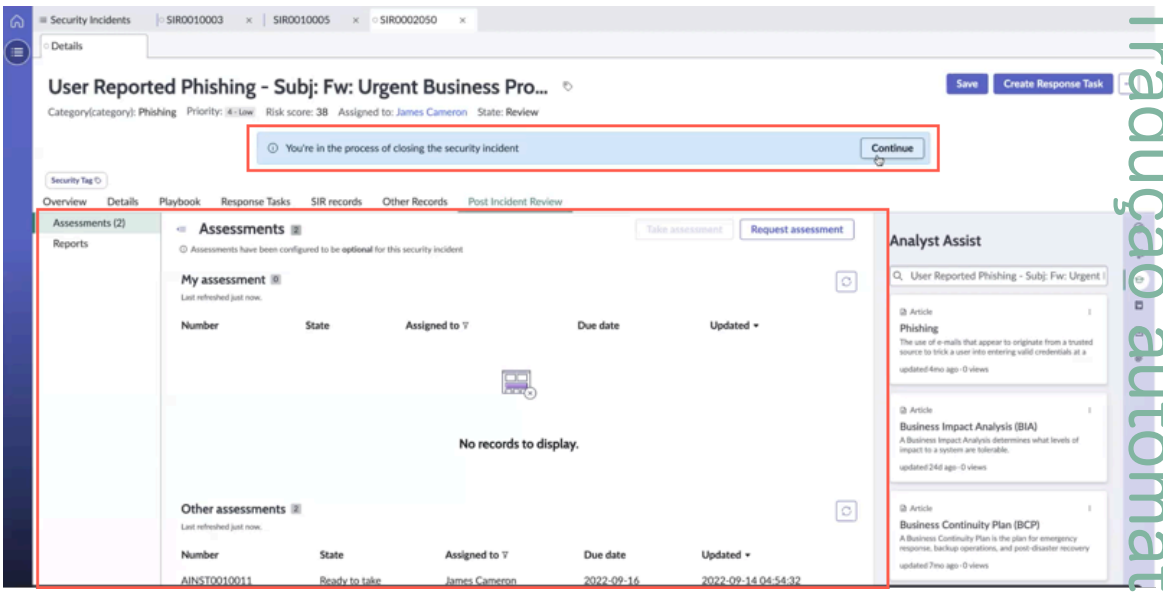
Tradução automática

- Relatório de revisão pós-incidente: agora você será movido para revisar as atividades pós-incidente para prosseguir com o fechamento. Se a avaliação for opcional, pule a etapa ou, se for obrigatória, faça a avaliação e conclua-a.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Revisar/fazer avaliação

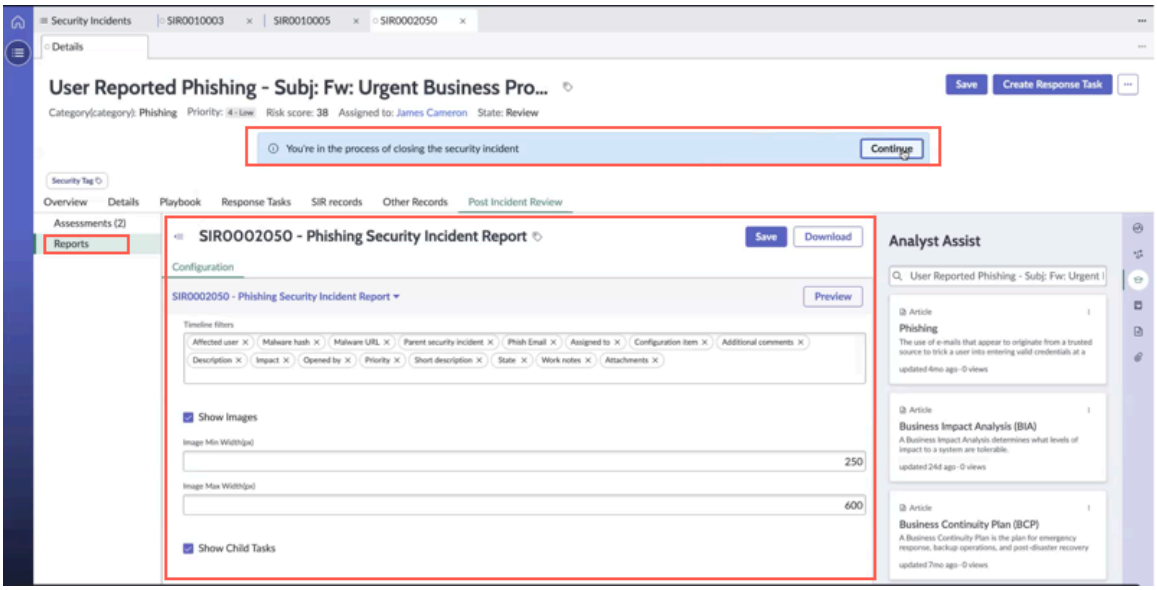




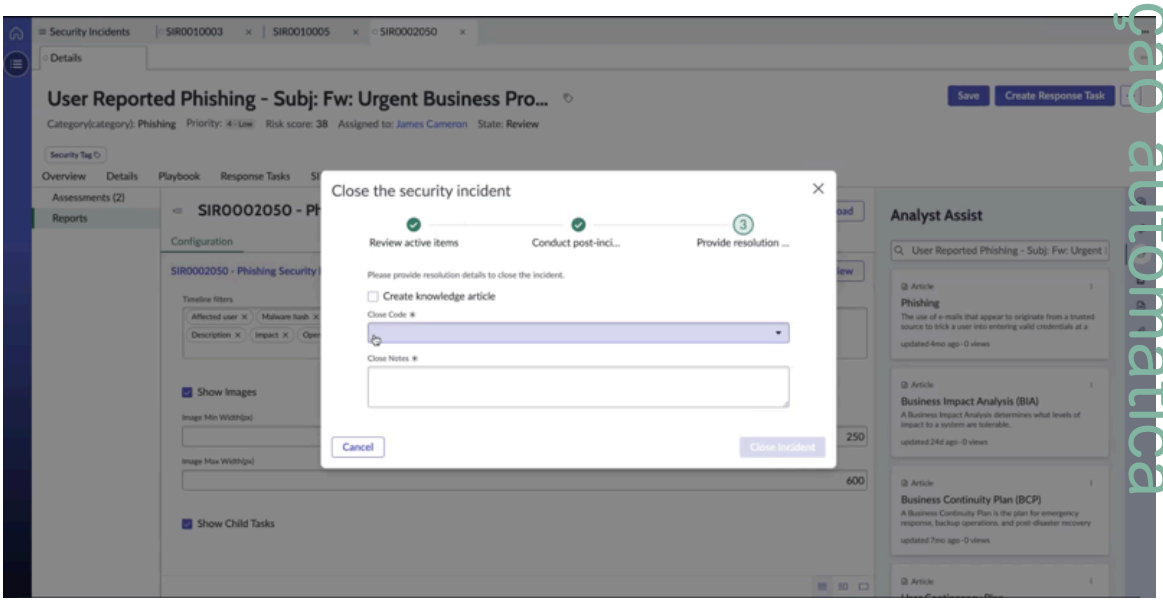
Tradução automática

- Configurar/visualizar relatório: esta é novamente uma etapa opcional. Clique no link para revisar o relatório e prosseguir para a **próxima** etapa.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- Fornecer detalhes da resolução: o analista pode marcar a caixa de seleção para criar artigos de conhecimento automaticamente.
- Forneça o Código de fechamento, as Anotações de fechamento e clique em **Fechar incidente**.



Nota:

Por alguma chance, se o analista cancelar a caixa de diálogo **Fechar o incidente de segurança**, o analista poderá navegar até a guia **Detalhes** e mudar o estado do incidente para **fechar** para continuar com o fechamento.

Exibição de painéis do espaço de SIR

Esta seção apresenta as métricas importantes para analisar seu processo Security Incident Response, como novos incidentes de segurança ou a idade média dos incidentes de segurança em aberto.

Na IU clássica, há alguns painéis padrão disponíveis na página inicial e Performance Analytics Painéis que estão disponíveis quando o plug-in Performance Analytics para Security Incident

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Response está instalado. Todos eles agora estarão disponíveis no novo espaço na seção **Painéis de SIR**.

Painéis padrão na página inicial:

- Visão geral do Security Incident Response
  - Visão geral do analista
  - Visão geral do gerente (compatível com versões futuras)
  - Visão geral do CISO (compatível com versões futuras)
- **Platform Analytics para** *Security Incident Response*
  - Explorador de incidentes de segurança
  - Painel do CISO (versão futura)
  - Gestão de incidentes de segurança
  - KPIs de Gestão de incidentes de segurança premium
  - Eficiência do Security Operations
  - Análise sensível ao contexto - Painel de SI

Nota:
Pode haver alguma repetição de painéis nas análises padrão e de plataforma para painéis de resposta a incidentes de segurança, como o painel CISO. Quando o plug-in estiver instalado, haverá conteúdo adicional nesses painéis e não estará disponível como duplicado.

Os usuários precisam instalar o plug-in dos painéis listados em Análise da plataforma para Painéis do Security Incident Response para que estejam presentes no espaço. Caso contrário, somente os painéis padrão estarão disponíveis.

Na versão atual do SIR Workspace, os painéis a seguir estão disponíveis na seção **Painéis de SIR**. Os outros painéis que estão ausentes estarão disponíveis em versões posteriores.

Painéis do Security Incident Response

Painel	Descrição
Painel padrão	
Visão Geral de Análise de Segurança	Com este painel, os analistas de segurança podem exibir os incidentes de segurança resumidos com base no trabalho de prioridade crítica do analista, no trabalho de alta prioridade, nos incidentes de segurança atribuídos ao analista, nas tarefas atribuídas aos analistas e na contagem de incidentes.
Painéis de Performance Analytics (PA) para Security Incident Response	
Explorador de incidentes de segurança	Com este painel, os gerentes e analistas de segurança podem exibir os incidentes de segurança resumidos e agrupados por categoria, subcategoria, local, prioridade e impacto nos negócios. Essas exibições permitem que gerentes e analistas obtenham informações rapidamente sobre a frequência com que os ataques estão ocorrendo e quais serviços de negócios são afetados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painéis do Security Incident Response

Painel	Descrição
Gestão de incidentes de segurança	Com este painel, os gerentes de segurança podem rastrear facilmente o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação.
Painel do CISO	Proposta para oferecer suporte em versão futura.
Eficiência do Security Operations	Com este painel, gerentes e analistas podem exibir métricas gerais de eficiência e medir o desempenho do SOC.
KPIs de Gestão de incidentes de segurança premium	Com este painel, os gerentes de segurança podem rastrear e exibir o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação.
Análise sensível ao contexto – S	Com este painel, os gerentes e analistas podem exibir os incidentes de segurança em aberto, a idade média dos incidentes de segurança em aberto, o tempo médio de encerramento dos incidentes de segurança, a porcentagem de incidentes de segurança que foram abertos e fechados no mesmo dia e a porcentagem do incidentes que não foram atualizados nos últimos 5 dias e 30 dias.

Acessar Painéis de SIR e PA

O ícone do **SIR Dashboards** é exibido no lado esquerdo da página inicial do espaço.

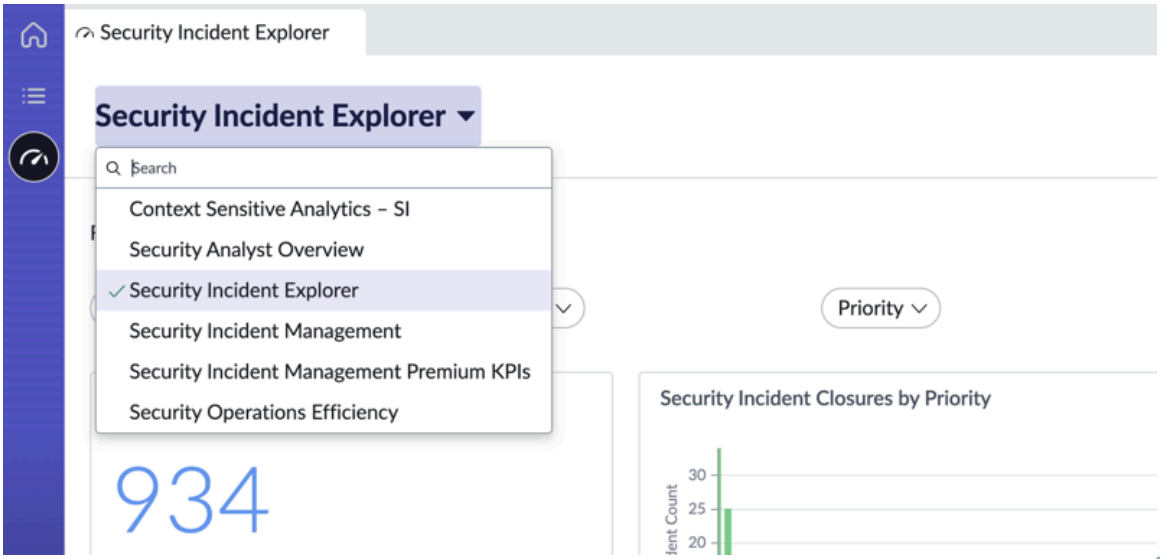
Nota:
Usuários com acesso sn_si.manager ou sn_si.admin podem editar os painéis. Os usuários devem estar no mesmo escopo dos painéis em que o usuário está tentando fazer edições. Por exemplo, o painel de visão geral do analista de segurança está disponível no espaço de SIR, então o usuário também deve estar no mesmo escopo de espaço de SIR para fazer as edições no painel.

1. Navegar até **Espaços** > **Espaço do Security Incident Management**.
2. Clique no do painel do **SIR Dashboards** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione o painel desejado na lista suspensa.



Você pode editar os painéis, adicionar novos elementos aos painéis e criar seus próprios painéis. Para obter mais informações sobre como usar painéis, consulte Como trabalhar com painéis dinâmicos .

Exibir painel Visão geral do analista de segurança

Com este painel, os analistas de segurança podem exibir os incidentes de segurança resumidos com base no trabalho de prioridade crítica dos analistas, no trabalho de prioridade alta, nos incidentes de segurança atribuídos ao analista, nas tarefas atribuídas aos analistas e na contagem de incidentes.

Antes de Iniciar

Por padrão, o painel Visão geral do analista de segurança é exibido para os usuários com acesso sn_si.analyst.

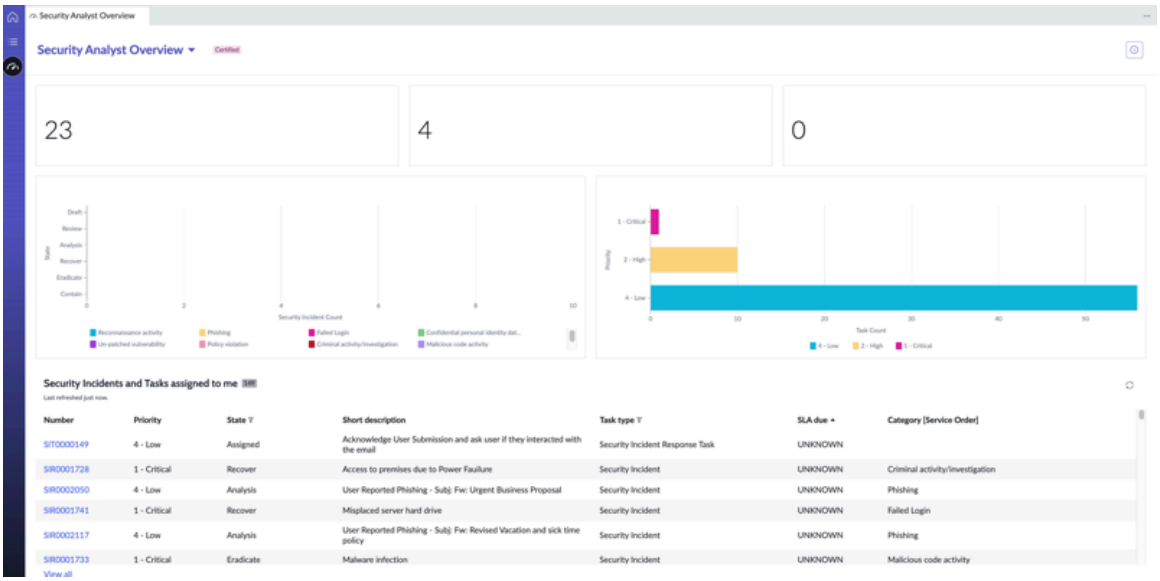
Função necessária: sn_si.analyst (Leitura), sn_si.manager ou sn_si.admin (Gravação)

Procedimento

1. Navegar até **Espaços** > **Security Incident Response**.
2. Clique no ícone **Painéis de SIR**, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Visão geral do analista de segurança** na lista suspensa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exiba o painel Visão geral do analista de segurança para obter outras ações. Para obter informações detalhadas sobre o painel Visão geral do analista de segurança, consulte Security Incident Response Soluções Análise da plataforma.

Exibir painel do Explorador de incidentes de segurança

Com este painel, os gerentes de segurança podem exibir os incidentes de segurança resumidos e agrupados por categoria, subcategoria, local, prioridade e impacto nos negócios.

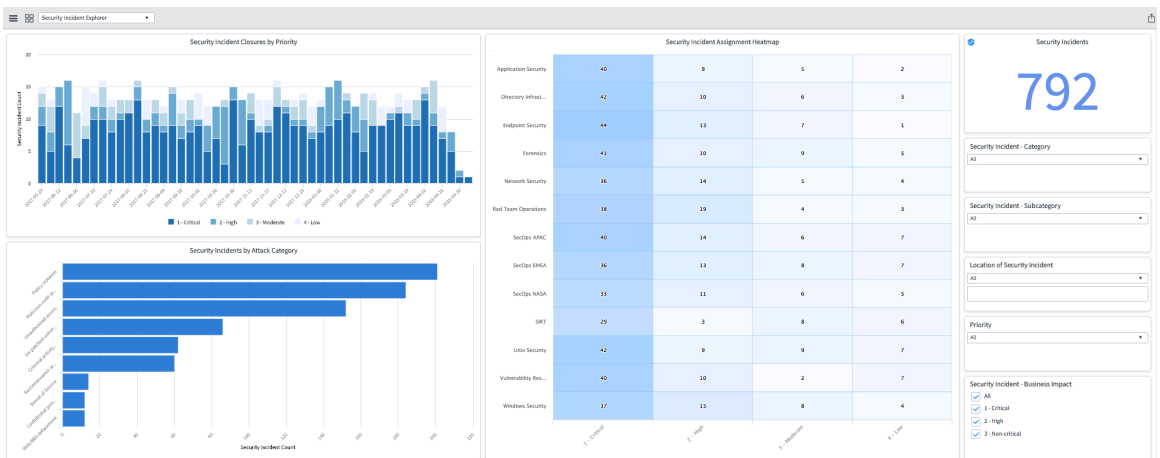
Antes de Iniciar

Por padrão, o painel do Security Incident Explorer é exibido para os usuários com acesso sn_si.manager.

Função necessária: sn_si.analyst (Leitura), sn_si.manager ou sn_si.admin (Gravação)

Procedimento

1. Navegar até **Espaços** > **Security Incident Response**.
2. Clique no ícone **Painéis de SIR**, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Explorador de incidentes de segurança** na lista suspensa.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exiba o painel do Security Incident Explorer para obter outras ações. Para obter informações detalhadas sobre o painel do Security Incident Explorer, consulte Painel do Security Incident Explorer.

Na versão atual, a lista de relatórios a seguir não é compatível com o painel do Security Incident Explorer:

- Mapa térmico de atribuição de incidente de segurança — A visualização do mapa térmico não está disponível.
- Mapa de incidente de segurança: a visualização do mapa não está disponível.

Exibir painel do Security Incident Management

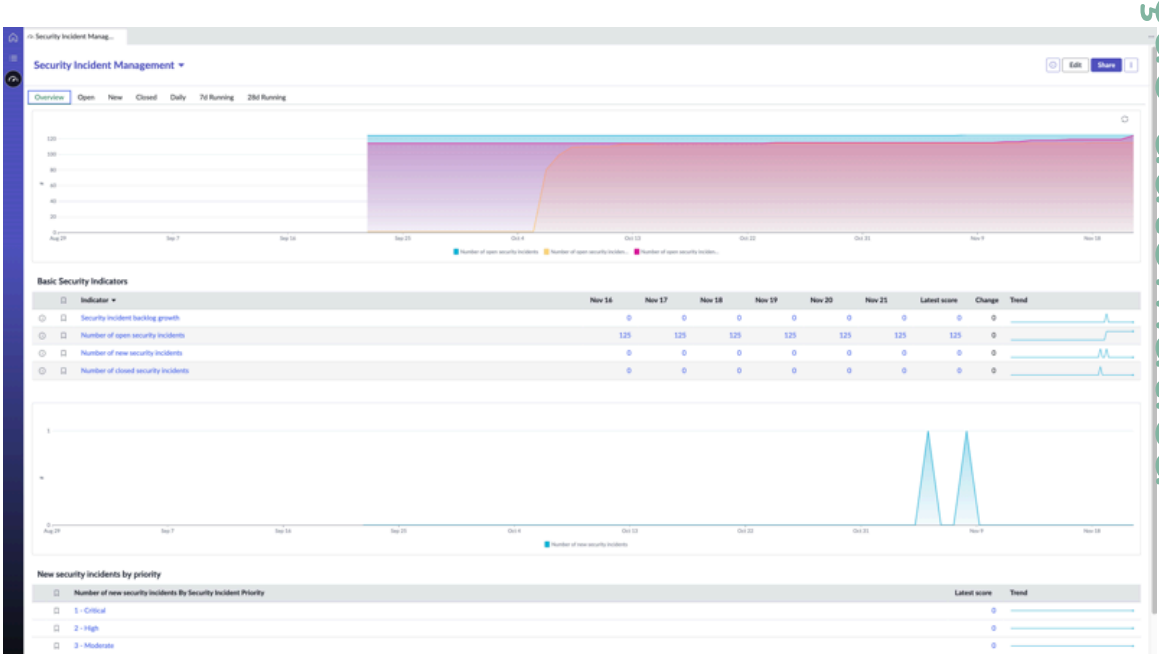
Com este painel, os gerentes de segurança podem rastrear facilmente o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Espaços** > **Security Incident Response**.
2. Clique no ícone **Painéis de SIR**, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Gestão de incidentes de segurança** na lista suspensa.



Exiba o painel do Security Incident Management para obter outras ações. Para obter informações detalhadas sobre o painel do Security Incident Management, consulte Painel do Security Incident Management.

Exibir painel do Security Operations Efficiency

Os gerentes do centro de operações de segurança (SOC) podem exibir as métricas gerais de eficiência e medir o desempenho individual dos membros da equipe do SOC na organização.

Antes de Iniciar

Na versão atual, o relatório a seguir não é compatível com o painel Eficiência do Security Operations:

Tradução automática

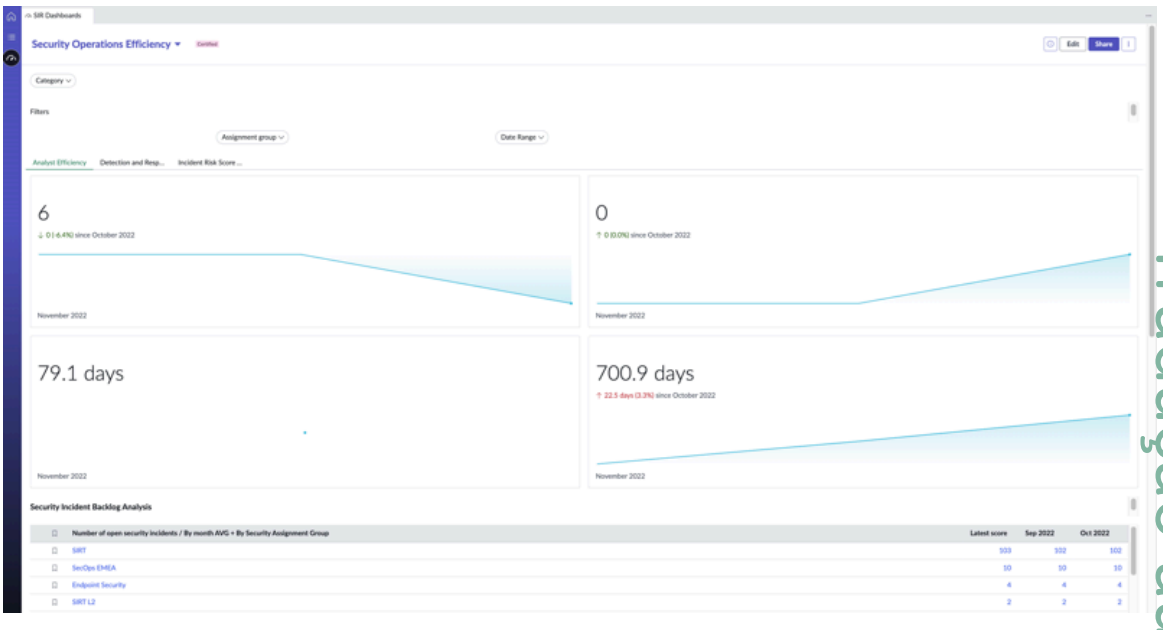
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Análise da fase do Incidente de segurança - Workbench não está disponível

Função necessária: sn_si.analyst (leitura), sn_si.manager ou sn_si.admin (gravação)

Procedimento

1. Navegar até **Espaços** > **Security Incident Response**.
2. Clique no ícone **Painéis de SIR**, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Eficiência do Security Operations** na lista suspensa.



Exiba o painel Eficiência do Security Operations para obter outras ações. Para obter informações detalhadas sobre o painel Eficiência do Security Operations, consulte Painel Eficiência do Security Operations.

Exibir painel de KPIs premium do Security Incident Response

Com este painel, os gerentes de segurança podem rastrear e exibir o volume, o desempenho e o andamento dos incidentes de segurança, desde a análise/detecção inicial até a contenção, erradicação e recuperação.

Antes de Iniciar

Na versão atual, a lista de relatórios a seguir não é compatível com o painel de KPIs Premium do Security Incident Response:

- Processar por estado - Workbench não está disponível
- Processar por Idade - Workbench não está disponível
- Incidentes de segurança em aberto por mais de 30 dias por grupo de atribuição e estado - a visualização de mapa térmico não está disponível.
- Incidentes de segurança não atualizados há mais de 30 dias por grupo de atribuição e estado - a visualização do mapa térmico não está disponível.
- Incidentes de segurança com designado que não está ativo - a visualização do mapa térmico não está disponível.

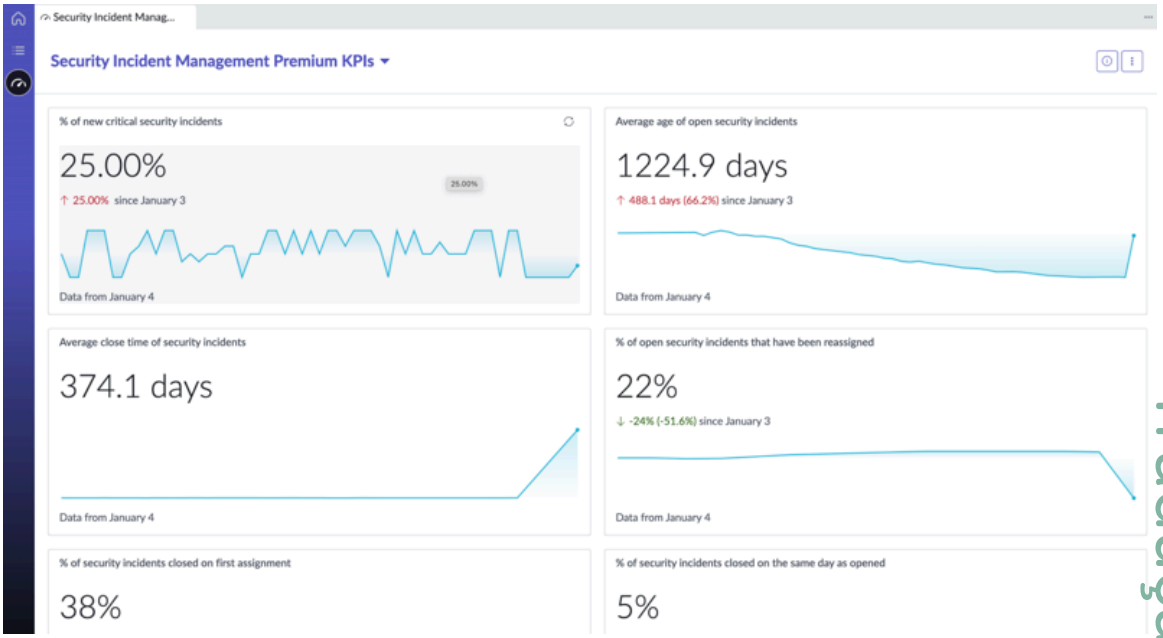
Função necessária: sn_si.analyst (leitura), sn_si.manager ou sn_si.admin (gravação)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Espaços** > **Security Incident Response**.
2. Clique no ícone **Painéis de SIR**, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **KPIs premium do Security Incident Response** na lista suspensa.



4. Exiba o painel de KPIs do Security Incident Response Premium para obter outras ações.
   Para obter informações detalhadas sobre o painel de KPIs Premium do Security Incident Response, consulte Painel do Security Incident Response Premium.

Exibir análise sensível ao contexto - Painel de SI

Com este painel, os gerentes e analistas podem exibir os incidentes de segurança em aberto, a idade média dos incidentes de segurança em aberto, o tempo médio de encerramento dos incidentes de segurança, a porcentagem de incidentes de segurança que foram abertos e fechados no mesmo dia e a porcentagem do incidentes que não foram atualizados nos últimos 5 dias e 30 dias.

Antes de Iniciar

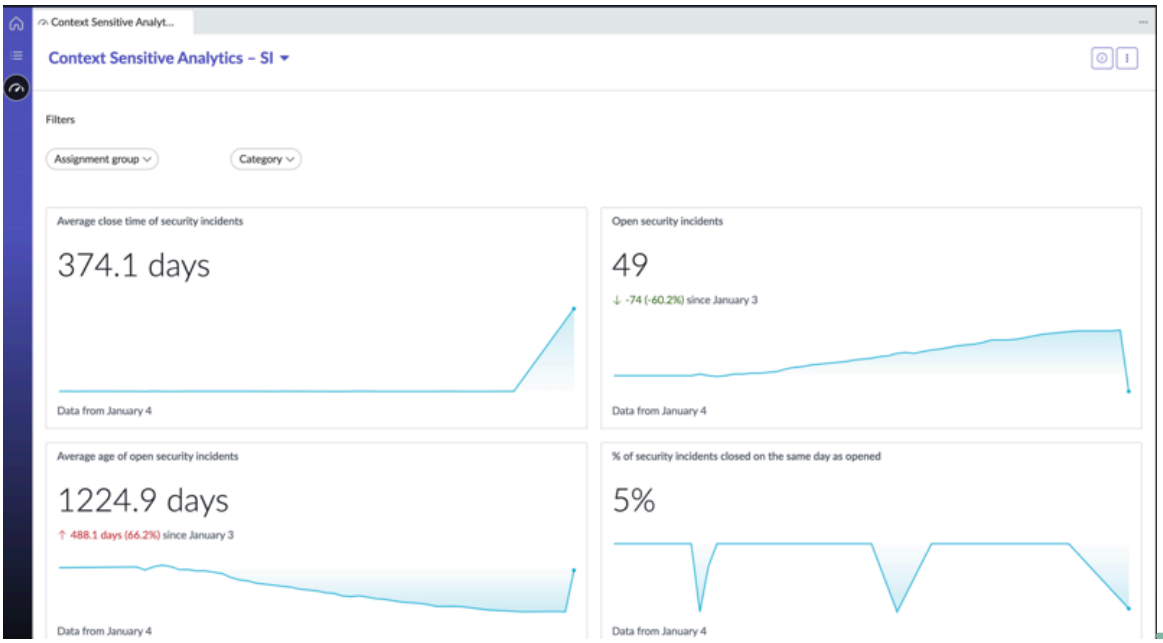
Função necessária: sn_si.analyst (leitura), sn_si.manager ou sn_si.admin (gravação)

Procedimento

1. Navegar até **Todos** > **Espaços** > **Security Incident Response**.
2. Clique no ícone **Painéis de SIR**, exibido no lado esquerdo da página inicial do espaço.
3. Selecione **Análise sensível ao contexto - SI** na lista suspensa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Exiba o painel Context Sensitive Analytics – SI para obter outras ações.

Exibir painel do CISO

Este painel fornece aos diretores de segurança da informação (CISOs) uma visão geral de alto nível dos incidentes de segurança e das tendências de incidentes semanais na instância na forma de gráficos. Esses gráficos ajudam a exibir e analisar com eficácia o desempenho do Security Operations Center (SOC).

Antes de Iniciar

- Função necessária: sn_si.admin e sn_si.ciso - Editar e exibir incidentes.
- Certifique-se de ter o aplicativo Performance Analytics para Security Incident Response instalado.

Por Que e Quando Desempenhar Esta Tarefa

Nota:
O painel CISO e o painel Visão geral do CISO eram dois painéis diferentes na IU clássica. Mas agora os recursos dos dois painéis foram mesclados no painel do CISO.

O painel do CISO fornece informações importantes sobre seus incidentes de segurança semanalmente. Você pode configurar indicadores e coletar snapshots de dados dos incidentes que correspondam às condições nas propriedades do indicador. Os dados coletados são visualizados usando widgets no painel.

Você pode visualizar as tendências semanais usando os widgets no painel do CISO. Os dados ou estatísticas das tendências de seus incidentes de segurança são coletados das propriedades do indicador de incidentes semanais que são definidas pela organização. Você pode obter informações importantes usando os seguintes gráficos:

- **Tempo médio de identificação (semanal)**: este gráfico ilustra o tempo médio semanal necessário para identificar um incidente de segurança.
- **Tempo médio de contenção (semanal)**: este gráfico ilustra o tempo médio semanal necessário para conter um incidente de segurança.

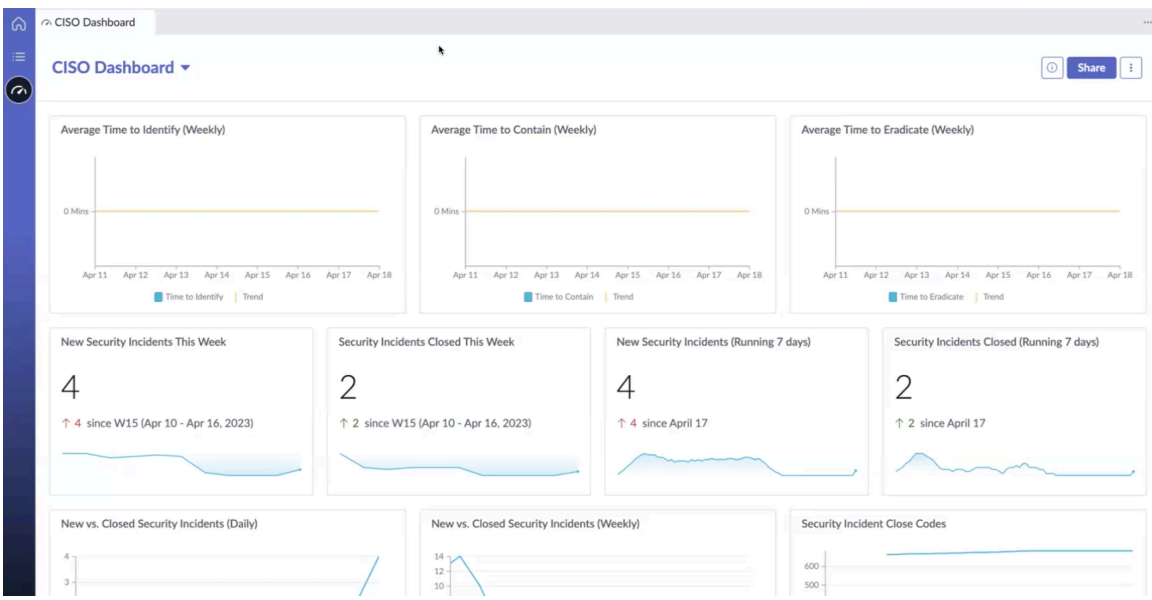
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Tempo médio para erradicar (semanalmente)**: este gráfico ilustra o tempo médio semanal necessário para erradicar um incidente de segurança.
- **Novos incidentes de segurança nesta semana**: este gráfico ilustra o número de novos incidentes de segurança nesta semana.
- **Incidentes de segurança encerrados nesta semana**: este gráfico ilustra o número de incidentes de segurança encerrados nesta semana.
- **Novos incidentes de segurança (em execução há 7 dias)**: este gráfico ilustra o número de novos incidentes de segurança em execução por uma semana.
- **Incidentes de segurança encerrados (em execução há 7 dias)**: este gráfico ilustra o número de novos incidentes de segurança que estão encerrados, mas estão em execução há uma semana.
- **Incidentes novos versus encerrados (diariamente)**: este gráfico ilustra a comparação entre os novos incidentes de segurança diários e os incidentes de segurança encerrados diariamente.
- **Incidentes novos versus encerrados (Semanalmente)**: este gráfico ilustra a comparação entre os novos incidentes de segurança semanais e os incidentes de segurança encerrados semanalmente.
- **Códigos**encerrados de incidentes de segurança : este gráfico ilustra os códigos encerrados dos incidentes de segurança.

Procedimento

1. Navegar até **Todos** > **Espaços** > **Security Incident Response**.
2. Clique no ícone **Painéis de SIR** no lado esquerdo da página inicial do espaço.
3. Selecione **Painel do CISO** na lista suspensa.



4. Exiba o painel do CISO para obter outras ações.

Exibir painel Visão geral de relatórios do CISO

Este painel fornece aos diretores de segurança da informação (CISOs) uma visão geral de relatório de alto nível dos incidentes de segurança e tendências de incidentes semanais

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

na instância na forma de gráficos. Esses gráficos ajudam a exibir e analisar com eficácia o desempenho do Security Operations Center (SOC).

Antes de Iniciar

Função necessária: sn_si.admin e sn_si.ciso - Editar e exibir incidentes.

Por Que e Quando Desempenhar Esta Tarefa

O painel Visão geral de relatórios do CISO fornece informações importantes sobre os incidentes de segurança semanalmente e você pode visualizar as tendências semanais usando widgets. Você pode obter informações importantes sobre o Relatório do CISO usando os seguintes gráficos:

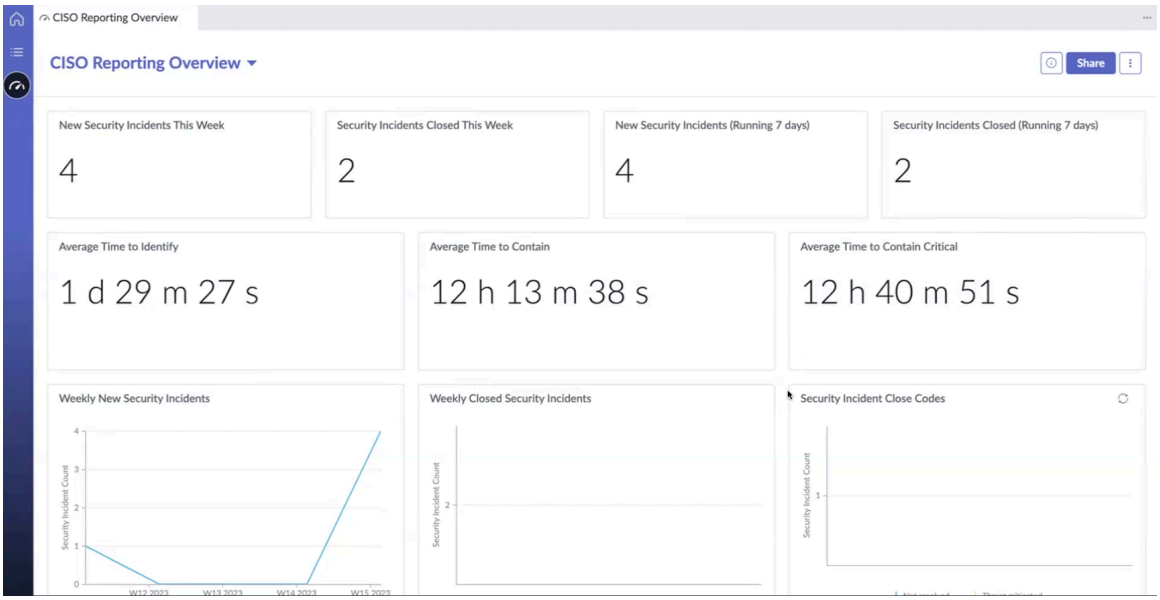
- **Novos incidentes de segurança nesta semana**: este bloco exibe o relatório do número de novos incidentes de segurança nesta semana.
- **Incidentes de segurança encerrados nesta semana**: este bloco exibe o relatório do número de incidentes de segurança encerrados nesta semana.
- **Novos incidentes de segurança (em execução há 7 dias)**: este bloco exibe o relatório do número de novos incidentes de segurança em execução por uma semana.
- **Incidentes de segurança encerrados (em execução há 7 dias)**: este bloco exibe o relatório do número de novos incidentes de segurança encerrados, mas que estão em execução há uma semana.
- **Tempo médio de identificação**: este bloco exibe o relatório do tempo médio semanal gasto para identificar incidentes de segurança.
- **Tempo médio de contenção**: este bloco exibe o relatório do tempo médio semanal necessário para conter os incidentes de segurança.
- **Tempo médio para conter incidentes de segurança críticos**: este bloco exibe o relatório do tempo médio semanal gasto para conter incidentes de segurança críticos.
- **Novos incidentes de segurança semanais**: este gráfico ilustra o relatório dos novos incidentes de segurança semanais.
- **Incidentes**de segurança encerrados semanalmente : este gráfico ilustra o relatório dos incidentes de segurança encerrados semanalmente.
- **Códigos de incidentes de segurança encerrados**: este gráfico ilustra o relatório dos códigos de encerramento dos incidentes de segurança.

Procedimento

1. Navegar até **Todos** > **Espaços** > **Security Incident Response**.
2. Clique no ícone **Painéis de SIR** no lado esquerdo da página inicial do espaço.
3. Selecione **Visão Geral de Relatórios do CISO** na lista suspensa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Exiba o painel de relatórios do CISO para obter outras ações.

Exibir painel Visão geral do gerenciador de incidentes de segurança

Este painel fornece aos gerentes uma visão geral de alto nível dos incidentes de segurança críticos ou de prioridade alta em um nível de equipe, SLAs que estão prestes a expirar em 24 horas e tendências de incidentes semanais na instância na forma de relatórios e gráficos.

Antes de Iniciar
Função necessária:

- sn_si.admin — Editar e exibir o painel.
- sn_si.manager — Exibir painel.

Por Que e Quando Desempenhar Esta Tarefa
Você pode analisar os incidentes de segurança críticos ou de prioridade alta, ou SLAs que precisam de atenção imediata. Você também pode visualizar as tendências semanais usando os widgets no painel Visão geral do Security Incident Manager. Os dados ou estatísticas das tendências semanais ou mensais de seus incidentes de segurança são coletados das tabelas de incidentes que são definidas pela organização. Você pode obter informações importantes usando os seguintes gráficos:

- **Incidentes de segurança críticos da equipe**: este bloco exibe o número de incidentes de segurança críticos da equipe nesta semana.
- **Incidentes**de alta segurança da equipe : este bloco exibe o número de incidentes de alta segurança da equipe nesta semana.
- **ANS que expiram em 24 horas**: este bloco exibe o número de ANS que expirarão em 24 horas.
- **Tempo médio de identificação**: este bloco exibe o tempo médio semanal necessário para identificar incidentes de segurança.
- **Tempo médio de contenção**: este bloco exibe o tempo médio semanal necessário para conter os incidentes de segurança.
- **Tempo médio para conter incidentes de segurança críticos**: este bloco exibe o tempo médio semanal necessário para conter incidentes de segurança críticos.

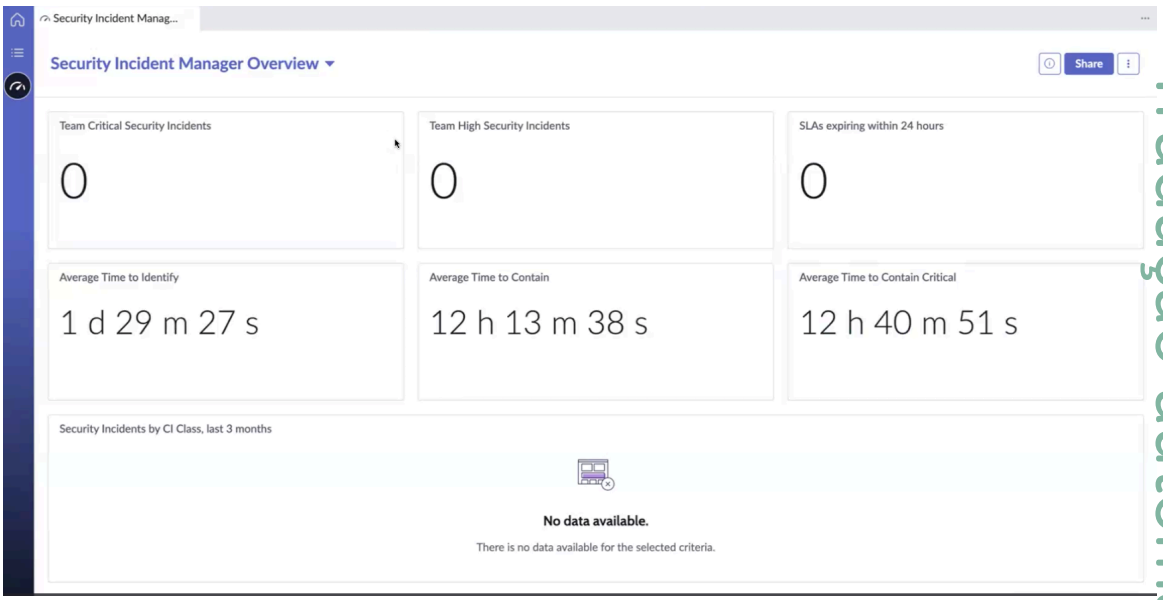
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Incidente de segurança por classe de IC, últimos 3 meses**: este gráfico ilustra as tendências de todos os incidentes de segurança com base na classe de IC nos últimos três meses.
- **Tendência de todos os incidentes de segurança por categoria**: este gráfico ilustra as tendências de todos os incidentes de segurança com base na categoria.
- **Tendência de todos os incidentes de segurança por prioridade**: este gráfico ilustra as tendências de todos os incidentes de segurança com base na prioridade.

Procedimento

1. Navegar até **Todos** > **Espaços** > **Security Incident Response**.
2. Clique no ícone **Painéis de SIR** no lado esquerdo da página inicial do espaço.
3. Selecione **Visão geral do gerenciador de incidentes de segurança** na lista suspensa.



4. Exiba a Visão geral do gerenciador de incidentes de segurança para obter outras ações.

Criação de incidente de segurança

Os incidentes de segurança podem ser criados manualmente a partir do formulário ou automaticamente por meio de eventos de segurança recebidos de ferramentas integradas de monitoramento de alertas de terceiros, como o Splunk.

Se você tiver uma função de segurança, poderá usar qualquer um dos métodos a seguir para criar incidentes de segurança manualmente.

Métodos para criar manualmente incidentes de segurança

Método	Descrição
Criado manualmente a partir da lista de Incidentes de segurança	Na lista Incidente de segurança, clique em **Novo** para criar um novo incidente de segurança.
Criado manualmente a partir do Catálogo de incidentes de segurança	Você pode criar incidentes de segurança selecionando as categorias de ameaças à segurança definidas no catálogo de incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métodos para criar manualmente incidentes de segurança

Método	Descrição
Gestão de incidentes	No formulário de Incidente no gerenciamento de incidentes, clique em **Criar incidente de segurança** para criar um novo incidente de segurança.
Convertido manualmente de uma solicitação de segurança	No formulário de solicitação de segurança, clique em **Converter em incidente de segurança** para criar um novo incidente de segurança.
Criado manualmente a partir de um alerta da Gestão de eventos	No formulário Alertas do Event Management, clique em **Criar incidente de segurança** para criar um novo incidente de segurança a partir de um alerta.
Criado manualmente a partir de um alerta	No formulário Alerta da Gestão de eventos, clique em **Criar incidente de segurança** para criar um novo incidente de segurança.
Convertido manualmente de um registro de vulnerabilidade (se o plug-in Vulnerability Response estiver ativado)	No formulário Itens de vulnerabilidade, clique em **Criar incidente de segurança** para criar um novo incidente de segurança.

Criação automática de incidentes de segurança

Geralmente, os administradores de segurança são responsáveis por configurar regras de alerta usadas para gerar automaticamente incidentes de segurança.

Método de administração de segurança para criar incidentes de segurança

Método	Descrição
Criado automaticamente usando regras de alerta	Os incidentes de segurança podem ser criados com base nas regras de alerta definidas na Gestão de eventos na aplicação do seu datacenter .

Criação manual de incidente de segurança

Você pode criar um incidente de segurança a partir do formulário de Incidente de segurança, bem como de vários outros formulários.

Você pode criar incidentes de segurança com base em um registro existente a partir dos seguintes formulários:

- Em qualquer lista de incidentes de segurança
- Formulário de incidente
- Gestão de eventos Formulário de alerta
- Formulário de itens vulneráveis
- Formulário de solicitação de segurança

Criar um incidente de segurança a partir da lista de Incidentes de segurança

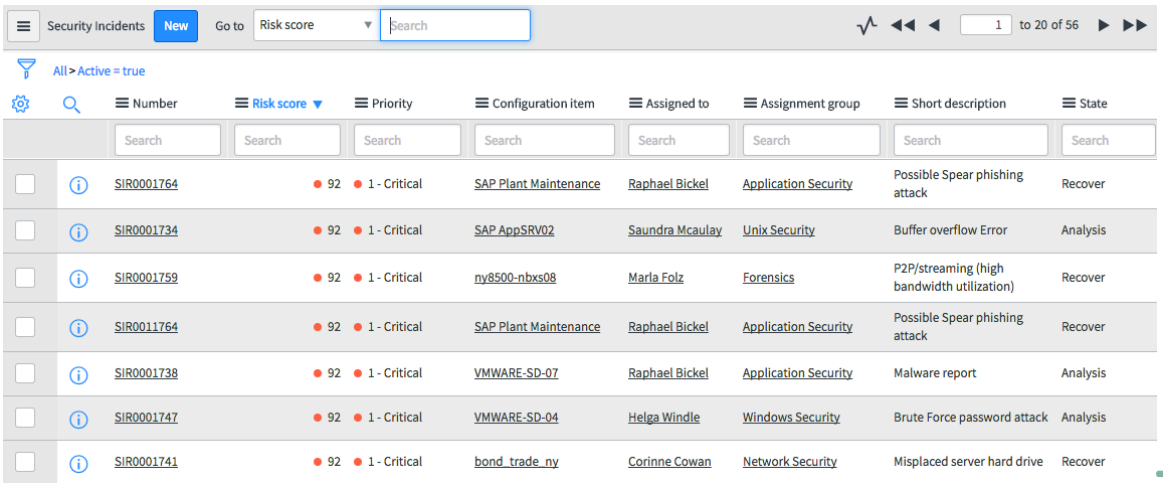
Além dos métodos automáticos para criar incidentes de segurança, você pode criá-los manualmente, conforme necessário.

Antes de Iniciar
Função necessária: sn_si.basic

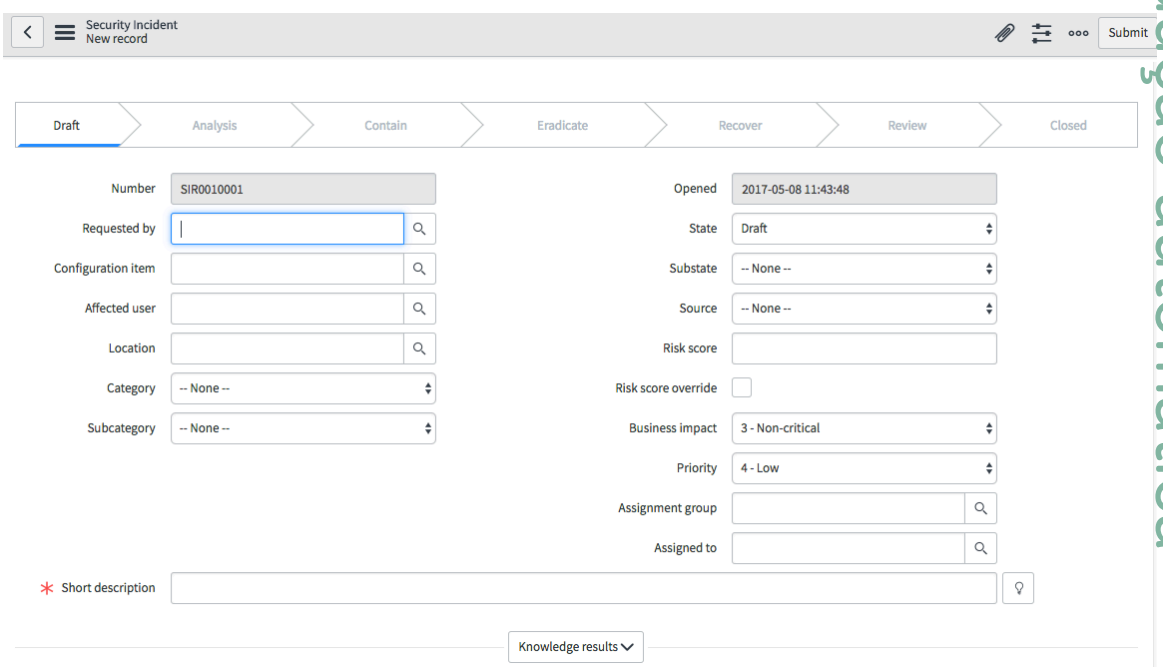
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até qualquer lista de incidentes de segurança (por exemplo, **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar Todos os Incidentes**).



2. Clique em **Nova**.



3. No formulário, preencha os campos.

Campo	Descrição
Selecione marcador de segurança	Se necessário, selecione um marcador de segurança para adicionar metadados ao registro ou identificar quem deve ter acesso a este registro de incidente de segurança. Este campo é exibido somente depois que o incidente de segurança foi salvo.
Número	[Somente leitura] O número do incidente de segurança.
Solicitados por	A pessoa que está solicitando o trabalho a ser realizado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Item de Configuração	O servidor, computador, roteador ou outro item de configuração afetado pelo problema de segurança.
Usuário afetado	A pessoa afetada pelo problema de segurança.
Local	O local do solicitante ou recurso. Se um **Item de configuração** não for selecionado, este campo será preenchido previamente com o local do solicitante.
Categoria	A categoria que identifica o tipo de problema de segurança. Se uma categoria for selecionada, um fluxo de trabalho para analisar esse problema será executado quando o registro for salvo. Por exemplo, se você selecionar **Negação de serviço**, o fluxo de trabalho Incidente de segurança - Negação de serviço - Modelo será executado. Para obter mais informações, consulte Modelos de fluxo de trabalho do Security Incident Response.
Subcategoria	A subcategoria que define ainda mais o problema.
Aberto	[Somente leitura] Exibe a data e a hora em que o incidente foi aberto.
Estado	O estado atual do incidente de segurança. Na criação do incidente de segurança, este campo é padronizado como **Rascunho**.
Subestado	Identifica se o incidente de segurança inclui um problema pendente ou uma mudança.
Fonte	Identifica a origem do incidente de segurança, como e-mail, chamada telefônica ou monitoramento de rede.
Sensor de alerta	Integração de segurança por meio da qual você ingere os dados de alerta ou evento, como Carbonblack, CrowdStrike, McAfee e assim por diante.
Regra de Alerta	A regra no produto de segurança que acionou a criação deste incidente de segurança.
Pontuação de risco	Exibe a pontuação de risco calculada para este incidente de segurança. O valor é baseado na prioridade do incidente de segurança, no tipo de incidente de segurança (denial of service, Spear Phishing ou atividade de código malicioso) e no número de origens que acionaram uma pontuação de reputação com falha em um indicador. A pontuação de risco ajuda a priorizar o trabalho de incidente de segurança para os analistas. Três propriedades de incidente de segurança permitem que você designe um ponto codificado por cor para aparecer ao lado da pontuação de risco na exibição de lista para torná-los mais facilmente identificáveis. Se você fizer mudanças em determinados campos no incidente de segurança, como **Impacto nos negócios** ou **Prioridade**, e salvar o registro, a **Pontuação de risco** será recalculada e exibida automaticamente. A mudança também se reflete nas anotações de trabalho e na lista relacionada Auditorias de pontuação de risco. **Nota:** A pontuação de risco também é recalculada quando os usuários afetados são associados a um incidente de segurança, serviços afetados ou itens vulneráveis. Você também pode inserir manualmente uma nova **Pontuação de risco**. Isso pode ser útil se você quiser manter um incidente de segurança específico no topo da lista de incidentes de segurança que estão sendo analisados.

Tradução automática

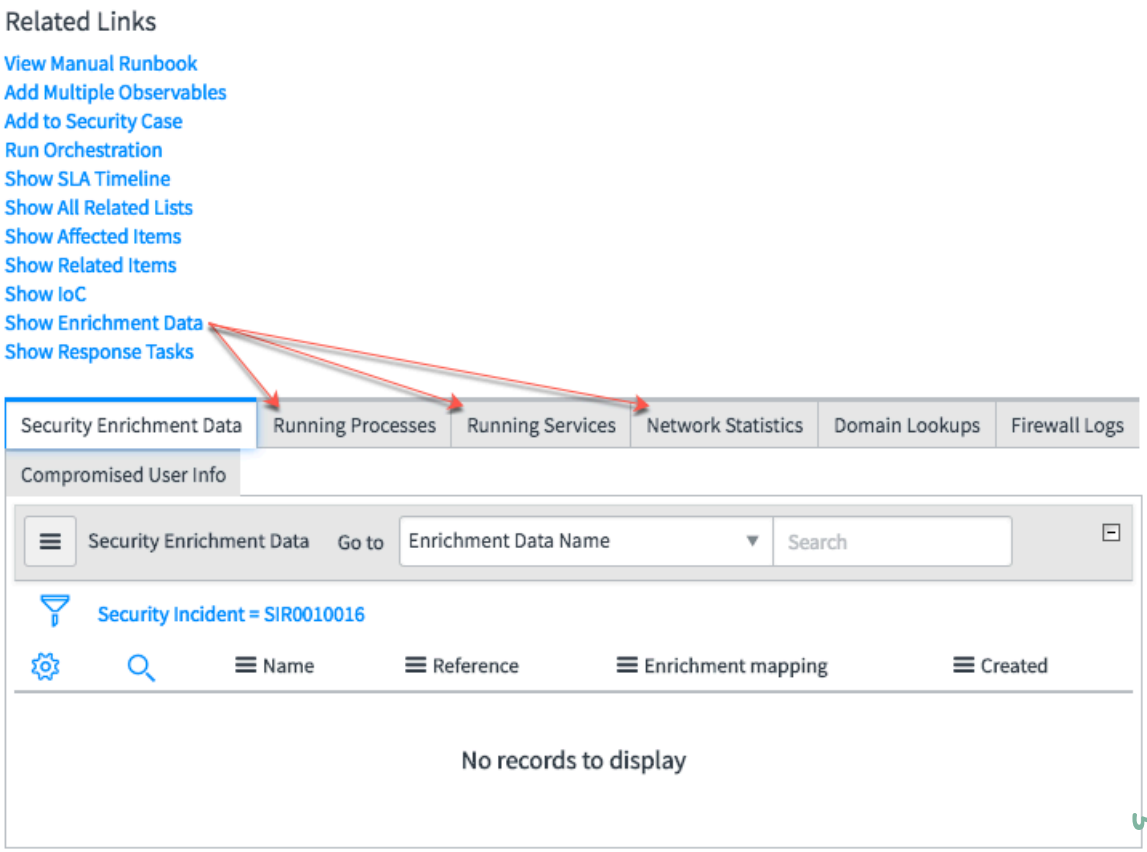
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Se você inserir uma nova Pontuação de **risco**, a caixa de seleção **Substituir pontuação de risco** será marcada automaticamente. Independentemente das mudanças feitas no incidente de segurança, uma pontuação de risco inserida manualmente não é recalculada automaticamente. **Nota:** Se você atualizou sua instância de uma versão anterior, as pontuações de risco foram calculadas para todos os seus incidentes de segurança em aberto. Para obter mais informações, consulte Noções básicas sobre calculadoras de incidentes de segurança.
Substituição de pontuação de risco	Marque esta caixa de seleção para substituir a atualização automática da pontuação de risco. A substituição será refletida nas anotações de trabalho.
Impacto nos negócios	Selecione a importância deste incidente de segurança para o seu negócio. O valor padrão é Não crítico. Se, depois que o registro do incidente de segurança for salvo, você alterar o valor nos campos **Prioridade** /ou **Risco**, o **Impacto nos negócios** será recalculado.
Prioridade	Selecione a ordem de abordagem deste incidente de segurança, com base na urgência. Se este valor for alterado depois que o registro for salvo, isso poderá afetar o cálculo do **impacto nos negócios**.
Grupo de atribuição	O grupo ao qual este incidente de segurança está atribuído.
Atribuído a	O indivíduo designado para analisar este incidente de segurança. As atribuições podem ser realizadas de forma manual ou automática. Para obter mais informações, consulte Atribuição de analistas de segurança.
Descrição resumida	Uma breve descrição do incidente de segurança.
Resultados de conhecimento	Conforme você digita a descrição resumida, são exibidos links para artigos relacionados da base de conhecimento. Verificar as informações pode resolver o problema.

4. Clique com o botão direito do mouse no cabeçalho do registro e selecione **Salvar**.
   Se você adicionou um novo IC ao incidente de segurança, os seguintes fluxos de trabalho de integração serão executados automaticamente:
   - Security Operations - Obter fluxo de trabalho de processos em execução. Este fluxo de trabalho recupera uma lista de processos em execução em um item de configuração (IC) de um host ou endpoint.
   - Fluxo de trabalho do Security Incident Response - Obter serviços em execução. Este fluxo de trabalho recupera uma lista de serviços em execução de ICs baseados no Windows.
   - Security Operations Integrations - Obter fluxo de trabalho de estatísticas de rede. Este fluxo de trabalho recupera uma lista de conexões de rede ativas de um host ou endpoint.
5. Para exibir as informações recuperadas por esses fluxos de trabalho, clique no link relacionado **Mostrar dados de aprimoramento** e clique em qualquer uma das guias indicadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:
Fluxos de trabalho adicionais são executados com base nas integrações de terceiros que você ativou da seguinte forma:

Integração da plataforma Tanium Endpoint: Tanium - Obter fluxo de trabalho de processos em execução

Tópicos relacionados

Configuração do Security Incident Response

Criar um incidente de segurança a partir do Catálogo de incidentes de segurança

Os usuários em sua empresa podem usar o Catálogo de incidentes de segurança para solicitar vários tipos de análise relacionada à segurança.

Antes de Iniciar

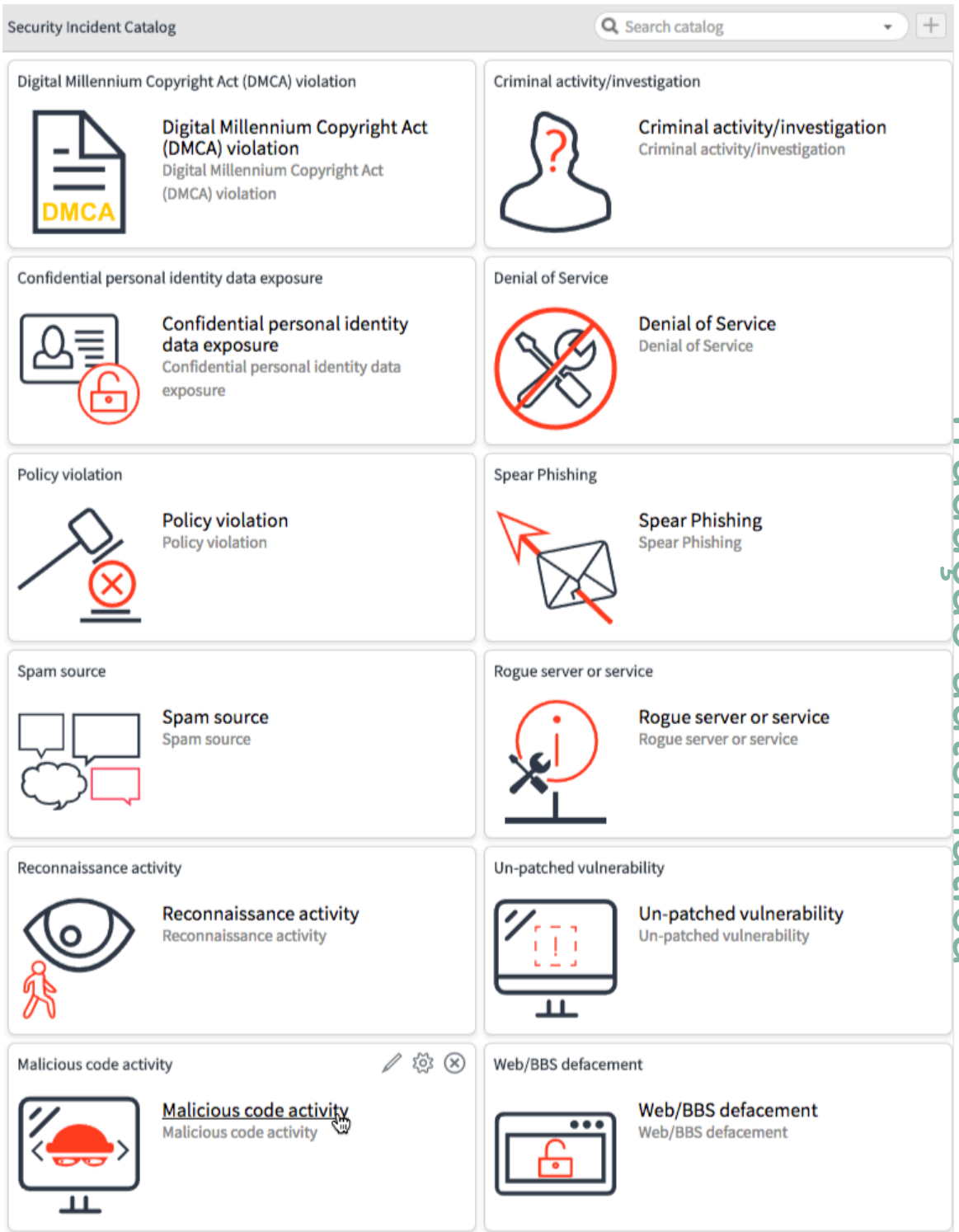
Função necessária: none

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

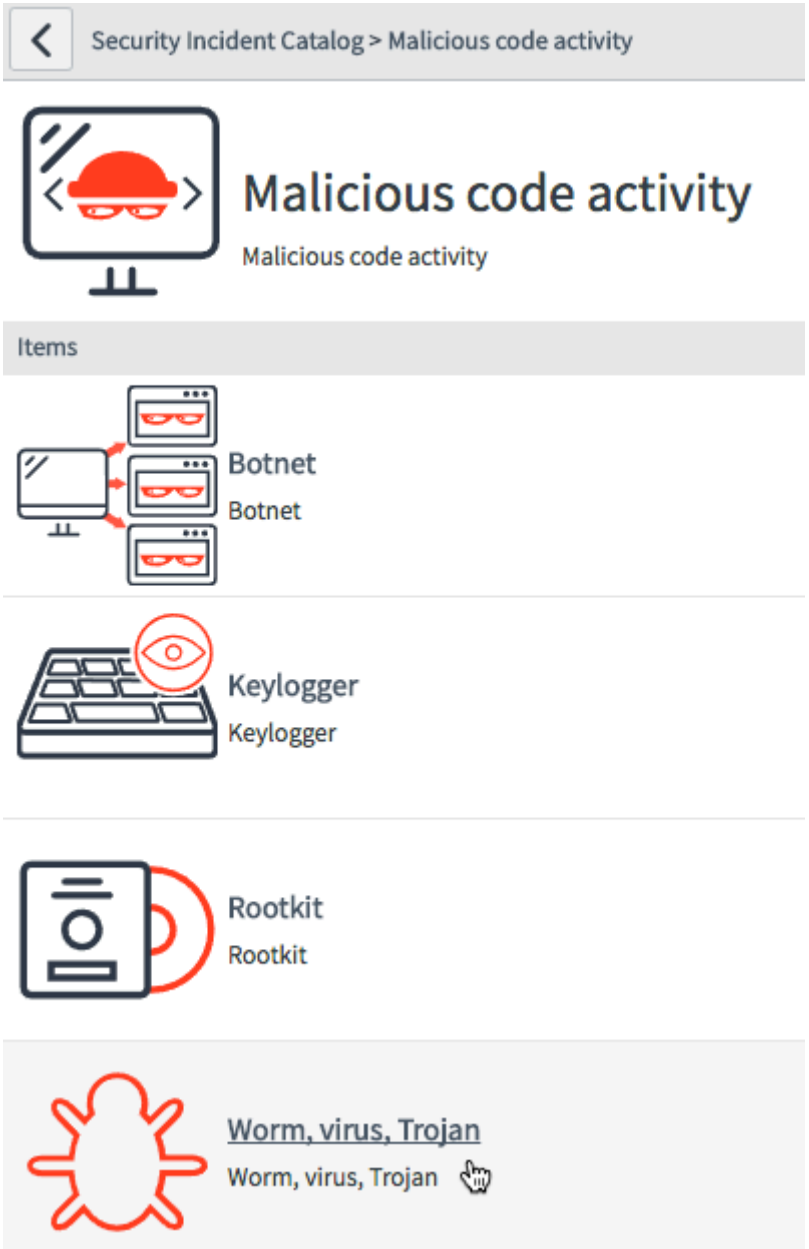
1. Navegar até **Todos** > **Autoatendimento** > **Catálogo de incidente de segurança**.



2. Clique no item do catálogo para o qual você deseja fazer uma solicitação.
   Se o item selecionado no catálogo principal contiver subcategorias, a lista será mostrada. No exemplo a seguir, **a atividade de código malicioso** foi selecionada.

Tradução automática

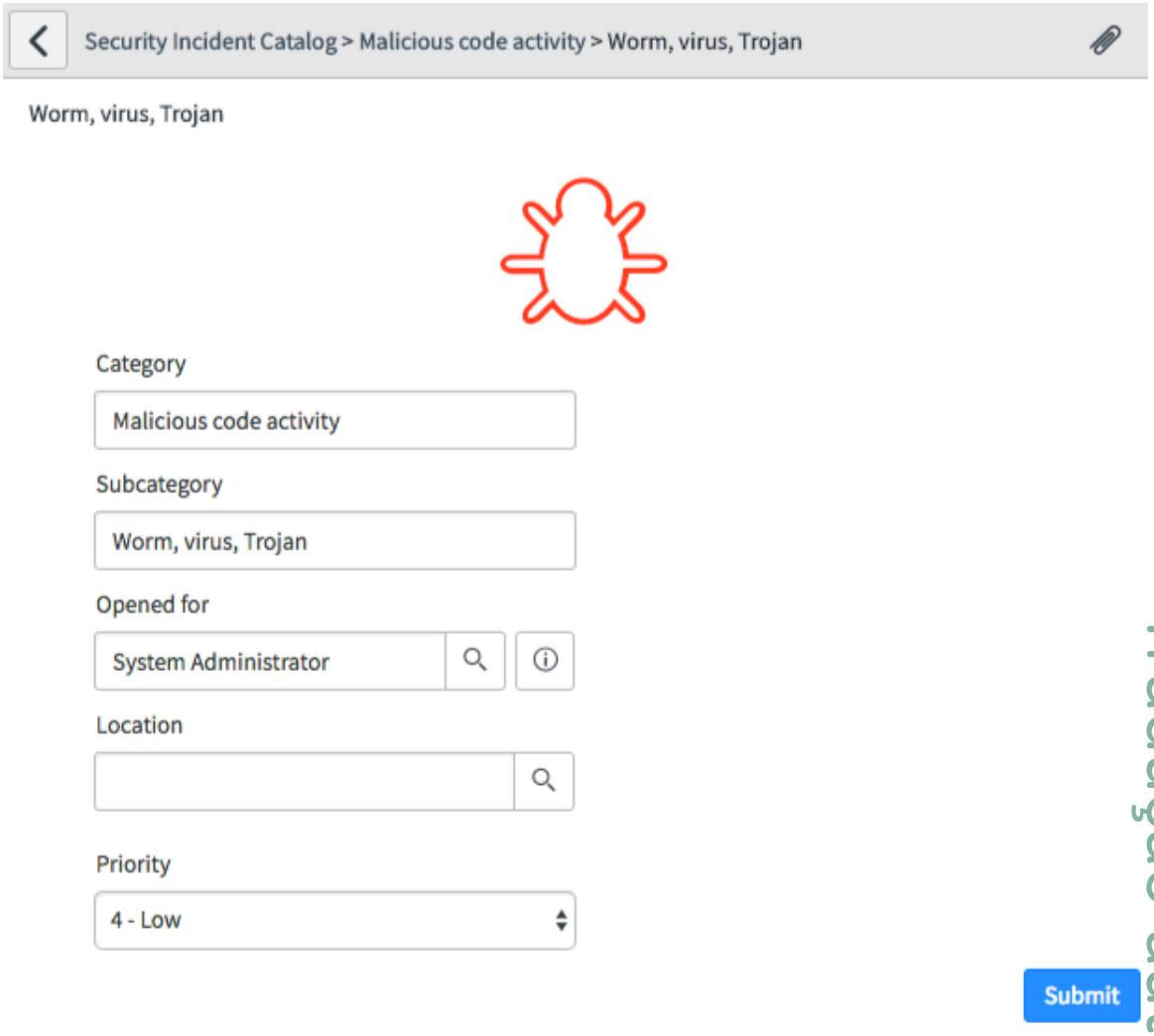
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique na subcategoria que melhor corresponde ao tipo de solicitação que você deseja fazer. Neste exemplo, a subcategoria **Verme, vírus e Cavalo de Troia** foi selecionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Insira as informações da solicitação e clique em **Enviar**.
   A solicitação é enviada ao departamento de incidentes de segurança.
5. Depois de enviar a solicitação, você pode acompanhar o andamento dela navegando até **Autoatendimento** > **Minhas solicitações**e inserindo o número da solicitação.

Criar um incidente de segurança a partir de um alerta da Gestão de eventos

Quando o Event Management está ativado, você pode criar incidentes de segurança manualmente a partir do formulário Alerta.

Antes de Iniciar

O plug-in Event Management requer uma assinatura separada e deve ser ativado pela equipe da ServiceNow. Este plug-in inclui dados de demonstração e ativa plug-ins relacionados, caso ainda não estejam ativos. O Service Analytics é ativado automaticamente quando o Event Management é ativado.
Função necessária: evt_mgmt_admin, evt_mgmt_operator ou evt_mgmt_user

Procedimento

1. Navegar até **Todos** > **Event Management** > **Todos os Alertas**.
2. Clique no **número**do alerta.
3. Clique **em Criar incidente de segurança**.
4. Clique em **Atualizar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criação automática de incidente de segurança

Ferramentas de monitoramento de terceiros, como o Splunk, podem ser integradas ao Security Incident Response para que os eventos de segurança importados dessas ferramentas gerem automaticamente incidentes de segurança. Você também pode importar dados de ferramentas de terceiros para alertas de segurança.

Para integrar ferramentas de monitoramento de alertas a Security Incident Response, você deve usar a REST API para gravar na tabela de importação de incidente de segurança [sn_si_incident_import]. Em seguida, usando os mapas de transformação **Transformação de incidente de segurança**, a tabela de origem do conjunto de importação é mapeada para campos na tabela de Incidente de segurança [sn_si.incident] de destino.

Se você tentar importar registros de IC que não sejam reconhecidos pelo mapa de transformação, o script do mapa de transformação verificará o registro para o seguinte (nesta ordem) em uma tentativa de fazer uma correspondência:

- sys_id
- Nome do IC
- nome de domínio totalmente qualificado
- Endereço IP

Nota:
Se você achar que o mapa de transformação **Transformação de incidente de segurança** não é adequado para a ferramenta de monitoramento de alertas de terceiros que você está usando, duplique o mapa de transformação, crie um novo e edite os campos, conforme necessário.

Incidentes de segurança criados a partir de eventos e alertas

Conforme os eventos são importados das ferramentas de monitoramento de alertas, eles são processados primeiro por Gestão de eventos e agrupados em alertas. Esses alertas podem ser usados para criar incidentes de segurança com base em regras de alerta personalizáveis ou revisados manualmente para selecionar os alertas a serem investigados como um incidente de segurança.

Você pode encontrar um exemplo de regra de alerta chamada **Criar incidentes de segurança a partir de alertas críticos** no módulo Regras de AlertaGestão de eventos da aplicação []. Esta regra de alerta cria automaticamente incidentes de segurança quando eventos críticos relacionados à segurança são recebidos de dentro de ServiceNow ou de aplicações de monitoramento de terceiros. Depois que o incidente de segurança tiver sido criado, ele será atualizado conforme novos eventos forem recebidos. Você pode modificar o modelo de tarefa na regra de alerta para mudar os valores iniciais do incidente de segurança criado por esta regra de alerta. Para lidar com cada variedade distinta de incidente de segurança que você deseja criar, é possível definir outras regras de alerta com condições diferentes.

Como alternativa, se você for um usuário com a função de administrador de segurança, poderá criar manualmente um incidente de segurança clicando no botão **Criar incidente de segurança** em qualquer alerta suspeito.

É importante que os eventos recebidos de ferramentas externas incluam as seguintes informações:

- O nó definido como o nome, endereço IP ou sys_id do IC que se torna o recurso afetado.
- A classificação do evento é definida como Segurança para diferenciá-los de outros eventos de TI.
- A descrição do evento, que preenche a descrição do incidente de segurança.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- As informações adicionais podem incluir qualquer informação extra que não se encaixe nos campos listados anteriormente ou em outros campos de evento, como categoria, vetores de ataque, URL de retorno ou ID de correlação. O formato é uma cadeia de caracteres que lista os nomes de campo junto com seus valores, usando o seguinte formato JSON:

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

Nota:
Para cada par de campo e valor, se o campo no incidente de segurança em que o nome da coluna corresponde ao fieldName estiver vazio, ele será definido como fieldValue. Se o campo no incidente de segurança não estiver vazio, ele não será alterado. Em qualquer um dos casos, o evento e todos os campos e valores codificados nas informações adicionais são registrados em uma entrada de anotações de trabalho que descreve o evento. Se nada mudar no incidente de segurança, uma entrada de anotação de trabalho não será criada. Todos os campos em um incidente de segurança, incluindo os campos personalizados adicionados à tabela, podem ser definidos.

Dados importados para alertas de segurança

Quando um evento é criado com mais dados codificados por JSON, esses dados são importados para qualquer campo com um nome que corresponda ao fieldName desse valor nos dados JSON.

Se você tiver dados em seu software de monitoramento de terceiros (por exemplo, Splunk) que não sejam comuns ao sistema de base, poderá adicionar novos campos à tabela Alerta para acomodar a importação de dados. O formato JSON para importar dados para alertas é o mesmo formato usado para criar incidentes de segurança a partir de eventos e alertas:

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

A única diferença é que os dados no campo são sempre substituídos pelo fieldValue.

Quando os dados do evento de segurança são importados, eles preenchem os campos na tabela Alerta com nomes de campo correspondentes. Se o alerta for posteriormente transformado em um incidente de segurança, os mesmos dados de informações adicionais preencherão os campos correspondentes no incidente de segurança.

Criar incidentes de segurança a partir de e-mails de phishing relatados pelo usuário

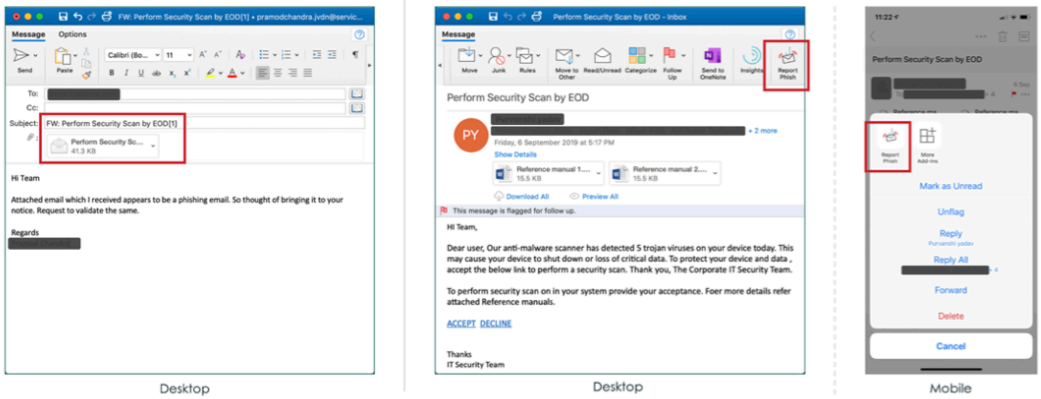
Use esse recurso para criar incidentes de segurança a partir de e-mails de phishing relatados pelo usuário.

A funcionalidade aprimorada de Phishing relatado pelo usuário inclui recursos de agregação, extração de cabeçalho de e-mail e configuração.

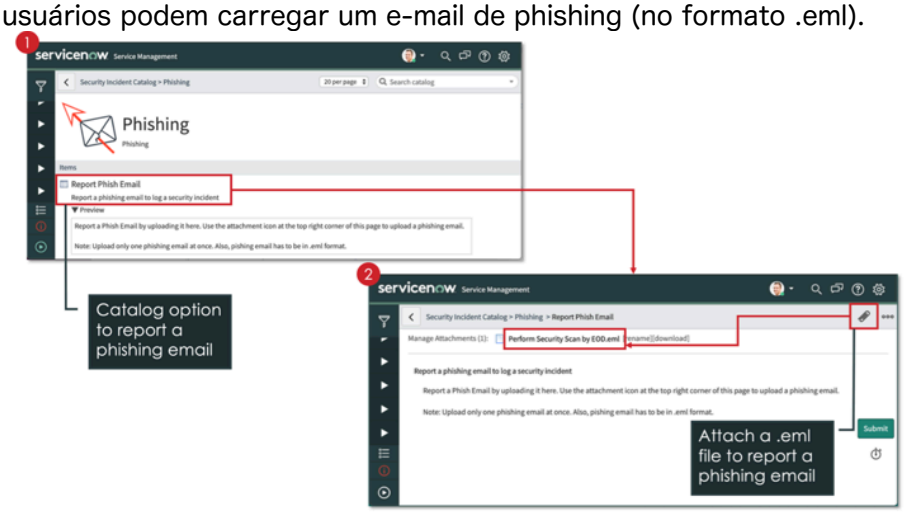
- Os usuários podem relatar e-mails de phishing de várias maneiras:
  - Os e-mails podem ser encaminhados como anexos.
  - Se o plug-in Wombat tiver sido configurado com o cliente Microsoft Outlook, os usuários poderão:
    - Clicar no botão **Relatar phishing**.
    - Encaminhar e-mails de phishing de um dispositivo móvel usando a opção **Relatar phishing**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- Os usuários podem carregar um e-mail de phishing (no formato .eml).



- O phishing relatado pelo usuário inclui **lógica de negócios de agregação** que identifica e-mails de phishing duplicados relatados por usuários em uma organização. Os usuários podem usar este recurso para:
  - Agregar incidentes de phishing relatados pelo usuário duplicados ou semelhantes (campanhas de phishing iniciadas pela empresa).
  - Evite fazer a triagem de incidentes de phishing relatados pelo usuário duplicados e reduza o esforço manual envolvido na consolidação de incidentes.
  - Permita que os analistas de segurança trabalhem em um único incidente de phishing relatado pelo usuário.
- Fornece cabeçalhos de e-mail de phishing no incidente de phishing relatado pelo usuário.
  - Os analistas de segurança podem verificar as principais informações do cabeçalho de e-mail no incidente.
  - O esforço manual na coleta de informações de cabeçalho de outras fontes não é mais necessário.
- O e-mail de phishing original enviado é armazenado como um **Registro de e-mail de phishing** em uma nova tabela.
- Os analistas de segurança podem exibir detalhes do e-mail de phishing original, como conteúdo do e-mail de phishing, cabeçalhos e origem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Os administradores de segurança podem configurar e fazer algumas melhorias que incluem:
  - Configurações para extrair cabeçalhos de e-mail do corpo do e-mail (envios de **relatório de phishing**).
  - Filtros para capturar cabeçalhos selecionados.
  - Configurações para lidar com a associação de incidentes primários-secundários quando registros de e-mail de phishing duplicados são identificados.
  - Configurações do Flow Designer para modificar a lógica de negócios de agregação com base nos requisitos.

Configurar regras de ingestão para phishing relatado pelo usuário

Como usuário com a função `sn_si.admin`, você pode definir regras de correspondência de e-mail para filtrar e-mails de phishing relatados pelo usuário com base em critérios específicos. Por exemplo, você pode definir uma regra em que todos os e-mails enviados diretamente ou por meio do botão Denunciar phishing para `security@acme.com` sejam categorizados como e-mails de phishing relatados pelo usuário. Para obter mais informações, consulte Configurar regras de ingestão para phishing relatado pelo usuário.

Definir propriedades de phishing relatadas pelo usuário

Defina as informações do cabeçalho que precisam ser capturadas dos e-mails de phishing relatados pelo usuário. Para obter mais informações, consulte Definir propriedades de Phishing Reportado pelo Usuário

Registros de e-mail de phishing criados a partir de e-mails de phishing relatados pelo usuário

Os e-mails de phishing relatados pelo usuário são convertidos em incidentes de segurança com base nas regras de correspondência de e-mail que foram definidas. Para obter mais informações, consulte Registros de e-mail de phishing criados a partir de e-mails de phishing relatados pelo usuário.

Transformar e-mail de phishing em incidente de segurança

O fluxo Transformar e-mail de phishing em incidente de segurança converte ou transforma registros de e-mail de phishing em incidentes de segurança. Para obter mais informações, consulte Transformar e-mails de phishing relatados pelo usuário em incidentes de segurança.

Registros de incidentes de segurança criados a partir de registros de e-mail de phishing

Exiba os detalhes do registro do incidente de segurança, incluindo as Listas relacionadas, anotações de trabalho e outras informações importantes. Para obter mais informações, consulte Registros de incidentes de segurança criados a partir de registros de e-mail de phishing.

Componentes e plug-ins necessários

O recurso Phishing relatado pelo usuário disponível nesta versão é uma versão aprimorada da funcionalidade existente de phishing relatado pelo usuário disponível na versão London. Consulte o tópico **Criar regras para validar ataques de phishing relatados pelo usuário** na documentação de Londres para obter detalhes.

Instruções importantes de instalação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta melhoria substitui o design existente do Phishing Relatado pelo Usuário. O novo design inclui as seguintes atualizações:

- As ações de entrada de e-mail de **phishing relatadas pelo usuário** existentes (Tipo = Encaminhar e Tipo = Novo) foram desabilitadas.
- Uma nova ação de entrada **Criar e-mail de phishing** está disponível.
- O Transformar e-mails de phishing relatados pelo usuário em incidentes de segurança é um novo fluxo que contém a lógica de negócios de criação e agregação de incidentes de segurança para o novo design. Você deve ativar este fluxo para que o novo design entre em vigor.
- As regras de phishing relatadas pelo usuário existentes foram preservadas durante o upgrade.

Nota:
Se você usar ações de entrada de e-mail personalizadas e fluxos de trabalho personalizados para envios de phishing relatados pelo usuário, deverá revisar os designs antigos e novos em busca de funcionalidades conflitantes ou sobrepostas.

Detalhes do aprimoramento de phishing relatado pelo usuário: estes são os detalhes do aprimoramento:

- Relatando o e-mail de phishing de várias maneiras: consulte Criar incidentes de segurança a partir de e-mails de phishing relatados pelo usuário para obter detalhes. O e-mail de phishing é movido para a tabela `sn_si_phishing_email`.
- Criação de registros de e-mail de phishing: se as regras de correspondência de e-mail forem atendidas (consulte Configurar regras de ingestão para phishing relatado pelo usuário), a ação **Criar e-mail de phishing** de entrada criará um registro de e-mail de phishing. Os cabeçalhos de e-mail analisados são armazenados na tabela cm`sn_si_phishing_email_header` e associados ao e-mail de phishing como uma lista relacionada.
- Agregar registros de phishing semelhantes em um único incidente de segurança: o fluxo Transformar e-mails de phishing relatados pelo usuário em incidentes de segurança cria incidentes de segurança a partir dos registros de e-mail de phishing e agrega registros semelhantes em um único incidente. As condições de agregação podem ser modificadas conforme necessário neste fluxo.

Nota:

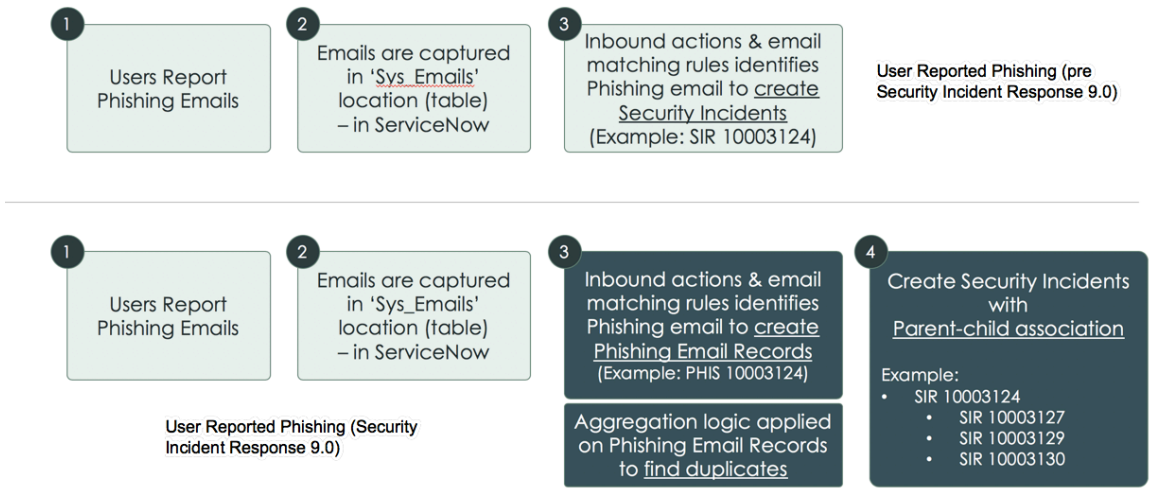
- As ações de entrada de **phishing relatadas pelo usuário** disponíveis antes da versão 9.0 do Security Incident Response agora estão desabilitadas. Os incidentes de segurança não são mais criados por meio de ações de entrada desabilitadas.
- A aplicação Security Operations spoke deve ser instalada para que o novo design entre em vigor. Isso inclui o fluxo Transformar e-mails de phishing relatados pelo usuário em incidentes de segurança que está disponível em um estado inativo por padrão. Ative este fluxo para criar incidentes de segurança a partir dos registros de e-mail de phishing.

A imagem a seguir mostra as diferenças entre o design antigo e o novo:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

What Happens When User Reports A Phishing Email?



Para usar o recurso aprimorado de Phishing relatado pelo usuário, os seguintes plug-ins e componentes são necessários:

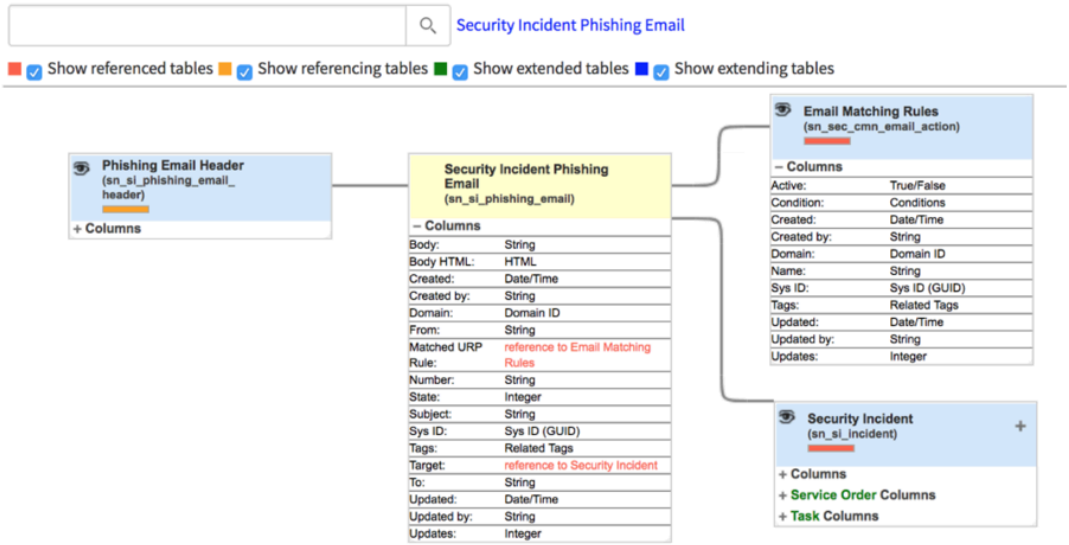
- Security Support Common (*sn_sec_cmn*): inclui:
  - Ação de entrada
  - Novo script EmailUserReportedPhishing
  - Tabela de regras de ingestão
- Security Incident Response (sn_si): inclui:
  - Tabela de incidentes de segurança (sn_si_incident)
  - Tabela de e-mails de phishing de segurança (sn_si_phishing_email)
  - Tabela de cabeçalhos de e-mail de phishing de segurança (sn_si_phishing_email_header)
  - Produtor de registro de upload de EML
- Security Operations Spoke

  Fluxos e subfluxos para agregar e-mails e transformar e-mails de phishing em incidentes de segurança.

A figura a seguir mostra a nova tabela de e-mails de phishing com referências à regra de URP correspondente e ao registro de incidente de segurança de destino (sn_si_incident).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Configurar regras de ingestão para phishing relatado pelo usuário

Como usuário com a função `sn_si.admin`, você pode definir regras de correspondência de e-mail para filtrar e-mails de phishing relatados pelo usuário com base em critérios específicos. Por exemplo, você pode definir uma regra em que todos os e-mails enviados diretamente ou por meio do botão Denunciar phishing para `security@acme.com` sejam categorizados como e-mails de phishing relatados pelo usuário.

Antes de Iniciar

Função necessária: sn_si.admin

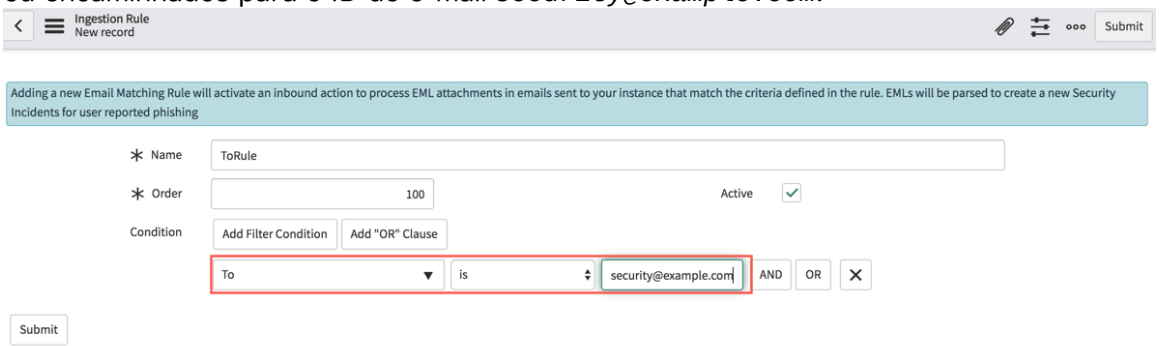
Procedimento

1. Navegar até **Todos** > **Security Operations** > **Processamento de E-mails** > **Propriedades do Phishing Reportado pelo Usuário**.
2. Clique em **Novo** para criar uma nova Regra de correspondência de e-mail.
3. Insira um nome e defina uma ou mais condições para a regra.
4. Clique em **Enviar** para salvar a regra.
   A seguir estão alguns exemplos de regras:

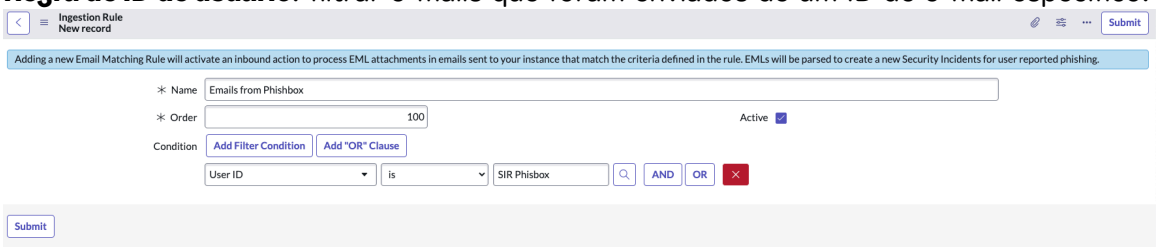
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Regra de regra**: filtrar e-mails que foram enviados diretamente ou encaminhados para o ID de e-mail *security@example.com*.



- **Regra de ID de usuário**: filtrar e-mails que foram enviados de um ID de e-mail específico.



Definir propriedades de Phishing Reportado pelo Usuário

Defina as informações do cabeçalho que devem ser capturadas dos e-mails de phishing relatados pelo usuário.

Antes de Iniciar

Função necessária: sn_si.admin

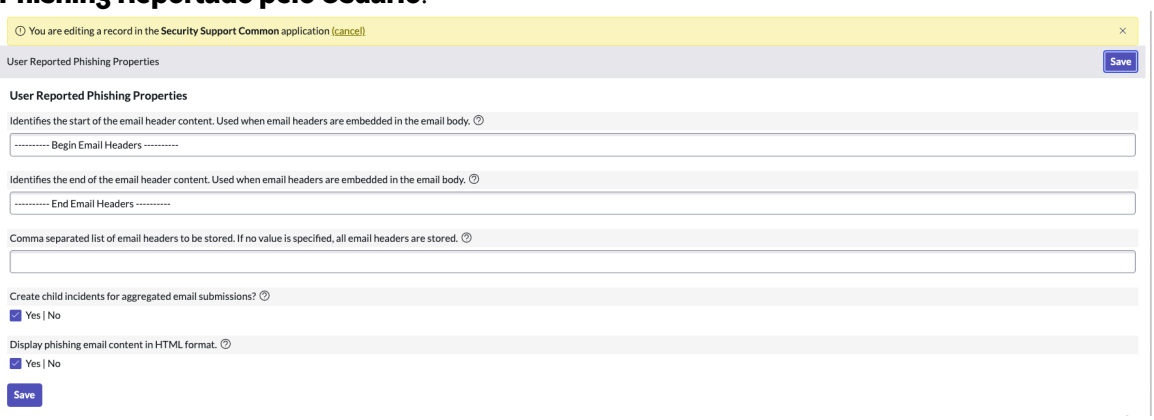
Por Que e Quando Desempenhar Esta Tarefa

Use essas opções para definir as seguintes configurações de phishing relatadas pelo usuário.

- Configuração para extrair cabeçalhos de e-mail do corpo do e-mail. (**Denunciar** envios de phishing.)
- Filtre para selecionar cabeçalhos.
- Habilitar ou desabilitar a associação primário-secundário.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Processamento de E-mails** > **Propriedades do Phishing Reportado pelo Usuário**.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Especifique a configuração para extrair cabeçalhos de e-mail do corpo do e-mail:
   - Insira uma cadeia de caracteres que identifique o início do cabeçalho do e-mail.
   - Insira uma cadeia de caracteres que identifique o final do cabeçalho do e-mail.

   Nota:
   Aplique essas configurações somente a cabeçalhos capturados como parte do corpo do e-mail de phishing. Por exemplo, se o plug-in Wombat tiver sido configurado com o cliente Microsoft Outlook, quando o usuário clicar no botão **Relatar phishing**, os cabeçalhos de e-mail serão capturados de acordo com a configuração definida aqui. As informações do cabeçalho não serão capturadas se o e-mail de phishing for encaminhado como anexo.

3. Especifique filtros para eliminar cabeçalhos que não são necessários para investigar o incidente de segurança.

   Insira uma lista separada por vírgulas de cabeçalhos de e-mail que devem ser capturados do e-mail de phishing relatado pelo usuário. Se você não especificar nenhum valor aqui, todas as informações do cabeçalho serão capturadas.

4. Habilitar ou desabilitar a associação primário-secundário.
   Por padrão, a opção **Sim** está habilitada. Selecione **Sim** para indicar que os incidentes de segurança secundários devem ser criados quando os e-mails de phishing relatados pelo usuário forem agregados. Se você selecionar **Não**, os incidentes de segurança secundários não serão criados, mas os e-mails de phishing relatados pelo usuário serão associados ao incidente de segurança e o registro do incidente de segurança será atualizado. Consulte Transformar e-mails de phishing relatados pelo usuário em incidentes de segurança para obter mais informações sobre como os incidentes de segurança secundários são criados.
5. Habilite ou desabilite a opção para exibir o conteúdo do e-mail de phishing no formato HTML.
   Por padrão, a opção **Sim** está habilitada. Selecione **Sim** para exibir o conteúdo do e-mail de phishing no formato HTML. Se você selecionar **Não**, o conteúdo do e-mail no formato HTML não ficará visível em um registro de phishing.

Registros de e-mail de phishing criados a partir de e-mails de phishing relatados pelo usuário

Os e-mails de phishing relatados pelo usuário são convertidos em incidentes de segurança com base nas regras de correspondência de e-mail que foram definidas.

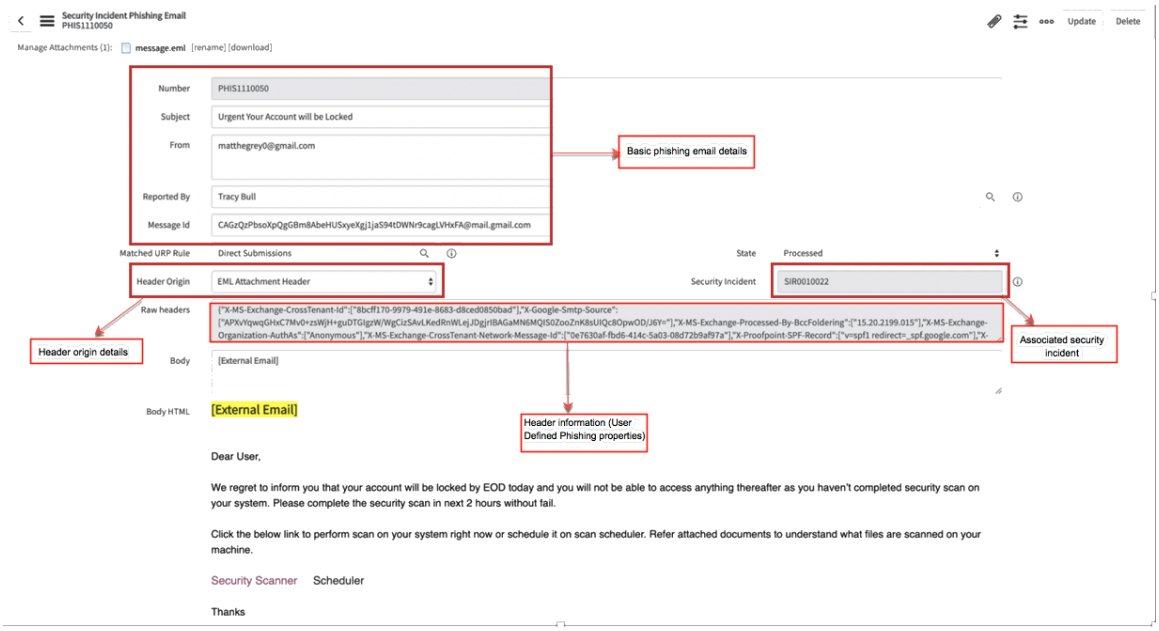
Quando um novo e-mail de phishing é relatado, as seguintes ações ocorrem:

- Um registro de e-mail é criado na tabela *sys_email*.
- A ação de entrada **Criar e-mail de phishing** é executada no registro de e-mail e usa as Regras de correspondência de e-mail (consulte Configurar regras de ingestão para phishing relatado pelo usuário) para determinar se é um e-mail de phishing.
- Quando ele é identificado como um e-mail de phishing, um registro de e-mail de phishing é criado na tabela sn_si_phishing_email.
- Por fim, o fluxo Transformar e-mails de phishing relatados pelo usuário em incidentes de segurança é aplicado para converter o registro de e-mail de phishing em um incidente de segurança.

Para exibir os detalhes do e-mail, navegue até **Incidente de segurança** > **Mostrar todos os e-mails de phishing**. Uma lista de registros de e-mail de phishing é exibida. Clique no link de data na coluna Criado para exibir o registro de e-mail.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



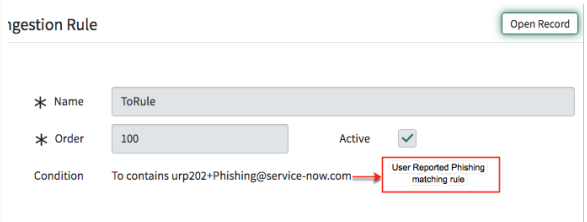
Detalhes do e-mail de phishing do incidente de segurança

Nome do campo	Descrição
Número	O número atribuído ao e-mail de phishing relatado pelo usuário.
Assunto	O assunto do e-mail. A regra do assunto é útil em campanhas ou testes de phishing simulados. Nesse caso, as organizações enviam e-mails enganosos para sua própria equipe para testar sua resposta a ataques de phishing e de e-mail semelhantes. Em testes de e-mail de phishing simulados, se o cliente de e-mail Microsoft Outlook com o plug-in Wombat estiver sendo usado, o usuário poderá clicar no botão **Relatar** phishing para relatar o e-mail de phishing. O e-mail é enviado para a equipe de Security Operations com o **Phishing simulado** anexado ao assunto do e-mail. Isso é usado para identificar o e-mail como um e-mail de phishing simulado.
De	O endereço de e-mail de origem deste e-mail de phishing. Essas informações estarão disponíveis se o e-mail de phishing for encaminhado como anexo de arquivo .EML ou se os cabeçalhos originais forem incorporados ao e-mail. Se o usuário encaminhou o e-mail de phishing diretamente, o endereço De pode não estar disponível.
Relatado por	O ID de e-mail do usuário que relatou este e-mail de phishing. Clique no ícone **Informações** para exibir detalhes adicionais.
ID da mensagem	O ID atribuído à mensagem.
Regra de URP correspondente	A regra de phishing relatada pelo usuário que será aplicada a este e-mail. Clique no ícone Informações para exibir detalhes adicionais.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

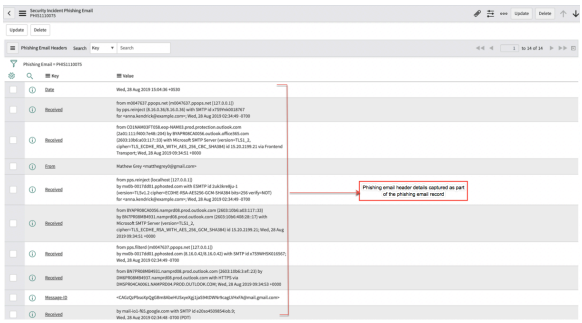
Detalhes do e-mail de phishing do incidente de segurança

Nome do campo	Descrição
 Como você pode ver, neste exemplo, o campo **Condição** mostra que o ToRule é aplicado neste e-mail e um incidente de segurança é criado. Consulte Configurar regras de ingestão para phishing relatado pelo usuário para obter mais informações sobre como definir regras de correspondência de e-mail.	
Estado	Quando um novo registro de e-mail de phishing é criado na tabela `sn_si_phishing_email`, o campo Estado é definido como **Novo**. Quando este registro de e-mail é convertido em um incidente de segurança (consulte Transformar e-mails de phishing relatados pelo usuário em incidentes de segurança), o campo Estado é atualizado para **Processado**.
Origem do cabeçalho	Este campo indica como os cabeçalhos do e-mail foram originados ou como o usuário relatou o e-mail de phishing: • **Cabeçalho do e-mail**: o usuário encaminhou o e-mail de phishing para a equipe de operações de segurança. • **Corpo do texto do e-mail:** ◦ O usuário clicou na opção **Relatar phishing** (se o plug-in Wombat tiver sido configurado com o cliente de e-mail). ◦ Com base na regra de phishing relatada pelo usuário definida, o e-mail de phishing é encaminhado para a equipe de operações de segurança. • **Cabeçalho do anexo EML**: ◦ Anexo: o usuário encaminhou o e-mail como anexo (arquivo .EML). ◦ Envio do catálogo de serviços: o usuário baixou o e-mail como um arquivo .EML para a área de trabalho e o carregou para um local especificado. O incidente de segurança é criado a partir do e-mail. • **Corpo do anexo EML**: ◦ O usuário clicou na opção **Relatar phishing** (se o plug-in Wombat tiver sido configurado com o cliente de e-mail). ◦ Com base na regra de phishing relatada pelo usuário definida, o e-mail de phishing é encaminhado como um anexo para a equipe de operações de segurança.
Incidente de segurança	Este campo fica em branco quando o e-mail de phishing relatado pelo usuário é relatado pela primeira vez. Quando o fluxo Transformar e-mails de phishing relatados pelo usuário em incidentes de segurança tiver sido executado, este e-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhes do e-mail de phishing do incidente de segurança

Nome do campo	Descrição
	mail será convertido em um registro de incidente de segurança e o número deste registro será exibido aqui.
Cabeçalhos brutos	Este campo mostra as informações completas do cabeçalho extraídas do e-mail, conforme definido na página Definir propriedades de Phishing Reportado pelo Usuário. Os cabeçalhos são analisados em pares de chave-valor e exibidos na lista Cabeçalhos de e-mail de phishing.
	
Corpo	Este é o corpo do e-mail de phishing relatado pelo usuário.

Transformar e-mails de phishing relatados pelo usuário em incidentes de segurança

O fluxo **Transformar e-mail de phishing em incidente de segurança** é um novo fluxo que converte ou transforma registros de e-mail de phishing em incidentes de segurança.

Antes de Iniciar

Nota:
Para habilitar a funcionalidade Phishing relatado pelo usuário, você deve fazer uma cópia do fluxo e ativá-lo. Se você tiver criado ações de entrada personalizadas e fluxos personalizados para lidar com envios de phishing relatados pelo usuário, as modificações de fluxo sugeridas aqui não serão necessárias.

- Função necessária: sn_si.admin
- O spoke do Flow Designer deve ser instalado.

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo é iniciado automaticamente quando um registro de e-mail de phishing relatado pelo usuário com o Estado definido como **Novo** é criado. Este fluxo contém a lógica para:

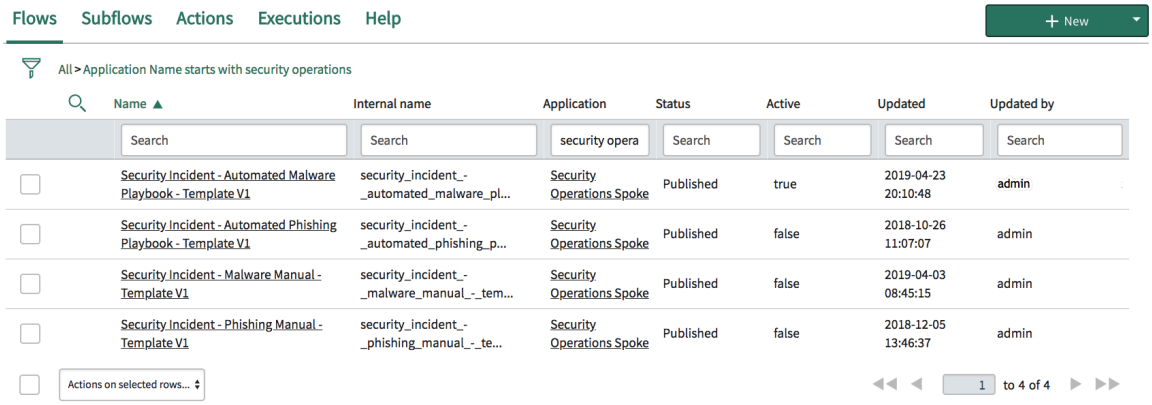
- Agregar incidentes de segurança.
- Atualize os incidentes de segurança com anotações relevantes.
- Adicione dados de cabeçalho.
- Crie incidentes secundários conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

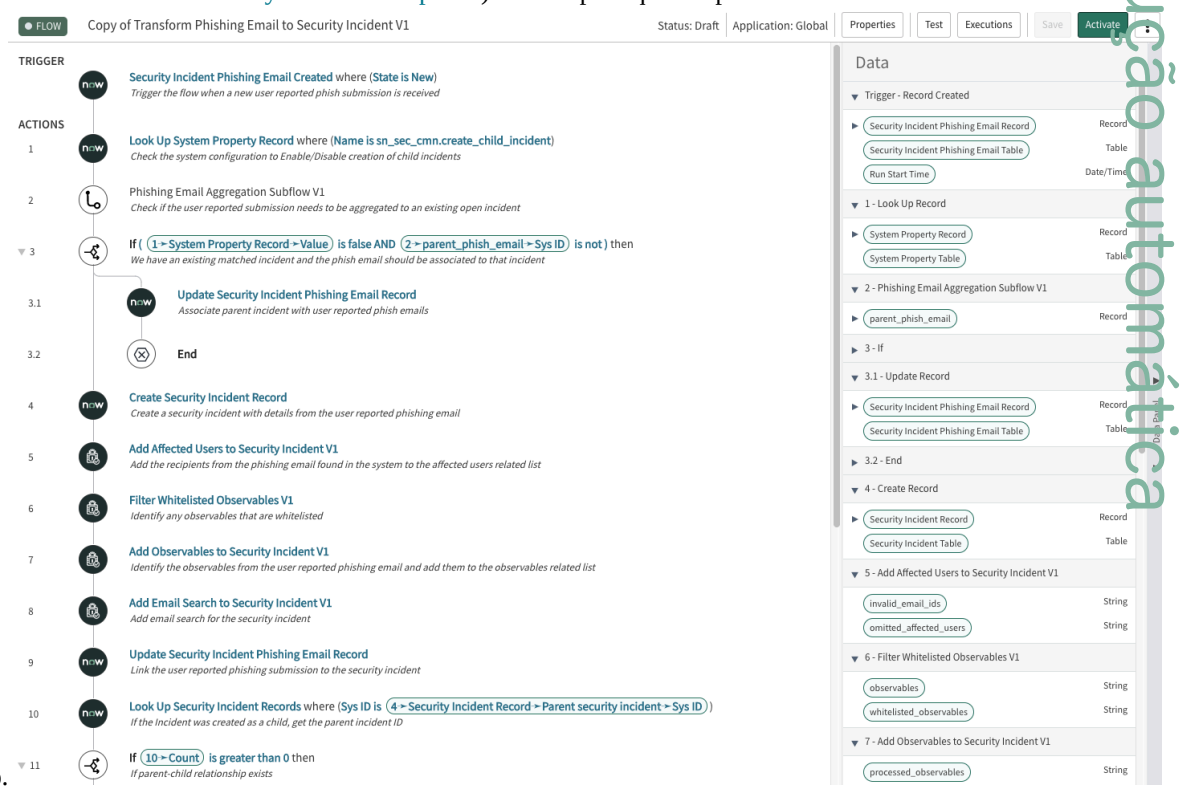
Procedimento

- Navegar até **Flow Designer** > **Designer** para exibir os fluxos disponíveis com o spoke do Security Operations.



- Clique no link **Transformar e-mail de phishing em incidentes de segurança** para exibir o fluxo.
- Este fluxo é fornecido com o sistema de base e está no modo **Somente leitura** e não pode ser usado.

  Clique no ícone mais ícone , faça uma cópia do fluxo e abra-o para uso. Agora você pode fazer mudanças no fluxo, como modificar condições ou ações do gatilho, ou adicionar e remover ações. Depois de fazer as mudanças necessárias, você deve ativar (Consulte Ativar um fluxo Security Incident Response) o fluxo para que ele possa ser executado.



  Esta figura mostra o gatilho e as etapas executadas com o fluxo. O painel à direita mostra o fluxo de dados. Clique em um ícone para expandir a etapa e exibir os detalhes.

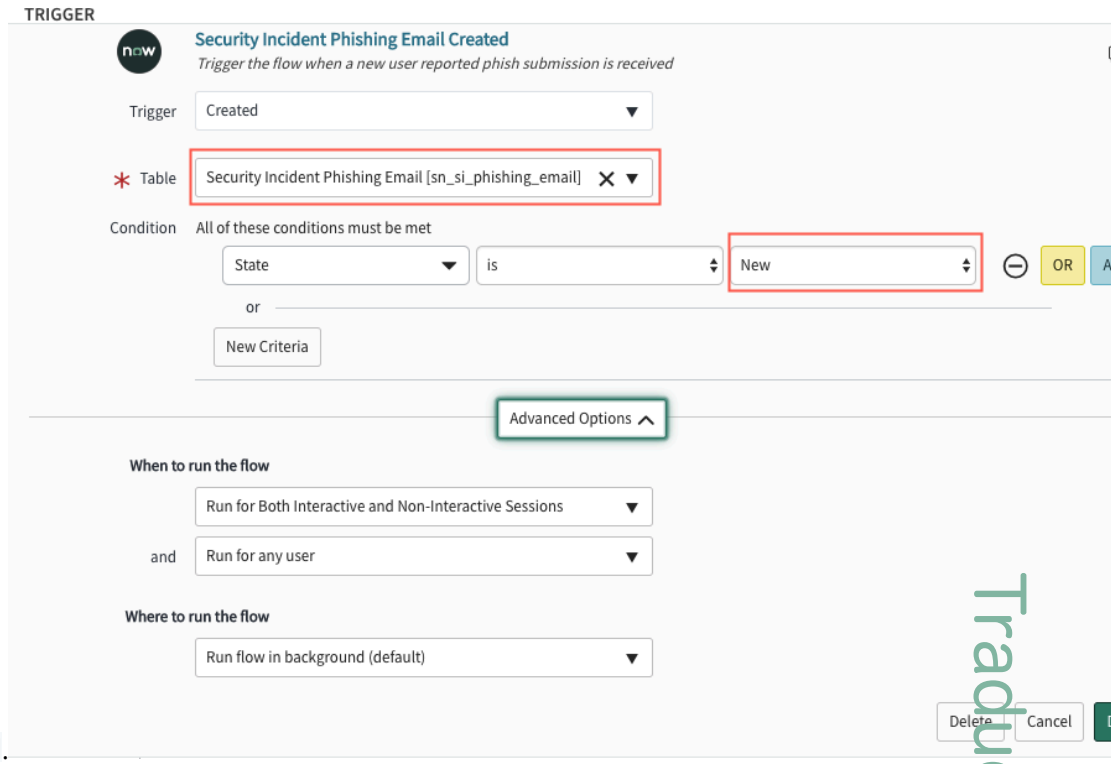
- Clique no ícone **Gatilho**.

  Na primeira etapa, você define ou define o gatilho do fluxo. Especifique as condições para o gatilho e a tarefa a serem executadas quando as condições forem

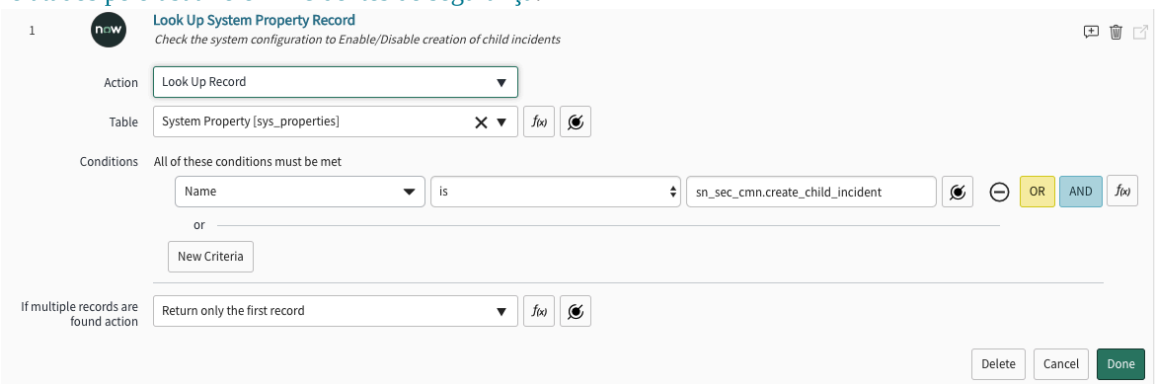
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

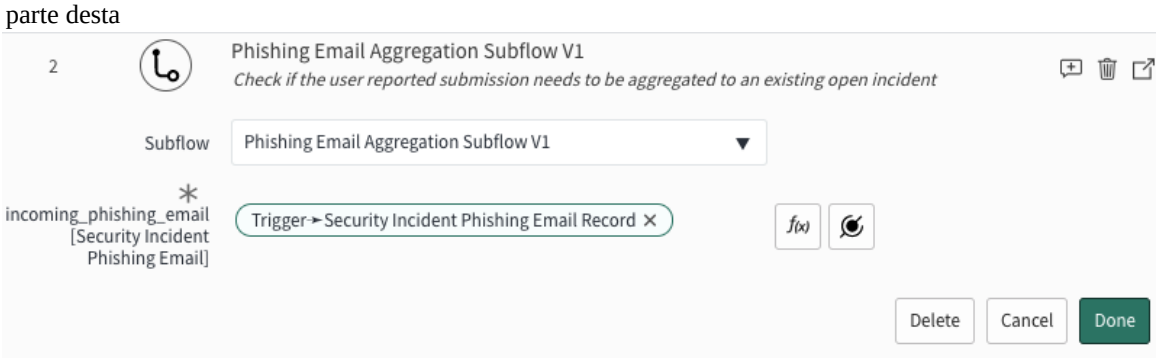
atendidas. Este fluxo é iniciado quando um **novo** registro é carregado na tabela sn_si_phishing_email.



- Na etapa 1, o fluxo verifica se a opção **Criar incidentes secundários para envios de e-mail agregados?** O sinalizador está habilitado ou desabilitado na página Transformar e-mails de phishing relatados pelo usuário em incidentes de segurança.



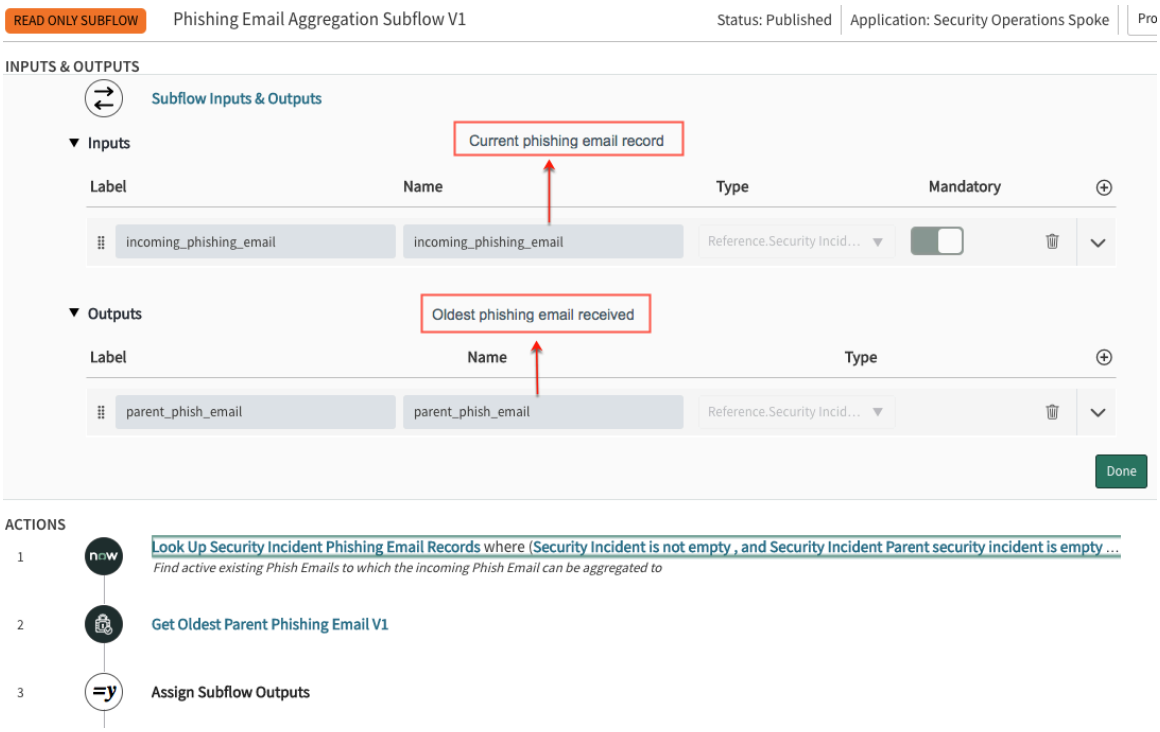
- Na etapa 2, o incidente de segurança primário mais antigo é identificado.
  Observe o ícone na etapa 2. Isso indica que o subfluxo de agregação de e-mail de phishing será executado como parte desta etapa.



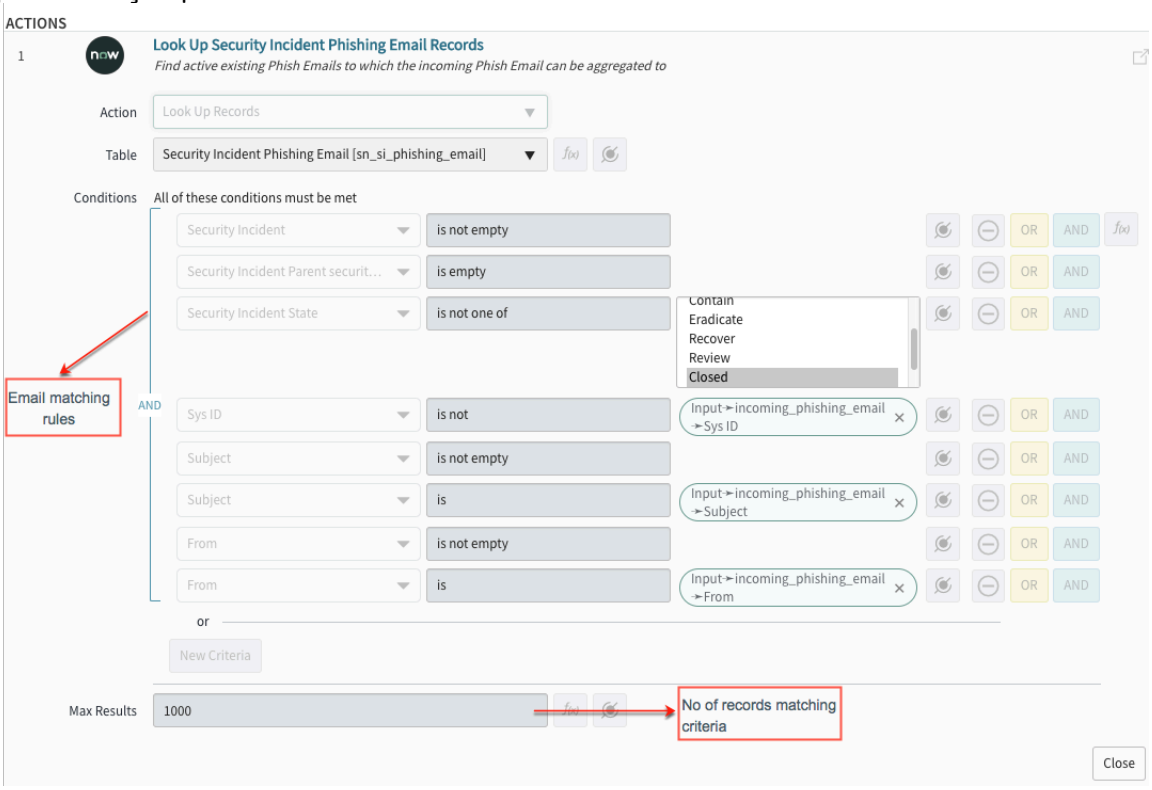
Clique no ícone do designer de ação para obter uma exibição detalhada da ação. Este subfluxo verifica o e-mail de phishing e o corresponde a um incidente de segurança existente com base nos critérios especificados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Essas duas ações são realizadas quando este subfluxo é executado. Clique no link da primeira ação para exibir detalhes adicionais.



Esta ação verifica os e-mails que correspondem aos critérios do novo e-mail de entrada com base em condições como:

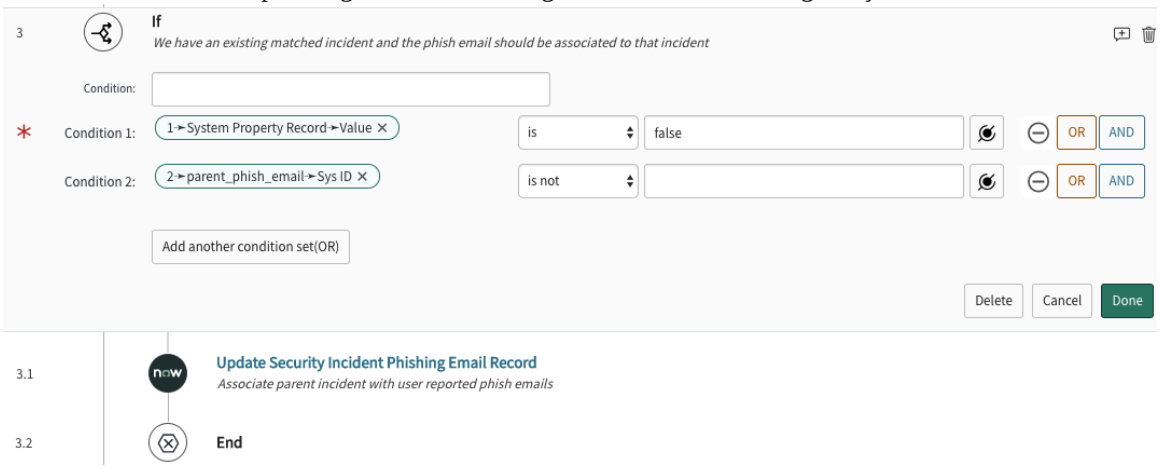
- O Estado do Incidente de segurança não é **Encerrado**.
- O assunto ou o valor de corresponde às condições da regra de correspondência de e-mail definidas (consulte Configurar regras de ingestão para phishing relatado pelo usuário).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se essas condições forem atendidas, você poderá ver o número de registros que correspondem aos critérios no campo Máximo de resultados. O registro mais antigo ou o primeiro na lista é designado como o registro primário em relação ao qual os incidentes de segurança serão agregados.

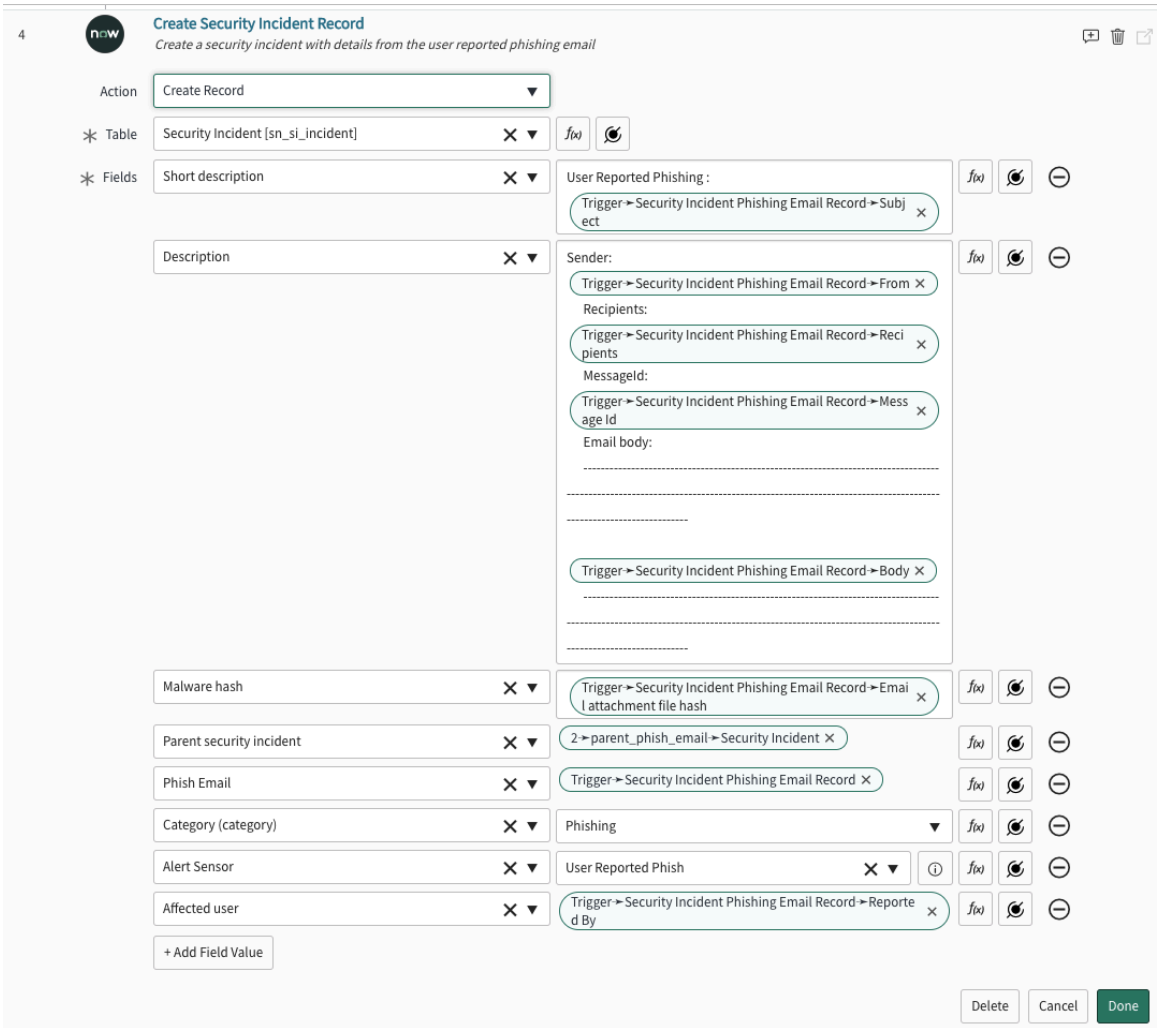
- A etapa 3 é aplicável somente se a **mensagem Criar incidentes secundários para envios de e-mail agregados?** O sinalizador foi definido como **Não** na página Transformar e-mails de phishing relatados pelo usuário em incidentes de segurança.
  Nesse caso, o e-mail de phishing é associado ao registro do incidente de segurança e o fluxo termina.



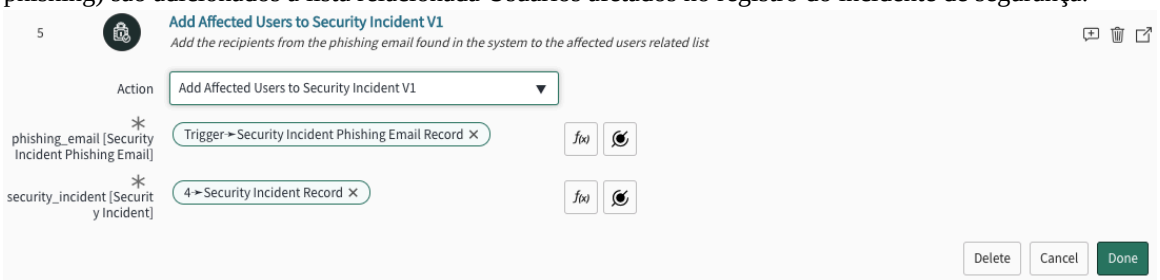
- Se a **opção Criar incidentes secundários para envios de e-mail agregados?** foi definido como **Sim**, o fluxo continuará a ser executado e um novo incidente de segurança será criado com base no e-mail de phishing relatado pelo usuário.

Tradução automática

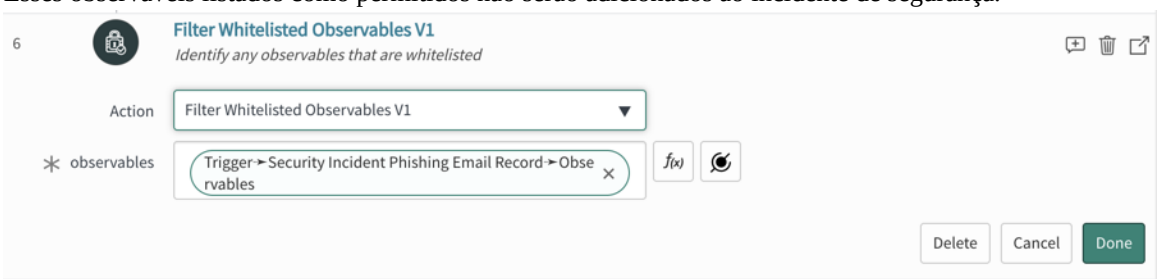
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- Na etapa 5, os usuários que receberam o e-mail de phishing (funcionários na lista Para e Cc do e-mail de phishing) são adicionados à lista relacionada Usuários afetados no registro do incidente de segurança.



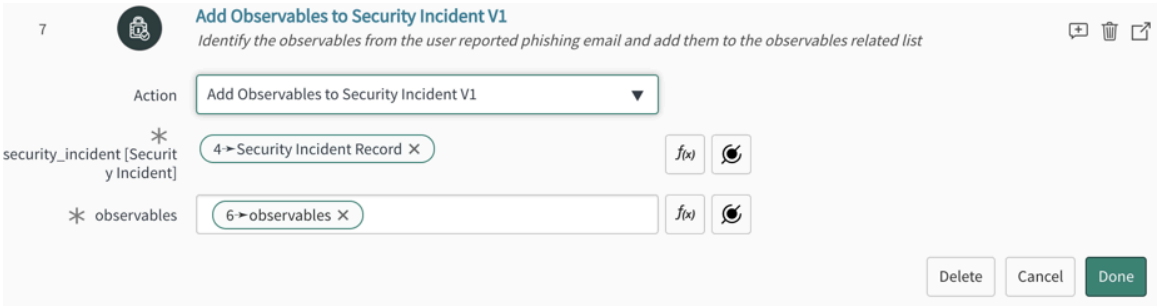
- Na etapa 6, permita que os observáveis listados sejam filtrados da lista de observáveis no incidente de segurança.
  Esses observáveis listados como permitidos não serão adicionados ao incidente de segurança.



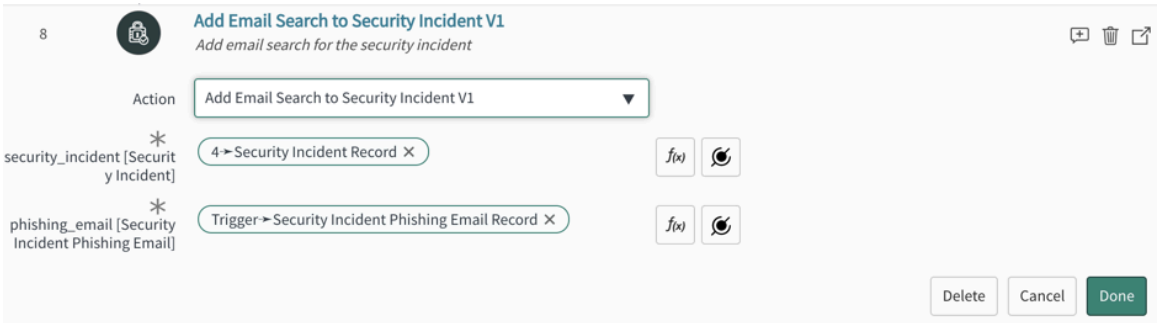
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

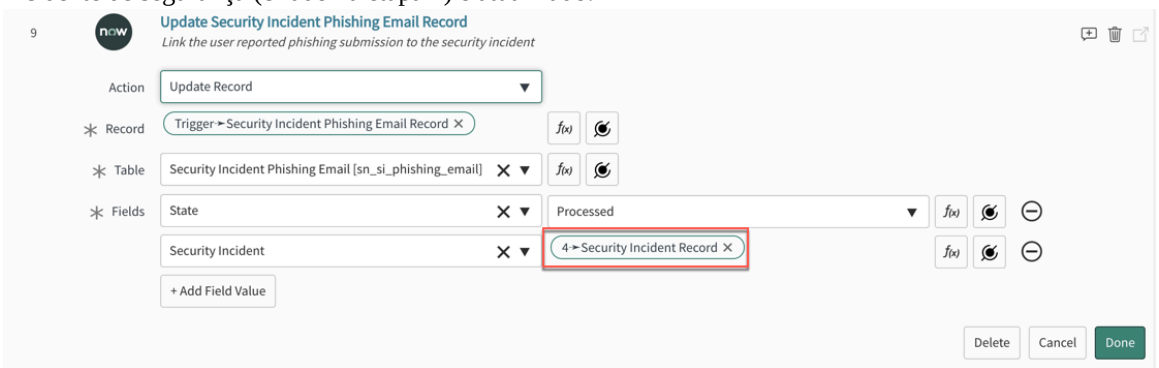
- Na etapa 7, os observáveis desconhecidos do e-mail de phishing relatado pelo usuário são identificados e adicionados à lista relacionada Observáveis.



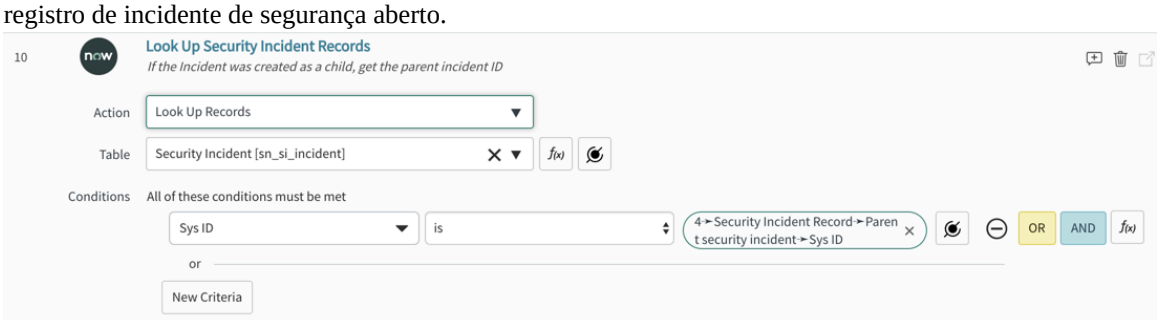
- Na etapa 8, uma consulta de pesquisa de e-mail é gerada, que é uma combinação do assunto e do endereço De do e-mail.
  Essas informações são úteis para identificar os funcionários da organização que foram alvo de phishing.



- Na etapa 9, o e-mail de phishing relatado pelo usuário é associado ao incidente de segurança e o registro do incidente de segurança (criado na etapa 4) é atualizado.



- Na etapa 10, o incidente de segurança primário é identificado e uma verificação é feita para ver se é um registro de incidente de segurança aberto.

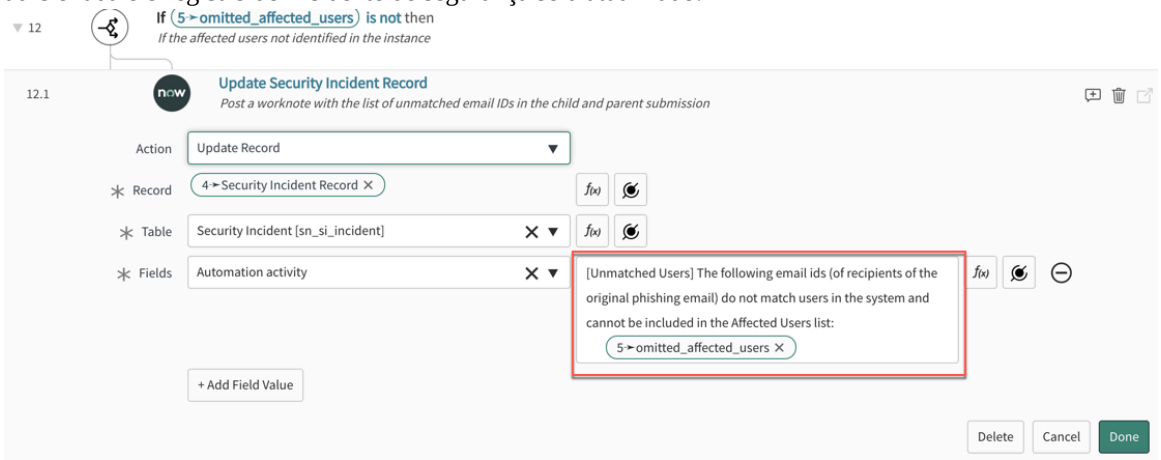


- Se a segurança primária estiver ativa, anotações serão adicionadas aos registros de incidente de segurança secundários e primários indicando como eles estão associados entre si.

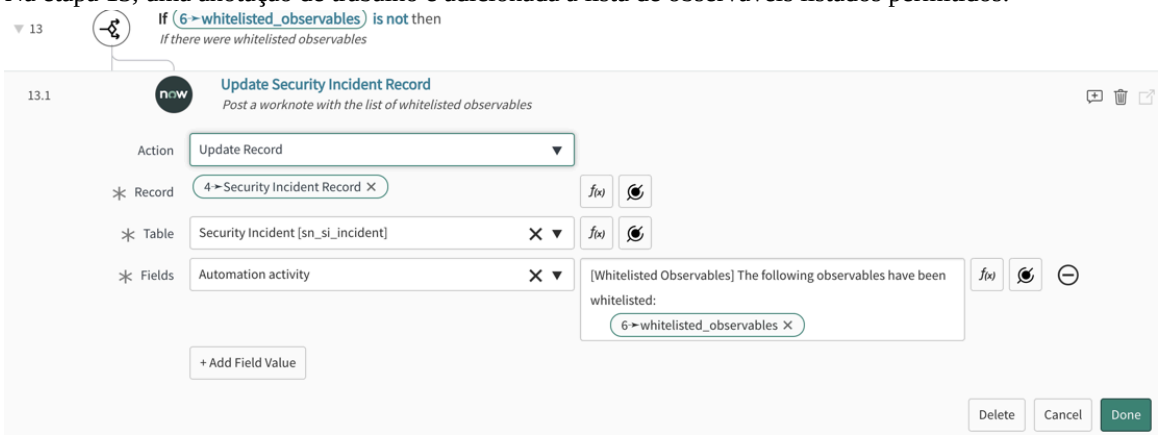
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Na etapa 12, se nenhum usuário afetado for encontrado (na etapa 5 do fluxo), uma anotação de trabalho será adicionada e o registro do incidente de segurança será atualizado.



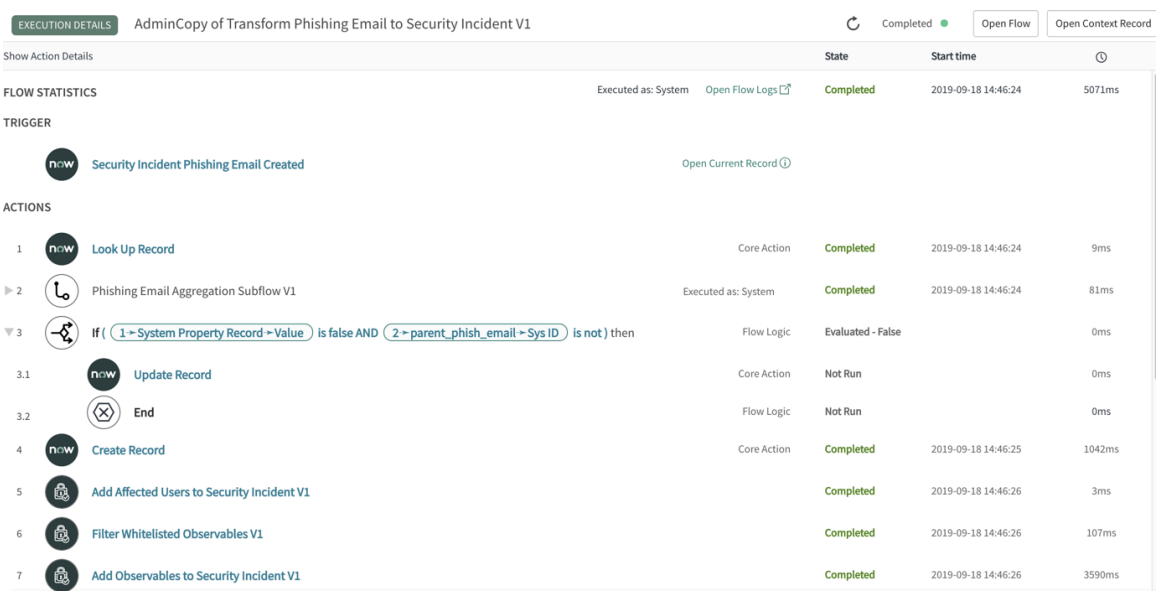
- Na etapa 13, uma anotação de trabalho é adicionada à lista de observáveis listados permitidos.



O que Fazer Depois

Você pode clicar em **Testar** para simular as ações no fluxo antes que ele seja publicado. Depois de testar o fluxo, clique em **Ativar** para ativar o fluxo para que ele possa ser executado.

Clique em **Execuções** para exibir os detalhes da execução do fluxo.



Tradução automática

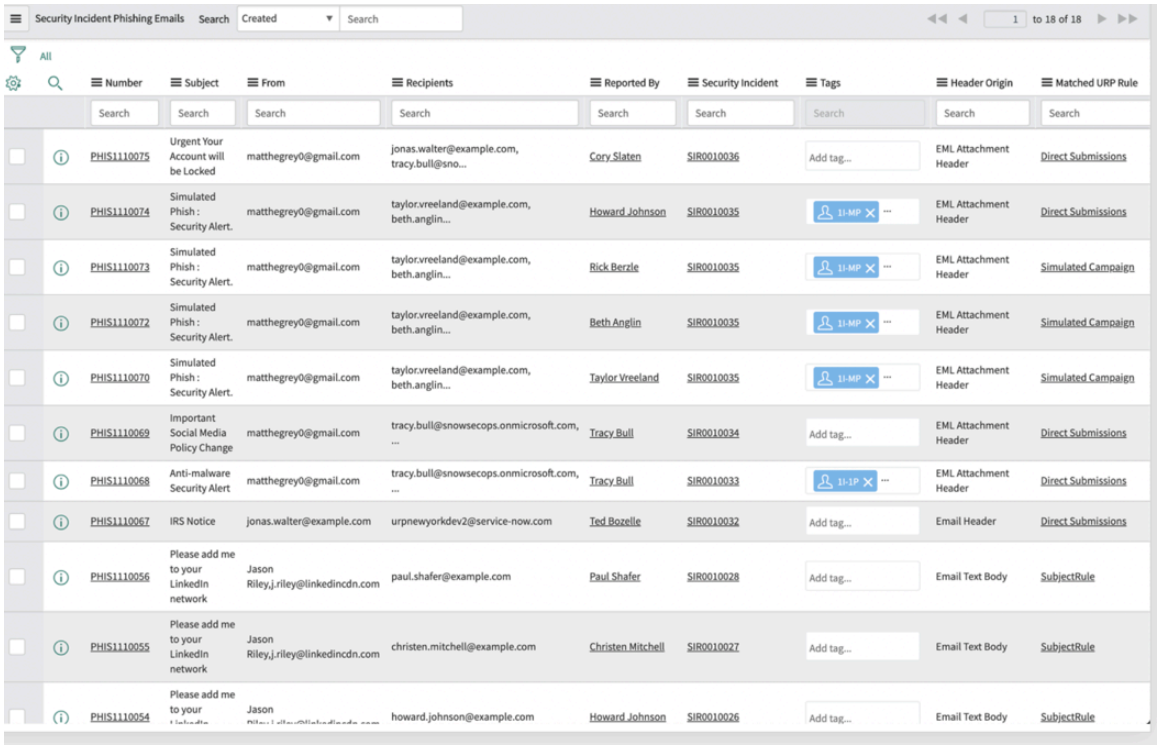
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando o fluxo tiver sido executado, o registro de e-mail de phishing será convertido em um incidente de segurança. Veja Registros de incidentes de segurança criados a partir de registros de e-mail de phishing

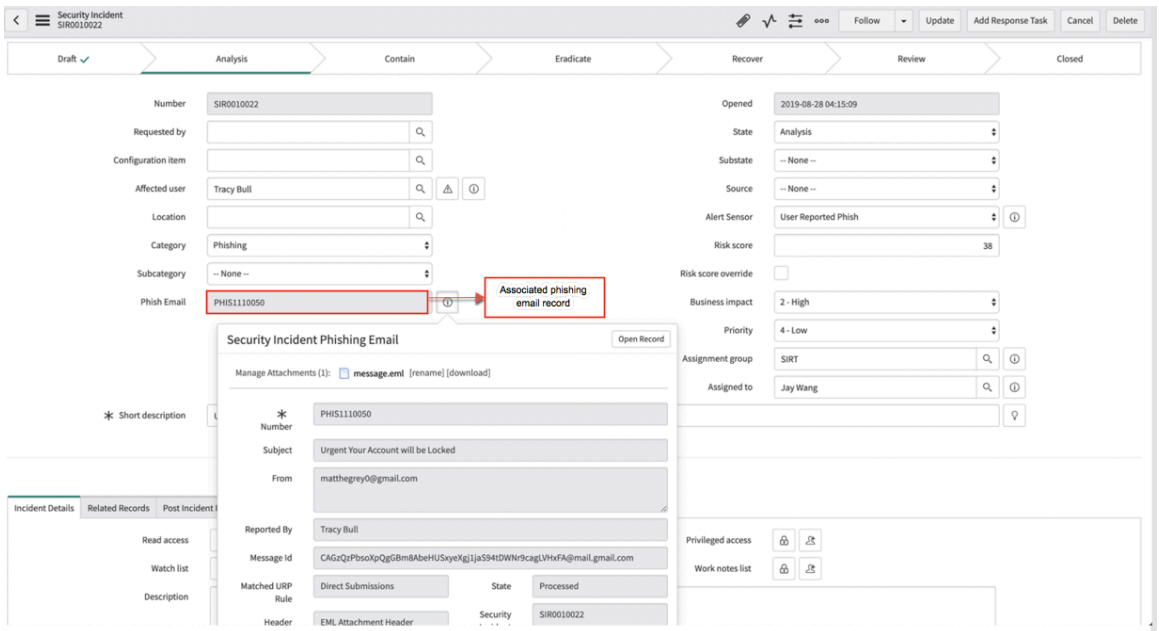
Registros de incidentes de segurança criados a partir de registros de e-mail de phishing

Os registros de e-mail de phishing armazenados na tabela `sn_si_phishing_email` são convertidos em registros de incidentes de segurança.

Para exibir o incidente de segurança associado ao registro de e-mail de phishing, clique em **Incidente de segurança** > **E-mail de Phishing** > **Mostrar todos os e-mails de phishing**.



Clique no link na coluna Incidente de segurança associada ao registro de e-mail de phishing. Os detalhes do incidente de segurança são exibidos.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

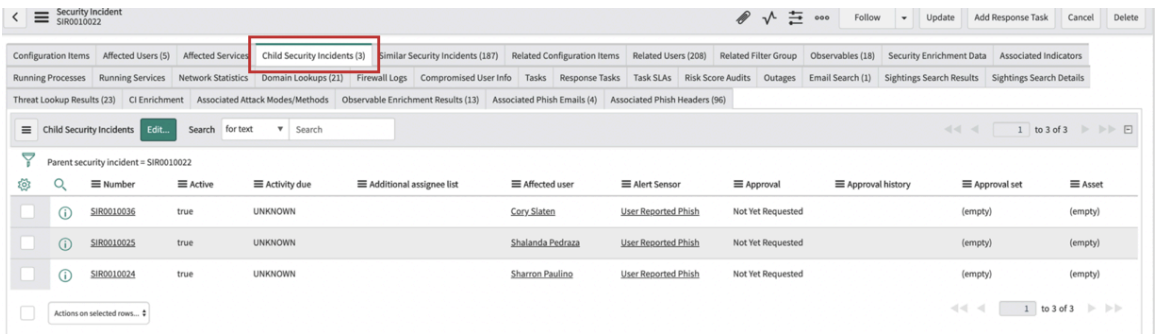
Listas relacionadas

Role para baixo até a seção Links relacionados do incidente de segurança e clique em **Mostrar tudo lista relacionada**. Exiba detalhes como incidentes de segurança secundários, usuários afetados, e-mails de phishing associados.

Incidentes secundários de segurança

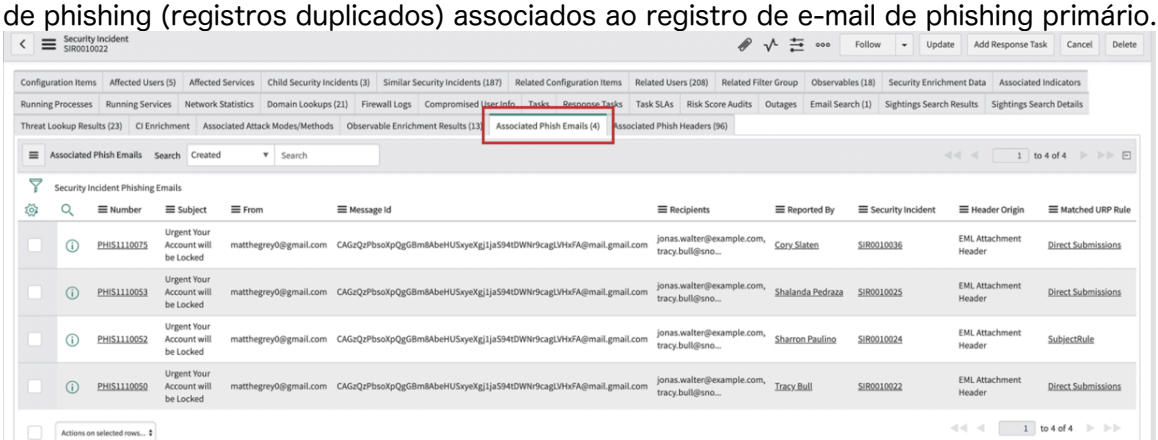
Clique na guia **Incidentes de segurança secundários**. Você pode ver uma lista de incidentes de segurança secundários associados ao incidente de segurança primário com base na lógica de agregação que foi aplicada. Para cada registro secundário adicionado, uma atividade automatizada do sistema é adicionada (na seção Anotação de trabalho) ao registro primário. Isso notifica o analista de segurança sobre o registro secundário agregado.

Nota:
Você poderá ver os incidentes de segurança secundários aqui somente se o sinalizador **Criar incidentes secundários para envios de e-mails agregados** estiver definido como **Sim** na página Propriedades do phishing relatado pelo usuário. Consulte Definir propriedades de Phishing Reportado pelo Usuário para mais detalhes.



E-mails de phishing associados

Clique na guia E- **mails de Phishing Associados**. Você verá uma lista de registros de e-mail de phishing (registros duplicados) associados ao registro de e-mail de phishing primário.

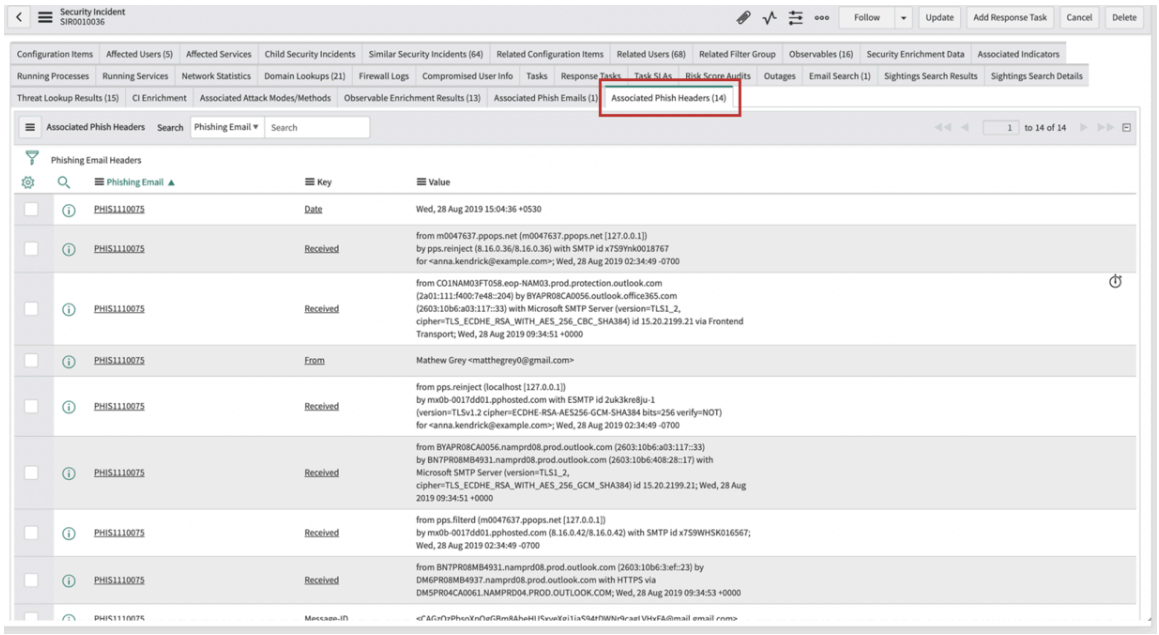


Cabeçalhos de e-mail de phishing associados

Clique na guia E- **mails de Phishing Associados**. Você vê os detalhes do cabeçalho do e-mail de phishing que foram capturados como parte do incidente de segurança. Você pode exibir os cabeçalhos acumulados de todos os registros secundários e registros de e-mail de phishing agregados ao incidente de segurança primário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

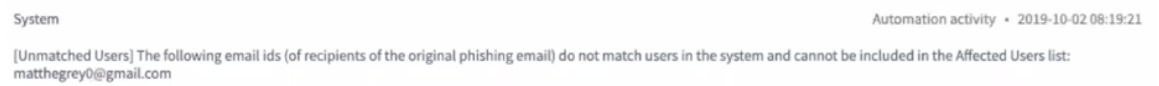


Lista de observáveis permitidos

Conforme o fluxo Transformar e-mails de phishing relatados pelo usuário em incidentes de segurança está sendo executado, você pode monitorar o status do incidente de segurança. Quando determinados observáveis são marcados como observáveis da lista permitida, eles não são adicionados à lista relacionada de observáveis. Ao marcar os observáveis para a lista de permissões, você pode garantir que somente os detalhes importantes sejam exibidos. Por exemplo, se www.google.com for um dos URLs marcados como permitidos, a seguinte mensagem do sistema será exibida. A lista de observáveis permitidos garante que somente os observáveis importantes sejam monitorados.

Captura de usuários incompatíveis

Alguns IDs de e-mail nas listas Para e Cc do e-mail de phishing podem não pertencer a usuários na organização. Esses IDs de e-mail são categorizados como usuários incompatíveis e não estão incluídos na lista relacionada Usuários afetados. Uma anotação de trabalho indicando que esses são usuários incompatíveis é exibida.



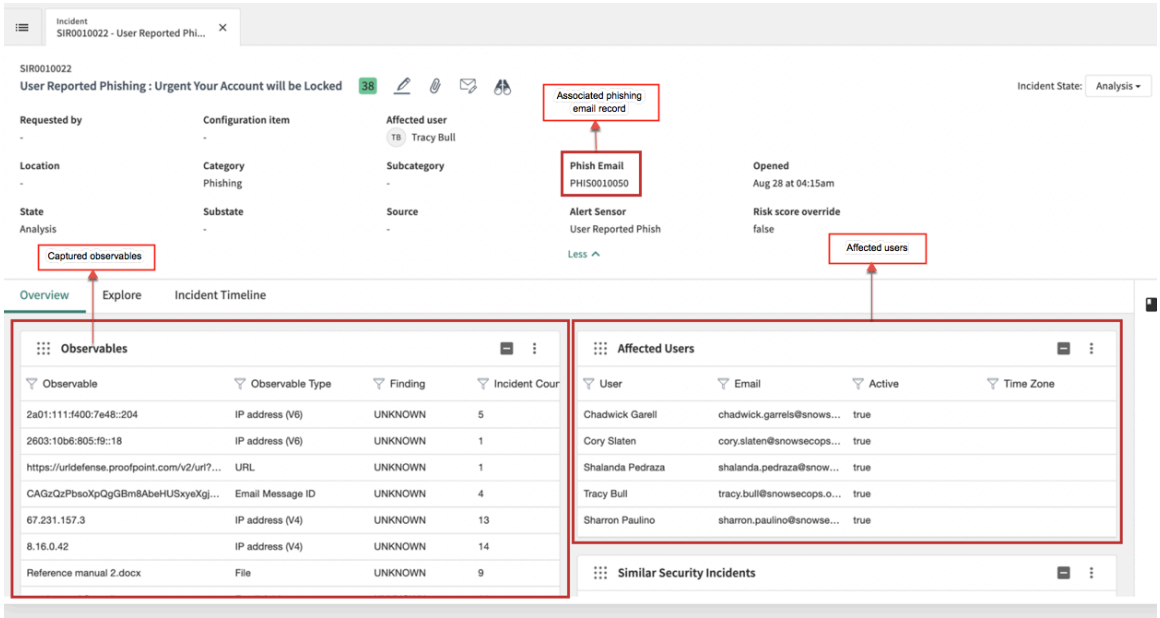
Phishing relatado pelo usuário no espaço do analista de segurança

Você pode exibir incidentes de segurança associados aos registros de e-mail de phishing no Security Analyst Workspace.

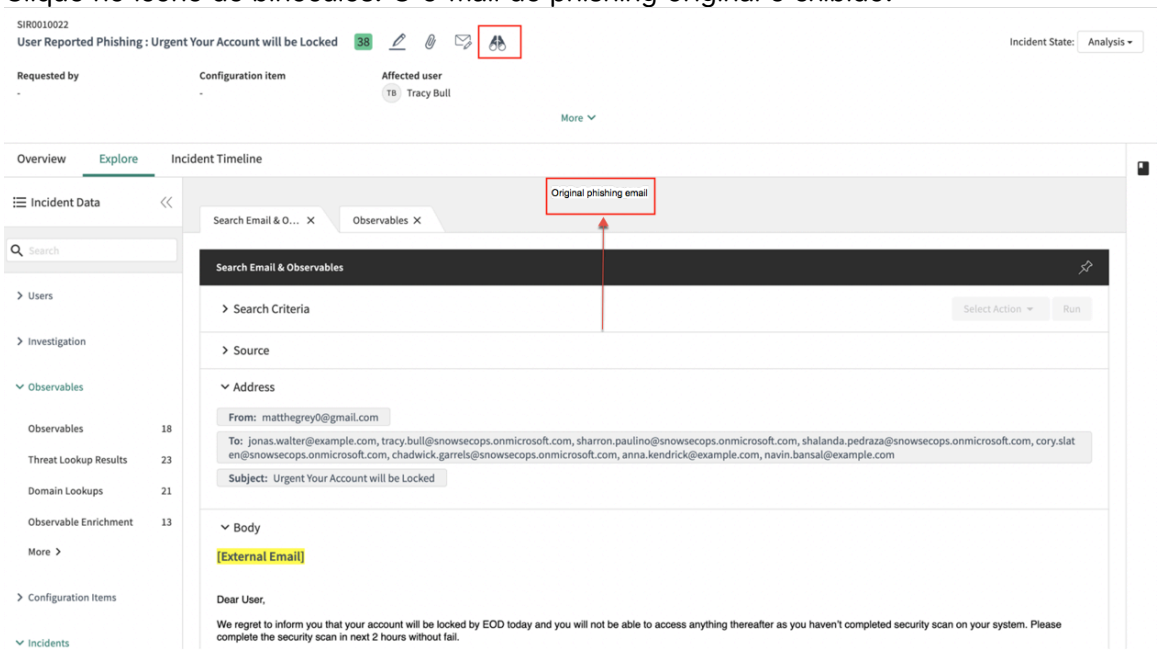
Navegar até **Incidente de segurança** > **Nova IU**. O espaço é aberto em uma guia separada do navegador. Clique no incidente de segurança associado ao registro de e-mail de phishing para exibir o incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



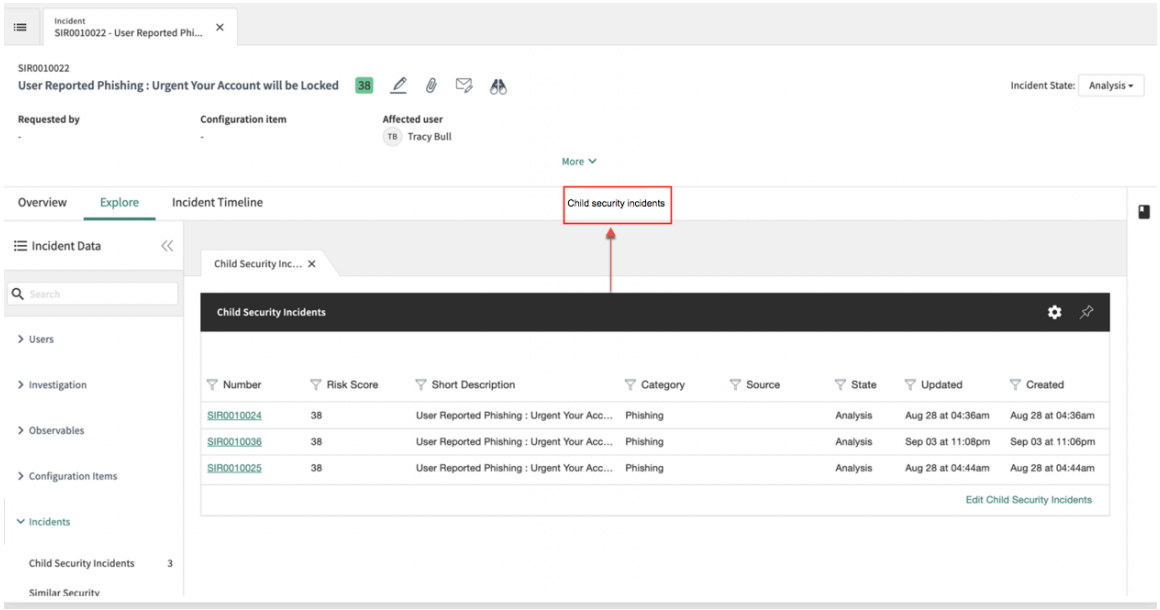
Clique no ícone de binóculos. O e-mail de phishing original é exibido.



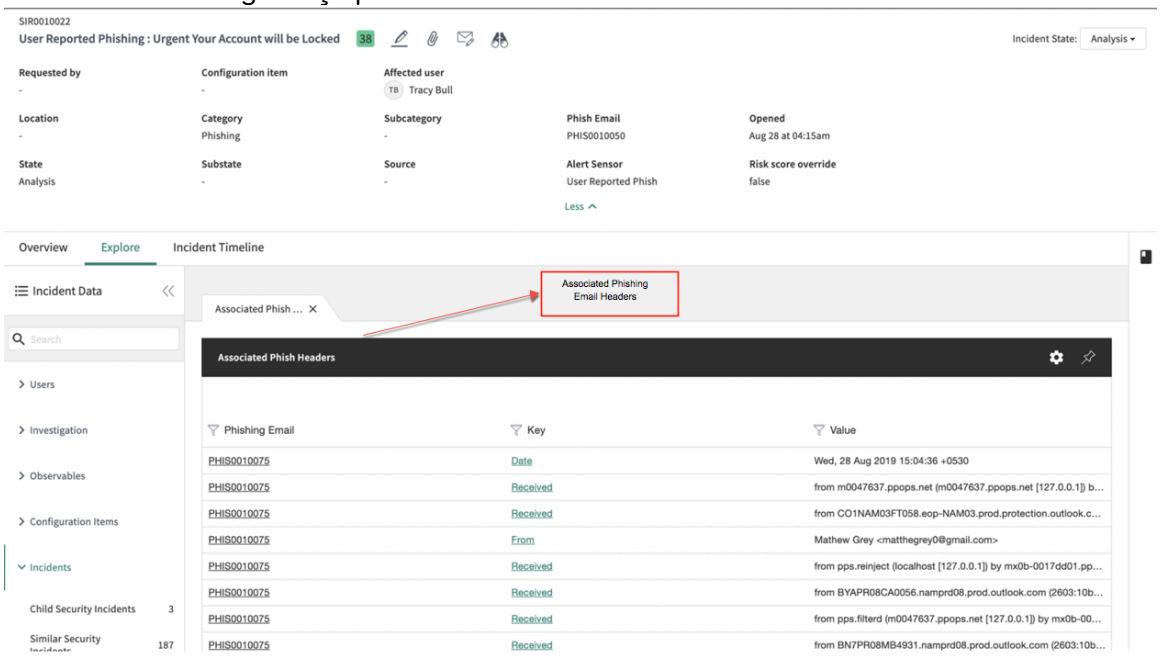
Na guia **Explorar**, clique em **Incidentes** > **Incidentes de segurança secundários**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



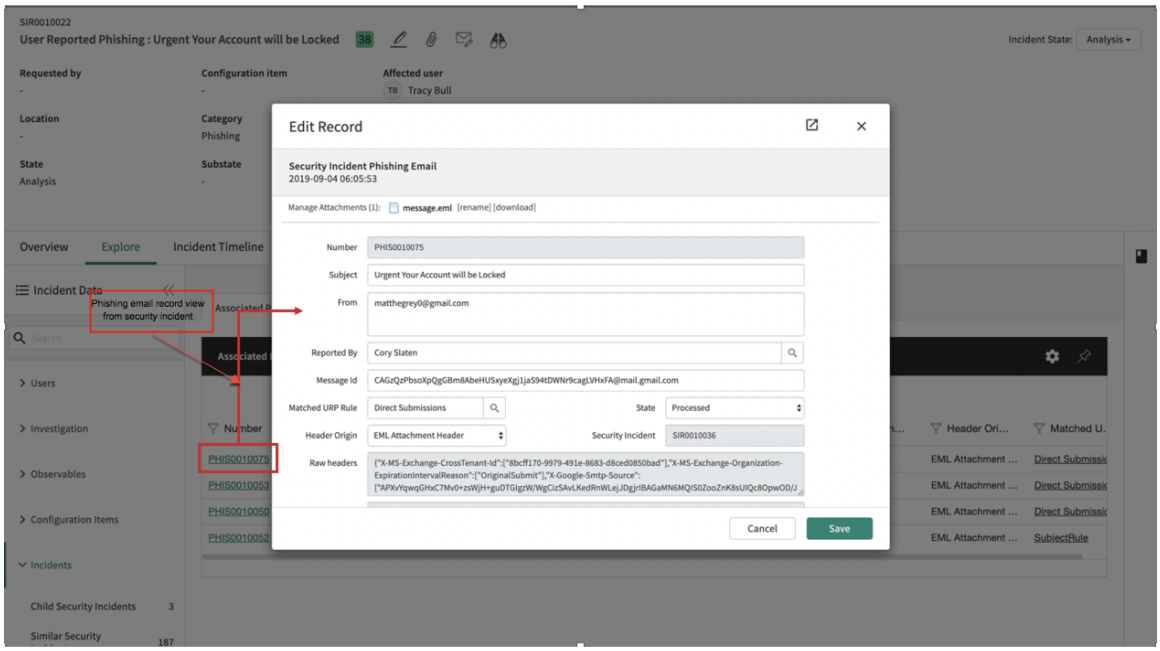
Clicar **Incidentes** > **Cabeçalhos de Phishing Associados** > . Você pode exibir os cabeçalhos acumulados de todos os registros secundários e registros de e-mail de phishing agregados ao incidente de segurança primário.



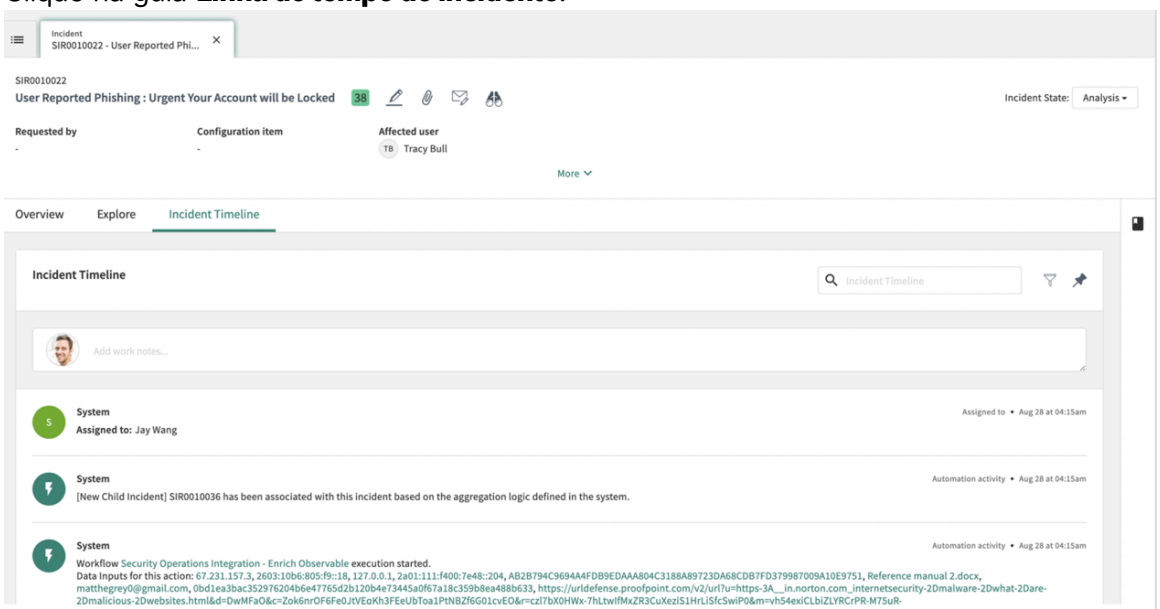
Clique no link do e-mail de phishing para exibir o registro de e-mail de phishing associado ao incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Clique na guia **Linha do tempo do incidente**.



Você pode exibir as atualizações do sistema que destacam:

- Registros secundários duplicados identificados.
- Observáveis da lista permitidos.
- Usuários incompatíveis que receberam o e-mail de phishing, mas não pertencem à lista Usuários afetados.

Perguntas frequentes

Esta seção aborda algumas das perguntas frequentes sobre o recurso aprimorado de Phishing relatado pelo usuário.

1. Instalei o novo spoke do Security Incident Response, mas não consigo exibir nenhum incidente de phishing relatado pelo usuário.

   Por padrão, a funcionalidade Phishing relatado pelo usuário foi desabilitada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para habilitar este recurso, você deve fazer uma cópia do fluxo somente leitura Transformar e-mails de phishing relatados pelo usuário em incidentes de segurança e ativá-lo antes de usar.

2. Ao ingerir e-mails de phishing e convertê-los em incidentes de segurança, quais medidas de precaução são usadas para lidar com links e anexos maliciosos nos e-mails de phishing?

   O scanner antivírus ServiceNow verifica esses anexos e links maliciosos. No entanto, para garantir que os analistas de segurança possam investigar os incidentes com precisão, a aplicação Security Incident Response captura todos os artefatos que fazem parte de um e-mail de phishing. Mas a funcionalidade de Phishing relatado pelo usuário silencia os links maliciosos no e-mail de phishing para que os analistas de segurança não cliquem acidentalmente nesses links. Em relação aos anexos maliciosos, os analistas de segurança devem ter cuidado ao baixá-los.

3. Capturamos todos os arquivos mal-intencionados que fazem parte dos e-mails de phishing para aprimoramento do incidente de segurança?

   Sim, capturamos todos os arquivos dos e-mails de phishing. Você pode exibir esses detalhes que estão disponíveis como parte dos observáveis de incidente de segurança na forma de um hash de arquivo.

4. Enviamos arquivos maliciosos e links de e-mails de phishing para uma instância de área restrita para investigação?

   Atualmente, não oferecemos suporte a integrações de área restrita prontas para uso para investigar arquivos e links mal-intencionados.

5. Há uma janela de tempo ou um gatilho que define a duração na qual os registros de e-mail de phishing duplicados recebidos são associados a um incidente de segurança primário?

   Registros de e-mail de phishing duplicados são agregados somente a um incidente de segurança primário ativo. Se o incidente primário for encerrado ou cancelado, o novo e-mail de phishing duplicado recebido será criado como um novo incidente de segurança. No entanto, neste cenário, no novo incidente de segurança, você pode exibir o incidente de segurança primário encerrado ou cancelado na lista relacionada **de Incidente de segurança semelhante**.

   Nota:
   Esse comportamento pode ser configurado usando o Flow Designer.

6. O recurso de phishing de relatório do usuário oferece suporte ao uso somente do plug-in Microsoft Outlook Wombat para capturar detalhes do cabeçalho do e-mail?

   A funcionalidade Relatada pelo usuário foi criada para analisar cabeçalhos de e-mail e está em conformidade com os padrões RFC822. Portanto, semelhante ao plug-in Wombat, todos os outros plug-ins do Microsoft Outlook que capturam cabeçalhos de e-mail com base nos padrões RFC822 são compatíveis.

Criação de registro a partir de incidentes de segurança

Depois de criar e salvar um incidente de segurança, você pode criar um registro de solicitação de mudança (CHG), incidente (INC) ou problema (PRB) a partir dele. Você também pode criar um caso de atendimento ao cliente a partir de qualquer incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar uma mudança, incidente ou problema a partir de um incidente de segurança

Depois de criar e salvar um incidente de segurança, você pode criar um registro de solicitação de mudança (CHG), incidente (INC) ou problema (PRB) a partir dele.

Antes de Iniciar

Função necessária: sn.si_basic ou superior

Procedimento

1. Abra um incidente de segurança usando um desses métodos.
   - Abra um incidente de segurança existente navegando até **Incidente de segurança** > **Não designado** > **Incidentes**e clicando em um incidente de segurança.
   - Crie um incidente de segurança navegando até **Incidente de segurança** > **Não designado** > **Incidentes**, clique em **Novo**, preencha o formulário e salve o registro.
2. Clique com o botão direito do mouse na barra de cabeçalho do incidente de segurança e clique em um dos seguintes:
   - **Criar Mudança**
   - **Criar incidente**
   - **Criar problema**

   Nota:
   Esta opção se aplica somente se a propriedade pop-up (sn_vul.popup) estiver habilitada. Quando você clica em um desses botões, uma janela de visualização é aberta para mostrar as informações do incidente de segurança que são usadas para criar a mudança, o incidente ou o problema. Ou seja, o item de configuração, seu local, sua prioridade e as descrições curtas e longas. Se você estiver criando uma solicitação de mudança, poderá editar os campos **Prioridade**, **Descrição resumida**e **Descrição**. Se você estiver criando um incidente, poderá editar os campos **Impacto**, **Urgência**, **Descrição resumida** e **Descrição**. Os campos na tela do incidente de segurança associado não são afetados.
3. Clique em **Enviar** para criar a mudança, o incidente ou o problema.

Criar um caso do Atendimento ao cliente a partir de um incidente de segurança

Security Incident Response é fornecido com um mapeamento de campo padrão que mapeia um incidente de segurança para um caso Atendimento ao cliente (CS). Você pode criar um caso de CS a partir de qualquer incidente de segurança, editar a **Prioridade**e também adicionar **Anotações opcionais**.

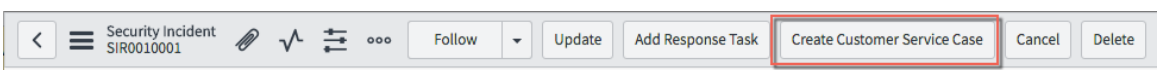
Antes de Iniciar

Função necessária: sn_si.basic e sn_customerservice_agent

Nota:
O plug-in Atendimento ao cliente deve ser ativado para executar esta tarefa.

Procedimento

1. Navegue até **Incidente de segurança**.
2. Abra o incidente de segurança ao qual você deseja adicionar um caso de CS.
3. Clique em **Criar caso de atendimento ao cliente** no cabeçalho superior.



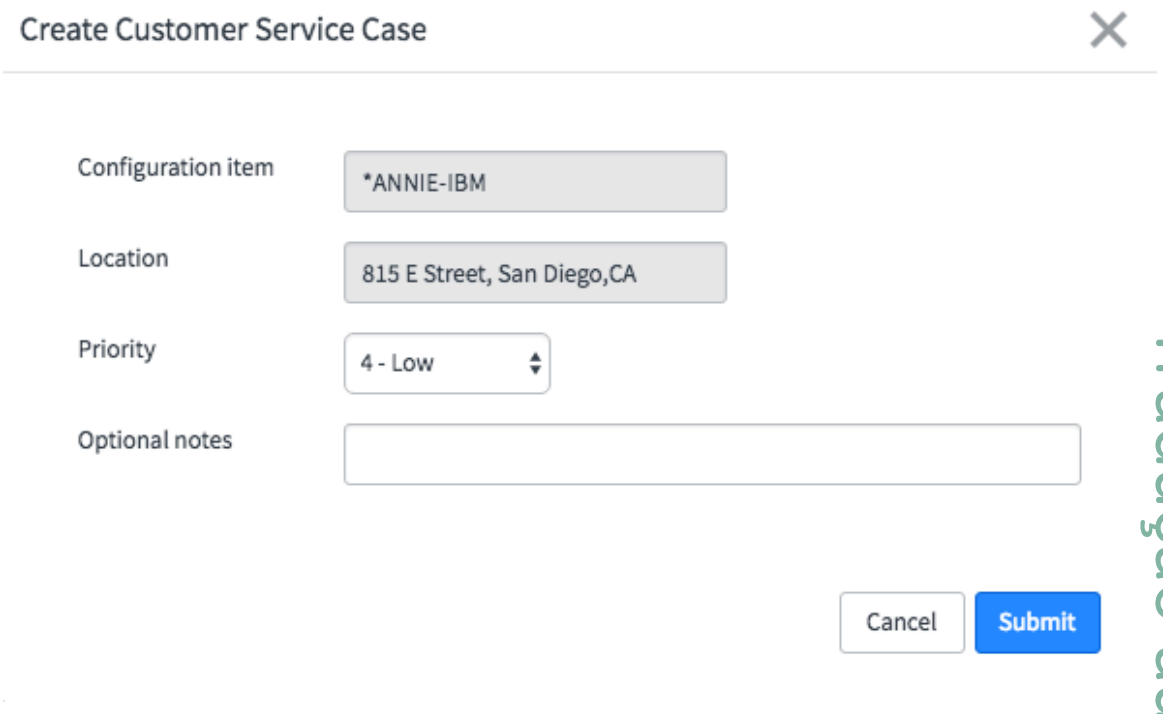
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A janela pop-up é preenchida previamente com informações do incidente de segurança com base no mapeamento de campo.

4. Você pode selecionar uma nova **Prioridade** e adicionar quaisquer **Anotações Opcionais**.

Nota:
O campo **Prioridade** substitui a configuração padrão. As **anotações opcionais** são anexadas ao incidente.



5. Clique em **Enviar**.
Um caso de CS é criado e exibido na lista relacionada Casos do Atendimento ao cliente no incidente de segurança.
6. Você pode clicar no link do caso de CS para acompanhar o caso.

Tópicos relacionados

Gestão de casos de atendimento ao cliente

Adicionar um incidente de segurança a um caso de segurança

Se você determinar que um incidente de segurança requer um nível superior de análise, adicione-o a um caso novo ou existente.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

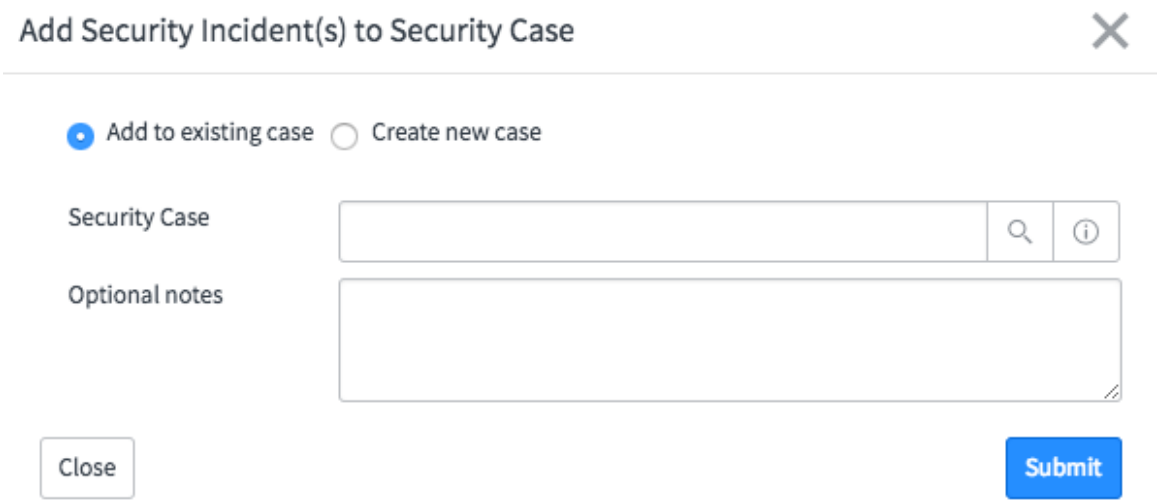
Função necessária: sn_si.admin, sn_ti.case_user_write

Procedimento

1. Navegue até o incidente de segurança que requer escalação clicando em **Incidente de segurança** > **Incidentes** > **Atribuídos a Mim**e abra o incidente de segurança.
2. Clique no link relacionado **Adicionar ao caso de segurança**.
A caixa de diálogo **Adicionar incidente(s) de segurança ao caso de segurança** é aberta.

Tradução automática

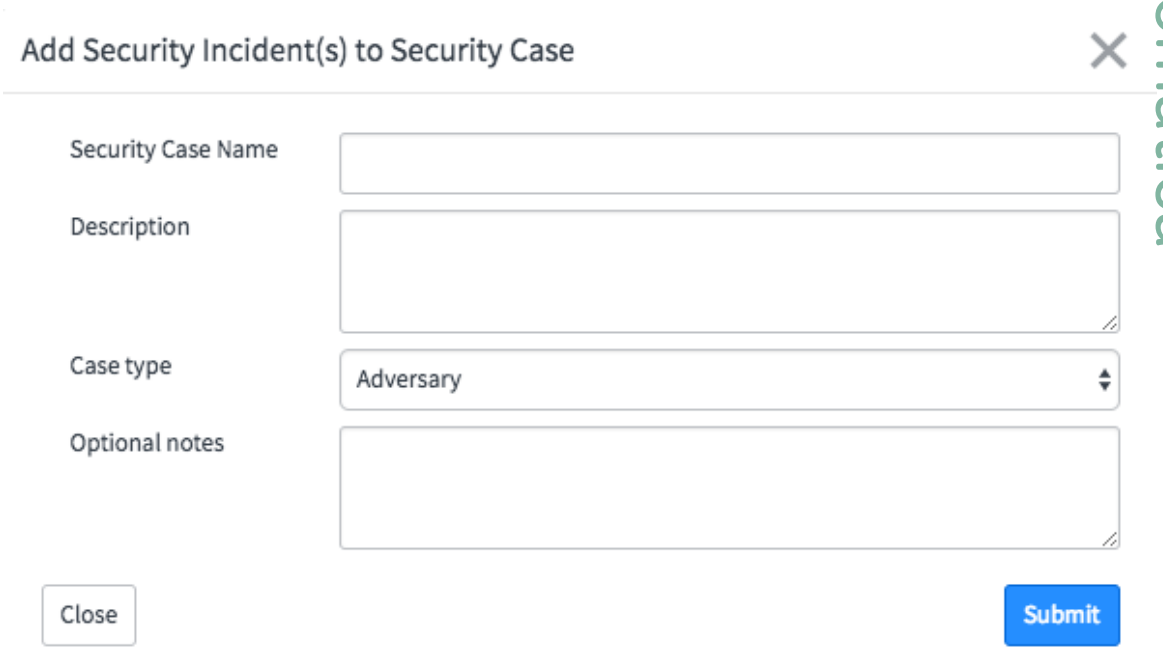
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Se você tiver um caso atribuído a você ao qual deseja adicionar este incidente de segurança, preencha os campos conforme apropriado e clique em **Enviar**.

Campo	Descrição
Caso de segurança	Selecione o caso de segurança.
Anotações opcionais	Conforme necessário, insira anotações adicionais que sejam valiosas para o analista de caso.

4. Se você tiver um ou mais casos atribuídos a você, mas quiser criar um novo caso e atribuir o incidente de segurança a ele, clique em **Criar novo caso** para mostrar campos adicionais.



Nota:
Se você não tiver nenhum caso atribuído a você, a tela acima será aberta primeiro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Preencha os campos, se for o caso.

Campo	Descrição
Nome do caso de segurança	Insira o nome do novo caso de segurança.
Descrição	Insira uma descrição para o caso.
Tipo de Caso	Selecione o tipo de caso que está sendo investigado.
Anotações opcionais	Conforme necessário, insira anotações adicionais que sejam valiosas para o analista de caso.

6. Clique em **Enviar**.
   Uma mensagem aparece na parte superior do incidente de segurança, junto com um link para o novo caso.

Tópicos relacionados

Security Case Management

Criar tarefas de resposta

Depois que um incidente de segurança foi criado, você pode criar tarefas de resposta para rastrear ações separadas a serem realizadas para responder ao problema de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Navegue até o local apropriado para abrir o incidente de segurança para o qual você deseja criar tarefas.
   Por exemplo:
   - Para criar uma tarefa de resposta com base em um incidente de segurança atribuído a você, selecione **Incidente de segurança** > **Incidentes** > **Atribuídos a Mim**.
   - Para criar uma tarefa de resposta com base em um incidente de segurança atribuído à sua equipe, selecione **Incidente de segurança** > **Incidentes** > **Atribuído à Equipe** > **Incidentes**.
   - Para criar uma tarefa de resposta com base em um incidente de segurança não atribuído, selecione **Incidente de segurança** > **Incidentes** > **Incidentes não atribuídos**.
2. Abra o incidente de segurança para o qual você deseja adicionar tarefas de resposta.
3. Clique no botão **Adicionar tarefa de resposta** no cabeçalho do formulário.

   Nota:
   Para criar qualquer outra tarefa, clique na guia **Tarefas** na Lista relacionada de incidentes. Para obter mais informações sobre como criar outros tipos de tarefas, consulte Crie uma tarefa.

4. Preencha os campos no formulário, conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidente de segurança

Campo	Descrição
Selecione marcador de segurança	Se você configurou e ativou marcadores de segurança, poderá selecionar um ou mais marcadores para adicionar metadados ao registro ou especificar o grau de confidencialidade da tarefa de resposta. Se você não configurou ou ativou marcadores de segurança, esta lista suspensa não será exibida.
Número	[Somente leitura] O número Security Incident Response gerado automaticamente.
Primário	[Somente leitura] O número do incidente de segurança relacionado.
Item de Configuração	O item de configuração (recurso) afetado pelo problema de segurança.
Usuário afetado	A pessoa afetada pelo problema de segurança.
Prioridade	A prioridade usada para determinar quando esta tarefa será realizada.
Estado	O estado atual da tarefa de resposta de segurança. Na criação da tarefa, este campo é padronizado como **Rascunho**.
Habilidades	A habilidade necessária para executar esta tarefa. Clique no ícone de cadeado e selecione a habilidade necessária. Depois de concluir suas seleções, clique no ícone de cadeado novamente.
Grupo de atribuição	O grupo de atribuição do qual o trabalhador atribuído é selecionado.
Atribuído a	O indivíduo atribuído para executar a tarefa.
Descrição resumida	Uma descrição da tarefa Security Incident Response.
Descrição	Uma descrição para a tarefa selecionada.
Notas de segurança	As anotações de trabalho que são criptografadas e não visíveis para o cliente.
Anotações de trabalho	As anotações de trabalho que não estão visíveis para o cliente.
Comentários adicionais	Comentários que você deseja que fiquem visíveis para o cliente.

Tradução automática

5. Ao concluir as entradas, clique em **Enviar**.

Nota:
Depois de criar Security Incident Response tarefas, você pode exibi-las usando qualquer uma das seguintes aplicações no módulo **Tarefas de resposta** :

- **Atribuído a mim**.
- **Atribuído à equipe**.
- **Mostrar Tarefas Abertas**

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Mostrar Todas as Tarefas**
- **Tarefas não atribuídas**.

Gerenciar Predictive Intelligence para phishing relatado pelo usuário

O recurso Predictive Intelligence for User Reported Phishing fornece uma solução significativa na triagem e priorização de e-mails de phishing relatados pelo usuário.

Esta seção descreve o seguinte:

- Inteligência preditiva para phishing denunciado por usuários
- Componentes e plug-ins necessários
- Geração de veredito final para phishing relatado pelo usuário
- Solução de problemas da Inteligência preditiva para phishing relatado pelo usuário

Inteligência preditiva para phishing denunciado por usuários

Este recurso ajuda os analistas de segurança na triagem e na priorização de e-mails de phishing relatados pelo usuário.

A estrutura Predictive Intelligence fornece soluções para treinar o sistema para prever, recomendar e organizar os resultados dos dados. Para obter mais detalhes sobre Predictive Intelligence, consulte Predictive Intelligence . Usando essa estrutura, você pode criar modelos para prever automaticamente se um e-mail de phishing relatado pelo usuário é suspeito ou legítimo.

Usando dados históricos de incidentes de segurança de Phishing Relatado pelo Usuário (cabeçalhos de e-mail, corpo de e-mail e resultados de triagem capturados por meio dos códigos de fechamento de incidentes de segurança), os analistas de segurança podem treinar o sistema para classificar os envios de phishing relatados pelo usuário de entrada como aqueles que precisam ser triados (prováveis) suspeitos) e aqueles que são envios legítimos.

Ao fazer a triagem de e-mails recebidos automaticamente, os analistas de segurança podem priorizar facilmente a fila de incidentes e se concentrar em incidentes que provavelmente representam um risco para a organização em primeiro lugar e gastar menos esforço em e-mails que provavelmente serão falsos positivos. O resultado da previsão também fornece uma pontuação de confiança na classificação para habilitar a priorização granular.

Componentes e plug-ins necessários

Para usar a Inteligência preditiva para Phishing relatado pelo usuário, você deve instalar as seguintes aplicações

Nome do plug-in	Versão mínima
Security Incident Response	9.0.1 ou 10.0.2
Predictive Intelligence	Versão do Orlando
Inteligência preditiva para phishing denunciado por usuários	10.0.2

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Os novos aprimoramentos a seguir estão disponíveis com o Security Incident Response 10.4:

- A capacidade de escolher códigos de encerramento de campos personalizados para treinamento do modelo.
- A capacidade de ativar explicitamente as previsões após a criação do modelo.
- A capacidade de gerar um veredito final no envio de Phishing relatado pelo usuário usando uma tabela de decisão. (requer Security Operations Spoke 10.3.0)

Para usar os novos aprimoramentos, você deve atualizar as seguintes aplicações:

Nome do plug-in	Atualizar para
Security Incident Response	10.0.4
Inteligência preditiva para phishing denunciado por usuários	10.3.1

Tabelas novas e atualizadas

- sn_sir_ml_urp_config (Novo): contém a configuração da aplicação URP ML.
- sn_sir_ml_urp_feature (Novo): registros extraídos da tabela de e-mail sn_si_phishing.
- sn_sir_ml_urp_feature_import (Novo): usado para carregar dados históricos de e-mail de phishing.
- sn_si_incident (atualizado): os seguintes novos campos foram adicionados:
  - Previsão aceita
  - Resultado da previsão
  - Pontuação de confiança
- **Script Includes**
  - URPMLUtil: recupera a configuração, executa o trabalho de previsão e rastreia o processo de previsão.
  - URPMLProcessor: extrai e processa dados da tabela sn_si_phishing_email.
  - URPMLAction: executa o fluxo para aceitar o resultado da previsão.

Geração de veredito final para phishing relatado pelo usuário

As equipes do Security Incident Response agora podem gerar o veredito finalizado para um registro de phishing relatado pelo usuário com base nos resultados da inteligência preditiva e das integrações de aprimoramento de ameaças.

Essa geração de veredito final é habilitada por meio de uma construção de tabela de decisão e aproveitada em um fluxo.

Pré-requisitos

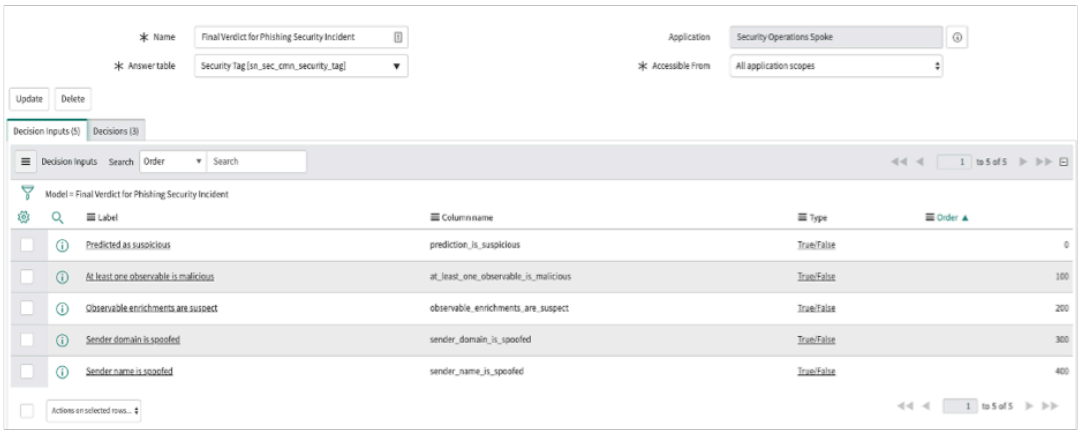
Certifique-se de que todos os plug-ins listados em Componentes e plug-ins necessários tenham sido instalados.

Navegar até **Inteligência preditiva para phishing** > **Veredito final** > **Veredito final para incidente de segurança de phishing**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

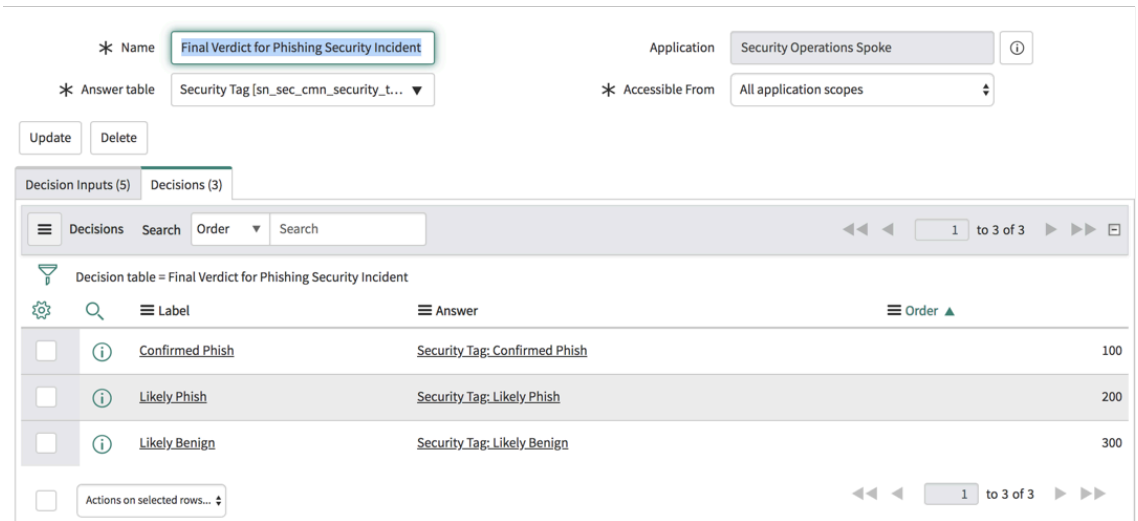
A guia **Entradas de decisão** mostra as diferentes condições que foram avaliadas para chegar ao veredito final.



As seguintes condições estão disponíveis com o sistema de base:

- Previsto como suspeito: quando a inteligência preditiva tiver classificado o e-mail de phishing relatado pelo usuário como **suspeito**.
- Pelo menos um observável é malicioso: quando um observável envolvido no incidente de segurança (por exemplo, URL, domínio, IP, hash) foi classificado como **malicioso** por fontes de inteligência contra ameaças.
- O enriquecimento de observáveis é suspeito: quando o enriquecimento em observáveis (por exemplo, recência de registro de domínio de phishing, país de registro de domínio de phishing) é considerado suspeito.
- O domínio do remetente é falsificado: quando o domínio de e-mail do fraudador é suspeito de falsificar um domínio confiável.
- O nome do remetente é falsificado: quando o endereço de e-mail do phishing é suspeito de falsificar um funcionário confiável de uma organização.

A guia **Decisões** mostra as opções de veredito final que podem ser obtidas para um determinado incidente de segurança.



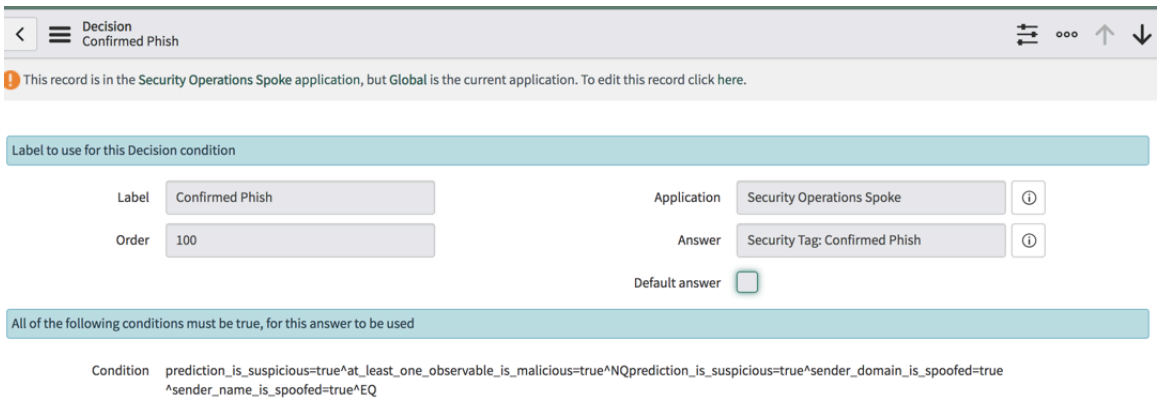
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As seguintes decisões estão disponíveis com o sistema de base:

- Phish confirmado: quando as condições levam ao veredicto final como sendo um e-mail de phishing confirmado.
- Provável phishing: quando as condições levaram ao veredito final como uma possível tentativa de phishing.
- Provável benigno: quando as condições levaram ao veredicto final como um envio benigno.

Você pode ver as condições que foram avaliadas para cada uma das opções de veredito final. Clique no link Rótulo para ver as condições.



Você pode personalizar a tabela de decisão fornecida com o sistema de base ou criar sua própria tabela de decisão. Esta tabela de decisão pode ser aproveitada em playbooks de resposta a incidentes de segurança. O subfluxo **Gerar veredito final para incidentes de segurança de phishing** está disponível com o sistema de base. Este subfluxo gera automaticamente o veredito final para um incidente de segurança de phishing e aplica um marcador de segurança com base nessa decisão. Você pode incluir este subfluxo como parte do playbook de **phishing automatizado**.

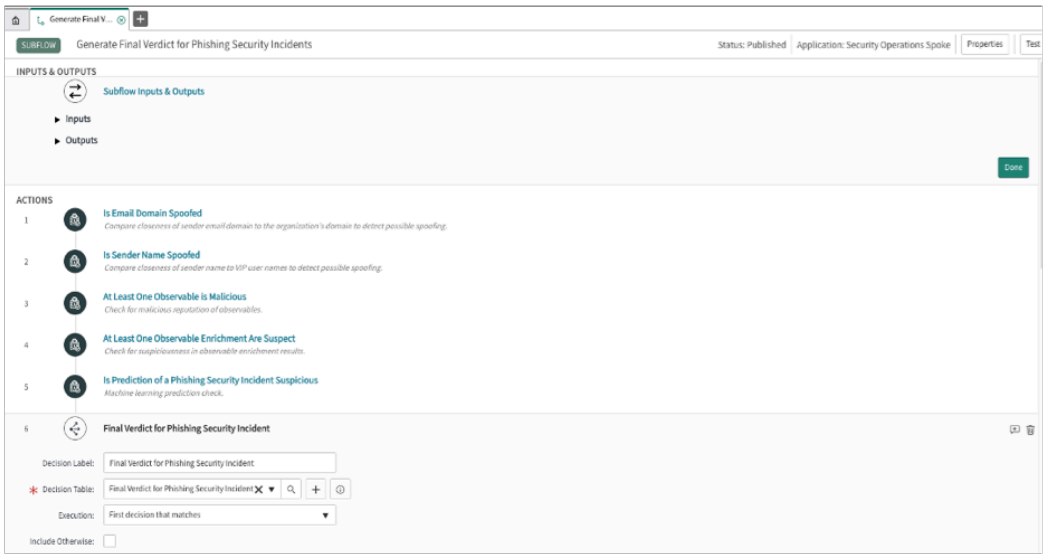
As entradas para este subfluxo são:

- incident_id: o ID do sistema do incidente de segurança de phishing.
- c_level_names: lista separada por vírgulas de nomes (por exemplo, nomes de executivos da organização) que provavelmente estão sendo falsificados no ataque de phishing.
- Trusted_domains: lista separada por vírgulas de domínios de e-mail confiáveis.
- richment_keywords: lista separada por vírgulas de palavras-chave que indicam a mal-intendência do observável dos resultados de aprimoramento.
- sender_email (opcional): o endereço de e-mail do remetente do e-mail de phishing.

A saída deste fluxo pode ser **Phish confirmado**, **Phish provável**ou **Benigno provável**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Solução de problemas da Inteligência preditiva para phishing relatado pelo usuário

Esta seção cobre alguns cenários de problemas comuns.

- Problema: não consigo modificar a configuração do Predictive Intelligence.

  Solução: verifique se você tem permissões para fazer isso. Você deve fazer login como um usuário com a função ml_admin para modificar limites. Alguns cenários podem exigir privilégios ainda maiores, como, por exemplo, você precisa modificar o limite de dados de treinamento. Para esses cenários, você deve entrar em contato com o Suporte ao cliente para obter assistência.

- Problema: o treinamento do modelo falhou.

  Solução: verifique se os URLs do programador de ML foram configurados. Navegar até **Propriedades do sistema** > **Todas as Propriedades** e verifique se a propriedade `glide.shared_service_scheduler.url` foi configurada.

- Problema: os resultados da previsão não estão disponíveis em um incidente de segurança.

  Solução:

  - Verifique se a URL da previsão foi configurada na propriedade do sistema `glide.prediction_service.url` e certifique-se de que o datacenter corresponda à URL.
  - Verifique se o trabalho programado Prever e-mail de phishing relatado pelo usuário está ativo.

Configurar Predictive Intelligence for User Reported Phishing

Configure e prepare o modelo para identificar e-mails de phishing relatados pelo usuário.

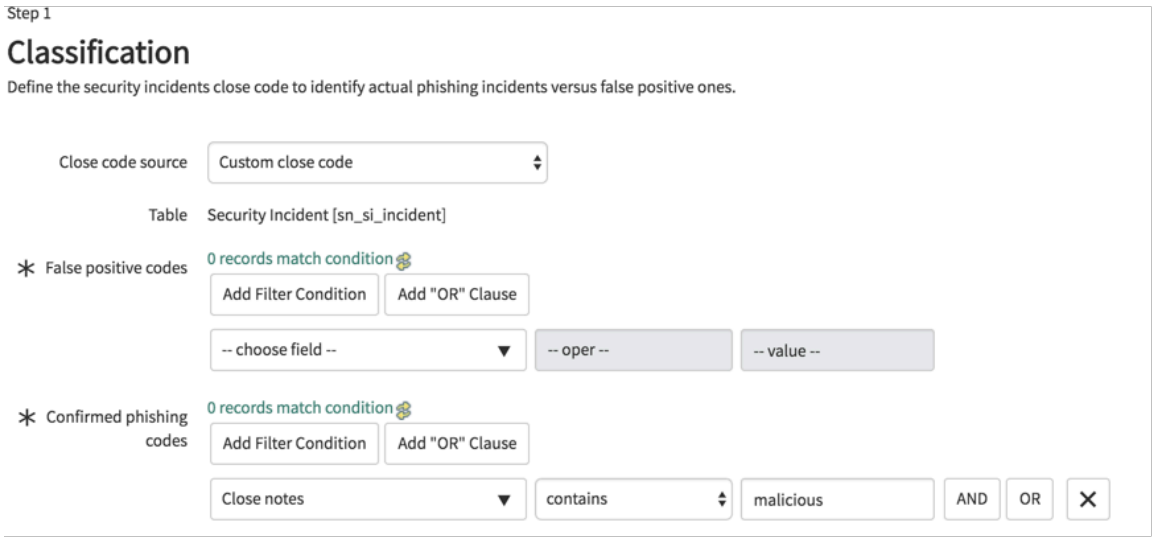
Antes de Iniciar
Função necessária: ml_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Inteligência preditiva para phishing** > **Configuração**.
2. Na Etapa 1 da configuração, selecione uma das seguintes opções na lista Fechar origem do código:
   - Código de encerramento padrão: selecione esta opção para especificar os códigos de encerramento de incidente de segurança padrão que devem ser usados pelo modelo de treinamento para identificar e-mails maliciosos e legítimos. Clique no ícone de cadeado e selecione um ou mais códigos falso-positivos ou códigos de phishing confirmados.
   - Código de encerramento personalizado: selecione a opção Código de encerramento personalizado se quiser definir códigos de encerramento de campos personalizados que podem ser usados como parte dos procedimentos de resposta do incidente existentes. Para definir um código de encerramento, selecione um campo na tabela de incidentes de segurança e especifique uma ou mais condições de filtro.



3. Na Etapa 2, importe dados históricos que podem ser usados para treinar o modelo.
   Selecione a fonte de dados para importar os dados históricos. Isso pode ser:
   - Tabela de e-mail de phishing relatada pelo usuário: você pode ver o número de registros que podem ser importados como dados históricos. Selecione esta opção e clique em **Importar**.
   - Fonte de dados personalizada: você pode anexar um único arquivo CSV formatado que contenha registros de dados históricos. Selecione o arquivo e clique em **Importar**.

   Nota:
   O arquivo CSV que você importa deve conter os seguintes cabeçalhos:
   - Rótulo
   - Cabeçalho
   - Texto do corpo

   Cada registro deve conter um marcador Mal-intencionado ou Legítimo na coluna Rótulo no arquivo CSV.

   Clique em **Cancelar importação** para parar de importar os dados. O processo de importação é cancelado e todos os registros que foram importados até o momento são excluídos.

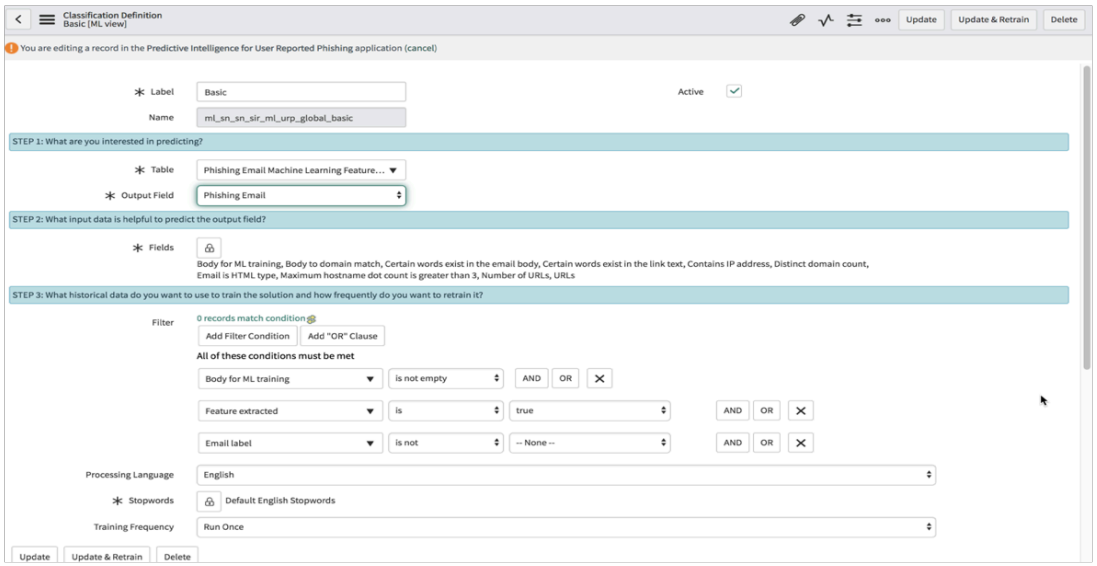
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Depois de importar os dados históricos, clique no link para atualizar a página.
   Você pode importar mais dados de treinamento ou continuar com a próxima etapa.
5. Na Etapa 3, verifique se o número de registros disponíveis para treinamento atende aos requisitos de limite mínimo.

> **Nota:**
> Os valores padrão para o número máximo e mínimo de registros de treinamento são exibidos. Esses limites podem ser modificados na página Propriedades do aprendizado de máquina da plataforma. Entre em contato com o Suporte ao cliente para obter assistência.

6. Se os dados de treinamento forem suficientes, clique em **Treinar modelo**.
   Você pode atualizar as entradas para treinamento na tela abaixo.



7. As entradas de previsão que você pode modificar incluem:
   - O que você está interessado em prever?
   - Quais dados de entrada são úteis para prever o campo de saída?
   - Quais dados históricos você deseja usar para treinar a solução e com que frequência deseja retreiná-la?

   Os valores padrão dessas entradas são exibidos. Você pode modificá-los e clicar em qualquer um dos seguintes:
   - **Atualizar**: atualiza a definição do modelo de treinamento.
   - **Atualizar e retreinar**: atualiza a definição do modelo de treinamento e retreina o modelo (aciona a função **Treinar modelo**).
8. Por fim, quando tiver concluído o treinamento do modelo, clique na caixa de seleção **Ativar previsão**.
   As previsões agora são fornecidas em todos os registros de phishing relatados pelo usuário usando esse modelo. Se você quiser parar de fornecer previsões nos registros de phishing relatados pelo usuário, desmarque a caixa de seleção **Ativar previsão** e clique em **Desativar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribuição de analistas de segurança

Dependendo das suas configurações na tela SIR Administração Configuração, você pode atribuir analistas de segurança a incidentes de segurança manualmente; automaticamente usando um fluxo de trabalho; ou automaticamente usando a atribuição automática.

Atribuição manual de analista

Você pode configurar a tela Configuração de administração Security Incident Response para exigir que os analistas de segurança sejam atribuídos manualmente sempre que alguém ou a aplicação SIR criar um incidente de segurança ou gerar uma tarefa de resposta de segurança.

Se um incidente de segurança ou tarefa de resposta não puder ser atribuído automaticamente, você poderá definir a tela SIR Configuração de administração para exigir a atribuição manual de analistas de segurança. Essa é uma boa opção se você tiver um número limitado de analistas de segurança para concluir solicitações ou se simplesmente não quiser atribuí-los automaticamente.

Atribuição de analista de segurança baseada em fluxo de trabalho

Você pode configurar a tela Security Incident Response Administração Configuração para usar um fluxo de trabalho selecionado para atribuir o analista de segurança sempre que alguém ou a aplicação SIR criar um incidente de segurança ou tarefa de resposta de segurança.

Na tela de configuração Administração de incidente de segurança, você pode optar por usar um fluxo de trabalho para atribuir um analista a cada incidente de segurança ou tarefa de resposta de segurança. Esta opção é uma boa opção para organizações que usam um processo personalizado para resolver problemas de segurança ou têm um processo que pode ser automatizado.

Atribuição automática de analista de segurança

Você pode configurar a tela Configuração de administração Security Incident Response para atribuir automaticamente o analista de segurança sempre que alguém ou a aplicação SIR criar um incidente de segurança ou uma tarefa de resposta de segurança. A atribuição automática permite que você defina, com base nas necessidades da sua organização, os critérios pelos quais os analistas são atribuídos automaticamente a incidentes de segurança.

Atribuição automática de agente com base nas classificações do agente

Se a atribuição automática estiver habilitada e um incidente de segurança ou uma tarefa de resposta for criada, ocorrerão as seguintes ações:

- Os analistas de segurança disponíveis são avaliados com base nos critérios definidos na configuração.
- Um analista de segurança apropriado é atribuído automaticamente à tarefa.
- A tarefa é movida para o estado **Atribuído**.

Se a configuração for definida para considerar mais de um conjunto de condições, como habilidades, local, fuso horário ou área de cobertura do grupo, os analistas de segurança serão avaliados com base nas configurações de propriedade de ponderação e outros critérios. Essas definições de configuração ajudam a atribuir agentes automaticamente com base em propriedades opcionais. As classificações calculadas são usadas para determinar o melhor agente para o incidente de segurança ou a tarefa de resposta.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Qualquer combinação de métodos baseados em classificação pode ser habilitada na tela de configuração da aplicação.

Quando uma tarefa é criada, uma classificação para cada tipo de critério de seleção habilitado é calculada para cada agente disponível. O agente cuja classificação total é mais alta é considerado para atribuição automática.

As configurações das propriedades de ponderação de atribuição automática, encontradas em **Incidente de segurança** > **Administração** > **Propriedades**, estão incluídos nos cálculos de classificação.

Esses valores ajudam a priorizar quais critérios de seleção de atribuição automática são mais importantes para sua organização. Defina os valores de prioridade entre 1 (menos importante) e 10 (importante).

Para obter um exemplo de como as propriedades de ponderação afetam as classificações do agente, consulte Atribuição automática de agente usando vários critérios de seleção.

Atribuição automática de agente usando o local

Os agentes podem ser atribuídos automaticamente com base no local inicial no registro do usuário e no local das tarefas.

A atribuição automática por local é realizada quando a opção **de configuração A seleção automática de agentes considerará o local dos agentes** está habilitada.

Quando uma tarefa (incidente de segurança ou tarefa de resposta) é criada, o agente mais próximo do local da tarefa é considerado para a tarefa. Se a aplicação estiver configurada para que somente a localização seja considerada, a tarefa será atribuída automaticamente ao agente mais próximo.

Quando uma tarefa é criada, os locais do agente são comparados aos intervalos a seguir para determinar a classificação de local de cada agente.

Cálculo de classificação do local

Distância (milhas) do agente até a tarefa	Classificação
0 a 0,1	1
0,11 a 0,5	0,9
0,51 a 5	0,7
5,1 a 10	0,5
10,1 a 20	0,4
20,1 a 30	0,3
30,1 a 40	0,2
40,1 a 100	0,1
> 100	0

Se a aplicação estiver configurada para usar outros critérios de seleção, como habilidades, fuso horário ou programação, as classificações de todos os critérios de seleção serão ponderadas e somadas. O agente com a classificação geral mais alta é atribuído automaticamente à tarefa. Consulte Atribuição automática de agente usando vários critérios de seleção para mais detalhes.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribuição automática de agente usando habilidades

Os agentes podem ser atribuídos automaticamente com base em suas habilidades e nas habilidades necessárias para executar a tarefa. Atribuir habilidades aos registros de usuário usando **Habilidades** > **Usuários**.

A atribuição automática por habilidades pode ser realizada quando a opção Seleção **automática de agentes para tarefas requer que eles tenham habilidades** está definida como **todos** ou **alguns**.

Quando uma tarefa que inclui habilidades é atribuída automaticamente, as habilidades de um agente são comparadas com as habilidades necessárias para executar a tarefa. Uma classificação é calculada com base na opção de configuração de habilidades. Se a opção estiver definida como **algum**, o agente com a correspondência de habilidades mais próxima será atribuído automaticamente à tarefa. Se a opção estiver definida como **all**, somente os agentes que possuem todas as habilidades necessárias serão considerados. Se nenhum agente possuir todas as habilidades necessárias para executar a tarefa, nenhum agente será atribuído automaticamente.

Uma classificação de habilidades é calculada como:

Skills_agent/Skills_task

Em que:

- Skills_agent é o número de habilidades possuídas pelo agente que correspondem às habilidades necessárias para a tarefa.
- Skills_task é o número total de habilidades necessárias para a tarefa.

Por exemplo, se uma tarefa requer quatro habilidades e o Agente A possui três delas e o Agente B possui duas delas:

- Classificação de habilidade do agente A = 3/4 ou 0,75
- Classificação de habilidade do Agente B = 2/4 ou 0,5

Se a aplicação estiver configurada para usar outros critérios de seleção, como local ou fuso horário, as classificações de todos os critérios de seleção serão ponderadas e somadas. O agente com a classificação geral mais alta é selecionado para a tarefa. Consulte Atribuição automática de agente usando vários critérios de seleção para mais detalhes.

Atribuição automática de agente usando fusos horários

Os agentes podem ser atribuídos automaticamente com base no fuso horário definido em seus registros de usuário e no fuso horário das tarefas.

Se a opção **A seleção automática de agentes considerará o fuso horário para a tarefa** estiver habilitada, a atribuição automática por fuso horário poderá ser realizada.

Quando uma tarefa é criada, os agentes no fuso horário mais próximo do fuso horário da tarefa são considerados para a tarefa. Se a aplicação estiver configurada para que somente o fuso horário seja considerado, somente um agente no mesmo fuso horário poderá ser atribuído automaticamente à tarefa.

Nota:
É importante que os fusos horários do agente e da tarefa estejam definidos corretamente.

Quando uma tarefa é criada, os agentes são classificados com base no fuso horário da tarefa e no fuso horário do agente usando a seguinte fórmula:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1 - [abs(Task_tz – Agent_tz) ÷ 12]

em que:

- abs é a função matemática para calcular o valor absoluto.
- Task_tz é o deslocamento entre o fuso horário da tarefa e o GMT.
- Agent_tz é a diferença entre o fuso horário do agente e o GMT.

Por exemplo, uma tarefa é criada na cidade de Nova York (GMT-4) e dois agentes estão disponíveis para executar a tarefa, um em Los Angeles (GMT-7) e um em Paris, França (GMT+1).

A classificação do agente em Los Angeles é calculada como:

1 - abs((-4) - (-7)) ÷ 12 ou 0,75

A classificação do agente em Paris é calculada como:

1 - abs((-4) - (+1)) ÷ 12 ou 0,58

Portanto, se a atribuição automática da tarefa for baseada somente no fuso horário, ela será atribuída ao agente de Los Angeles.

Se a aplicação estiver configurada para usar outros critérios de seleção, como habilidades ou localização, as classificações de todos os critérios de seleção serão ponderadas e somadas. O agente com a classificação geral mais alta é selecionado para a tarefa. Consulte Atribuição automática de agente usando vários critérios de seleção para mais detalhes.

Atribuição automática de agente usando áreas de cobertura de grupo

Os agentes podem ser atribuídos automaticamente com base na área de cobertura do grupo definida em seus registros de usuário.

Atribuição automática de agente usando vários critérios de seleção

Quando uma tarefa é criada, as classificações dos agentes são calculadas. Para obter mais informações, consulte:

- Atribuição automática de agente usando o local
- Atribuição automática de agente usando habilidades
- Atribuição automática de agente usando fusos horários

A atribuição automática é baseada no seguinte cálculo:

(Classificação de Criteria_1 x peso de Criteria_1) + (classificação de Criteria_2 x peso de Criteria_2) + (classificação de Criteria_3 x peso de Criteria_3) / Número de tipos de critério usados em que:

Número de tipos de critérios usados = 1, 2 ou 3, dependendo das configurações de local, habilidade e fuso horário usadas.

Este exemplo calcula a atribuição automática do agente com base no local e nas habilidades. O exemplo é baseado nas seguintes suposições.

- A opção de configuração A **seleção automática de agentes considerará a localização dos agentes** está habilitada para a aplicação.
- A **seleção automática de agentes exige que eles tenham algumas das habilidades necessárias para que a opção de configuração de tarefa** esteja habilitada para a aplicação.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A propriedade **Peso das habilidades** é definida como 10 para a aplicação.
- A propriedade **Peso** do local é definida como 5 para a aplicação.
- Os agentes A e B estão disponíveis para executar uma tarefa e a tarefa requer quatro habilidades específicas.
- O local do Agente A fica a 8 km do local da tarefa e possui três das quatro habilidades necessárias.
- O local do Agente B está a um quarto de milha do local e possui duas das habilidades necessárias.

A atribuição automática para os agentes usa este cálculo: `[(classificação do local x peso do local) + (classificação de habilidades x peso das habilidades)]/ 2`

- O cálculo de atribuição automática para o Agente A é: `[(0,7 x 0,5) + (0,75 x 1)]/ 2 = 0,55`
- O cálculo de atribuição automática para o Agente B é: `[(0,9 x 0,5) + (0,5 x 1)]/ 2 = 0,475`

Neste exemplo, a tarefa é atribuída automaticamente ao Agente A.

Gerenciamento de incidentes de segurança e solicitações de entrada

Depois que um incidente de segurança foi criado, vários tipos de informações podem ser adicionados e exibidos conforme sua análise do problema avança em direção à resolução.

Esta seção descreve o seguinte:

- Criar uma solicitação de entrada
- Gerenciar observáveis
- Gerenciar pesquisas e verificações
- Gerenciar oorquestração de n-demand
- Calcular a severidade de um incidente de segurança
- Gerenciar atividades pós-incidente
- Fechar incidentes de segurança

Criar uma solicitação de entrada

Ao contrário dos incidentes de segurança, as solicitações de entrada geralmente têm uma prioridade mais baixa. Solicitações de pesquisa, verificação ou um novo selo são exemplos de solicitações de entrada.

Antes de Iniciar

Funções necessárias: função sn_si.basic ou superior

Procedimento

1. Navegue até um dos formulários de Solicitações.
   Por exemplo, **Todos** > **Incidente de segurança** > **Solicitações de Entrada** > **Atribuídos a Mim**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitação de segurança

Campo	Descrição
Número	[Somente leitura] O número da solicitação de segurança gerado automaticamente.
Empresa	A empresa do solicitante.
Local	O local do IC, se aplicável. Este campo é preenchido previamente quando o IC é selecionado.
Item de Configuração	O item de configuração afetado pela solicitação.
Prioridade	A prioridade da solicitação.
Aberto	[Somente leitura] A data e a hora em que a solicitação foi aberta.
Estado	O estado atual da solicitação de segurança. Na criação da solicitação de segurança, este campo é padronizado como **Rascunho**.
Grupo de atribuição	O grupo de atribuição do qual o trabalhador atribuído é selecionado.
Atribuído a	O indivíduo atribuído para executar o trabalho.
Descrição resumida	Uma breve descrição da solicitação de segurança, que é visível para o solicitante.
Descrição	A descrição completa da solicitação, que está visível para o solicitante.
Anotações de trabalho	Anotações de trabalho, que ficam visíveis para o solicitante.

4. Ao concluir as entradas, clique em **Enviar**.
5. Se você precisar escalonar a solicitação para um incidente de segurança, clique em **Converter em incidente de segurança**.

Gerenciar observáveis

Observáveis são artefatos encontrados em uma rede ou sistema operacional que provavelmente indicam uma invasão. Os observáveis típicos são endereços IP, hashes MD5 de arquivos de malware ou URLs ou nomes de domínio. Inteligência contra ameaças dados da tabela observável estão disponíveis em um incidente de segurança.

As informações dos observáveis incluem valor, tipo, contexto e carimbo de data/hora.

Você pode criar ou excluir observáveis manualmente ou automaticamente por meio de solicitações de pesquisa.

Uma nova coluna de **descoberta** foi adicionada à guia **Resultados da pesquisa de ameaças**. Os valores possíveis são: Mal-intencionado e Desconhecido.

> Se uma solicitação de pesquisa de IoC não encontrar um observável de incidente de segurança, ele será rotulado como Desconhecido.
>
> Se uma solicitação de pesquisa de IoC encontrar um observável de incidente de segurança, ele será rotulado como Mal-intencionado.

Durante uma atualização, os itens existentes têm a coluna **Descoberta** definida como Mal-intencionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Embora os dados da tabela de observáveis Inteligência contra ameaças façam parte de um incidente de segurança, nenhuma outra interação com o módulo Inteligência contra ameaças está incluída. Para obter a funcionalidade de ameaça completa, o plug-in Inteligência contra ameaças está disponível por assinatura.

Tópicos relacionados

Criar um observável de incidente de segurança

Mostrar informações de IoC para um incidente de segurança

Você pode exibir informações de IoC, como resultados de pesquisa de observáveis e detecções associados a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança para o qual você deseja exibir as informações relacionadas ao IoC.
2. Clique no link relacionado **Mostrar IoC**.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações do incidente de segurança.

Guia	Descrição
Observáveis	Exiba ou adicione ou edite manualmente observáveis associados ao incidente de segurança. Para obter mais informações, consulte Gerenciar observáveis.
Indicadores associados	Se Inteligência contra ameaças estiver ativado, você poderá exibir quaisquer outros indicadores associados a qualquer um dos mesmos registros de ameaça.
Resultados da pesquisa de detecções	Contém resultados de pesquisa de detecções.
Detalhes de Pesquisa de detecções	Contém detalhes do registro de pesquisa de detecções.
Pesquisas de ameaças	Armazena dados de aprimoramento de sistemas de detecção de malware. Esta guia é exibida somente quando o plug-in Inteligência contra ameaças está instalado.
Modos/métodos de ataque associados	Se Inteligência contra ameaças estiver ativado, você poderá exibir qualquer outro tipo de ataque associado a qualquer um dos mesmos registros de ameaça.
Solicitações de Verificação de Segurança	Se Inteligência contra ameaças estiver ativado, você poderá exibir solicitações de verificação e pesquisa anexadas ao incidente de segurança.
Recursos com IoC Semelhante	Se Inteligência contra ameaças estiver ativado, você poderá exibir outros recursos com indicadores semelhantes.
Usuários com IOC Semelhante	Se Inteligência contra ameaças estiver ativado, você poderá exibir outros usuários com indicadores semelhantes.

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Mostrar itens afetados
- Mostrar itens relacionados
- Mostrar dados de aprimoramento
- Mostrar tarefas de resposta

5. Ao concluir as entradas, clique em **Enviar**.

Criar um observável de incidente de segurança

Você pode criar e exibir um observável em um incidente de segurança e tomar as medidas apropriadas. Ter observáveis disponíveis no incidente de segurança é escalonável e reduz o tempo de resposta.

Antes de Iniciar

Função necessária:

- sn_ti_observable.write (gravação)
- sn_ti_observable.read (leitura)
- sn_ti_observable.admin (excluir)

Procedimento

1. Navegue até **Incidente de segurança**.
2. Escolha um incidente.
3. Clique na guia da lista relacionada **de observáveis de incidente de segurança**.
4. Clique em **Nova**.
5. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Selecionar marcador de classificação	Se você configurou e ativou marcadores de segurança para adicionar metadados ao registro, poderá selecionar um ou mais marcadores para especificar o grau de confidencialidade do observável. Se você não configurou ou ativou marcadores de segurança, esta lista suspensa não será exibida.
Valor	O valor (por exemplo, endereço IP ou hash) associado ao observável. **Nota:** Se uma verificação de ameaça em um endereço IP ou hash retornar malware ou alguma outra falha, o endereço IP ou o valor de hash será adicionado automaticamente à tabela Observável [sn_ti_observable]. Como tal, ele pode ser pesquisado no formulário Observáveis.
Tipo de observável	Selecione a classificação observável, como um endereço IP ou hash de arquivo. Esses tipos de observável são definidos no módulo **Tipos de observável**.
Contagem de incidentes	O número de vezes que o valor observável foi encontrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
É composição	Este campo é exibido somente depois que o registro observável foi salvo. Se o **Tipo de observável** estiver definido como qualquer outra coisa que a **Composição de observável**e este novo observável for uma composição, marque esta caixa de seleção. Se o **tipo de observável** já estiver definido como **Composição de observável**, a caixa de seleção será marcada e somente leitura. Uma composição de observável é um observável que contém observáveis secundários.
Descoberta	Selecione uma das seguintes propriedades: ○ **Mal**-intencionado : indica que o observável é prejudicial à organização. ○ **Suspeito**: indica que o observável pode ser prejudicial para a organização. ○ **Limpar**: indica que o observável não é prejudicial à organização. ○ **Desconhecido**: indica que ainda não determinamos a descoberta do observável. ○ Valor padrão: desconhecido. Para obter mais informações, consulte Calculadoras descobertas de pesquisa de ameaças. **Nota:** Após um upgrade, os observáveis existentes são marcados como Mal-intencionados.
Operador	Este campo é exibido somente quando a caixa de seleção **É composição** está marcada. Dependendo da sua configuração neste campo, os observáveis e seus secundários são considerados ao decidir se um indicador associado está presente. Defina este campo como **E** se todos os observáveis secundários devem estar presentes para que um indicador associado seja considerado presente. Defina-o como **OU** se algum dos observáveis secundários estiver presente para que um indicador associado seja considerado presente.
Não deve estar presente	Este campo é exibido somente depois que o registro observável foi salvo. Se selecionado, este campo significa que a ausência do observável é o possível problema (por exemplo, uma chave de registro ausente).
Localização	Usando as configurações em duas propriedades e uma definição de inclusão de script, você pode carregar Carregar mais dados de IoC neste campo.
Anotações	Insira anotações adicionais sobre o observável.

6. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**.
Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais.

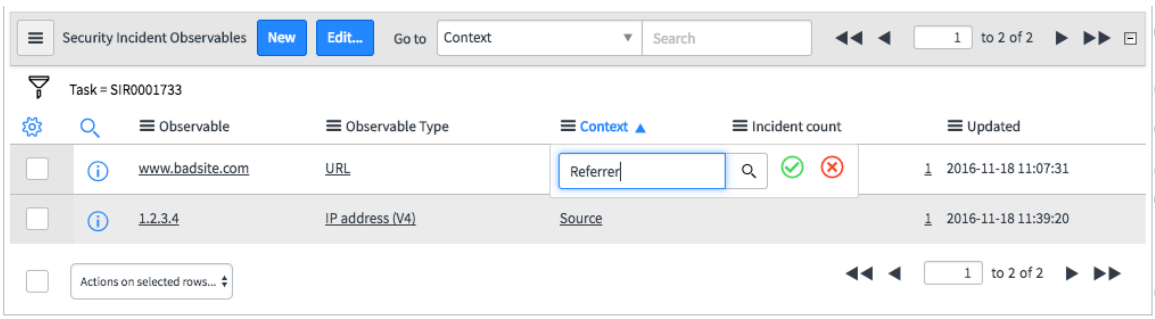
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Descrição
Indicadores relacionados	Lista os indicadores que foram identificados pela origem da ameaça.
Tarefas Associadas	Lista as mudanças associadas ao observável.
Observáveis secundários	Lista os observáveis relacionados que foram identificados pela origem da ameaça.
Recursos correspondentes para IP	Se o observável for um endereço IP, esta lista mostrará todos os recursos (itens de configuração) que tenham um endereço IP correspondente.
Origens observáveis	Lista as origens deste observável, junto com o nível de confiança da origem.
Anotações de segurança	Lista as anotações de segurança adicionadas a este observável.

7. Retornando ao incidente de segurança, as seguintes informações estão disponíveis.

Nota:
Quando você adiciona um observável ao incidente de segurança, o sistema verifica se há outros itens de configuração ou usuários associados a ele. As guias da lista relacionada **Itens de configuraçãorelacionados e Usuários** relacionados são atualizadas de acordo.



Coluna	Definição
Observável	O valor (por exemplo, endereço IP ou hash) associado ao observável.
Tipo de Observável	O tipo específico de observável.
Contexto	Selecionado pelo usuário. As opções são: ○ IP - Origem ou Destino **Nota:** Se Inteligência contra ameaças e Palo Alto Networks - Firewall estiverem ativados, alterar ou adicionar um valor a este campo fará com que o fluxo de trabalho Fluxo de trabalho Obter dados de log Security Operations Palo Alto Networks - Obter dados de log seja executado. O fluxo de trabalho recupera dados de log de ameaças aprimorados do firewall e os anexa ao incidente de segurança. As informações também são analisadas e exibidas na seção Logs de firewall na guia **Dados** de aprimoramento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Coluna	Definição
	○ URL - Referenciador **Nota:** Quando o usuário clica em um link em um e-mail de phishing, um referenciador é o URL do salto final antes que o URL do malware seja acessado.
Contagem de Incidentes	O número de incidentes em que este observável aparece. Este valor é atualizado automaticamente quando o observável é adicionado a outro incidente manualmente ou por meio de um fluxo de trabalho.
Atualizado em	Data e hora em que a lista foi atualizada pela última vez.

Nota:
Se o plug-in Inteligência contra ameaças estiver instalado, você também poderá exibir o observável na lista **Observáveis** no **Repositório IoC**.

Tópicos relacionados

Editar uma lista de observáveis de incidente de segurança

Adicionar vários observáveis de incidente de segurança

Gerenciar observáveis de arquivo

Gerenciar observáveis de arquivo fornece medidas de segurança rígidas para armazenar os arquivos suspeitos e permite que os observáveis de tipo de arquivo para integração de área restrita.

Antes de Iniciar

Função necessária: sn_ti_maliciosa_attachment_access (upload)

Carregar os observáveis de tipo de arquivo:

- Automaticamente: quando os incidentes de segurança são criados para os e-mails de phishing, os anexos no e-mail de phishing são criados como observáveis de tipo de arquivo.
- Manualmente: um analista de segurança também pode carregar os arquivos suspeitos para criar observáveis de tipo de arquivo.

Por Que e Quando Desempenhar Esta Tarefa

Você pode criar e exibir observáveis de tipo de arquivo para um incidente de segurança. Os arquivos suspeitos que fazem parte dos observáveis são armazenados em um local específico, que pode ser acessado pelo analista de segurança para baixar o arquivo somente com uma função específica.

Procedimento

1. Navegue até um incidente de segurança.
2. Selecione **Observáveis** na guia **Mostrar todas as listas relacionadas**.

   Se houver algum anexo no e-mail de phishing, por padrão, esses anexos serão criados como observáveis de tipo de arquivo no incidente de segurança correspondente. Cada

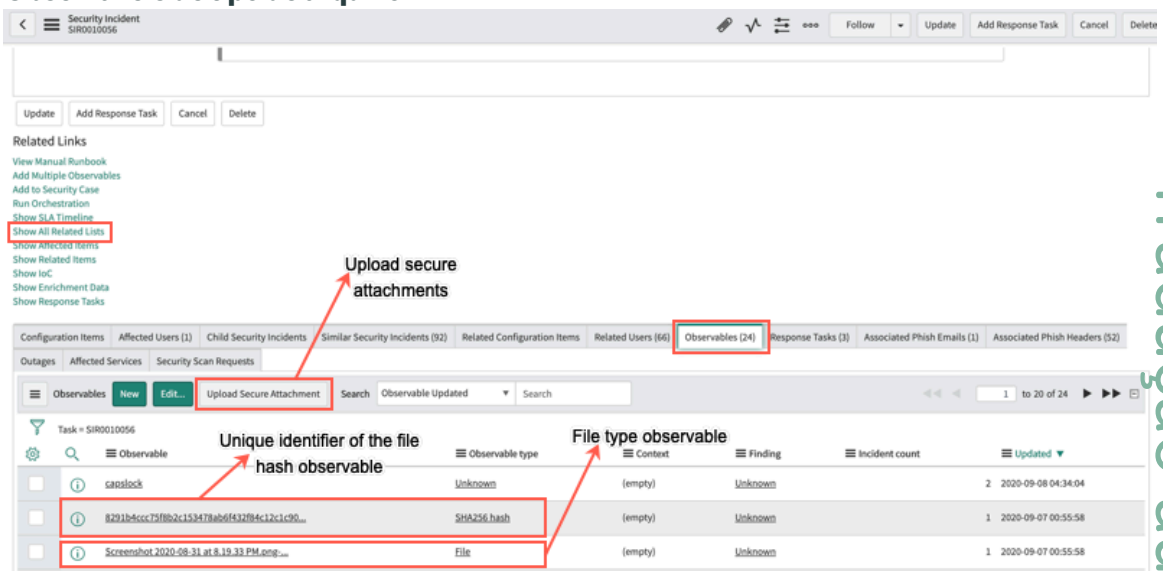
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

anexo é criado como dois observáveis, como tipo de arquivo e observável de hash de arquivo.

3. Para carregar os anexos seguros manualmente:
   - Clique **em Carregar anexo seguro**.
   - Em Carregar anexos seguros, clique em **Escolher arquivo** para carregar um ou mais arquivos. Cada arquivo é considerado como um único registro observável.
   - Clique em **Criar observáveis de arquivo** para criar os observáveis do tipo de arquivo, como um é o tipo de arquivo e outro é o hash do arquivo, que é um identificador exclusivo.

Observáveis de tipo de arquivo



Selecione o tipo de arquivo observável a ser processado para integrações adicionais, como área restrita, pesquisa de ameaças. Além disso, você também pode baixar os anexos do tipo de arquivo observável.

Nota:

A pesquisa de ameaças (VirusTotal) recupera o arquivo dos anexos protegidos para os novos observáveis de tipo de arquivo e as propriedades do sistema abaixo não são aplicáveis aos novos observáveis de tipo de arquivo.

- sn_ti.scan.delete_attachment_after_hash
- sn_ti.scan.use_file_hash

Para uma referência rápida, o tipo de arquivo observável é mapeado como secundário para o observável de hash e o observável de hash é mapeado como secundário para observável de arquivo.

Se os anexos de e-mail de phishing excederem o tamanho definido, os observáveis não serão criados. Você deve modificar as propriedades do sistema para oferecer suporte a arquivos de tamanho maior.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do sistema de tamanho de arquivo

Propriedade do sistema	Descrição
glide.email.inbound.max_total_attachment_size_bytes	Se você estiver encaminhando o e-mail de phishing diretamente, use este valor de propriedades do sistema para aumentar o tamanho do arquivo de 18 MB para o tamanho desejado.
com.glide.attachment.max_get_size	Se você estiver encaminhando o e-mail de phishing como anexo, use este valor de propriedade do sistema para criar as propriedades do sistema abaixo no escopo global para aumentar o tamanho do arquivo de 5 MB para o tamanho desejado.

Você também pode criar um novo tipo de arquivo observável da seguinte forma:

a. Clique em **Nova**.

b. Selecione a **Categoria do tipo de observável: arquivo**

c. Clique em **Carregar** para anexar um arquivo.

Editar uma lista de observáveis de incidente de segurança

Você pode editar quais observáveis na lista associada a um incidente de segurança serão exibidos.

Antes de Iniciar

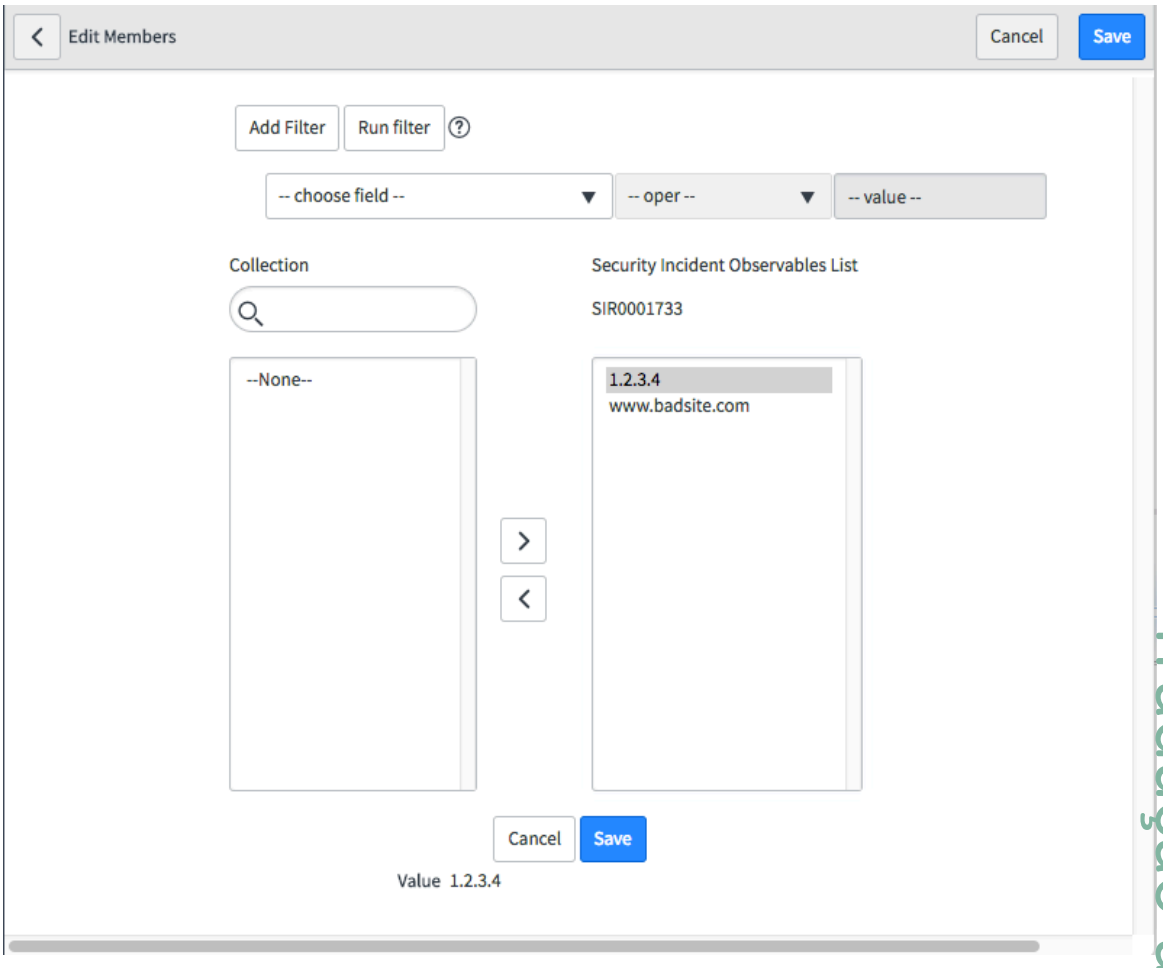
Função necessária: sn_si.basic

Procedimento

1. Navegue até **Incidente de segurança**.
2. Escolha um incidente.
3. Clique na guia da lista relacionada **de observáveis de incidente de segurança**.
4. Clique em **Editar**.
5. Adicione ou remova observáveis da lista.
   Crie um filtro para listas longas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Clique em **Salvar**.

> **Nota:**
> Quando você adiciona um observável ao incidente de segurança, o sistema verifica se há outros itens de configuração ou usuários associados a ele. As guias da lista relacionada **Itens de configuraçãorelacionados e Usuários** relacionados são atualizadas de acordo. Além disso, se o plug-in Inteligência contra ameaças estiver ativado e você tiver pelo menos uma implementação de integraçãoIntegrações do Security Incident Response ativada, o Integração do Security Operations - Pesquisa de ameaças executará um ou mais fluxos de trabalho, e as pesquisas de segurança de ameaças serão realizadas nos observáveis adicionados. Os resultados aparecem na guia **Resultados da pesquisa de ameaças**.

Tópicos relacionados

- Adicionar vários observáveis de incidente de segurança
- Criar um observável de incidente de segurança

Adicionar vários observáveis de incidente de segurança

Para economizar tempo, você pode adicionar vários observáveis de incidente de segurança à lista de observáveis de incidente de segurança.

Antes de Iniciar

Função necessária: sn_ti_write

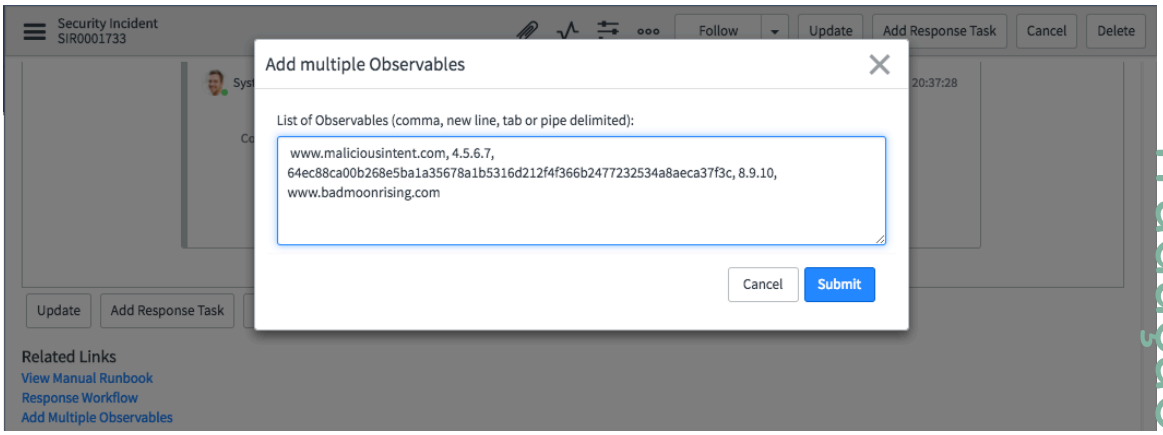
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Ao adicionar vários observáveis de incidente de segurança, as duplicatas são ignoradas durante o processamento.

Procedimento

1. Navegue até **Incidente de segurança**.
2. Escolha um incidente.
3. Clique no link relacionado **Adicionar vários observáveis**.
4. Insira ou cole vários observáveis.
   As entradas podem ser de qualquer tipo de observável. Os formatos aceitos são: vírgula, nova linha, guia ou separadores verticais.



Nota:
Quando você adiciona um observável ao incidente de segurança, o sistema verifica se há outros itens de configuração ou usuários associados a ele. As guias da lista relacionada **Itens de configuraçãorelacionados e Usuários** relacionados são atualizadas de acordo.

Observação: os valores observáveis não detectados automaticamente são atribuídos ao tipo Desconhecido.

5. Clique **em Enviar.**.

Aprimoramento automático de dados de log observável de incidente de segurança

Quando determinadas aplicações e integrações são configuradas, incluindo Inteligência contra ameaças e a integração Palo Alto Networks - Firewall, as informações de observáveis em um incidente de segurança podem ser aprimoradas automaticamente com dados de log de ameaças sempre que o IP de origem de seus observáveis for modificado.

Quando ocorre uma modificação, uma regra de negócios inicia um fluxo de trabalho que recupera dados de logs de ameaça no firewall e enriquece as informações observáveis no incidente de segurança.

Antes que os observáveis possam ser aprimorados, as etapas a seguir devem ser realizadas.

- A Inteligência contra ameaças deve ser ativada.
- A integração do Firewall da Palo Alto Networks deve ser ativada e configurada. Isso também pode incluir Configurar credenciais SSH para o MID Server.

Depois que a configuração for concluída, o ato de alterar o IP de origem dos observáveis associados a um incidente de segurança faz com que uma regra de negócios execute o

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

fluxo de trabalho **Security Operations Palo Alto Networks - Obter dados de log**. As atividades de fluxo de trabalho enfileiram uma consulta de pesquisa no firewall e retornam um ID de trabalho que é usado para recuperar dados de logs de ameaças do firewall e anexá-los como um arquivo XML ao incidente de segurança.

Tópicos relacionados

- Obter fluxo de trabalho de aprimoramento de informações da sessão do AutoFocus
- Fluxo de trabalho de integração do Security Operations Palo Alto Networks inicializador de firewall
- Security Operations Palo Alto Networks - Fluxo de trabalho de verificar e bloquear valor
- Fluxo de trabalho Obter dados de log
- Obter fluxo de trabalho de aprimoramento de dados do WildFire

Publicar observáveis em uma lista de observação de terceiros

Você pode publicar um ou mais observáveis ou indicadores associados em uma lista de observação de terceiros. Atualmente, a única implementação compatível com essa funcionalidade é o CrowdStrike Falcon Host.

Antes de Iniciar

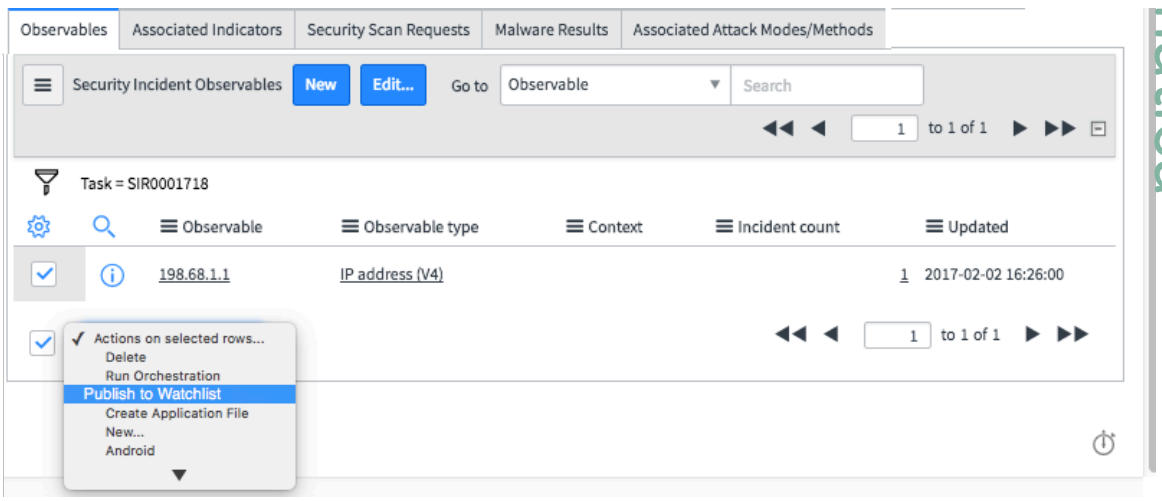
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Nota:
Se não houver implementações disponíveis, as ações de recurso não serão exibidas nos menus do produto.

Procedimento

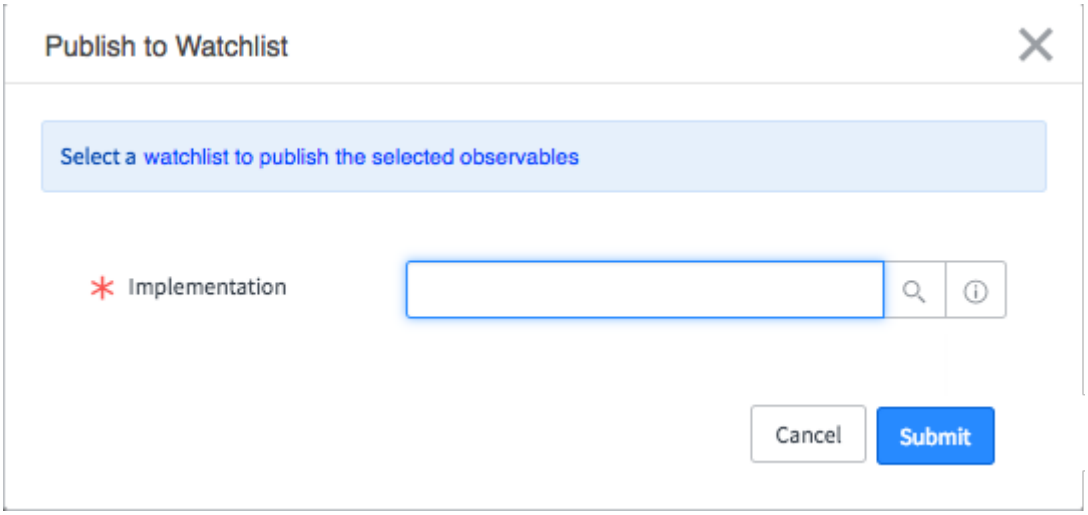
1. Navegue até um incidente de segurança.
2. Selecione **Observáveis** na guia **Lista relacionada**.
3. Clique **em Publicar na lista de observação** no menu suspenso **Ações nas linhas selecionadas...**



A caixa de diálogo é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Insira ou escolha a implementação.

> **Nota:**
> Um fluxo de trabalho é acionado pelo Integração do Security Operations - Capacidade de publicar na lista de observação ao selecionar a implementação do CrowdStrike Falcon Host.

5. Clique em **Enviar**.

Gerenciar pesquisas e verificações

Você pode executar pesquisas e verificações de vulnerabilidade de incidentes de segurança e do catálogo de incidentes de segurança para identificar possíveis ameaças e vulnerabilidades.

Enviar uma solicitação de pesquisa de IoC a partir de um incidente de segurança

Uma pesquisa de IoC é executada automaticamente sempre que observáveis são adicionados a um incidente de segurança. Além disso, se o seu incidente de segurança tiver anexos, eles poderão ser encontrados facilmente com o pressionar de um botão.

Antes de Iniciar

Para pesquisas automáticas de IoC, o plug-in Inteligência contra ameaças deve ser ativado.

Função necessária: sn_si.basic

> **Nota:**
> Por padrão, o **tipo de pesquisa** de **arquivo** está inativo.

Procedimento

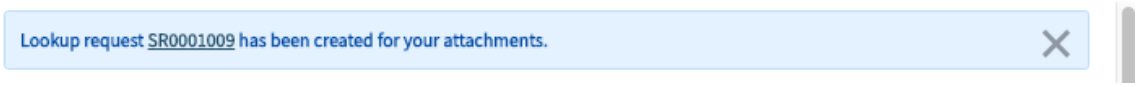
1. Crie um novo incidente de segurança ou abra um existente se você pretender anexar novos arquivos a ele.
2. Clique no ícone de clipe de papel no cabeçalho do formulário e anexe um ou mais arquivos.
3. Ao concluir suas entradas no formulário, clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**.
   Depois que o registro for salvo, um botão **Pesquisar anexos** será exibido.
4. Clique **em Pesquisar anexos**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
As anotações de trabalho em **Detalhes do incidente** relatam o andamento do processo de pesquisa.

5. Você pode clicar no número de pesquisa no final da mensagem para exibir o registro de pesquisa.
Você pode clicar no link de referência de pesquisa para exibir resultados detalhados.



Enviar uma solicitação de pesquisa de IoC do Catálogo de incidentes de segurança

Se o plug-in Security Incident Response estiver ativado, você poderá enviar pesquisas de ameaças para arquivos, valores de hash, URLs e endereços IP do Catálogo de incidentes de segurança. As solicitações são enviadas e você pode exibir os resultados no módulo **Minhas solicitações**.

Antes de Iniciar
Função necessária: none

Por Que e Quando Desempenhar Esta Tarefa
As pesquisas são realizadas automaticamente para o tipo de pesquisa padrão de cada origem de pesquisa listada no registro de pesquisa. Os resultados da solicitação de pesquisa estão disponíveis no módulo **Minhas solicitações**.

Procedimento

1. Navegar até **Todos** > **Autoatendimento** > **Catálogo de incidente de segurança**.
2. Clique **em Pesquisa de IoC**.
3. Clique **em Pesquisar arquivos, valores de hash, URLs ou endereços IP**.
4. Insira um ou mais dos seguintes:

Solicitação de pesquisa de IoC

Item a ser pesquisado	Descrição
Arquivos	Clique no ícone de clipe de papel e localize e anexe os arquivos que deseja pesquisar. **Nota:** Por padrão, o **tipo de pesquisa** de **arquivo**está inativo. Os arquivos são convertidos e enviados como um valor de hash.
URLs	No campo **URLs**, insira os URLs que você deseja pesquisar, separados por vírgulas. Por exemplo: www.abc.com,www.xyz.net.
Endereços IP	No campo **Endereços IP**, insira os endereços IP que você deseja pesquisar, separados por vírgulas.
Valores de hash	No campo **Valores de hash**, insira os valores de hash que você deseja pesquisar, separados por vírgulas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item a ser pesquisado	Descrição
	Nota: Quando o **tipo de pesquisa** de **arquivo** está inativo, este valor é a ação padrão para os valores de **arquivo** e **hash**.

5. Depois de fazer suas seleções, clique em **Enviar**.
6. Para exibir o status e/ou os resultados das pesquisas, navegue até **Autoatendimento** > **Minhas solicitações**.
7. Clique no número SR da solicitação.
   As anotações de trabalho em **Atividade** listam as tarefas realizadas durante a pesquisa, incluindo a criação de pesquisas individuais para cada arquivo, valor de hash, URL ou endereço IP e os resultados da pesquisa.

Enviar uma solicitação de verificação de vulnerabilidade a partir de um incidente de segurança

Se o seu incidente de segurança tiver um ou mais itens de configuração (servidores, computadores e assim por diante), eles poderão ser verificados quanto a vulnerabilidades no formulário Security Incident Response.

Antes de Iniciar

O plug-in Vulnerability Response deve ser ativado.

Função necessária: sn_si.write

Procedimento

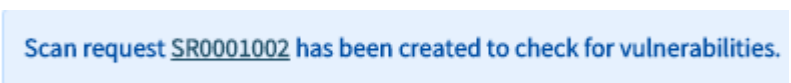
1. Crie um incidente de segurança e inclua pelo menos um recurso.
   Você também pode abrir um incidente existente que tenha itens de configuração.
2. Ao concluir suas entradas no formulário, clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**.
   Depois que o registro for salvo, um link relacionado a **Verificar vulnerabilidades** será exibido.

   Nota:
   Se a lista relacionada **Verificar vulnerabilidades** não for mostrada, você deverá navegar até **Vulnerabilidade** > **Scanners**, configure pelo menos um scanner e defina seu padrão como **verdadeiro**.

3. Clique **em Verificar vulnerabilidades**.

   Nota:

   Uma mensagem aparece na parte superior do formulário de incidente de segurança, junto com um link para o registro de verificação.

4. Você pode clicar no número da solicitação de verificação para exibir o registro de verificação.
   Os detalhes do incidente mostram os resultados da verificação no registro de solicitação de verificação de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Enviar uma solicitação de verificação de vulnerabilidade do catálogo do Security Incident Response

Você pode enviar verificações de vulnerabilidade para ICs e endereços IP do catálogo Security Incident Response. As solicitações são enviadas e você pode exibir os resultados no módulo **Minhas solicitações**.

Antes de Iniciar
Função necessária: none

Procedimento

1. Navegar até **Todos** > **Autoatendimento** > **Catálogo de incidente de segurança**.
2. Clique em Verificação de **vulnerabilidade**.
3. Clique **em Verificar item de configuração e endereços IP**.
4. Insira um ou mais dos seguintes a serem verificados.

Scanners de vulnerabilidade

Item a ser verificado	Descrição
Item de configuração	No campo **Item de configuração a ser verificado**, selecione o IC a ser verificado.
Endereços IP	No campo **Endereços IP a serem verificados**, insira os endereços IP, separados por vírgulas.

5. Depois de fazer suas seleções, clique em **Enviar**.
   Se um observável for encontrado, um indicador será criado, de acordo com os padrões STIXX.
6. Para exibir o status e/ou os resultados das verificações, navegue até **Autoatendimento** > **Minhas solicitações**.
7. Clique no número SR da solicitação.
   As anotações de trabalho em **Atividades** listam as tarefas realizadas durante a verificação, incluindo a criação de verificações individuais para cada IC ou endereço IP e os resultados das verificações.

Gerenciar oorquestração de n-demand

Durante a análise de Security Incident Response, um analista de segurança pode executar uma tarefa orientada por um fluxo de trabalho de incidente de segurança. Por exemplo, execute um despejo de processo em um IC específico. Isso pode ser realizado com a orquestração sob demanda.

Cada aplicação Security Operations registrada inclui várias orquestrações sob demanda no sistema de base. Você pode definir orquestrações personalizadas sob demanda, conforme necessário.

A orquestração sob demanda pode ser invocada de uma lista de seleção na parte inferior das seguintes listas e formulários em Security Incident Response:

- Formulário Incidente de segurança
- Lista de incidentes de segurança
- Lista relacionada de observáveis de incidente de segurança
- Lista relacionada de itens de configuração

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Uma propriedade no Security Support Common chamada **sn_sec_cmn.use_on_demand_tbl_as_allowed** define quais fluxos de trabalho estão disponíveis para execução sob demanda.
- Se a propriedade for definida como **verdadeiro**, somente os fluxos de trabalho especificados na tabela On Demand Orchestration [sn_sec_cmn_on_demand_orchestration] estarão disponíveis.
- Se a propriedade for definida como **falsa** (padrão), todos os fluxos de trabalho das aplicações configuradas no registro da aplicação SecOps ficarão disponíveis.
- Dependendo da configuração da propriedade, a lista de fluxos de trabalho disponíveis é personalizada para o tipo de informação que está sendo analisada.

Executar orquestração sob demanda a partir do formulário de Incidente de segurança

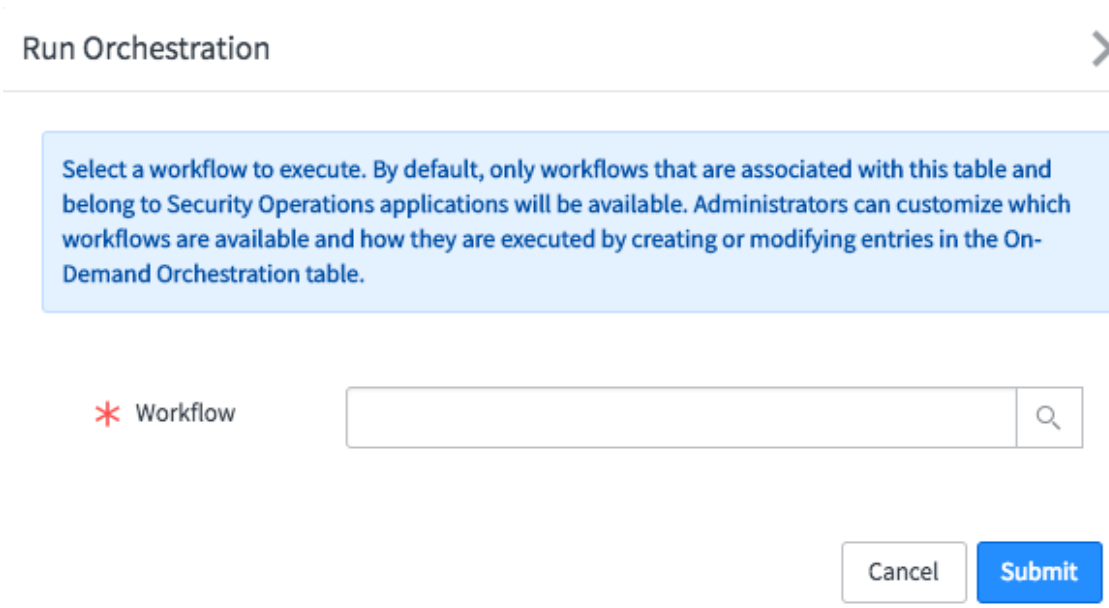
A orquestração sob demanda pode ser invocada a partir de uma lista de seleção na parte inferior do formulário de Incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.write

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar incidentes em aberto**.
2. Selecione o registro (incidente de segurança, observável ou IC) para o qual você deseja executar um fluxo de trabalho.
3. Clique no link relacionado **Executar Orquestração**.
   A caixa de diálogo **Executar Orquestração** é aberta. A aparência da caixa de diálogo depende da configuração da propriedade sn_sec_cmn.use_on_demand_tbl_as_whitelist no Security Support Common.



4. Clique no ícone de pesquisa e selecione o fluxo de trabalho que deseja executar.
   O fluxo de trabalho selecionado é executado. Para obter detalhes, consulte Orquestração de resposta de incidente de segurança fluxos de trabalho e atividades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Executar orquestração sob demanda da lista de Incidentes de segurança

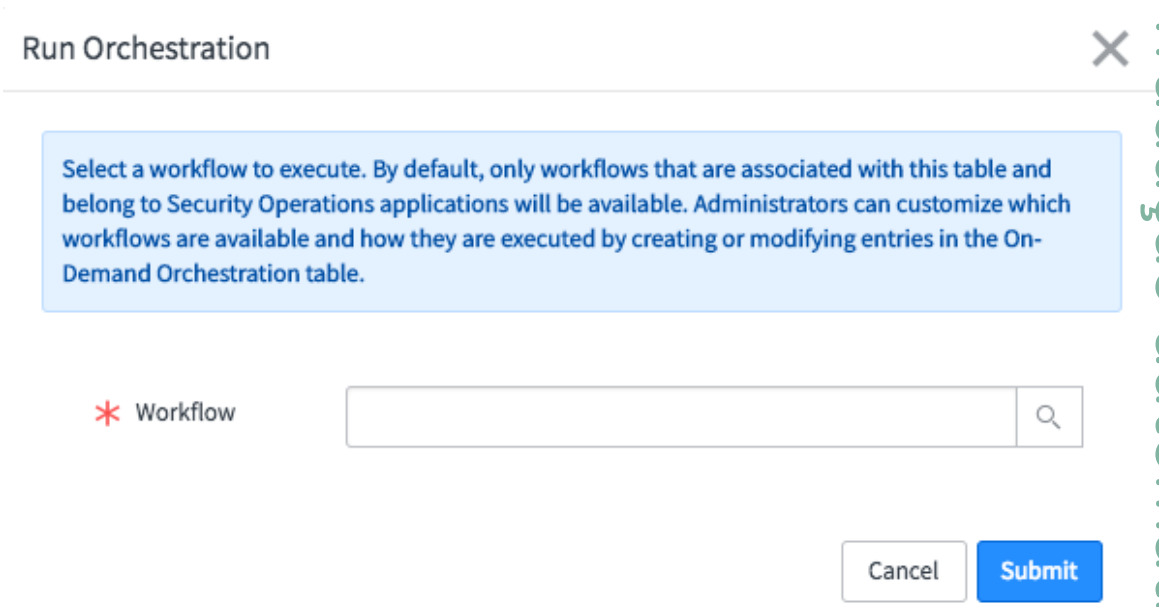
A orquestração sob demanda pode ser invocada a partir da lista de Incidentes de segurança, bem como de listas relacionadas em Security Incident Response.

Antes de Iniciar

Função necessária: sn_si.write

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar incidentes em aberto**.
2. Marque a caixa de seleção ao lado do incidente de segurança para o qual você deseja executar um fluxo de trabalho.
3. Clique na lista de seleção **Ações nas linhas selecionadas** na parte inferior da tela e clique em **Executar Orquestração**.
   A caixa de diálogo **Executar Orquestração** é aberta. A aparência da caixa de diálogo depende da configuração da propriedade sn_sec_cmn.use_on_demand_tbl_as_whitelist no Security Support Common.



4. Clique no ícone de pesquisa e selecione o fluxo de trabalho que deseja executar.
   O fluxo de trabalho selecionado é executado. Para obter detalhes, consulte Orquestração de resposta de incidente de segurança fluxos de trabalho e atividades.

Definir novas orquestrações sob demanda

No sistema de base, você pode selecionar orquestrações sob demanda que executam fluxos de trabalho predefinidos. Você pode definir novas orquestrações sob demanda para personalizar como os fluxos de trabalho são invocados nas listas de seleção **Executar Orquestração**.

Antes de Iniciar

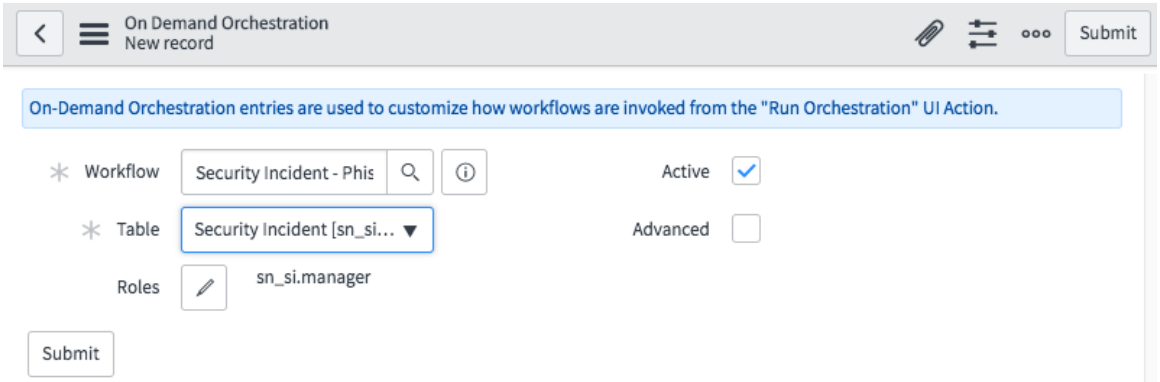
Função necessária: sn_si.write

Procedimento

1. Navegar até **Tudo** > **Security Operations** > **Utilitários** > **Orquestração sob Demanda**
2. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Preencha os campos, se for o caso.

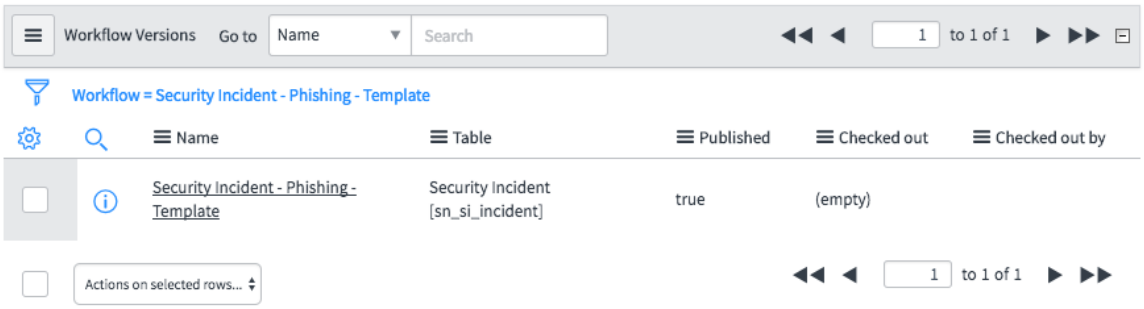
Orquestração sob Demanda

Campo	Descrição
Fluxo de trabalho	Selecione o fluxo de trabalho a ser incluído na lista de seleção **Executar Orquestração**.
Tabela	Selecione a tabela na qual o fluxo de trabalho selecionado será executado. Se a tabela não corresponder à tabela configurada para o fluxo de trabalho selecionado, você deverá marcar a caixa de seleção **Avançado** e modificar o **script de execução** para passar o registro correto para o fluxo de trabalho na execução.
Funções	Conforme necessário, selecione funções adicionais para restringir quem pode ver este fluxo de trabalho na lista de seleção **Executar Orquestração**.
Ativo	Marque esta caixa de seleção para ativar este registro de orquestração sob demanda.
Avançado	Marque esta caixa de seleção para modificar o script de execução para que ele passe o registro correto para a tabela selecionada para este fluxo de trabalho.
Script de execução	Modifique o script de execução para que ele passe o registro correto para a tabela selecionada para este fluxo de trabalho. Este campo aparece apenas se a caixa de seleção **Avançado** estiver marcada.

4. Clique com o botão direito do mouse no cabeçalho do registro e selecione **Salvar**.
A lista relacionada **Versões do fluxo** de trabalho é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Se você precisar fazer modificações adicionais no fluxo de trabalho, será necessário fazer check-out.

Tópicos relacionados

Trabalhar com versões de fluxo de trabalho

Registrar novas aplicações Security Operations para orquestração sob demanda

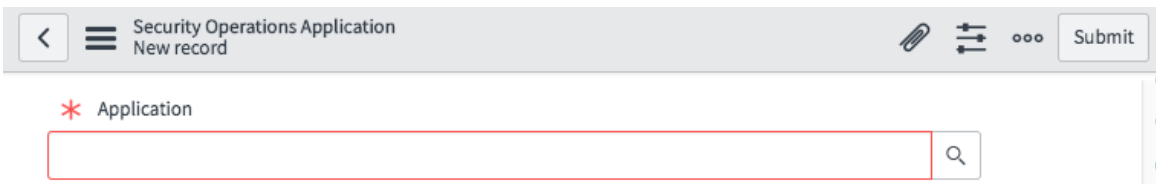
No sistema básico, as aplicações Security Operations são registradas automaticamente quando são ativadas. O registro permite que os fluxos de trabalho associados às aplicações estejam disponíveis para solicitações de orquestração sob demanda. Se necessário, você pode definir novas aplicações e associar fluxos de trabalho a elas para orquestração sob demanda.

Antes de Iniciar

Função necessária: sn_si.write

Procedimento

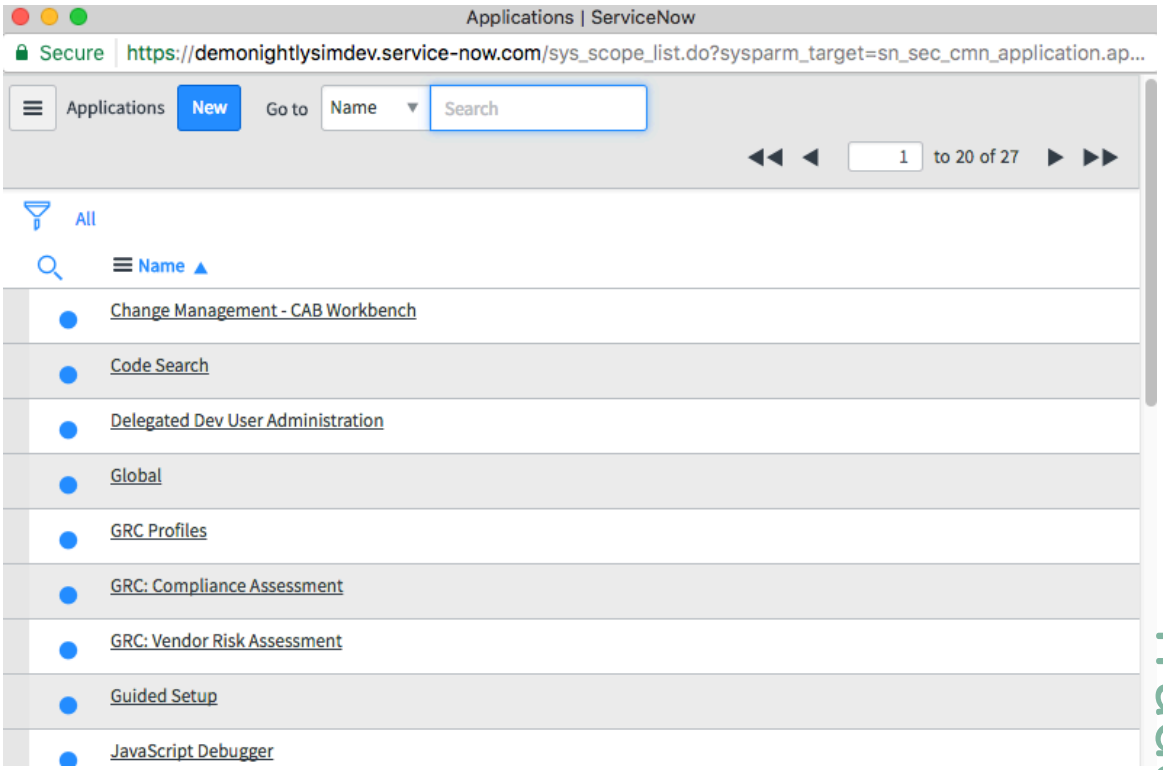
1. Navegar até **Todos** > **Security Operations** > **Utilitários** > **Registro da aplicação SecOps**e clique em **Registrar aplicação**.
   A tela da aplicação Security Operations é exibida.



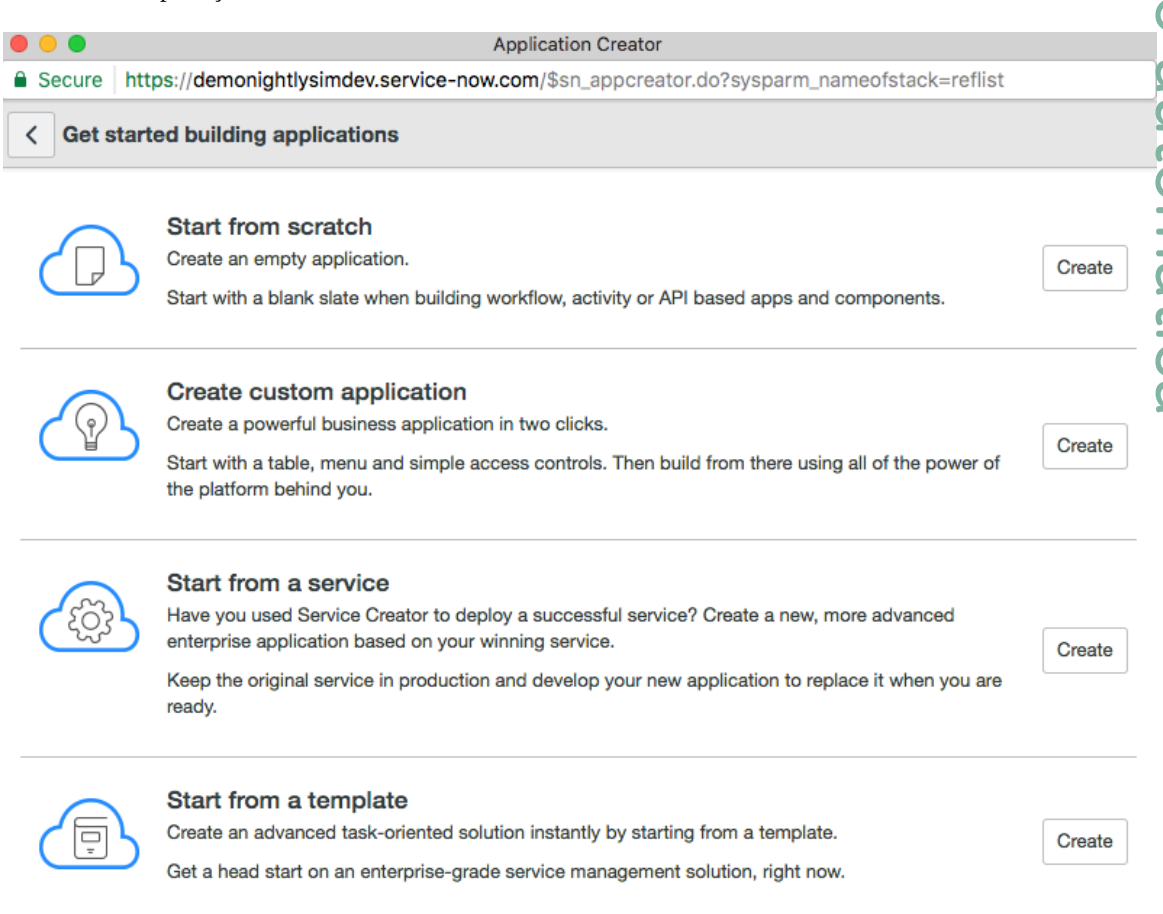
2. No campo **Aplicação**, clique no ícone de pesquisa (lupa).
   A tela Aplicações é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em **Nova**.
A tela do Criador de aplicações é exibida.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
As opções exibidas dependem dos aplicativos que você ativou. Para obter informações detalhadas sobre como criar novas aplicações, consulte Building applications .

4. Depois que a aplicação tiver sido gerada, você poderá criar scripts para configurar a orquestração sob demanda.

Nota:
Configurar a orquestração sob demanda para novas aplicações requer conhecimento técnico avançado de script e criação de gatilhos para os scripts (regras de negócios, ação de IU, fluxos de trabalho e assim por diante). Para obter mais informações, entre em contato com ServiceNow Serviços profissionais.

Adicionar informações a um incidente de segurança

Depois que um incidente de segurança é criado, você pode adicionar mais detalhes para ajudar na análise, como funções de acesso e diferentes tipos de anotações.

Antes de Iniciar

Função necessária: sn_si.basic

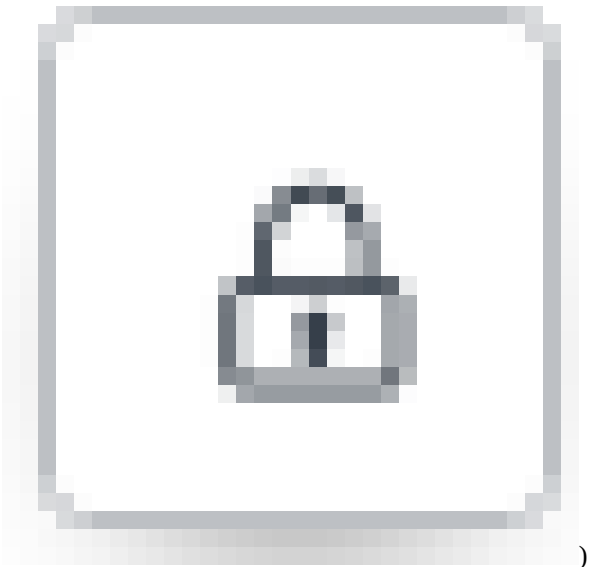
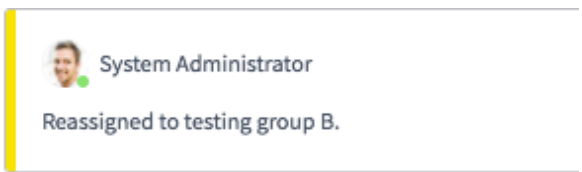
Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança que você deseja atualizar.
2. Clique na guia **Detalhes do incidente**.
3. Preencha os campos, conforme necessário.

Campo	Descrição
Acesso de leitura	Concede a um usuário com a função **de acesso especial acesso** de leitura ao incidente de segurança. O usuário pode ler e escrever anotações de trabalho. **Nota:** ◦ Se um usuário for adicionado às listas de acesso de **leitura e de acessoprivilegiado**, somente as permissões de **acesso privilegiado** persistirão. ◦ O usuário com a função sn_si.admin só pode modificar o acesso de leitura e o acesso privilegiado.
Lista de observação	Clique no ícone de cadeado para adicionar usuários que serão notificados quando ocorrerem mudanças no incidente de segurança. Depois que o campo é desbloqueado, as opções ficam disponíveis para adicionar ou remover vários usuários ou inserir endereços de e-mail do usuário. Ao concluir as entradas, clique no ícone de cadeado para bloquear o campo.
Acesso privilegiado	Concede a um usuário com a função **de acesso especial acesso de** leitura e gravação a todos os campos do incidente de segurança, exceto **Atribuído a**. Usuários com funções de acesso especial têm seu próprio módulo que contém todos os incidentes de segurança atribuídos a eles. Nenhum outro módulo está disponível para eles. Ninguém mais pode ver o módulo **Visível para mim**.

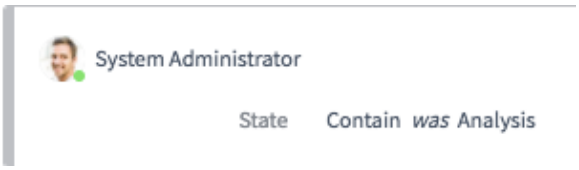
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

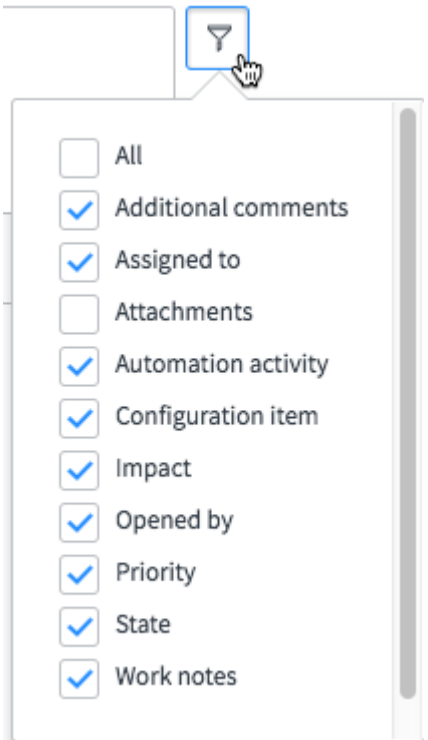
Campo	Descrição
	Nota: Somente um usuário atribuído ou alguém com uma função de segurança (por exemplo, sn_si_analyst ou sn_si.admin) pode alterar o campo **Atribuído a**. Se um usuário for adicionado às listas de acesso de **leitura e de acessoprivilegiado**, somente as permissões de **acesso privilegiado** persistirão. Se um usuário for adicionado às listas de acesso de **leitura e de acessoprivilegiado**, somente as permissões de **acesso privilegiado** persistirão.
Lista de Anotações de trabalho	 Clique no ícone de cadeado ( ) para adicionar usuários que serão notificados quando novas anotações de trabalho forem adicionadas. Depois que o campo é desbloqueado, as opções ficam disponíveis para adicionar ou remover vários usuários ou inserir endereços de e-mail do usuário. Ao concluir as entradas, clique no ícone de cadeado para bloquear o campo.
Descrição	Insira uma descrição completa do incidente de segurança, junto com qualquer informação que possa ajudar a encontrar a causa ou resolver o problema.
Notas de segurança	Somente as funções de usuário com sn_si.admin e sn_si.analyst podem exibir ou editar as anotações seguras.
Anotações de trabalho	Digite anotações de trabalho que não estão visíveis para o cliente. As anotações de trabalho aparecem na área de **Atividade**.
Atividade	Exibe informações inseridas manualmente em anotações de trabalho e todas as atividades de tarefa atualizadas dinamicamente (ações, comentários, anotações de trabalho e assim por diante) em registros relacionados a este incidente de segurança. As anotações de trabalho aparecem com uma faixa amarela. 

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	As anotações geradas automaticamente aparecem com uma faixa cinza. 

4. Você pode limitar os tipos de informações exibidos no campo **Atividade** clicando no ícone de filtro ( ).



Nota:
A caixa de seleção **Atividade de automação** permite que você inclua qualquer aprimoramento realizado por este incidente de segurança, incluindo atividades de fluxo de trabalho, atualizações de pontuação de risco e assim por diante.

5. Clique em qualquer uma das seguintes guias para atualizar ainda mais o incidente de segurança:
   - Registros relacionados
   - Análise pós-incidente
   - Informações de Fechamento
6. Ao concluir as entradas, clique em **Enviar**.

Adicionar problemas, mudanças e incidentes relacionados a um incidente de segurança

Você pode adicionar registros relacionados, como problemas, mudanças e incidentes a incidentes de segurança existentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança que você deseja atualizar.
2. Clique na guia **Registros relacionados**.
3. Preencha os campos, conforme necessário.

Campo	Descrição
Problema	Selecione um registro de problema (PRB) que resolva o problema subjacente que causou a criação deste incidente de segurança. Os PRBs para este incidente são normalmente criados clicando com o botão direito do mouse no cabeçalho do formulário de incidente de segurança e selecionando **Criar problema**.
Primário	Selecione um registro de tarefa relacionado ao problema subjacente que causou a criação deste incidente de segurança.
Incidente de segurança primário	Selecione um registro de incidente de segurança relacionado ao problema subjacente que causou a criação deste incidente de segurança. Consulte Relacionamentos entre incidentes de segurança primários e secundários.
Incidente	Selecione um registro de Incidente (INC) que resolva o problema subjacente que causou a criação deste incidente de segurança. O incidente é normalmente criado clicando com o botão direito do mouse no cabeçalho do formulário de incidente de segurança e selecionando **Criar incidente**.
Solicitação de mudança	Selecione um registro de Solicitação de Mudança (CHG) que resolva o problema subjacente que causou a criação deste incidente de segurança. A solicitação de mudança normalmente é criada clicando com o botão direito do mouse no cabeçalho do formulário de incidente de segurança e selecionando **Criar mudança**.

4. Clique em qualquer uma das seguintes guias para atualizar ainda mais o incidente de segurança:
   - Detalhes de Incidentes
   - Análise pós-incidente
   - Informações de Fechamento
5. Ao concluir as entradas, clique em **Enviar**.

Invocar um despejo de processo para um processo aprimorado no Windows

Um analista de segurança pode executar um despejo de processo em um processo específico, despejá-lo em um arquivo e publicá-lo em um site compartilhado em uma rede interna. Um analista pode exibir um processo da lista de proibições, destacado em vermelho em um incidente de segurança, e realizar análises adicionais.

Antes de Iniciar
São necessários:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Um cliente executando o Windows Vista ou superior ou um servidor executando o Windows Server 2008 ou superior.
- O utilitário de linha de comando ProcDump instalado, com uma variável de ambiente do sistema que aponta para o caminho do arquivo executável do procdump. O nome da variável deve ser PROCDUMP. Este nome é usado em um script do PowerShell.

Função necessária: sn_si.analyst

Procedimento

1. Navegue até o incidente de segurança com o processo aprimorado no qual você deseja invocar um procdump clicando em **Todos** > **Incidente de segurança** > **Mostrar incidentes em aberto**e abra um incidente de segurança.
2. Clique na guia **Dados** de aprimoramento.
3. Clique no registro de aprimoramento **Recuperar processos em execução**.
4. Marque as caixas de seleção dos processos em execução para os quais você deseja executar um procdump, clique na lista suspensa Ações nas linhas selecionadas na parte inferior da lista e clique em **Executar procdump**.
   Um **fluxo de trabalho de produção iniciado para a mensagem do processo selecionado** aparece na parte superior da lista e o fluxo de trabalho do **Security Incident Response - Executar procdump** é executado.

Exibir informações em um incidente de segurança

Você pode executar várias outras ações em um incidente de segurança existente usando os links relacionados.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança que você deseja atualizar.
2. Em **Links relacionados**, você pode executar as seguintes tarefas,

Opção	Descrição
Exibir Runbook Manual	Exiba uma lista de runbooks disponíveis para este incidente de segurança.
Fluxo de trabalho de resposta	Exiba qualquer fluxo de trabalho associado a este incidente.
Adicionar Vários Observáveis	Adiciona uma lista de observáveis em formatos delimitados por vírgula, nova linha, guia ou pipe.
Adicionar ao Caso de Segurança	Adiciona o incidente de segurança a um ou mais casos de segurança. Você também pode criar um novo caso de segurança e adicionar este incidente de segurança a ele.
Obter resumos de IP do QRadar	Se uma integração do QRadar estiver disponível e contiver ICs válidos, origem e endereços IP de destino, ela acionará os fluxos de trabalho do QRadar e exibirá os resultados em anotações de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Executar Orquestração	Escolha e execute um fluxo de trabalho do Security Operations.
View SLA timeline	Você pode exibir uma linha do tempo de SLA de um registro de SLA de tarefa ou de uma definição do ANS.
Mostrar Todas as Listas Relacionadas	Exibe todas as listas relacionadas padrão e todas as listas adicionadas manualmente. **Nota:** Itens adicionados manualmente estão disponíveis somente nesta exibição.
Mostrar itens afetados	Exibe as listas de ICs, usuários e serviços diretamente afetados por este incidente
Mostrar itens relacionados	Exibe as listas de incidentes relacionados, ICs, usuários e grupos afetados por este incidente.
Mostrar IoC	Exibe as listas de observáveis, indicadores, malware, modos e métodos e solicitações de verificação de segurança associadas a este incidente.
Mostrar dados de aprimoramento	Exibe as listas de dados de aprimoramento, processos, serviços, estatísticas, pesquisas, logs de firewall e informações de usuário comprometidas associadas a este incidente.
Mostrar tarefas de resposta	Exibe as listas de tarefas, SLAs, auditorias de pontuação de risco, indisponibilidades e pesquisas do Exchange associadas a este incidente.
Exibir detalhes no sistema externo	Se este incidente de segurança foi gerado a partir de uma aplicação externa, diretamente ou por eventos, e um link para os dados de origem foi fornecido, a ação **Exibir detalhes no sistema externo** abre o URL. Você pode exibir e pesquisar os logs que geraram este incidente.
Verificar vulnerabilidades	Se Vulnerability Response estiver ativado e você tiver selecionado pelo menos um IC afetado para o incidente de segurança, poderá enviar uma solicitação de verificação para determinar quais vulnerabilidades existem no IC.

Relacionamentos entre incidentes de segurança primários e secundários

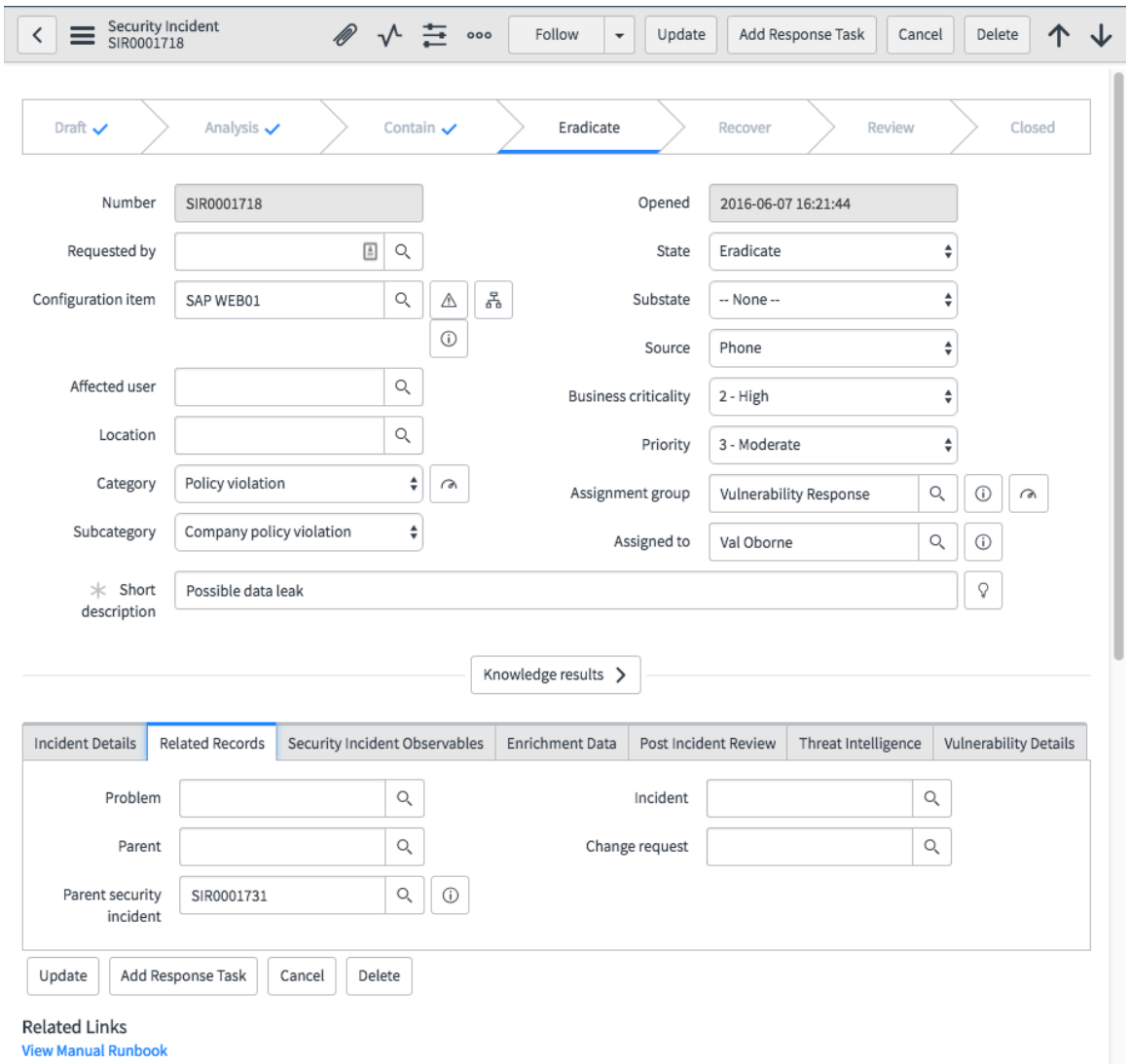
Você pode associar e rastrear o impacto de qualquer problema usando relacionamentos de incidente de segurança primário e secundário em Security Incident Response.

Usando a guia **Registros relacionados**, você pode adicionar um problema de **incidente de segurança primário** a qualquer formulário Security Incident Response. Este recurso torna automaticamente o incidente um secundário que aparece na guia **Listas relacionadas - Incidentes de segurança secundários** do problema primário.

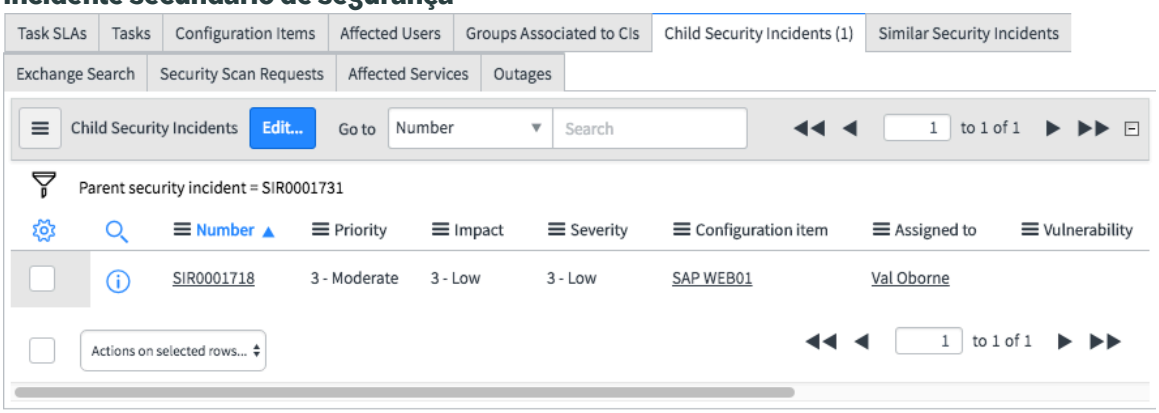
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Você não pode transformar um incidente de segurança primário existente em seu próprio secundário usando o mesmo número para ambos os incidentes.



Incidente secundário de segurança

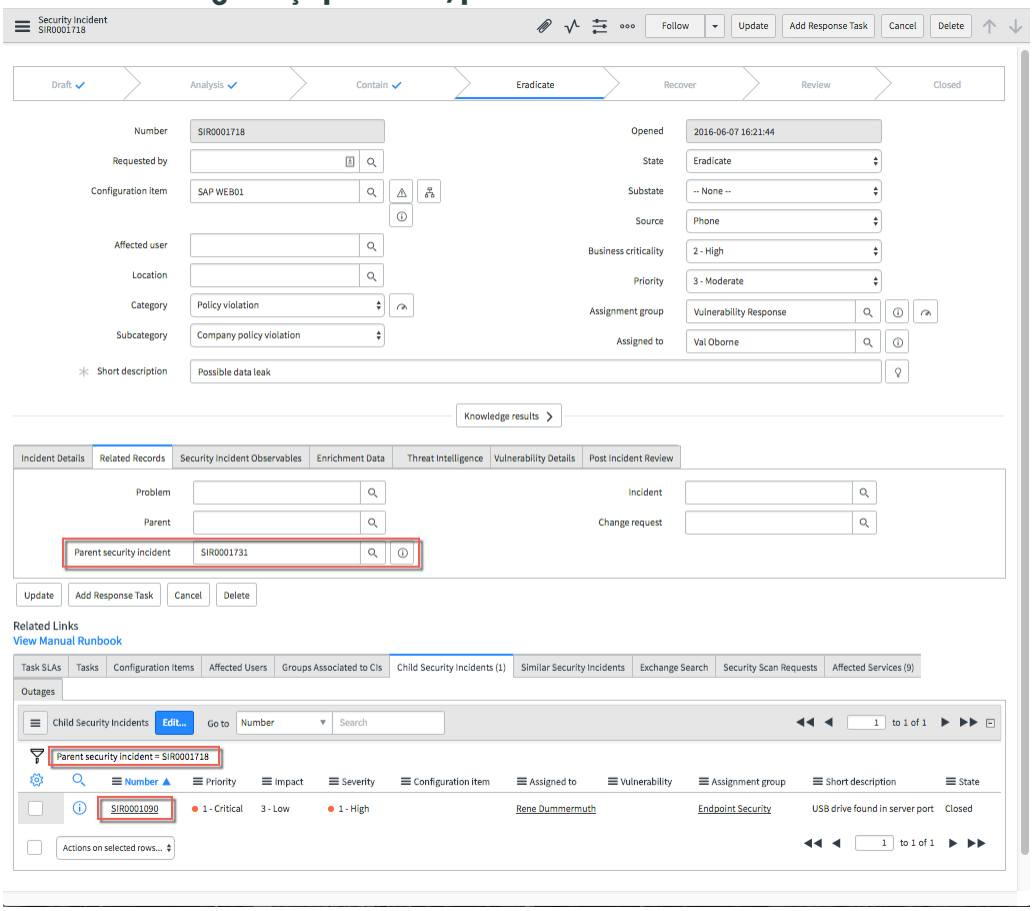


Você também pode adicionar um ou mais **incidentes de segurança secundários** a qualquer registro de incidente de segurança, usando o botão **Editar** na guia **Incidentes de segurança secundários**. No exemplo a seguir, todos os três registros estão conectados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidentes de segurança primários, primários e secundários



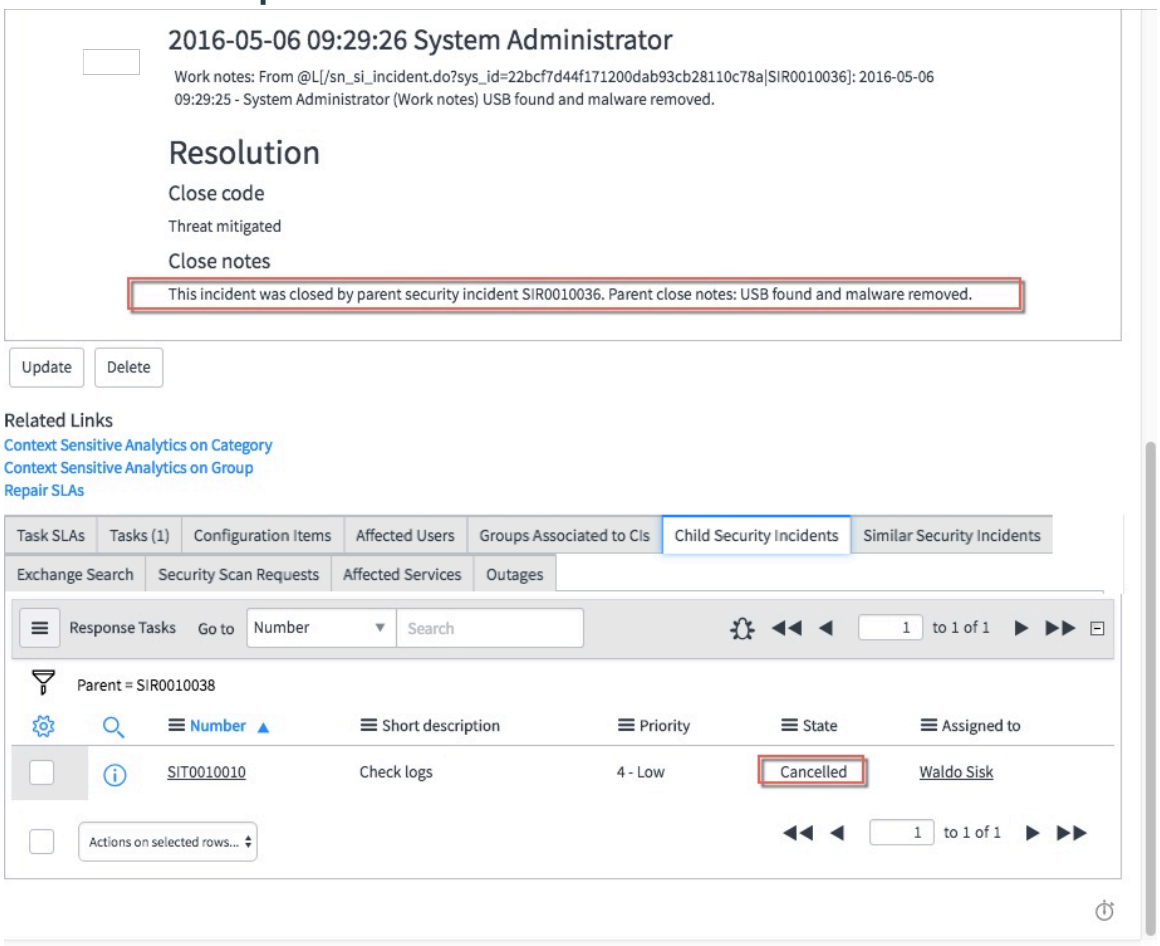
Observação: todas as anotações de trabalho registradas no primário são propagadas para todos os secundários ativos em **Atividades** na guia **Detalhes do incidente**.

Quando um primário é fechado ou cancelado, todos os secundários ativos também são fechados ou cancelados. Todas as **Tarefas de resposta** ativas nos incidentes secundários são canceladas. Se não houver outras **tarefas**abertas, o incidente secundário será fechado. Quando encerrada, a **Entrevista pós-incidente** registra o fechamento e as informações encontradas na guia **Informações de fechamento** são propagadas do primário para os secundários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fechar tarefa de resposta secundária



Exibir itens afetados por um incidente de segurança

Você pode exibir itens afetados, como ICs, usuários afetados e serviços afetados associados a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança para o qual você deseja exibir os itens afetados.
2. Clique no link relacionado **Mostrar itens afetados**.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações do incidente de segurança.

Guia	Descrição
Itens de configuração	Itens de configuração (IC) afetados. Depois que os ICs afetados forem identificados, você poderá adicionar manualmente os recursos afetados dessa lista relacionada.
Usuários afetados	Depois que os usuários afetados forem identificados, você poderá adicionar manualmente os usuários afetados dessa lista relacionada.
Serviços afetados	Exiba ou adicione serviços de negócios associados ao incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia	Descrição
	Nota: Se um IC afetado for adicionado depois que o incidente de segurança for aberto, convém clicar com o botão direito do mouse no cabeçalho do formulário e selecionar **Atualizar serviços afetados**.

Nota:
Se a funcionalidade de integração Security Operations Integration - Obter processos em execução estiver ativa e você adicionar um IC a um incidente de segurança, o fluxo de trabalho Obter processos em execução será executado e recuperará uma lista de processos em execução no IC.

Se a funcionalidade de integração Security Operations Integration - Isolate Host estiver ativa, você poderá selecionar um ou mais ICs e restringir suas conexões de sistema a outros dispositivos. Para fazer isso, marque as caixas de seleção dos ICs e clique em **Isolar host** na lista de seleção **Ações nas linhas selecionadas**.

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:
   - Mostrar itens relacionados
   - Mostrar IoC
   - Mostrar dados de aprimoramento
   - Mostrar tarefas de resposta
5. Ao concluir as entradas, clique em **Enviar**.

Exibir itens relacionados a um incidente de segurança

Você pode exibir itens relacionados, como incidentes de segurança semelhantes e secundários, usuários relacionados, grupos de vulnerabilidades e itens vulneráveis associados a um incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança para o qual você deseja exibir os itens relacionados.
2. Clique no link relacionado **Mostrar itens** relacionados.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações do incidente de segurança.

Guia	Descrição
Incidentes de segurança secundários	Selecione um registro de tarefa relacionado ao problema que causou a criação deste incidente de segurança.
Incidentes de segurança semelhantes	Exibir quaisquer outros incidentes de segurança associados a qualquer um dos mesmos registros observáveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia	Descrição
Itens de Configuração Relacionados	Exibe uma lista de incidentes de segurança que contêm itens de configuração com o mesmo observável que este incidente de segurança. Esta lista pode ser filtrada usando o grupo de filtros de **exclusões de IC**. Quando um observável é adicionado a um incidente de segurança, essa lista é atualizada automaticamente. Por padrão, os observáveis com um tipo de contexto de Destino são excluídos.
Usuários relacionados	Exibe uma lista de incidentes de segurança que contêm usuários com os mesmos observáveis que este incidente de segurança. Esta lista pode ser filtrada usando o grupo de filtros **de exclusão de usuário**. Quando um observável é adicionado a um incidente de segurança, essa lista é atualizada automaticamente. Por padrão, os observáveis com um tipo de contexto de Destino são excluídos.
Grupo de filtros relacionados	Depois que os itens de configuração são identificados, todos os ICs ou grupos de filtros correspondentes são adicionados automaticamente.
Grupos de Vulnerabilidades	Se Vulnerability Response estiver ativado, você poderá exibir grupos de vulnerabilidades associados a este incidente de segurança.
Itens vulneráveis	Se Vulnerability Response estiver ativado, você poderá exibir itens de vulnerabilidade associados a este incidente de segurança.
Riscos	Se qualquer um dos plug-ins principais do Risk Management (Policy and Compliance Management, Audit, Management ou Risk Management) estiver ativado, você poderá exibir ou adicionar riscos associados ao incidente de segurança. Você pode adicionar esta lista relacionada no menu de contexto do cabeçalho do formulário em **Configurar** > **Listas relacionadas**.
Eventos de item de configuração	Se Gestão de eventos estiver ativado, você poderá exibir eventos.
Alertas de item de configuração	Se Gestão de eventos estiver ativado, você poderá exibir alertas.
Casos de atendimento ao cliente	Se Atendimento ao cliente estiver ativado, você poderá exibir Atendimento ao cliente informações do caso.

Tradução automática

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:
   - Mostrar itens afetados
   - Mostrar IoC
   - Mostrar dados de aprimoramento
   - Mostrar tarefas de resposta
5. Ao concluir as entradas, clique em **Enviar**.

Exibir dados de aprimoramento para um incidente de segurança

Você pode exibir dados de aprimoramento, como processos em execução, serviços em execução e estatísticas de rede associadas a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança para o qual você deseja exibir dados de aprimoramento.
2. Clique no link relacionado **Mostrar dados de aprimoramento**.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações do incidente de segurança.

Nota:
Os detalhes dos dados brutos são armazenados em um anexo no registro de dados de aprimoramento. Se eles excederem o limite do campo, os detalhes exibidos serão truncados.

Guia	Descrição
Processos em execução	Armazena os registros criados pelo fluxo de trabalho Security Incident Response **Obter processos em execução**.
Serviços em execução	Armazena os registros criados pelo fluxo de trabalho Security Incident Response **Obter serviços em execução**.
Estatísticas de Rede	Armazena os registros criados pelo fluxo de trabalho Security Incident Response **Obter estatísticas de rede**.
Pesquisas de domínio	Se o plug-in WhoisXML API Integration estiver ativado, armazenará os registros criados por uma pesquisa Whois.
Logs de Firewall	Armazena dados de aprimoramento de logs de firewall, como os logs de firewall da Palo Alto Network.
Informações de usuário comprometidas	Armazena contas identificadas como comprometidas por meio de Have I Been Pwned? pesquisa.

Observação: a guia **Dados de aprimoramento de segurança** mostra dados de aprimoramento brutos de Security Incident Response fluxos de trabalho, como a recuperação de estatísticas de rede ou a execução de processos. Esta guia pode ser exibida clicando no link relacionado **Mostrar todas as listas** relacionadas.

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:
   - Mostrar itens afetados
   - Mostrar itens relacionados
   - Mostrar IoC
   - Mostrar tarefas de resposta
5. Ao concluir as entradas, clique em **Enviar**.

Exibir informações da tarefa de resposta para um incidente de segurança

Você pode exibir informações da tarefa de resposta, como SLAs de tarefa, auditorias de pontuação de risco. e indisponibilidades associadas a um incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.basic

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança para o qual você deseja exibir as tarefas de resposta.
2. Clique no link relacionado **Mostrar tarefas de resposta**.
3. Clique em qualquer uma das listas relacionadas para exibir ou adicionar informações do incidente de segurança.

Guia	Descrição
Tarefas	Exibe tarefas já definidas para o incidente de segurança. Você pode criar manualmente uma tarefa de resposta ou crie outro tipo de tarefa a partir desta lista relacionada.
Tarefas de resposta	Exibe ações a serem realizadas em resposta ao incidente de segurança.
ANSs de tarefas	Exiba ou adicione SLAs de tarefa ativos que foram definidos para o incidente de segurança.
Auditorias de Pontuação de Risco	Um registro de auditoria para cada instância de uma pontuação de risco que está sendo alterada.
Indisponibilidades	Exiba ou adicione manualmente novos registros de indisponibilidade associados ao incidente de segurança.
Pesquisa de e-mail	Uma lista de registros que contém critérios de pesquisa para executar consultas em um servidor de e-mail, como um Microsoft® Exchange Server (com base na implementação instalada) e armazena os resultados recebidos. **Nota:** se o Integração do Security Operations - Capacidade de pesquisa e exclusão de e-mail não estiver ativo, o link relacionado à **Pesquisa de e-mail** não será exibido.

4. Clique em qualquer um dos links relacionados a seguir para atualizar ainda mais o incidente de segurança:
   - Mostrar itens afetados
   - Mostrar itens relacionados
   - Mostrar IoC
   - Mostrar dados de aprimoramento
5. Ao concluir as entradas, clique em **Enviar**.

Exibir eventos e alertas relacionados em incidentes de segurança

Conforme um incidente de segurança está sendo trabalhado, você pode exibir os detalhes dos eventos. Para alertas, você pode exibir e confirmar esses alertas e criar incidentes ou incidentes de segurança a partir deles conforme necessário.

Antes de Iniciar

Você deve ter o plug-in de suporte Security Incident Response Event Management ativado.

Função necessária: si.sn_agent

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até qualquer lista de incidentes de segurança (por exemplo, **Todos** > **Incidente de segurança** > **Incidentes** > **Incidentes não atribuídos**).
2. Se os recursos afetados pelo incidente de segurança que você está exibindo tiverem recebido alertas ou eventos nas últimas 24 horas, uma ou ambas as listas relacionadas a seguir serão exibidas.
   - Alertas de IC de incidente de segurança
   - Eventos de IC de incidente de segurança
3. Clique na lista relacionada que você deseja exibir.

Lista relacionada	Descrição
Alertas de IC de incidente de segurança	Você pode exibir detalhes de alertas recebidos nas últimas 24 horas. Você tem a opção de clicar em **Reconhecer** para indicar que está ciente do alerta e que ele está sendo tratado. Use **Fechar** para indicar que o alerta não é importante.
Eventos de IC de incidente de segurança	Você pode exibir detalhes do evento recebido nas últimas 24 horas.

Exibir incidente de segurança para mapeamento de caso de atendimento ao cliente

Security Incident Response é fornecido com um mapeamento de campo padrão que mapeia um incidente de segurança para um caso Atendimento ao cliente. Você pode exibir o incidente de segurança para o mapa padrão de caso de CS.

Antes de Iniciar

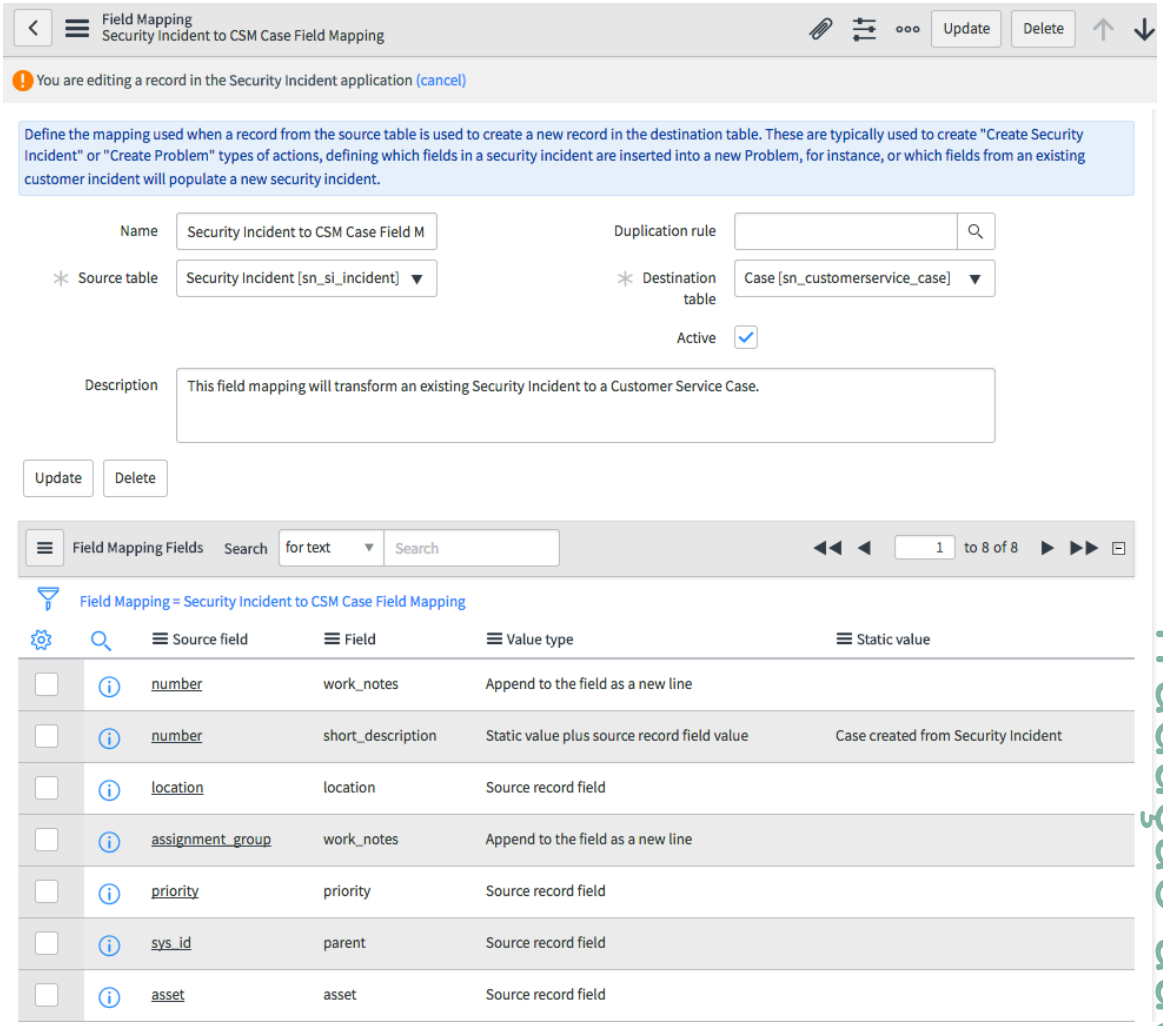
Função necessária: sec_cmn.read

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Utilitários** > **Mapeamento de Campos**.
2. Clique **em Incidente de segurança para mapeamento de campo de caso de CSM** para exibir o mapa padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Você pode editar o mapeamento, conforme necessário.
4. Ao concluir as mudanças, clique em **Atualizar**.

Exibir um runbook do Security Incident Response

Os runbooks fornecem acesso a procedimentos relacionados às tarefas nas quais você está trabalhando.

Antes de Iniciar

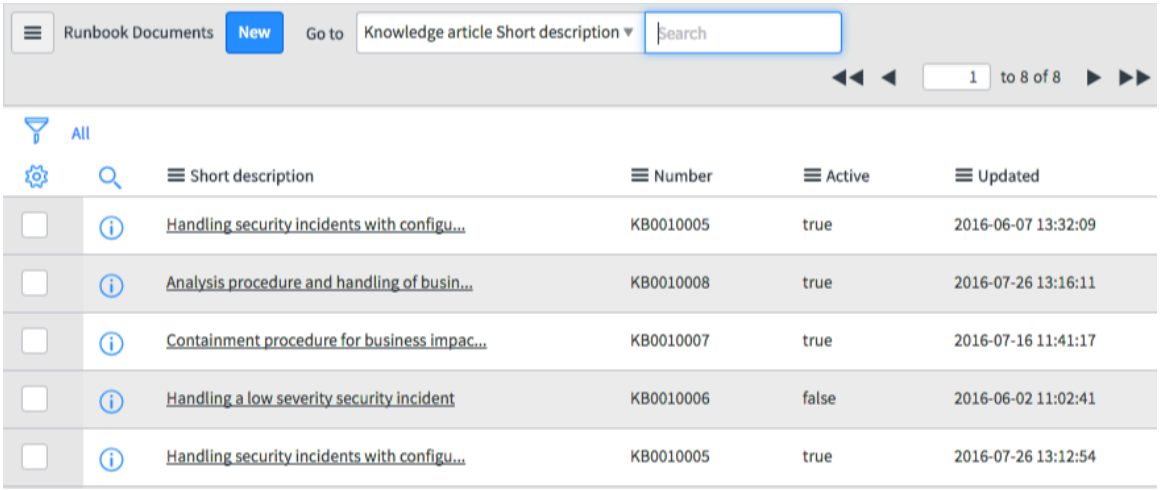
Função necessária: sn.si.knowledge_admin

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Runbook manual** > **Exibir Documentos do Runbook**.
2. Selecione um runbook na lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para criar um runbook, clique em **Novo**.
   Para obter mais informações, consulte Criar um runbook.

Identificar todos os itens de configuração afetados por um incidente de segurança

Se você souber qual recurso (servidor, desktop ou outro item de configuração) está por trás de um incidente de segurança e quiser identificar os recursos relacionados e os serviços de negócios que podem ser afetados, use o mapa do Business Service Management (BSM).

Antes de Iniciar
Função necessária: admin ou sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
O mapa de BSM exibe as dependências ascendentes e descendentes de um IC raiz selecionado.

Existem dois métodos que você pode usar para exibir o mapa de BSM para um IC:

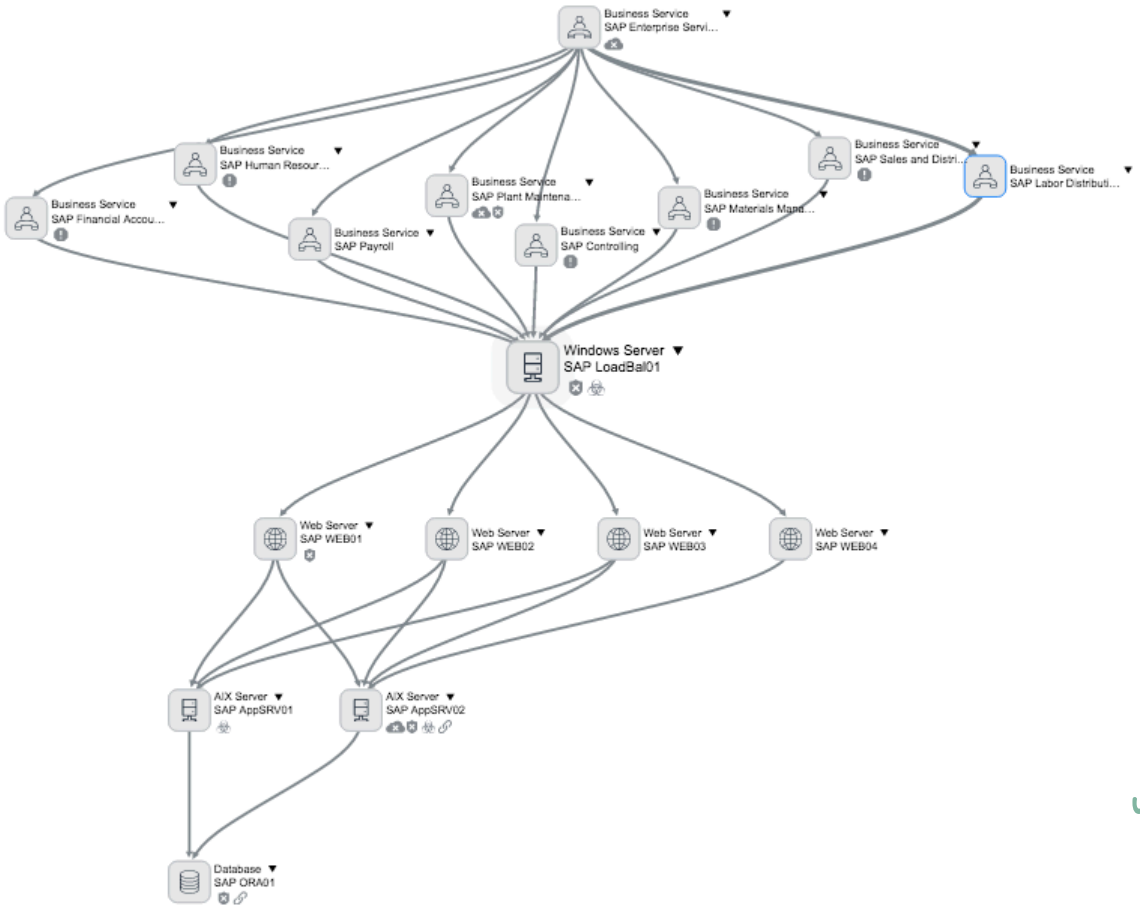
- Se você quiser exibir os ICs no contexto de uma tarefa, exiba no formulário de incidente de segurança.
- Se você não quiser exibir ICs do ponto de vista de uma tarefa, exiba na barra de navegação.

Procedimento

1. No formulário Incidente de segurança, preencha o campo **Item de configuração** e clique no ícone de mapa de BSM ( ).
   A tela do mapa de BSM exibe o mapa do último incidente acessado no Incident Management ou o último incidente de segurança acessado no Security Incident Management.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Clique nos ícones ao lado de um item de configuração para exibir diferentes tipos de detalhes sobre o recurso (servidor, desktop ou outro IC).

   Por exemplo, clique no ícone de alerta (⚠) para exibir alertas associados ao IC.

   Nota:
   Para exibir uma lista de todos os ícones disponíveis, clique em **Filtros** acima do mapa de BSM e expanda **Filtrar tipos de tarefa**.

3. Para organizar o mapa em diferentes configurações, selecione qualquer um dos formatos listados acima do mapa (**Vertical**, **Horizontal**, **Radal**) ou clique em **Filtros** para filtrar o mapa e facilitar a exibição.

4. Se você abriu o mapa de BSM do formulário de incidente de segurança, poderá adicionar um IC dependente ao incidente de segurança clicando com o botão direito do mouse no IC e selecionando **Adicionar ICs afetados**.

   Você também pode adicionar vários ICs de uma vez. Arraste uma caixa em torno dos ICs que você deseja adicionar, clique com o botão direito do mouse na caixa e selecione **Adicionar ICs afetados**.

   Os ICs são adicionados à lista relacionada ICs afetados do incidente de segurança.

Calcular a severidade de um incidente de segurança

Você pode calcular a severidade de um incidente de segurança usando calculadoras predefinidas.

Antes de Iniciar

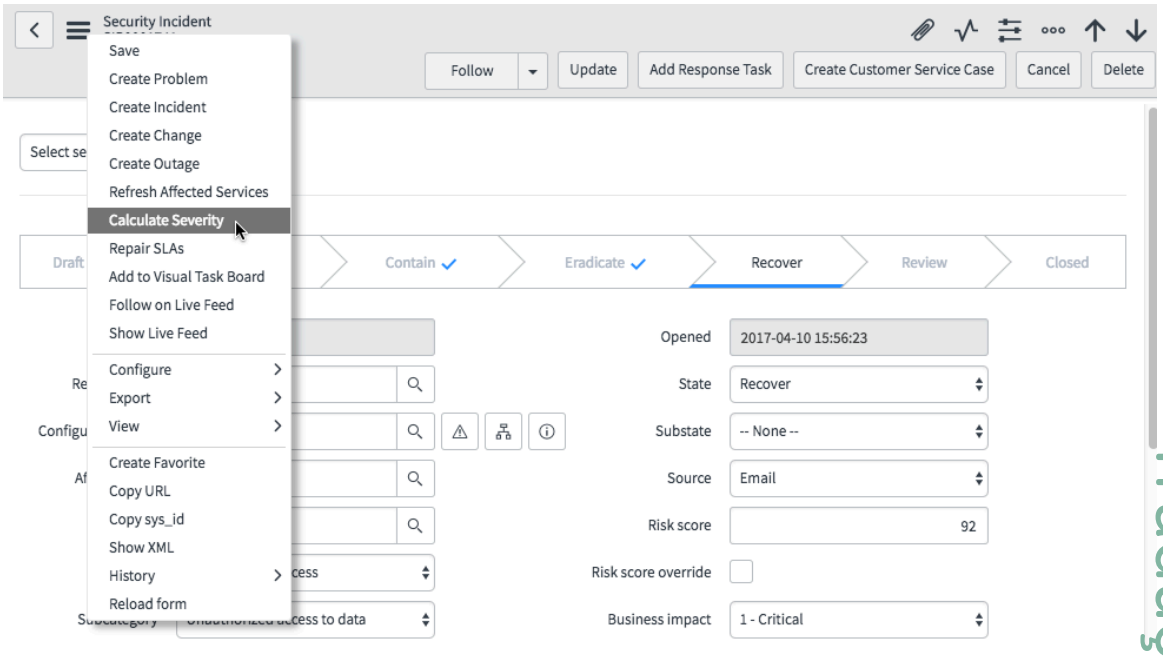
Função necessária: sn_si.basic

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança para o qual você deseja calcular a severidade.
2. Clique no menu de contexto do cabeçalho do formulário e selecione **Calcular severidade**:



A severidade é calculada com base nas regras predefinidas das calculadoras básicas. Para obter mais informações, consulte Noções básicas sobre calculadoras de incidentes de segurança.

Pesquisar e excluir e-mails de phishing

A exclusão de e-mails de phishing pode ajudar a reduzir a exposição a um ataque específico em uma organização. Você pode gerenciar e-mails de phishing no seu servidor de e-mail pesquisando, concedendo aprovações e excluindo-os.

Antes de Iniciar

Funções necessárias: sn_sec_cmn.cap_email_read

Você pode determinar quantos usuários foram alvo de um ataque de phishing consultando um registro de e-mail associado a um incidente de segurança.

Software compatível:

- Microsoft® Exchange Server 2010

Limitação: ao pesquisar o corpo dos e-mails, você pode pesquisar no máximo 1.500 caixas de correio.

Por Que e Quando Desempenhar Esta Tarefa

Este recurso é usado pelo Integração do Security Operations - Fluxo de trabalho de pesquisa e exclusão de e-mails para executar uma consulta no seu servidor de e-mail. Dependendo dos critérios de pesquisa selecionados, a pesquisa identifica todos os e-mails em um ataque de phishing e retorna o número total de e-mails afetados ou detalhes dos e-mails afetados.

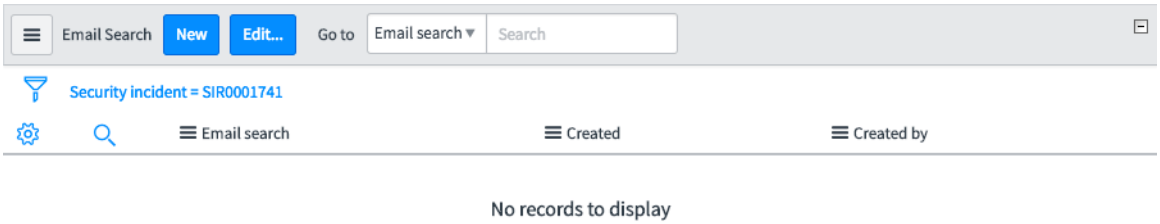
Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar incidentes em aberto**.
2. Escolha um incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

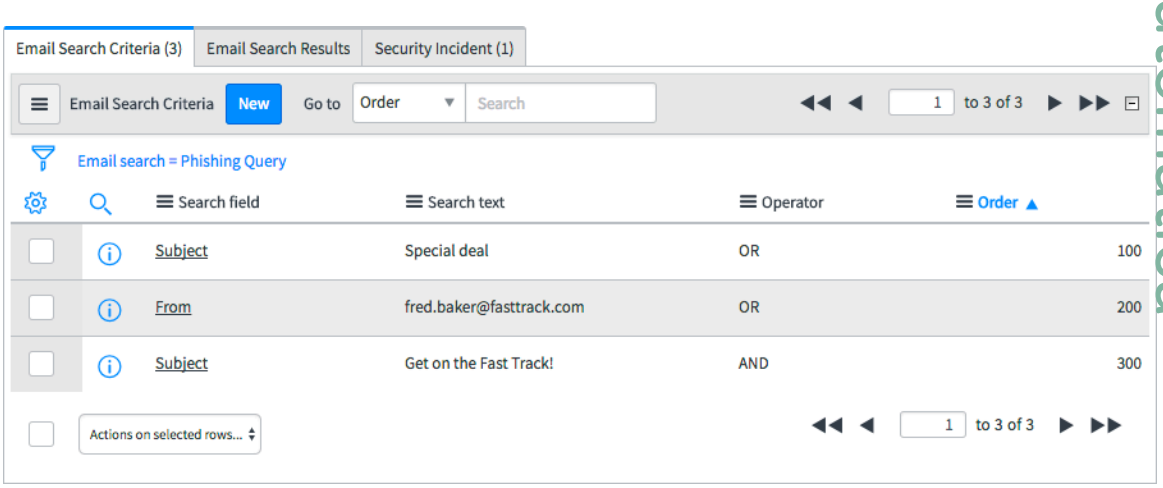
3. Se a lista relacionada **Pesquisa de e-mail** não estiver visível, clique no link relacionado **Mostrar todos os links** relacionados.
4. Clique na lista relacionada **Pesquisa de e-mail**.



5. Clique em **Nova**.
6. Preencha os campos, se for o caso.

Campo	Descrição
Nome	Nome da consulta de pesquisa
Consultar pelo critério	Uma visualização da consulta executada no servidor de e-mail. Gerado a partir de todos os registros de critérios de pesquisa ativos associados.
Descrição	Descreva o que a consulta de pesquisa está procurando.

7. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.



8. Clique na guia **Critérios de pesquisa de e-mail** e clique em **Novo**.
9. Preencha ou edite os campos, conforme apropriado.

Campo	Descrição
Pesquisa de e-mail	Exibe o nome da pesquisa de e-mail. Você pode alterá-lo, se necessário.
Campo de pesquisa	Campo para pesquisar no servidor de e-mail.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O campo de pesquisa tem as seguintes opções: **Assunto** Este critério pesquisa e-mails que contêm o texto da linha de assunto especificado no campo **Texto de pesquisa**. Para e-mails que atendem a esses critérios de pesquisa, são retornados o número total de e-mails de phishing e os detalhes de cada e-mail, incluindo a data de recebimento do e-mail, o status de leitura do e-mail, o destinatário e o ID da mensagem. **De** Este critério pesquisa e-mails que contêm o endereço de e-mail completo do remetente (por exemplo, jane.doe@abc.com) especificado no campo de **texto de pesquisa**. Para e-mails que atendem a esses critérios de pesquisa, são retornados o número total de e-mails de phishing e os detalhes de cada e-mail, incluindo a data de recebimento do e-mail, o status de leitura do e-mail, o destinatário e o ID da mensagem. **Nota:** Você não pode usar os campos **De** e **Destinatário** na mesma consulta. **Destinatário** Este critério pesquisa e-mails que contêm o endereço de e-mail completo do destinatário (por exemplo, john.doe@abc.com) especificado no campo **Pesquisar texto**. Ele também pesquisa e-mails nos campos Para, Cc e Bcc. Para e-mails que atendem a esses critérios de pesquisa, são retornados o número total de e-mails de phishing e os detalhes de cada e-mail, incluindo a data de recebimento do e-mail, o status de leitura do e-mail, o destinatário e o ID da mensagem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

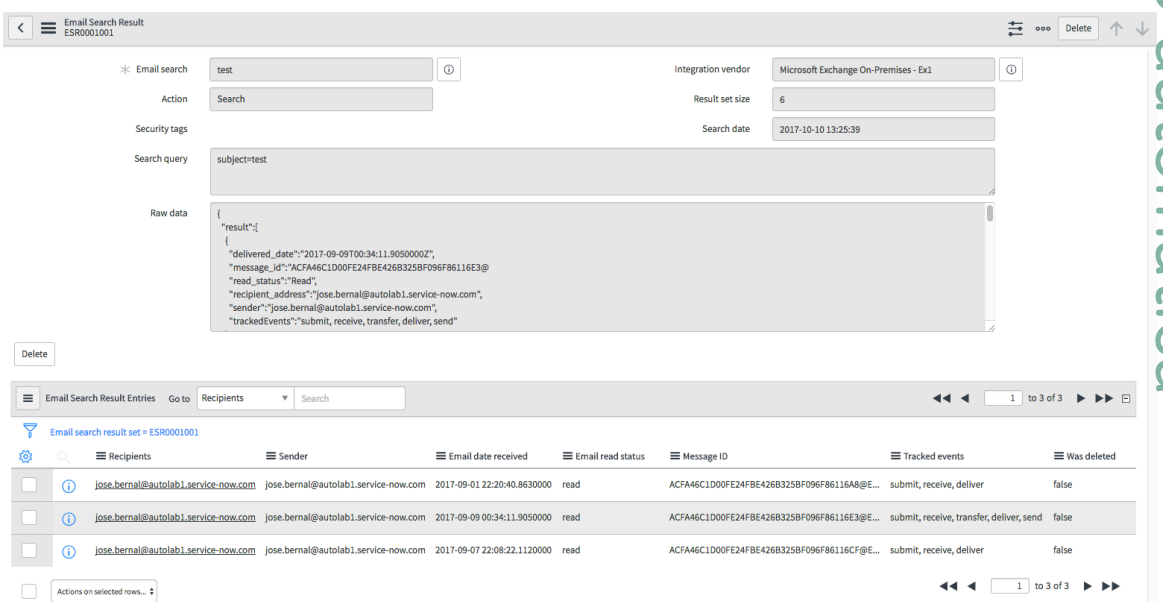
Campo	Descrição
	Nota: Você não pode usar os campos **De** e **Destinatário** na mesma consulta. **Corpo** Este critério pesquisa e-mails que contêm o texto do corpo especificado no campo **Texto de pesquisa**. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing é retornado. **Nota:** Ao pesquisar o corpo dos e-mails, você pode pesquisar no máximo 1.500 caixas de correio. **Cc:** Este critério pesquisa e-mails que contêm o endereço de e-mail completo Cc (por exemplo: jane.doe@abc.com) especificado no campo de **texto de pesquisa**. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing é retornado. **Bcc:** Este critério pesquisa e-mails que contêm o endereço de e-mail completo Cco (por exemplo: jane.doe@abc.com) especificado no campo de **texto de pesquisa**. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing é retornado. **Anexo** Este critério pesquisa e-mails que contêm o nome de arquivo do anexo ou o conteúdo do anexo especificado no campo **Texto de pesquisa**. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing é retornado. **Nota:** Somente anexos de texto simples são compatíveis para pesquisar o conteúdo do anexo. **Política de retenção**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Este critério pesquisa e-mails que contêm números de política de retenção especificados no campo **Texto de pesquisa**. Para e-mails que atendem a esses critérios de pesquisa, o número total de e-mails de phishing é retornado.
Ativo	Marque esta caixa de seleção para ativar esta consulta de pesquisa de e-mail.
Operador	Os valores possíveis são AND e OR. Você pode definir como os critérios de pesquisa são combinados para serem executados no servidor de e-mail.
Pedido	A ordem na qual a consulta de pesquisa é criada a partir dos critérios de pesquisa.
Pesquisar Texto	O texto a ser pesquisado. Aspas simples, aspas duplas e dois pontos não são compatíveis.

10. Clique em **Enviar**.
11. Repita conforme necessário para definir critérios de pesquisa adicionais.
12. Você pode exibir os resultados da pesquisa clicando na guia **Resultados da pesquisa de e-mail**.

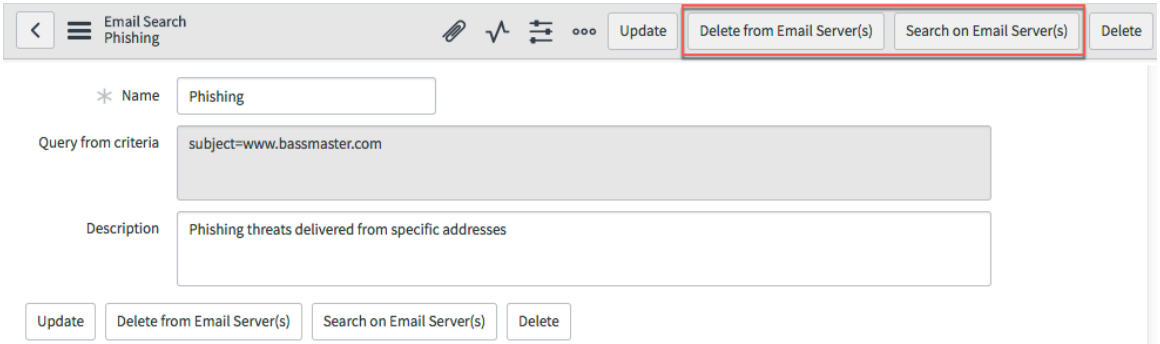


Cada linha do formulário de entradas de resultado da pesquisa de e-mail representa um e-mail separado.

13. Depois de criar um registro de critérios de pesquisa, dois botões aparecem no formulário de Pesquisa de e-mail: **Excluir do(s) servidor(es)** de e **-mail e Pesquisar no(s)**servidor(es) de e-mail.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



14. Para pesquisar e-mails no servidor selecionado que atendam aos critérios de pesquisa definidos, clique **em Pesquisar em servidores de e-mail**.

Criar um artigo de conhecimento de incidente de segurança

Conforme você trabalha com incidentes de segurança e tarefas de resposta, os artigos de conhecimento são exibidos automaticamente para fornecer informações pertinentes sobre a tarefa que você está executando. Sua organização pode criar e manter artigos na base de conhecimento de incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.knowledge_admin

Por Que e Quando Desempenhar Esta Tarefa

Os artigos de conhecimento compartilham informações de segurança, documentam os tipos de ameaças cibernéticas que sua organização enfrenta e fornecem respostas e respostas para essas ameaças.

Se necessário, você pode organizar artigos de conhecimento em runbooks, que criam associações entre os artigos e tarefas específicas. Por exemplo, você pode configurar um runbook com condições que fazem com que um artigo da base de conhecimento sobre phishing seja exibido ao criar um incidente de segurança para um ataque de phishing. Para obter mais informações, consulte Criar um runbook do Security Incident Response.

Artigos de conhecimento em runbooks também podem ser associados a tarefas específicas em um playbook. Para obter mais informações, consulte Associar um artigo de conhecimento a uma tarefa do playbook.

Os benefícios dos artigos de conhecimento incluem o seguinte.

- Os funcionários têm uma fonte de informações fácil de pesquisar.
- As informações podem ser mantidas atualizadas, pois os artigos de conhecimento têm um ciclo de vida definido: criar, revisar e atualizar, publicar e desativar.
- Quando você cria manualmente uma solicitação de segurança, incidente ou tarefa de resposta, uma lista de artigos relevantes é apresentada conforme você digita a descrição resumida.

Nota:
É importante atribuir um gerente de conhecimento para cada base de conhecimento de incidente de segurança.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Catálogo e Conhecimento** > **Conhecimento**.
2. Clique no ícone Criar um artigo (ícone).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos no formulário, conforme apropriado.

Formulário de conhecimento

Campo	Descrição
Número	O número de KB gerado automaticamente.
Base de conhecimento	A base de conhecimento selecionada para este artigo.
Categoria	A categoria deste artigo.
Publicado	Quando este artigo de conhecimento foi publicado. Este valor é definido quando o artigo é criado e atualizado quando o artigo é publicado.
Válido até	Quando este artigo de conhecimento expira. Este artigo não aparecerá nos resultados da pesquisa após esta data ou se uma data não for selecionada.
Imagem	Uma imagem que aparece ao lado do artigo ao pesquisar no portal de conhecimento legado.
Fluxo de trabalho	[Somente leitura] O estado de publicação do artigo, como Rascunho ou Publicado. Quando Ao inserir um novo artigo a partir de um artigo existente, o estado do novo artigo é redefinido para **Rascunho**.
Fonte	A tarefa para a qual este artigo de conhecimento foi criado em resposta, se houver. Este campo é definido automaticamente quando você cria o artigo de conhecimento a partir de um registro de tarefa.
Link de anexo	Marque a caixa para baixar um arquivo anexado automaticamente quando um usuário acessar o artigo, em vez de abrir a exibição do artigo. Adicione um anexo ao artigo para usar esta opção.
Exibir anexos	Caixa de seleção para exibir anexos para usuários que exibem este artigo de conhecimento. Os anexos aparecem abaixo do texto do artigo. Adicione um ou mais anexos ao artigo para usar esta opção.
Descrição resumida	O título do artigo. Este título aparece ao navegar e pesquisar conhecimento e na parte superior do artigo.
Texto	Conteúdo do artigo. Use o editor de HTML WYSIWYG para criar conteúdo. Uma visualização do conteúdo aparece ao navegar e pesquisar conhecimento.

Nota:
Se você estiver criando um artigo de conhecimento a ser associado a uma tarefa do playbook, defina o campo **Base de conhecimento** como **Runbook do Security Incident Response**.

4. Clique em **Enviar** para criar o artigo.

O que Fazer Depois

Todas as etapas adicionais necessárias para publicar o artigo, como aprovações, dependem do fluxo detrabalho de publicação para a base de conhecimento.

Tópicos relacionados

Criar um runbook do Security Incident Response

Escalar um incidente de segurança

Se houver um caminho de escalação para um incidente de segurança, o botão Escalar estará disponível no cabeçalho do incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

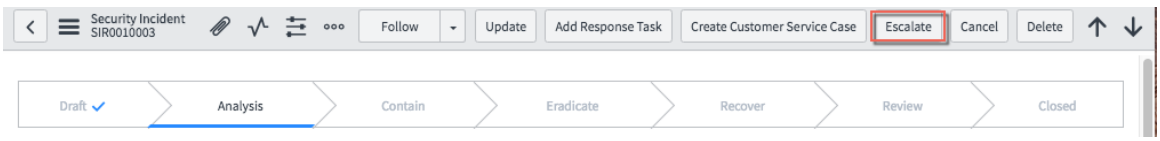
Antes de Iniciar

Função necessária: sn_si.admin

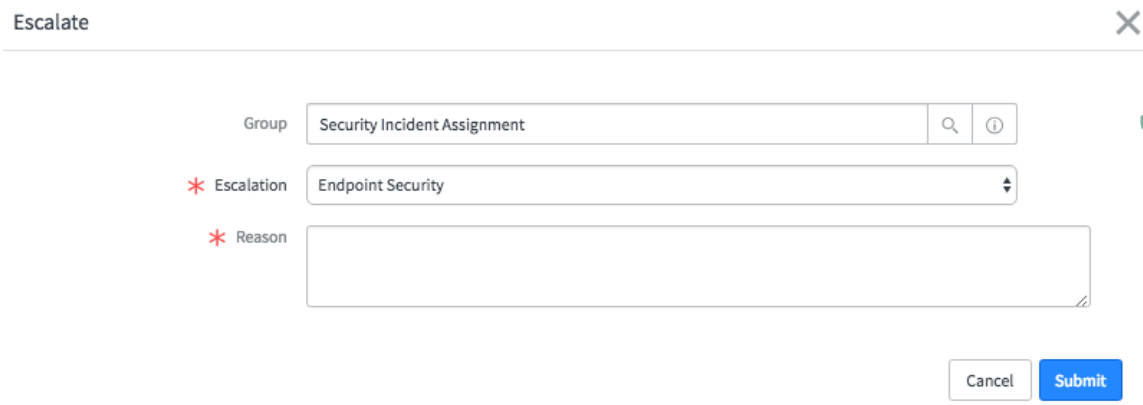
Você deve ter um grupo de escalação criado para ver este botão. Para obter mais informações, consulte Criar um grupo de escalação definido pelo usuário Security Operations.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Mostrar incidentes em aberto**.
2. Abra o incidente que você deseja escalar.
3. Clique no botão **Escalar**.



4. Escolha um grupo de escalação.
5. Insira um motivo para a escalação.



6. Clique em **Enviar**.
   Atualiza o **Grupo de atribuição** e **Atribuído a** no incidente de segurança.

Gerenciar atividades pós-incidente

Com base nos requisitos da sua empresa, uma revisão das origens e o tratamento de incidentes de segurança geralmente são necessários.

A funcionalidade Análise pós-incidente em ServiceNow fornece muitas ferramentas para automatizar, rastrear, auditar e simplificar este processo.

Esta seção descreve o seguinte:

- Atribuir funções de análise pós-incidente
- Configurar uma condição do gatilho de avaliação
- Realizar uma revisão pós-incidente baseada em questionário
- Criar regras de atribuição de PIR
- Relatório de análise pós-incidente

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribuir funções de análise pós-incidente

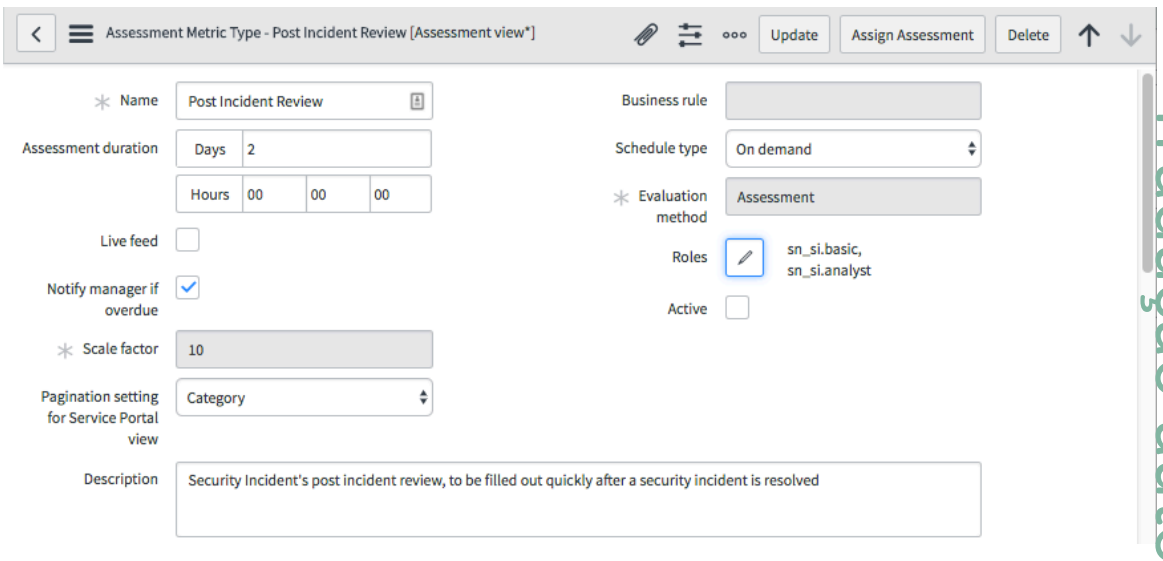
Você pode direcionar perguntas para grupos predefinidos específicos atribuindo funções às categorias de Análise pós-incidente (PIR).

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Tudo** > **Avaliações** > **Definição de métrica** > **Tipos**.
2. Na coluna **Tipos**, pesquise um registro **de Análise pós-incidente**.
3. Abra o registro.
4. Atribua uma ou mais funções para esta categoria de perguntas.



5. Clique em **Atualizar**.
6. Navegar até **Administração de usuários** > **Usuários**.
7. Escolha um usuário
8. Adicione uma ou mais funções de tipo de métrica ao registro do usuário.

Nota:
As funções devem corresponder às funções atribuídas na categoria Análise pós-incidente.

Relatório de análise pós-incidente

O recurso de relatórios de Revisão pós-incidente (PIR) permite que você configure e baixe os relatórios de revisão pós-incidente usando a guia Revisão pós-incidente.

O administrador de segurança pode criar e configurar os modelos de relatório e mapear esses modelos para o incidente de segurança usando a configuração de relatório. Um analista de segurança pode exibir ou baixar o relatório depois que o incidente de segurança for resolvido e o status for atualizado para o estado Revisar.

Um relatório em PDF é gerado e anexado ao incidente de segurança quando o incidente é movido para o estado Encerrado após a configuração bem-sucedida.

Nota:
O recurso de relatórios é aplicável e compatível com o Orlando Patch9.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para personalizar seus relatórios de análise pós-incidente, você deve fazer a configuração a seguir.

1. **Modelos de relatório**: personalize e configure os seguintes recursos de modelo de relatório para adicionar informações adicionais ao relatório:
   a. Linha do tempo
   b. Identidade visual
   c. Scripts do Modelo
2. **Configuração de Relatório**

Esta seção descreve o procedimento de configuração:

Modelos de relatório

Use a seção Modelos de relatório para criar modelos de relatório primários e adicionais que são aplicados aos incidentes de segurança para gerar o relatório de análise pós-incidente. Você pode formatar e configurar o relatório com base em seus requisitos. Os modelos também ajudam a incluir os detalhes da avaliação no modelo.

A seguir estão algumas etapas opcionais que podem ser realizadas ao criar o modelo:

1. Configurando as informações de identidade visual.
2. Configurando o tamanho e a margem da página.
3. Adicionar campos relacionados a incidentes de segurança (personalizados e padrão).
4. Usando os seguintes tokens personalizados predefinidos:
   a. `$sessionUser`: retorna o nome de usuário conectado
   b. `$date`: retorna a data atual
   c. `$if_not_null_start#&#$if_not_null_end`se esses marcadores forem usados em qualquer campo, os marcadores serão exibidos somente se o valor existir. Por exemplo:
      - `${if_not_null_start:problem}`
      - `Problem Category: ${problem.category}`
      - `${if_not_null_end:problem}`
5. Incluindo os dados da lista relacionada usando os scripts de modelo. Para obter mais informações, consulte a seção abaixo em **Scripts de modelo**.
6. Incluindo as informações da linha do tempo usando os filtros de linha do tempo. Para obter mais informações, consulte a seção abaixo na **Linha**do tempo.
7. Gerenciar e formatar o conteúdo do modelo, como anexos, tabelas e imagens.

Nota:
Os recursos da barra de ferramentas do modelo de relatório aprimorado estão disponíveis somente na versão Paris.

Pontos principais dos modelos de relatório:

1. As imagens anexadas ao modelo de relatório são exibidas no relatório de análise pós-incidente somente quando são incluídas na tabela sys_attachment.

Nota:
As imagens selecionadas na tabela db_image não serão exibidas no relatório de análise pós-incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Os vídeos não são compatíveis com o relatório de análise pós-incidente.
3. Os URLs no PDF não podem ser clicados. Para habilitar os URLs não clicáveis (.) é indicado como (ponto).
4. O relatório não será gerado se o tamanho do modelo de relatório exceder 50 MB.
5. A família de fontes selecionada para o conteúdo do modelo de relatório não será aplicada ao PDF se não for compatível com o gerador de PDF.

Nota:
Se a fonte correspondente não estiver presente, o gerador de PDF identificará a fonte alternativa mais próxima e gerará o PDF.

6. Se você fornecer valores de margem de página mais altos, haverá falha na geração do relatório de análise pós-incidente. Por exemplo, Margem superior e inferior > 450 e Margem esquerda e direita > 450.
7. Se um texto grande for incluído no modelo de relatório sem espaços, o texto poderá ficar truncado. Visualize o texto e modifique-o de acordo.

O administrador de segurança pode visualizar o relatório usando o botão **Visualizar relatório** disponível na página Modelo de relatório.

Nota:

Selecione um incidente de segurança para visualizar um relatório com esta opção de modelo e clique em **Visualizar relatório**.

Identidade visual

Você pode adicionar o nome do modelo de identidade visual, a imagem do cabeçalho e rodapé, o texto do cabeçalho e rodapé, gerar números de página e incluir o registro de identidade visual no modelo de relatório depois que ele for criado.

A seguir está um exemplo de formato de relatório de identidade visual:

Pontos principais da identidade visual do modelo de relatório:

1. O tamanho máximo permitido para a imagem do cabeçalho e do rodapé é de 5 MB. Se o tamanho exceder o limite especificado, uma mensagem de erro, "O formato da imagem não pode ser reconhecido", será exibida no incidente de segurança.
2. O tamanho do texto do rodapé está limitado a 100 caracteres.
   a. Se o texto da imagem do rodapé e o conteúdo do relatório forem sobrepostos durante a visualização, você deverá fazer mudanças no registro de identidade visual.
   b. Se o texto do rodapé contiver um link de URL, ele poderá se sobrepor à imagem do rodapé. Visualize e corrija conforme necessário.

Linha do tempo

A configuração da linha do tempo permite criar e modificar os filtros da linha do tempo conforme necessário. Você pode filtrar os tipos de atividade que devem ser incluídos no relatório, configurar se as tarefas secundárias devem ser incluídas ou excluídas no relatório e configurar se as imagens devem ser incluídas ou excluídas no relatório.

Se você quiser utilizar e preencher qualquer configuração de linha do tempo, adicione o marcador conforme mencionado abaixo: `${timeline:timeline name}`. Duas configurações de linha do tempo de exemplo são fornecidas na configuração usada no

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

modelo de relatório de phishing e no modelo de relatório padrão. Você pode modificar e reutilizar as configurações.

Scripts do Modelo

Use os scripts de modelo para incluir os dados das listas relacionadas, o carimbo de data e hora e quaisquer outros dados que não sejam diretamente orientados por pontos. A seguir está um exemplo:

Crie um script de modelo para exibir a lista relacionada no modelo de relatório:

1. Para preparar os dados da lista relacionada, chame o método PostIncidentReportUtils.fetchRelatedListDataForReport.
2. Para representar os dados da etapa1 no formato e estilo da tabela, chame o método ReportTemplateUtil.constructTablefunction.

Se você quiser utilizar e preencher qualquer script de modelo, deverá adicionar o marcador de script de modelo como `${template_script:script name}`.

A seguir estão alguns exemplos de scripts de modelo fornecidos para configurar e modificar seus relatórios pós-incidente.
Pontos principais dos scripts de modelo de relatório:

1. Se uma lista relacionada for adicionada com mais de 5 colunas, os dados da tabela serão truncados durante a geração do PDF. A largura mínima de cada coluna é definida como 124px.
2. Se um script de modelo não puder carregar o conteúdo no modelo de relatório devido a problemas técnicos, uma mensagem de erro será exibida no relatório, "Erro ao avaliar o script de modelo", e o administrador de segurança deverá avaliar a exatidão do script para resolver o problema. problema.
3. si_assessments: por padrão, todas as categorias de avaliação são adicionadas ao relatório. O administrador de segurança pode filtrar os dados modificando o script de modelo conforme necessário. Adicione o parâmetro `categories: sys_id1,# sys_id2;` para filtrar os dados.
4. Tempo de resolução e tempo de identificação de scripts: use os registros de definição que fazem parte da lista relacionada de métrica. Se os registros de definição não estiverem disponíveis para o incidente de segurança, crie ou adicione esses registros de definição para preencher os valores dos dois campos.

Nota:

Por padrão, o administrador de segurança não tem acesso para exibir os registros de versão de qualquer tabela. Você deve adicionar a função de administrador para acessar os registros da versão e reverter para a versão anterior.

Configuração de Relatório

Use a seção Configuração de relatório para configurar as condições e aplicar os modelos de relatório aos Incidentes de segurança. Você pode adicionar um relatório primário e um ou mais modelos de relatório adicionais à mesma condição.

A seguir está um exemplo de condição que é fornecido para aplicar o modelo de relatório de phishing aos incidentes da categoria de phishing e outro para aplicar o modelo de relatório padrão a todos os incidentes de segurança. O modelo de relatório padrão será aplicado aos incidentes de segurança se as condições não forem atendidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento para desativar a nova implementação

1. Desative as seguintes regras de negócios:
   a. Gerar PDF de PIR
   b. Criar conhecimento no novo fechamento
2. Ative as seguintes regras de negócios:
   a. Gerar PIR ao revisar e fechar
   b. Criar conhecimento no fechamento
   c. [Regen PIR em fechamento/cancelamento/exclusão]
3. Ative a regra de IU, `Hide PIR field when empty`.
4. Vá para o layout do formulário no formulário de incidente de segurança. Na seção **Análise pós-incidente** :
   a. Remover seletor de relatório PIR da seção PIR
   b. Adicionar campo Relatório pós-incidente à seção PIR

Configurar propriedades do relatório de análise pós-incidente (PIR) para incidentes de segurança secundários

Você tem a opção de configurar as duas propriedades do relatório PIR a seguir para incidentes de segurança secundários:

- **sn_si.generate_pir_report_for_child_si**
- **sn_si.include_child_si_timeline_in_pir**

Nota:
Usuários com a função de administrador do sistema [admin] podem exibir as propriedades. Usuários com a função de administrador de segurança [sn_si.admin] podem modificá-las.

Configurar propriedades do relatório PIR para incidentes de segurança secundários

Propriedade	Uso
sn_si.generate_pir_report_for_child_si	Opção para habilitar a geração de relatórios de análise pós-incidente (PIR) para incidentes de segurança secundários. • **Tipo**: verdadeiro | falso • **Valor-padrão**: falso • **Local**: Navegue até Todos > Propriedades do sistema > Todas as propriedades.
sn_si.include_child_si_timeline_in_pir	Opção para incluir a linha do tempo dos incidentes de segurança secundários no relatório PIR do incidente de segurança primário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar propriedades do relatório PIR para incidentes de segurança secundários

Propriedade	Uso
	• **Tipo**: verdadeiro | falso • **Valor-padrão**: falso • **Local**: Navegue até Todos > Propriedades do sistema > Todas as propriedades.

Gerenciar relatório de análise pós-incidente

Gerenciar relatório de revisão pós-incidente inclui as informações que foram configuradas e aplicadas pelo administrador de segurança, e os analistas de segurança podem modificar os filtros da linha do tempo no tempo de execução e baixá-los.

Antes de Iniciar

Função necessária: sn.si_analyst

Por Que e Quando Desempenhar Esta Tarefa

O analista de segurança pode selecionar um dos modelos de relatório primários ou adicionais disponíveis e configurar os filtros da linha do tempo, visualizar e baixar o relatório. O analista de segurança também pode baixar diretamente o relatório com a configuração da linha do tempo que foi aplicada pela última vez.

O analista de segurança pode acessar os relatórios usando a guia Revisão pós-incidente.

Procedimento

1. Navegue até o incidente de segurança no estado Revisão.
2. Clique na guia **Revisão pós-incidente**.
3. Se o incidente de segurança estiver no estado **Revisão** :
   Modelo de relatório:
   - Por padrão, o modelo de relatório primário que foi configurado na página de configuração será aplicado ao incidente de segurança e estará disponível para download.
   - O analista pode escolher outros relatórios na lista suspensa para configurar e baixar o relatório.
4. **Configurar/Visualizar:**

   Um analista de segurança pode visualizar e modificar a configuração do modelo de relatório. Na configuração atual, o analista de segurança só pode modificar os filtros da linha do tempo.

   Caso a configuração seja modificada para o relatório primário antes do encerramento do incidente de segurança, o relatório de revisão pós-incidente anexado ao incidente de segurança será atualizado de acordo com as modificações feitas pelo analista de segurança. Após o fechamento, o analista poderá modificar a configuração e baixar o relatório em qualquer lugar. No entanto, o relatório anexado seguiria a última configuração antes do fechamento.

   Para Configurar/Visualizar o relatório, execute as seguintes etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Selecione o modelo de relatório desejado na lista suspensa **Modelo** de relatório na guia **Revisão pós-incidente**.

b. Clique na guia **Configurar/Visualizar**.

c. **Atualize** ou configure os filtros da linha do tempo conforme necessário.

d. Use a caixa de seleção **Mostrar imagens** para incluir ou excluir as imagens da linha do tempo. Se desmarcada, somente os nomes das imagens serão incluídos na seção da linha do tempo.

e. Use a caixa de seleção **Mostrar tarefas** secundárias para listar todas as tarefas secundárias associadas ao incidente de segurança.

5. **Salve** a configuração e clique na guia **Visualizar** para visualizar e baixar o relatório.

6. Clique em **Download** para baixar diretamente o relatório.

Configurar uma condição do gatilho de avaliação

Defina condições de regra e gere avaliações obrigatórias e opcionais para incidentes de segurança específicos.

Antes de Iniciar

Função necessária: sn_si.admin

Nota:
Para usar o recurso Condições do gatilho de avaliação de análise pós-incidente, você deve atualizar para Security Incident Response 11.0. Antes de atualizar, você deve reverter todas as personalizações feitas no tipo de métrica de análise pós-incidente e nas condições do gatilho. Além disso, talvez você também precise reverter as personalizações feitas nas regras de negócio específicas para a revisão pós-incidente.

- Exigir que as avaliações sejam concluídas
- Armazenar designado

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Administração** > **Análise pós-incidente - Configuração de avaliações**.

2. Na seção **Condições do gatilho de avaliação Configurar**, clique em **Configurar**.

Nota:
No formulário Configurações de avaliação e na seção Configurações de avaliações, a caixa de seleção **Gerar avaliações** é marcada por padrão.

- Quando você marca a caixa de seleção, uma avaliação opcional é criada para cada incidente de segurança.
- Quando você desmarca a caixa de seleção, as avaliações não são geradas. As regras de avaliação não são exibidas e você não pode configurar condições para os incidentes de segurança.

3. No formulário Configurações de avaliação, na seção Condições, especifique as informações necessárias.

a. No campo **Nome**, especifique o nome da regra.

b. No campo **Execução**, especifique o tipo de execução.

Tradução automática

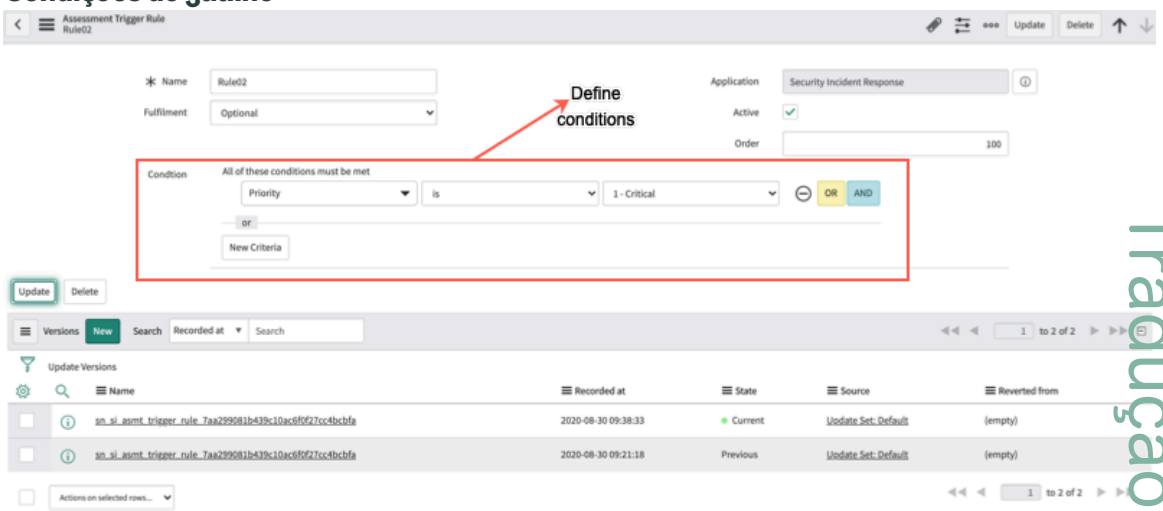
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Para configurar uma condição, clique no registro da regra e defina as condições no campo **Condição**.

Nota:

- Se você criar uma regra sem definir uma condição no campo **Condição**, a condição será avaliada como verdadeira e a regra será aplicável a todos os incidentes de segurança.
- Você pode definir uma regra específica para tornar as avaliações obrigatórias ou opcionais, e as avaliações não serão geradas para os incidentes de segurança restantes, que não correspondem às regras definidas.

Condições do gatilho



Exemplos de condições do gatilho de avaliação

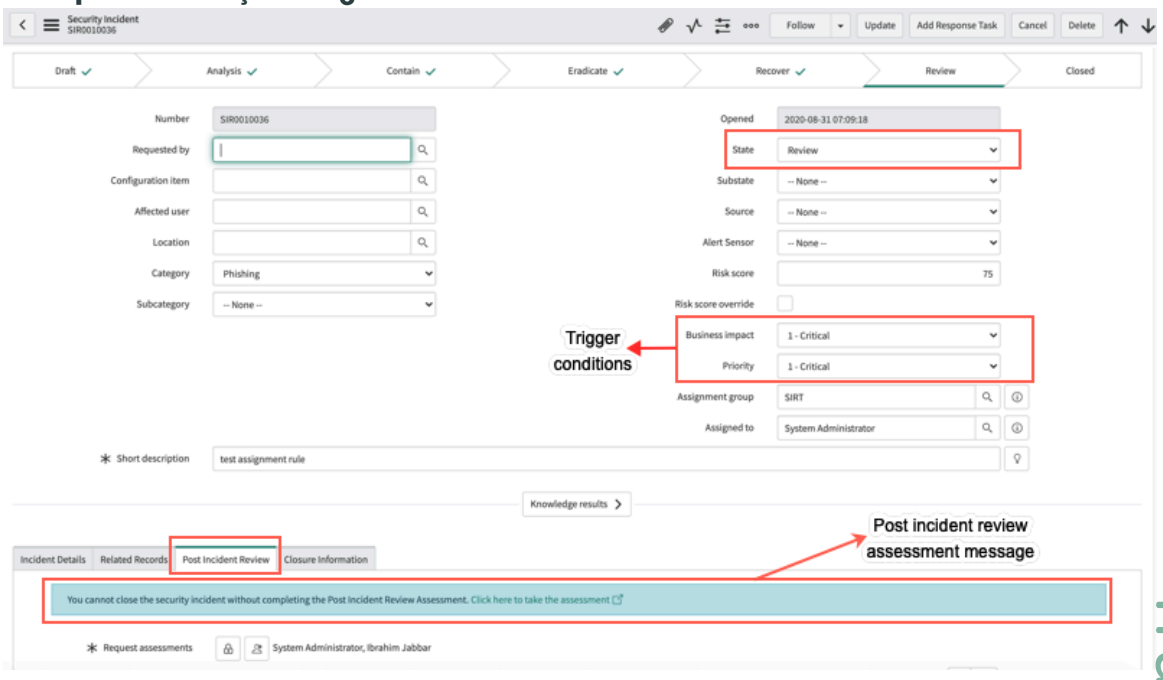
Os exemplos a seguir fornecem diferentes cenários sobre como as condições do gatilho de avaliação obrigatória e opcional são geradas.

- No formulário Condição do gatilho de avaliação, gere avaliações obrigatórias quando a **Prioridade** e o **Impacto nos negócios** de um incidente de segurança estiverem definidos como **Críticos** na página **Regra do gatilho de avaliação**. Nesse cenário, os analistas de segurança não podem fechar o incidente até que as avaliações obrigatórias sejam concluídas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de avaliação obrigatória



- Como você pode ver, neste exemplo, se um incidente de segurança estiver em um estado de **revisão**, os analistas de segurança não poderão fechar o incidente de segurança sem concluir a **avaliação de análise pós-incidente**. Um link de avaliação está disponível para levar a avaliação aos analistas de segurança atribuídos (ou que solicitaram a avaliação) ao incidente.
- No formulário Condição do gatilho de avaliação, gere avaliações opcionais quando a **Prioridade** e o **Impacto nos negócios** de um incidente de segurança estiverem definidos como **Altos**. Neste exemplo, se os analistas de segurança não concluírem as avaliações e fecharem o incidente de segurança, as avaliações serão canceladas automaticamente.
- No caso, se as avaliações obrigatórias ou opcionais não corresponderem ao incidente de segurança, as avaliações não serão geradas para esses incidentes de segurança. Um analista de segurança pode fechar o incidente de segurança sem concluir a avaliação de análise pós-incidente.

Realizar uma revisão pós-incidente baseada em questionário

Você pode decidir que uma revisão pós-incidente do incidente de segurança é garantida. Uma revisão pós-incidente descreve o que aconteceu, ajuda a determinar por que o incidente ocorreu e identifica como ele pode ser evitado ou tratado no futuro.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.manager, sn_si.analyst

Nota:

Qualquer usuário pode participar de um questionário de análise pós-incidente, independentemente da função. As funções podem ser atribuídas a uma revisão.

Por Que e Quando Desempenhar Esta Tarefa

A aplicação ServiceNow Security Incident Response pode automatizar a coleta de informações de análise pós-incidente de todos os envolvidos com um incidente de segurança usando questionários. Se você decidir usar um questionário como parte de uma revisão pós-incidente, uma lista de perguntas relevantes para o incidente de segurança será enviada para a lista de participantes definida pelo usuário. Conforme cada usuário conclui o

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

questionário, o relatório pós-incidente é gerado automaticamente. O relatório compila todas as informações relacionadas ao incidente de segurança, bem como todas as respostas para a revisão pós-incidente.

Embora uma lista inicial de perguntas seja fornecida com o sistema básico, ela é personalizável. Você pode criar categorias e adicionar novas perguntas a elas ou pode mudar perguntas individuais em categorias existentes. Você pode fazer perguntas com base em funções. Você pode definir quando determinadas perguntas são feitas. Pode haver perguntas que você faz somente para seus servidores UNIX, por exemplo, ou somente quando há atividade criminal. Você pode definir perguntas que são feitas dependendo da resposta a outra pergunta ou do valor em um campo no formulário. Pode até haver perguntas que são preenchidas inteiramente consultando o banco de dados.

Depois que o incidente de segurança é resolvido e movido para o estado **Revisão**, as avaliações são geradas para todos os usuários atribuídos e usuários que são adicionados diretamente da lista **Solicitar avaliações**.

O questionário pode ser uma ferramenta útil para coletar informações sobre o tratamento do incidente de segurança de várias fontes.

Durante a revisão, você pode adicionar mais usuários à lista ou remover usuários existentes da lista, a menos que eles já tenham começado a preencher o questionário. Se você adicionar novos usuários à lista, eles receberão as perguntas quando o registro for salvo. O incidente de segurança não pode ser encerrado até que todos os questionários tenham sido concluídos. Conforme os questionários são preenchidos por cada usuário, o relatório pós-incidente é gerado automaticamente (e gerado novamente) e exibido na guia **Revisão pós-incidente**.

Para iniciar uma revisão pós-incidente:

Procedimento

1. Crie um incidente de segurançaou abra um existente navegando até **Incidente de segurança** > **Incidentes** > **Atribuído a mim (ou Atribuído à equipe ou Incidentes não atribuídos)**.
2. Clique na guia **Análise pós-incidente**.
3. O campo **Solicitar avaliações** é padronizado para o indivíduo no campo **Atribuído a**.
   Clique no ícone de cadeado para adicionar outros usuários à lista de revisão. Depois que o campo é desbloqueado, as opções ficam disponíveis para adicionar ou remover vários usuários, funções ou inserir endereços de e-mail do usuário.
4. Ao concluir as entradas, clique no ícone de cadeado para bloquear o campo.

   Nota:
   Você também pode definir condições que, quando atendidas em um incidente de segurança, podem fazer com que usuários específicos sejam adicionados automaticamente ao campo **Solicitar avaliações** para esse incidente de segurança. Por exemplo, quando uma **Categoria** de incidente de segurança é alterada para **Phishing**, indivíduos específicos que têm experiência em ameaças de phishing podem ser adicionados à lista de revisão pós-incidente. Para obter mais informações, consulte Criar regras de atribuição de PIR.

5. Clique em **Atualizar**.
   Quando o incidente entra no estado **Revisão** (ou imediatamente, se já estiver no estado **Revisão**), cada um dos usuários na lista de revisão recebe uma notificação inicial por e-mail . Os lembretes são enviados conforme a data de vencimento se aproxima. Quando cada usuário acessa o questionário a partir do link de e-mail ou acessando **Análise pós-incidente** > **Minhas Revisões Pendentes**, as perguntas mostradas são extraídas de todas as categorias que se encaixam neste incidente de segurança. Se novos usuários forem

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

adicionados à lista de revisão antes do prazo, eles receberão notificações quando o incidente de segurança for salvo.

Conforme os usuários preenchem seus questionários, o relatório pós-incidente compila os dados e exibe o relatório na guia **Revisão pós-incidente**. Os dados do questionário são exibidos na guia **Descobertas**.

Criar categorias de questionário de revisão pós-incidente

Você pode usar as categorias de questionário que vêm com o sistema de base ou criar suas próprias categorias.

Antes de Iniciar

Função necessária: sn.si_admin

Por Que e Quando Desempenhar Esta Tarefa

Para criar uma nova categoria de perguntas:

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Análise pós-incidente**.
2. Clique **em Revisar perguntas**.
   Uma lista de categorias é exibida, junto com sua ordem e filtros que definem sob quais condições as perguntas são feitas (por exemplo, somente quando a categoria de incidente de segurança é `Atividade criminal`). Cada categoria é uma seção no questionário de revisão pós-incidente e as perguntas em cada categoria são incluídas somente quando o incidente de segurança corresponde ao filtro Condição. Por exemplo, para uma categoria de perguntas que se aplica somente a servidores Linux, você configuraria um filtro que selecionasse incidentes de segurança em que o tipo de recurso afetado fosse Servidor Linux. Nessa categoria, você criaria todas as perguntas necessárias quando um incidente de segurança estivesse em um servidor Linux. Você usa uma das categorias fornecidas no sistema de base ou cria uma nova categoria. Este procedimento pressupõe que você deseja criar uma nova categoria antes de definir perguntas.
3. Clique em **Novo** na lista de categorias.
4. Preencha os campos no formulário, conforme apropriado.

Incidente de segurança

Campo	Descrição
Nome	Nome da categoria que aparece no questionário de incidente de segurança.
Tipo	A análise pós-incidente é o padrão.
Criar Partes Interessadas	Não usado por Security Incident Response.
Tabela	Este campo é atribuído automaticamente quando o formulário é enviado.
Filtro	Insira a condição que determina quando as perguntas nesta categoria são usadas. Se um registro de incidente de segurança corresponder a este filtro, as perguntas serão incluídas em uma revisão pós-incidente para esse incidente de segurança. Os filtros podem usar qualquer dado no registro ou em outros registros vinculados a este registro. Por exemplo, o departamento do gerente do usuário solicitante.
Aplicação	Aplicação de escopo para o incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ponderação	Valor numérico que representa a importância dessa métrica relativa a outras métricas na mesma categoria. Por padrão, o peso é 10.
Total de métricas	Número de métricas usadas pela categoria.
Descrição	Descrição do questionário.

5. Clique em **Enviar** para salvar a categoria.

Redigir perguntas de análise pós-incidente

Você pode usar as perguntas que vêm com o sistema de base ou criar suas próprias perguntas.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Os métodos para coletar informações de revisão pós-incidente podem estar na forma de perguntas ou como dados coletados automaticamente usando scripts.

As perguntas podem depender das respostas a outras perguntas. Por exemplo, você pode perguntar se todos os logs necessários estavam disponíveis. Se a resposta for Não, faça uma pergunta de acompanhamento para verificar quais dos logs necessários não foram habilitados.

A coleta de dados com script, também chamada de métricas de script, coleta dados relacionados ao incidente de segurança por meio de scripts que você grava. Esta ação pode ir muito além dos dados no próprio registro de incidente de segurança. Por exemplo, uma métrica de script pode coletar o tempo de indisponibilidade recente de um servidor afetado por este incidente de segurança.

Por fim, você pode combinar os dois tipos. As perguntas podem ter valores padrão obtidos de um script ou simplesmente de um campo no registro de incidente de segurança. Ao usar um tipo de pergunta Resposta padrão de ..., você pode escolher se deseja que o usuário sempre responda à pergunta - com o valor padrão fornecendo a ele um valor inicial - ou se deseja que o usuário só faça a pergunta se o O script ou o campo aparece vazio.

Para criar uma nova pergunta:

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Análise pós-incidente**.
2. Clique na categoria para a qual você deseja criar uma nova pergunta.
3. Clique na guia **Métricas de avaliação**.
4. Clique em **Nova**.
   Você também pode clicar em uma pergunta existente para modificá-la.
5. Preencha os campos no formulário, conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de métrica

Campo	Descrição
Nome	Nome da métrica (pergunta ou script). Se a métrica for uma coleta de dados com script, este nome aparecerá no relatório pós-incidente.
Categoria	A categoria à qual a métrica pertence. O sistema preencherá automaticamente essa categoria se você criar uma métrica a partir do formulário Categoria de métrica. **Nota:** Você não poderá mudar a categoria se o campo **Depende de** estiver definido ou se outra métrica depender dessa métrica
Método	Indica o tipo de métrica, da seguinte forma: ○ *Assessment*: uma pergunta que não tem valor padrão. Existem vários tipos de dados que podem ser definidos no campo **Tipo de dados** na guia **Tipo** de campo, como caixas de seleção, listas de seleção e entrada de texto. ○ *Script*: métrica com script. Obtenha valores gravando um script personalizado. O método *Script* é compatível com os tipos de dados **Duração**, **Número**e **Percentual**. ○ *Default answer from field*: uma pergunta em que a resposta padrão vem de um campo selecionado no incidente de segurança. A seleção desta opção adiciona dois campos à guia **Geral** : ▪ *Default answer*: selecione o campo no incidente de segurança que contém a resposta padrão para a pergunta. Por exemplo, para a pergunta: "Quem relatou inicialmente este incidente?", o campo **Solicitado por** seria uma opção provável. ▪ *Ask question*: especifica quando fazer a pergunta: sempre ou somente se o campo **Resposta padrão** estiver vazio. Usando o exemplo acima, a pergunta seria feita se o campo **Solicitado por** estivesse vazio. ○ *Default answer from script*: uma pergunta em que a resposta padrão vem de um script. A resposta pode ser um número, uma cadeia de caracteres ou uma porcentagem. A guia **Geral** adiciona um campo: *Ask question*: como Especifica quando fazer a pergunta: sempre ou somente se o script não fornecer uma resposta padrão. O script é definido na guia **Tipo de campo**. **Nota:** Se você selecionar um **Tipo de dados** incompatível com o **Método**selecionado, o sistema mudará automaticamente o **Método** para um valor compatível.
Ponderação	[Obrigatório] Valor numérico que representa a importância dessa métrica relativa a outras métricas na mesma categoria. Por padrão, o peso é 10.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Esse campo ficará visível e será obrigatório somente se o **Tipo de dados** for **Data**, **Data/Hora** ou **Cadeia de caracteres**. Esses tipos de dados não são incluídos nos cálculos de resultados.
Pedido	[Obrigatório] Valor numérico que determina a ordem da pergunta de métrica em questionários de avaliação, em relação a outras perguntas de métrica na mesma categoria. A métrica com o menor valor de ordem aparece como a primeira pergunta na seção de categoria. Por padrão, a ordem é 100. **Nota:** Não importa qual valor de ordem você usa para métricas com o método de script, já que eles não aparecem em questionários.
Ativo	Caixa de seleção que determina se essa métrica é usada. Se a caixa de seleção não estiver marcada, será como se o registro de métrica não existisse.
Obrigatório	Marque a caixa que torna a pergunta de métrica obrigatória (selecionada) ou opcional (desmarcada) em questionários de avaliação. Os usuários não podem enviar questionários até que eles forneçam respostas válidas a todas as perguntas obrigatórias, que são indicadas por um indicador de status de campo vermelho. Este campo ficará visível somente se o campo **Depende de** estiver vazio e o tipo de dados não for **Caixa**de seleção.

6. Clique na guia **Geral** e preencha os campos, conforme apropriado.

Guia Geral

Campo	Descrição
Pergunta	Texto a ser usado como pergunta em questionários de análise de incidentes de segurança. Insira uma pergunta clara e direta que seja fácil de responder, como **Como contivemos o incidente**
Descrição	Informações sobre a métrica e o que ela avalia. Se o `Method` for **Avaliação**, inclua detalhes que ajudem os usuários a entender como responder à pergunta. Esse texto aparece como uma dica quando um usuário aponta para o texto da pergunta no questionário.
Depende de e Exibido quando	Selecione uma pergunta no campo **Depende de da** qual a pergunta atual depende. Por exemplo, a pergunta "Quais logs adicionais foram necessários?" depende da pergunta "Todos os logs necessários estavam disponíveis?" Em seguida, use o campo **Exibido quando** para identificar quando você deseja que a pergunta dependente apareça nos questionários. Por exemplo, se você quiser que a pergunta dependente seja feita somente quando o usuário responder **Não** à pergunta "Todos os logs necessários estavam disponíveis?" pergunta, selecione **Não** no campo **Exibido quando**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: O sistema evita a criação de dependências recursivas entre métricas. Por exemplo, se a Métrica A depender da Métrica B, a Métrica B não poderá depender da Métrica A.

7. Clique na guia **Tipo de campo** e preencha os campos, conforme apropriado.

Guia Tipo de campo

Campo	Descrição
Tipo de dados	O tipo de dados da resposta esperada da qual a lista de tipos disponíveis depende para o método selecionado. Se o método for **Avaliação**, o tipo de dados determinará como os usuários responderão à pergunta correspondente nos questionários. Se o método for **Script**, o tipo de dados determinará como o sistema calculará os resultados da avaliação. **Nota:** Se outra pergunta depender dessa métrica, você não poderá mudar o tipo de dados.
Respostas aleatórias	Caixa de seleção que determina se as opções de resposta para essa pergunta de métrica devem ser apresentadas em uma ordem aleatória sempre que um usuário abrir um questionário de avaliação que contém a pergunta. A preferência de resposta pode ser influenciada pela ordem em que as opções de resposta aparecem. Isso pode resultar em resultados tendenciosos. As opções de resposta de aleatoriedade podem ajudar a evitar essa tendência. Este campo ficará visível somente se você selecionar **Escala Likert** ou **Opção** no campo **Tipo de dados**.
Plug-in dependente	[Obrigatório se o *Method* for **Script**.] Plug-in que contém as tabelas consultadas no script. O sistema executará o script de métrica somente se o plug-in estiver ativo. Os valores padrão disponíveis são **Asset Management**, **CMDB**, **Core**, **Cost Management**, **Procurement**e **Software Asset Management**. Este campo ficará visível somente se o *Method* for **Script**. **Nota:** ○ Se o valor padrão do Núcleo for usado, o script será sempre executado. ○ Se você for um administrador, poderá adicionar mais opções de plug-ins ao campo.
Definição de escala	Configuração que determina se valores numéricos menores ou maiores são iguais a uma boa pontuação nos cálculos de resultados da avaliação. Selecione **Baixo** se valores numéricos menores forem melhores, como para uma métrica que mede o número de defeitos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	de um fornecedor. Selecione **Alto** se valores numéricos maiores forem melhores, como para uma métrica que mede a satisfação do usuário em uma escala de um a cinco. O valor padrão é **Alto**. Este campo ficará visível e será obrigatório se o *Data type* for **Data**, **Data/Hora**ou **Cadeia de caracteres**. Os resultados para esses tipos de dados não são incluídos nos cálculos de resultados.
Mínimo	O valor numérico mais baixo a ser usado como uma opção de resposta em avaliações ou como um valor com escala em uma métrica com script. Esse campo é visível e obrigatório somente quando determinados tipos de dados são selecionados. Se o tipo de dados for **Opção** ou **Escala Likert**, este campo será somente leitura e será definido automaticamente com base na menor definição de métrica *Value*.
Máximo	Maior valor numérico a ser usado como opção de resposta ou valor com escala. Esse campo é visível e obrigatório somente quando determinados tipos de dados são selecionados. Se o tipo de dados for **Opção** ou **Escala Likert**, este campo será somente leitura e será definido automaticamente com base na maior definição de métrica *Value*.
Script	Script que obtém as informações do sistema desejadas. O script tem uma variável de entrada, definida com o ID do incidente de segurança (primário), e três variáveis de saída possíveis definidas pelo script, string_result, scaled_result e actual_result. Quando o tipo de dados é Cadeia de caracteres, somente string_result é necessário. Este campo é visível e obrigatório quando o *Method* é **Script**ou o valor padrão vem de um script.
Modelo	Um conjunto predefinido de respostas comuns a serem usadas para a pergunta. Por exemplo, um modelo de frequência provavelmente iniciaria com um valor de "Nunca" e iria até o valor superior de "Sempre". Este campo será visível e obrigatório somente se o *Data type* for **Modelo**. **Nota:** Se outra métrica depender dessa métrica, você não poderá mudar o modelo.

8. **Opcional:** Ao concluir as entradas, clique em **Atualizar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar regras de atribuição de PIR

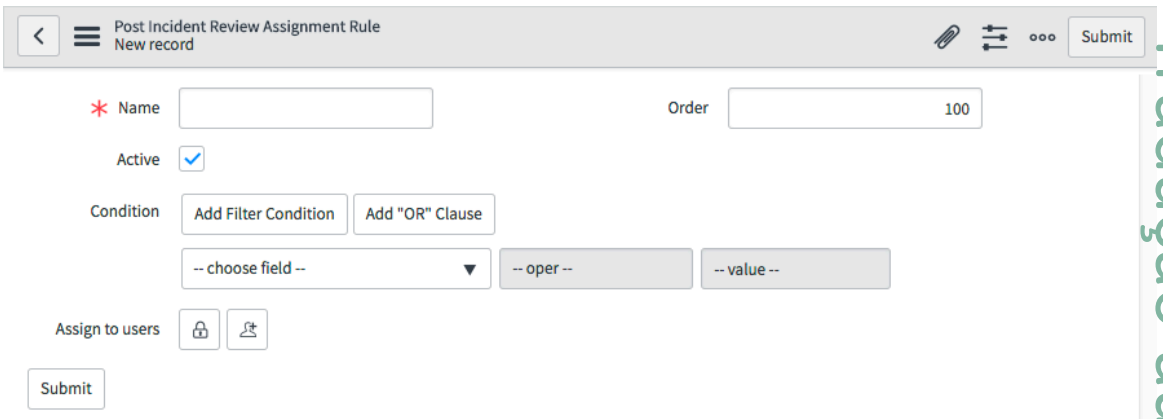
Além de adicionar manualmente a lista de avaliação de revisão pós-incidente de usuários para um incidente de segurança, você pode definir regras de atribuição para adicionar usuários automaticamente à lista.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.manager, sn_si.analyst

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Administração** > **Análise pós-incidente - Configuração de avaliações**.
2. Faça uma busca detalhada na seção **Regras de atribuição de usuário**.
3. Clique em **Configurar**.
4. Clique em **Nova**.



5. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta regra de atribuição.
Ativo	Marque esta caixa de seleção para tornar a regra ativa.
Ordem	Insira um valor numérico para especificar onde essa regra deve aparecer na lista de regras de atribuição. Os números mais baixos aparecem na parte superior da lista. **Nota:** Somente a primeira regra de atribuição correspondente é executada e somente os usuários definidos nessa regra são adicionados à lista de avaliação.
Condição	Use o Construtor de condição para definir as condições que devem ser atendidas no incidente de segurança para que esta regra seja executada. Para obter mais informações, consulte o exemplo abaixo.
Atribuir a usuários	Clique no ícone de cadeado para adicionar usuários à lista de revisão. Depois que o campo é desbloqueado, as opções ficam disponíveis para adicionar ou remover vários usuários, funções ou inserir endereços de e-mail do usuário.

6. Clique em **Enviar**.

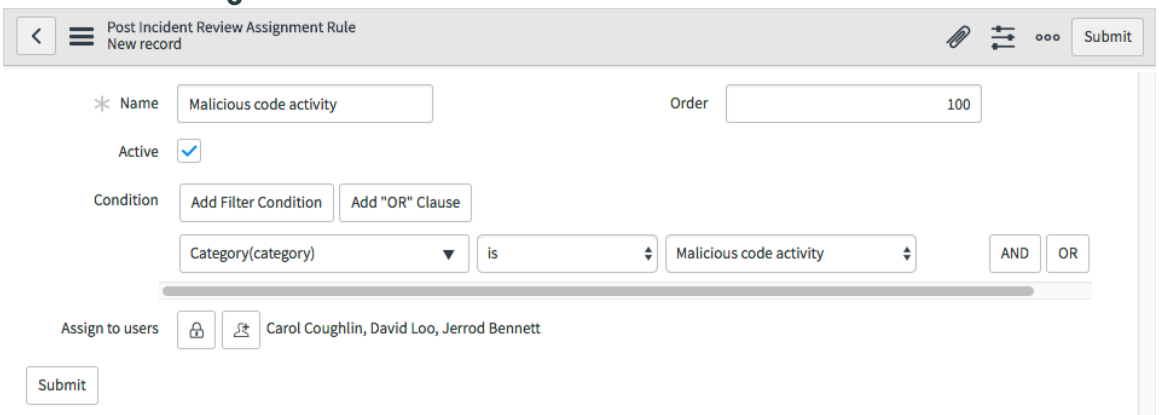
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example: Atividade de código malicioso

Na regra de atribuição de revisão pós-incidente mostrada aqui, quando um incidente de segurança com o campo **Categoria** definido como **Atividade de código mal** -intencionado faz a transição para o estado **Revisão**, os três usuários identificados (que são especialistas em lidar com atividade de código mal-intencionado) são adicionados à lista de usuários que receberão o questionário de revisão pós-incidente para este incidente de segurança.

Atividade de código malicioso



Fechar incidentes de segurança

Quando um incidente de segurança faz a transição para o estado Revisão, é possível fechá-lo e inserir um código de fechamento apropriado. Os códigos de fechamento podem ser pesquisados posteriormente para facilitar a localização.

Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

Nota:
Nas versões anteriores do Security Incident Response, os usuários podiam fechar incidentes de segurança ou solicitações como spam. Na versão Istanbul, a opção de spam não está mais disponível. Incidentes ou solicitações de segurança de spam podem ser cancelados ou excluídos, conforme apropriado.

Procedimento

1. Se o incidente de segurança que você deseja fechar ainda não estiver aberto, navegue até **Incidente de segurança** > **Incidentes** > **Mostrar Todos os Incidentes**e localize o incidente de segurança que você deseja fechar.

   Nota:
   Se houver avaliações de revisão pós-incidente que não tenham sido concluídas para este incidente de segurança, o incidente de segurança não poderá ser encerrado. Retornar a **Incidente de segurança** > **Análise pós-incidente** > **Todas as Revisões Incompletas**, localize as revisões que estão incompletas e peça aos revisores para concluir suas revisões ou cancelar as avaliações restantes.

2. Clique na guia **Informações de fechamento** e preencha os campos, conforme apropriado.

Incidente de segurança

Campo	Descrição
Criar artigo de conhecimento	Selecione este campo para criar automaticamente um rascunho de artigo da base de conhecimento que contenha o conteúdo da revisão pós-incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Código de fechamento	Selecione o código de fechamento que melhor descreve o motivo pelo qual você está fechando este incidente de segurança. ○ Investigação concluída ○ Ameaça mitigada ○ Vulnerabilidade corrigida ○ Vulnerabilidade inválida ○ Não resolvido ○ Falso positivo
Encerrado por	Exibe o usuário que encerrou o incidente de segurança depois que o registro foi atualizado.
Encerrado	Exibe a data e a hora do fechamento depois que o registro é atualizado.
Anotações de encerramento	Insira anotações adicionais que descrevam o resultado do encerramento deste incidente de segurança.

3. Clique em **Atualizar**.
4. O usuário atribuído pode alterar manualmente o **Estado** para **Encerrado**.
   Quando um incidente primário é encerrado, todas as tarefas de resposta pertencentes ao incidente secundário são canceladas. Se não houver outros tipos de tarefas, o incidente secundário também será fechado.

Adicionar informações de fechamento a um incidente de segurança

Quando um incidente de segurança está no estado Revisão ou Encerrado, você pode inserir informações de fechamento.

Antes de Iniciar

Função necessária: sn_si.basic

Procedimento

1. Se ainda não estiver aberto, abra o incidente de segurança que você deseja atualizar.
2. Clique na guia **Registros relacionados**.
3. Preencha os campos, conforme necessário.

Campo	Descrição
Criar artigo de conhecimento	Marque esta caixa de seleção para gerar um artigo de conhecimento usando o conteúdo do relatório pós-incidente.
Código de fechamento	Selecione o código de fechamento que melhor descreve o motivo para fechar o incidente de segurança.
Encerrado por	[Somente leitura] Exibe o usuário que encerrou o incidente de segurança.
Encerrado	[Somente leitura] Exibe a data e a hora em que o incidente de segurança foi encerrado.
Anotações de encerramento	Como o incidente de segurança foi encerrado, incluindo lições aprendidas, resolução e assim por diante.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em qualquer uma das seguintes guias para atualizar ainda mais o incidente de segurança:
   - Detalhes de Incidentes
   - Análise pós-incidente
5. Ao concluir as entradas, clique em **Enviar**.

Restringir o acesso a incidentes de segurança

Gerencie o acesso dos incidentes de segurança que contêm informações confidenciais. Você pode impor restrições de incidente de segurança para determinar quem pode acessar um determinado incidente e limitar o acesso somente a usuários ou grupos específicos.

Antes de Iniciar

Função necessária: sn_si.admin

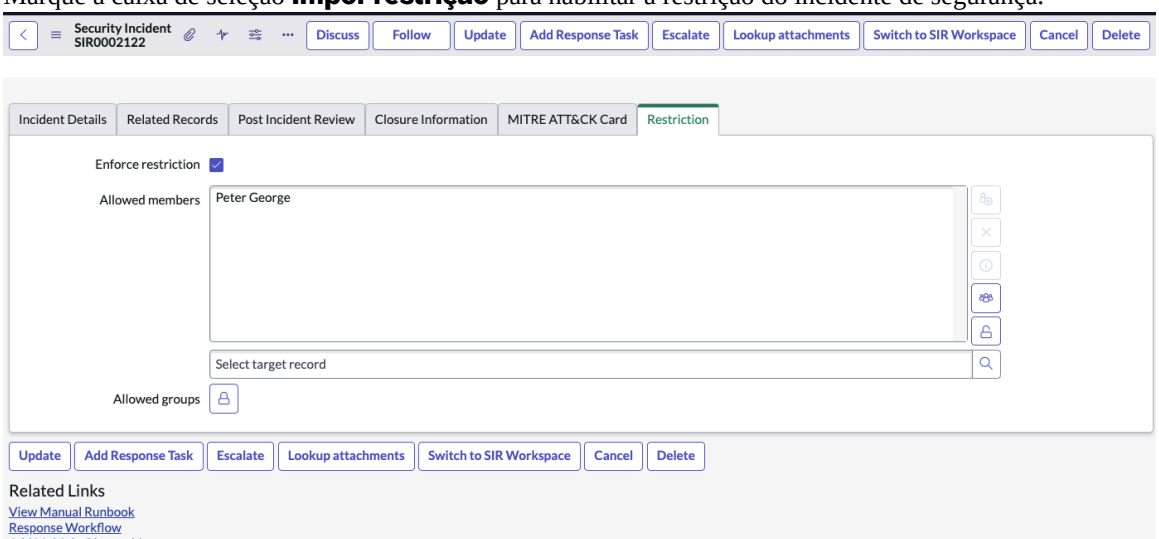
Por Que e Quando Desempenhar Esta Tarefa

As restrições de incidente de segurança permitem que você oculte incidentes de segurança críticos de serem acessados por outros usuários em uma organização específica. Essas restrições permitem que você forneça uma maneira mais granular de controlar os incidentes de segurança que um usuário pode acessar. Você pode impor uma restrição de incidente de segurança habilitando a caixa de seleção **Impor restrição** e selecionando os usuários ou grupos que têm permissão para acessar o incidente de segurança específico.

Depois de impor a restrição em incidentes de segurança específicos e limitar o acesso a determinados usuários ou grupos, todos os outros usuários restantes em sua organização não poderão acessar esses incidentes de segurança, mesmo que eles pesquisem um incidente de segurança restrito específico.

Procedimento

1. Abra um incidente de segurança que você deseja restringir.
2. Se você estiver usando a IU clássica, execute o seguinte:
   a. Clique na guia **Restrição**.
   b. Marque a caixa de seleção **Impor restrição** para habilitar a restrição do incidente de segurança.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. No campo Membros permitidos, clique no para selecionar os usuários que podem acessar o incidente de segurança.

d. Selecione o para adicionar a si mesmo como o usuário permitido.

e. Selecione o ícone para adicionar ou remover usuários.

f. No campo Grupos permitidos, clique no para selecionar os grupos que podem acessar o incidente de segurança.

g. Selecione o ícone para adicionar ou remover grupos.

Nota:
Depois que a caixa de seleção **Impor restrição** estiver habilitada para o incidente de segurança, somente o sn_si.admin e os membros ou grupos permitidos terão acesso ao incidente de segurança.

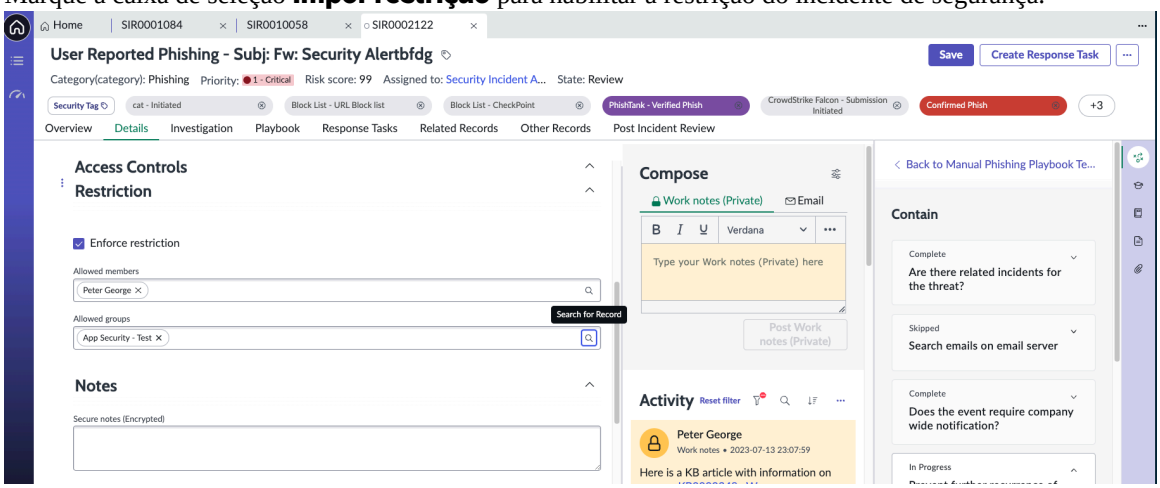
h. Clique em **Atualizar**.

3. Se você estiver usando o Espaço de SIR, execute o seguinte:

a. No incidente de segurança, clique na guia **Detalhes**.

b. Role para baixo e clique na seção **Restrição**.

c. Marque a caixa de seleção **Impor restrição** para habilitar a restrição do incidente de segurança.



d. No campo Membros permitidos, selecione os usuários que podem acessar o incidente de segurança usando a opção Pesquisar.

e. No campo Grupos permitidos, selecione os grupos que podem acessar o incidente de segurança usando a opção Pesquisar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Depois que a caixa de seleção **Impor restrição** estiver habilitada para o incidente de segurança, somente o sn_si.admin e os membros ou grupos permitidos terão acesso ao incidente de segurança.

f. Clique em **Salvar**.

Gerenciar ameaças à segurança usando o Espaço do analista de segurança

Security Incident Response inclui uma nova interface de usuário chamada Espaço do analista de segurança que apresenta ferramentas poderosas para auxiliar na análise, incluindo o playbook, a exibição de exibição e as guias para trabalhar em vários incidentes de segurança.

Criadas especificamente para analistas de segurança, as ferramentas poderosas em Espaço do analista de segurança permitem que você analise o volume cada vez maior de dados associados a incidentes de segurança. E as ações automatizadas reduzem significativamente o tempo de investigação de incidentes de segurança, o que pode ser a diferença entre interromper um ataque e sofrer uma violação.

Antes de usar o Espaço do analista de segurança

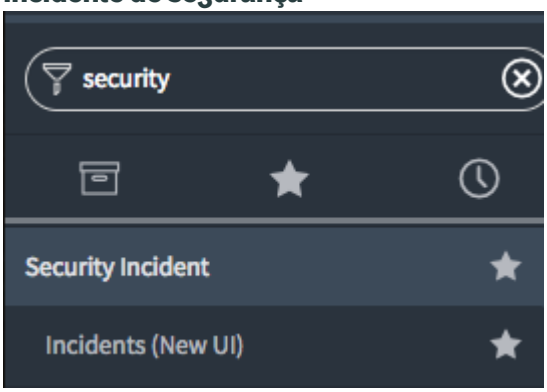
Antes de começar a usar o Espaço do analista de segurança, você deve garantir que sua instância tenha pelo menos o London Patch 3 instalado, que você tenha as funções corretas definidas e tenha baixou a aplicação de IU do Security Incident Response da ServiceNow Store.

Nota:
Se sua instância estiver executando uma versão anterior ao London Patch 3, você deverá solicitar o plug-in Security Incident Response UI por meio do sistema de atendimento ao cliente HI.

Como acessar o Espaço do analista de segurança

Para acessar este novo espaço, navegue até **Incidente de segurança** > **Incidentes (Nova IU)**.

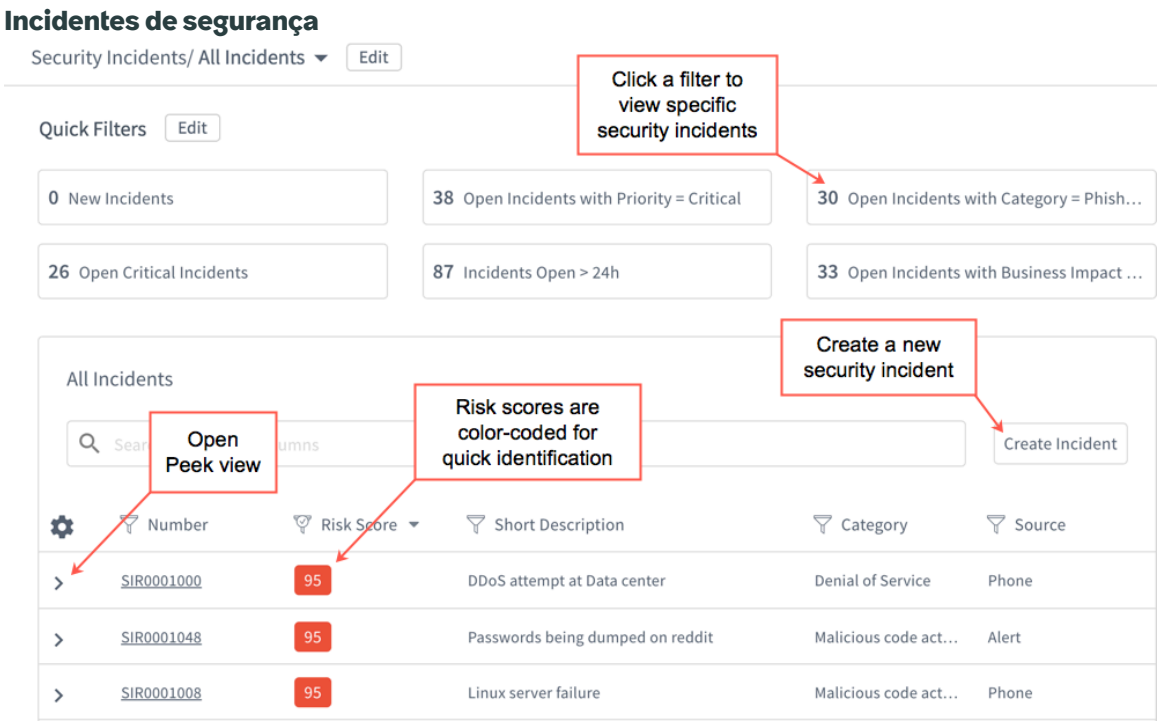
Incidente de segurança



O espaço é aberto em uma guia separada do navegador.

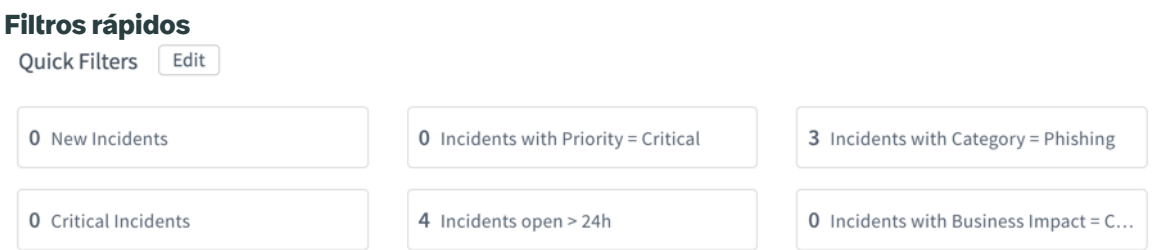
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Localize os incidentes de segurança que você deseja analisar com filtros rápidos

O Espaço do analista de segurança fornece várias ferramentas para filtrar a lista de incidentes de segurança para que você possa encontrar rapidamente os incidentes de segurança que deseja analisar. Os Filtros rápidos permitem selecionar um subconjunto dos incidentes de segurança com base nos critérios do filtro.



Basta clicar no filtro rápido que você deseja usar.

Nota:
Você pode clicar em um botão **Editar** para identificar quais filtros rápidos você deseja exibir na tela da lista. Um mínimo de um filtro deve ser selecionado, até um máximo de seis.

Você pode definir filtros rápidos adicionais, bem como filtros primários para Espaço do analista de segurança, usando o ambiente clássico. Para obter mais informações, consulte Configurar filtros primários e secundários para Espaço do analista de segurança.

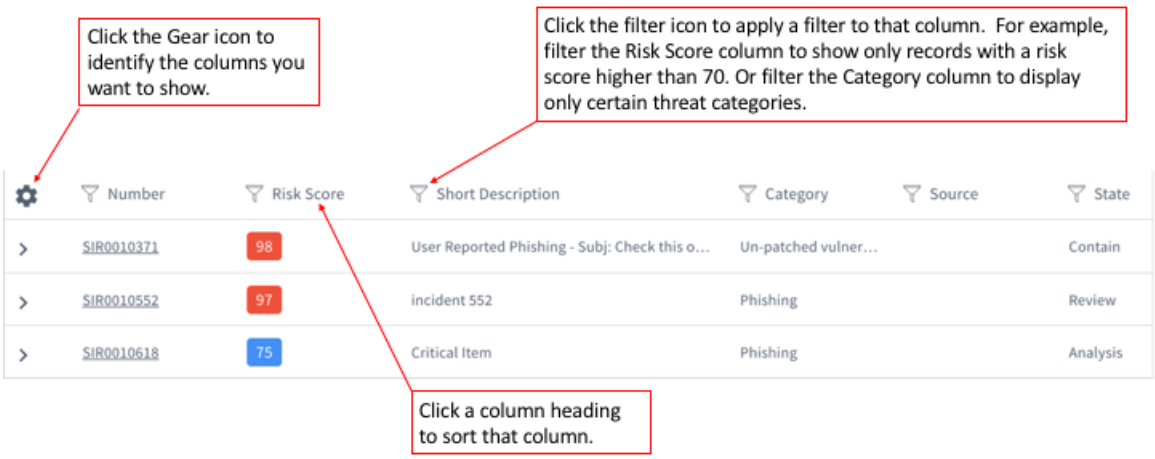
Personalizar a lista de incidentes de segurança

Assim como acontece com todas as listas em sua instância, o Espaço do analista de segurança fornece ferramentas para personalizar a lista e classificar as informações exibidas para atender às suas necessidades de análise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

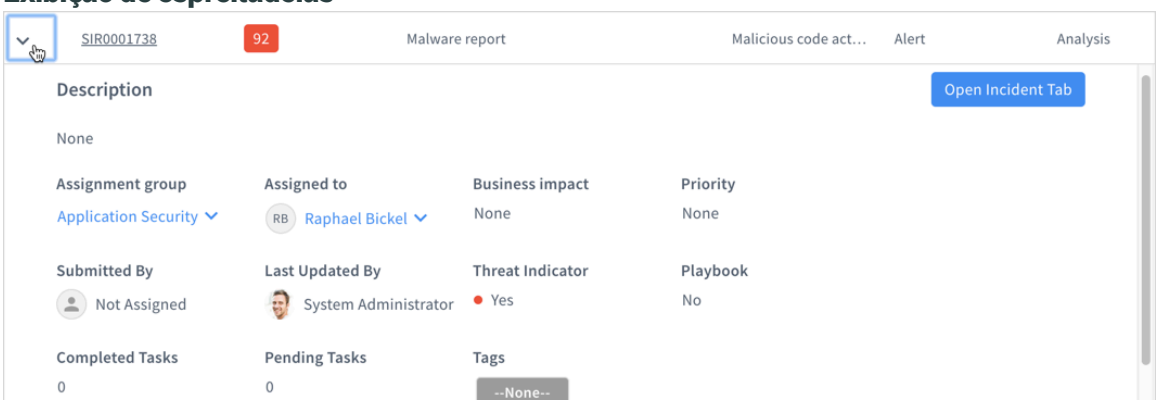
Personalizar a lista de incidentes de segurança



Economize tempo com a exibição Peek

Antes de abrir um registro de incidente de segurança, você pode economizar tempo usando a exibição Peek. Este recurso permite que você localize rapidamente artefatos de segurança vitais sem precisar recarregar a página inteira. Basta clicar no ícone **>** à esquerda de um número de incidente de segurança para dar uma olhada.

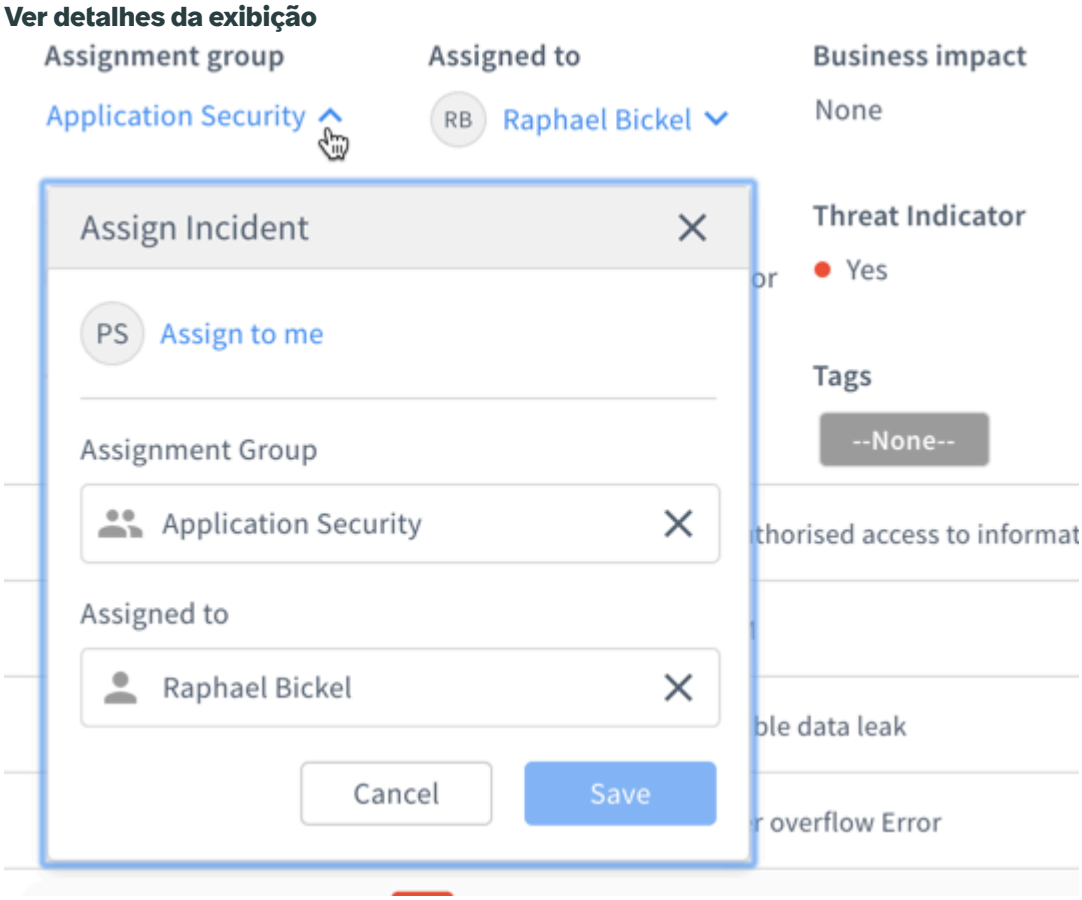
Exibição de espreitadelas



A exibição peek fornece um snapshot de informações vitais em uma única exibição. Essa exibição pode economizar um tempo valioso ao trabalhar com vários incidentes. Você pode clicar nas setas para baixo em determinados campos para fazer atualizações instantâneas, como atribuir um grupo de atribuição ou um analista específico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Executar ações rápidas em um incidente de segurança

Depois de selecionar e abrir um incidente de segurança específico, você pode executar ações de economia de tempo no registro.

- Se o incidente de segurança estiver aberto, clique no ícone **Editar registro** para fazer mudanças rápidas em qualquer um dos campos. Se o registro for encerrado, você poderá alterar somente seu marcador.
- Clique em **Gerenciar anexos** para anexar arquivos ao incidente de segurança. Você também pode baixar ou remover arquivos anexados e editar a criptografia aplicada aos anexos.
- Clique em **Compor e-mail** para enviar um e-mail rápido a um colega. Os e-mails podem ser de forma livre ou você pode enviar e-mails predefinidos selecionados em uma lista de modelos. Os e-mails enviados e as respostas recebidas são capturados na Linha do tempo do incidente.

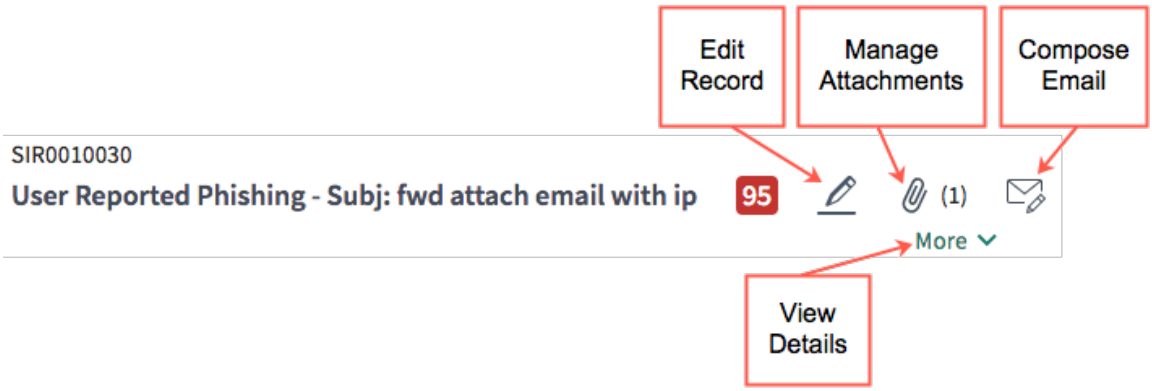
  Nota:
  Você pode criar modelos personalizados que contenham conteúdo reutilizável para e-mails e notificações por e-mail. As variáveis podem ser usadas para inserir informações específicas do incidente ou alerta de segurança, como a linha de assunto, a prioridade ou a categoria de ameaça. Use a tabela Incidente de segurança [sn_si_incident] para e-mails e notificações por e-mail relacionados a Security Incident Response. Para obter mais informações, consulte Modelos de e-mail .

- Clique em **Mais** para exibir um snapshot rápido do incidente de segurança, como a descrição, o impacto nos negócios e a prioridade. Você também pode clicar na seta para baixo nos campos **Grupo de atribuição** e **Atribuído a** para fazer mudanças instantâneas nesses campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

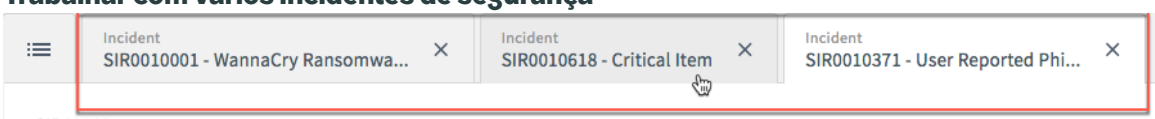
Grupo de atribuição



Trabalhar com vários incidentes de segurança

A interface com guias permite que você mantenha vários incidentes de segurança abertos simultaneamente para que você possa alternar entre eles com um único clique. Isso pode economizar tempo e permitir que você tenha uma visão geral quando forem identificadas ameaças de várias origens.

Trabalhar com vários incidentes de segurança



Exibir informações de análise nas guias de incidente de segurança

Quando você abre um registro de incidente de segurança, três guias são mostradas:

- Visão geral
- Explorar
- Linha do tempo do Incidente

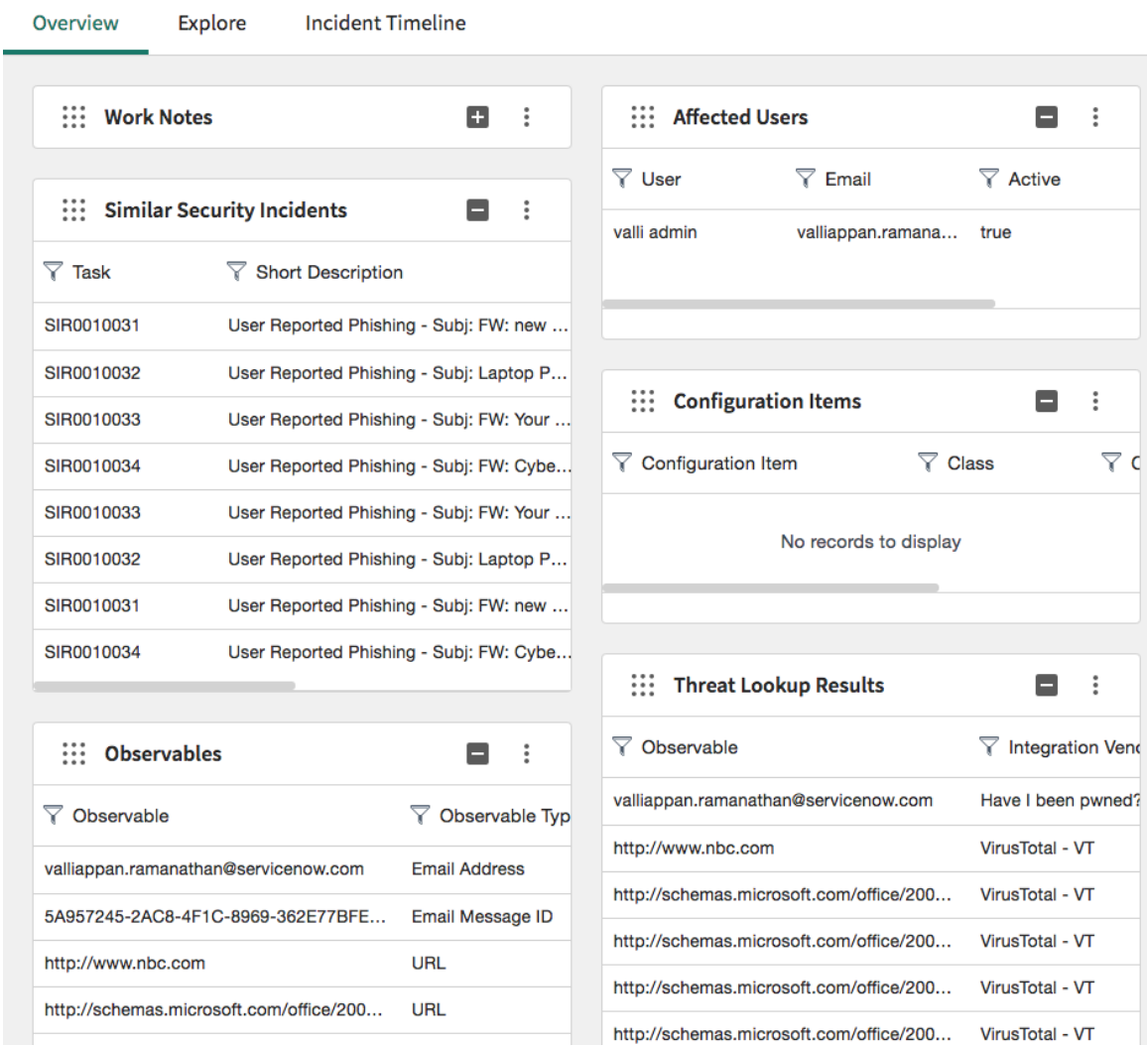
Guia Visão geral

Use a guia **Visão geral** para exibir informações em um incidente de segurança em um único local. Não há necessidade de abrir outro aplicativo ou console.

Tradução automática

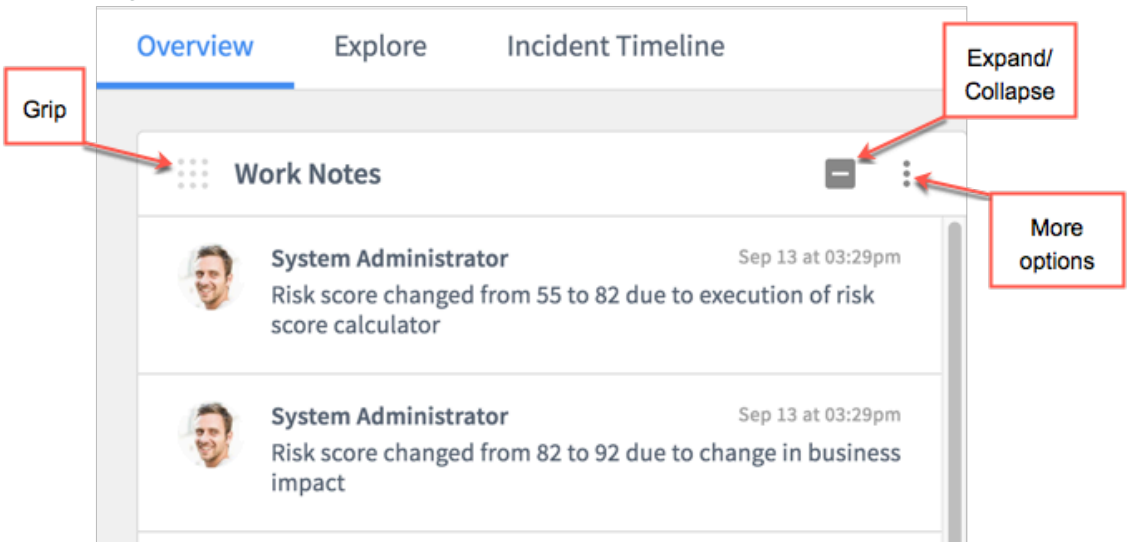
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral



Os blocos exibidos na guia **Visão geral** são personalizáveis. Você pode recolhê-los e expandi-los conforme necessário e movê-los arrastando o ícone de **Punho**. Clique no ícone **Mais opções** para excluir um bloco ou mudar o texto do título.

Guia Visão geral



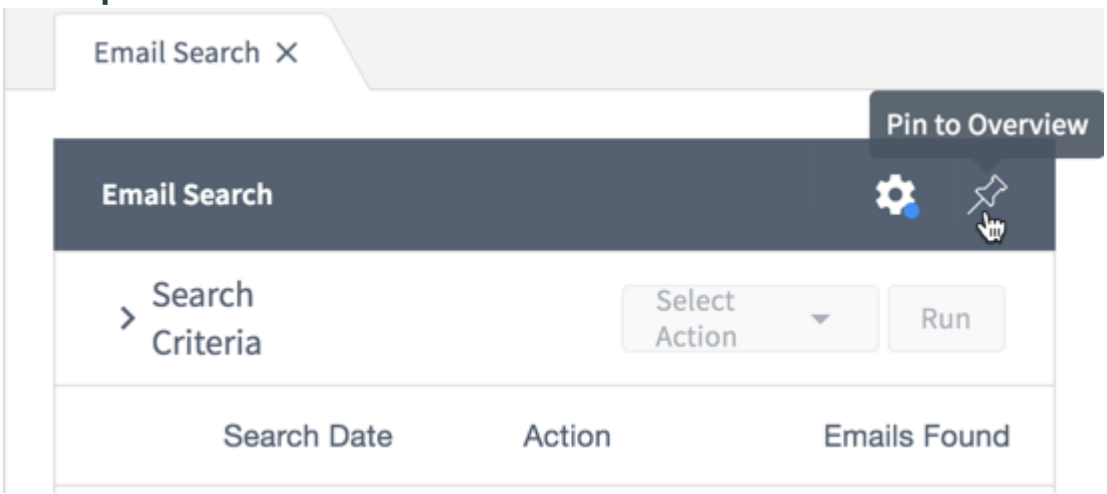
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Explorar

Configure os blocos exibidos na guia **Visão geral** usando a guia **Explorar**. Basta selecionar os blocos que você deseja exibir no painel esquerdo e clicar no ícone **Fixar**. Os blocos fixados aparecem automaticamente na guia **Visão geral**.

Guia Expor



O painel esquerdo da guia **Explorar** inclui uma ampla variedade de informações que você pode exibir na guia **Visão geral**. Por exemplo, expanda **Observáveis** para exibir essas listas relacionadas.

- Observáveis
- Resultados da Pesquisa de ameaças
- Resultados da verificação de segurança
- Pesquisas de domínio
- Aprimoramento de Observável

Listas relacionadas adicionais estão disponíveis em **Usuários**, **Itens de configuração**e **Incidentes**.

Guia Linha do tempo do incidente

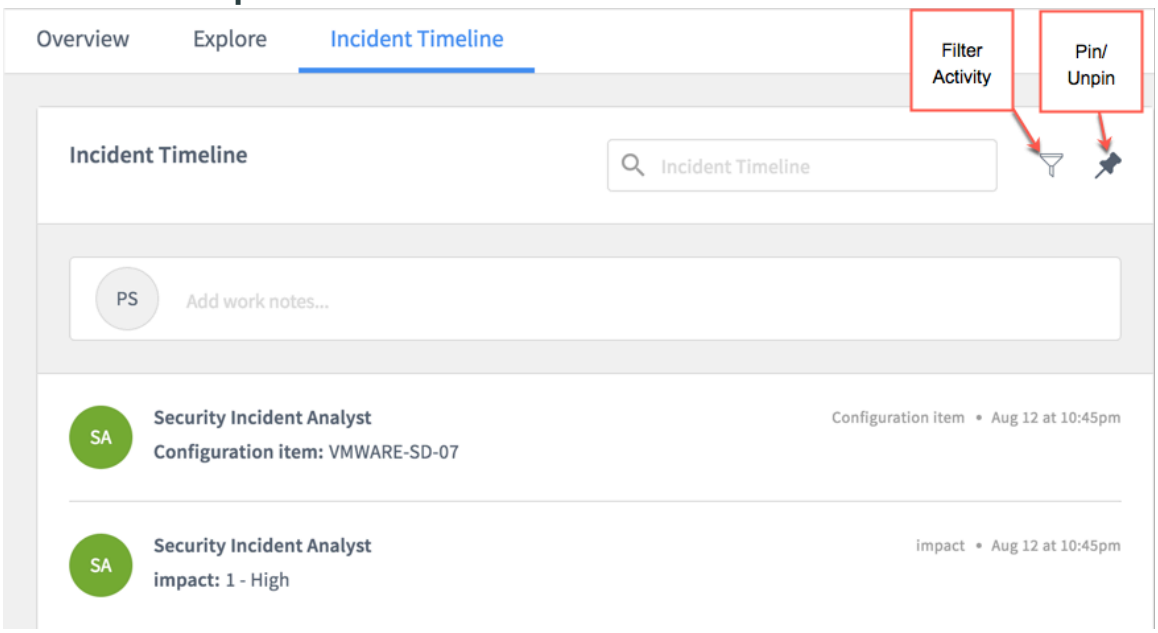
Use a guia **Linha do tempo do incidente** durante sua investigação para fins de acompanhamento. Toda vez que uma ação é realizada em um incidente de segurança, o sistema a registra na Linha do tempo do incidente.

- Você também pode adicionar anotações de trabalho manualmente à linha do tempo, digitando-as na caixa **Adicionar anotações de trabalho** e clicando em **Publicar**.
- Você pode pesquisar uma atividade específica da linha do tempo usando a caixa Pesquisar.
- O ícone **Filtrar atividade** permite exibir somente os tipos de atividade da linha do tempo que você deseja ver (por exemplo, somente incidentes criados por um analista específico).
- Você pode adicionar ou remover a Linha do tempo do Incidente na guia **Visão geral** usando o ícone **Fixar/Desmarcar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Linha do tempo do incidente



Manipular incidentes de segurança usando o Playbook

Resolva determinados tipos de ameaças à segurança passo a passo usando os Playbooks do analista de segurança internos. Por exemplo, um analista pode usar o playbook para resolver ataques de phishing e ameaças causados por atividades de código mal-intencionado. Para obter mais informações, consulte Resolver ameaças à segurança com o playbook.

Resolver ameaças à segurança com o playbook

Use o Playbook para resolver determinados tipos de ameaças à segurança passo a passo. Por exemplo, você pode resolver ataques de phishing e ameaças causados por atividade de código mal-intencionado usando playbooks.

Antes de Iniciar

Função necessária: sn_si.admin ou admin

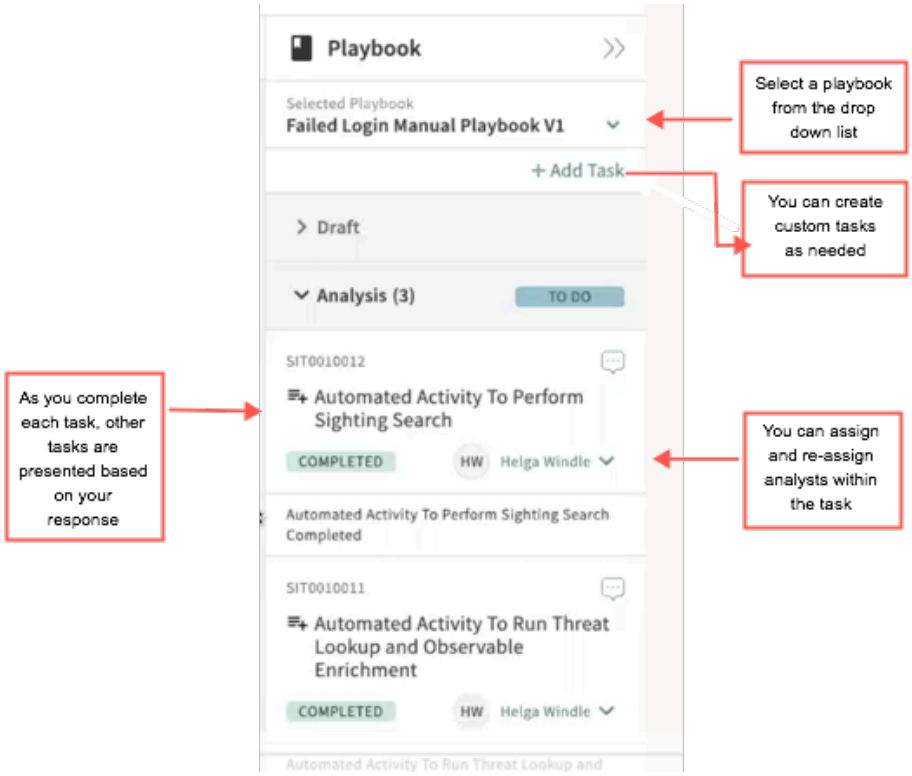
Por Que e Quando Desempenhar Esta Tarefa

Cada grupo de tarefas (Análise, Contenção e assim por diante) orienta você em uma série de perguntas e outras atividades para resolver a ameaça.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

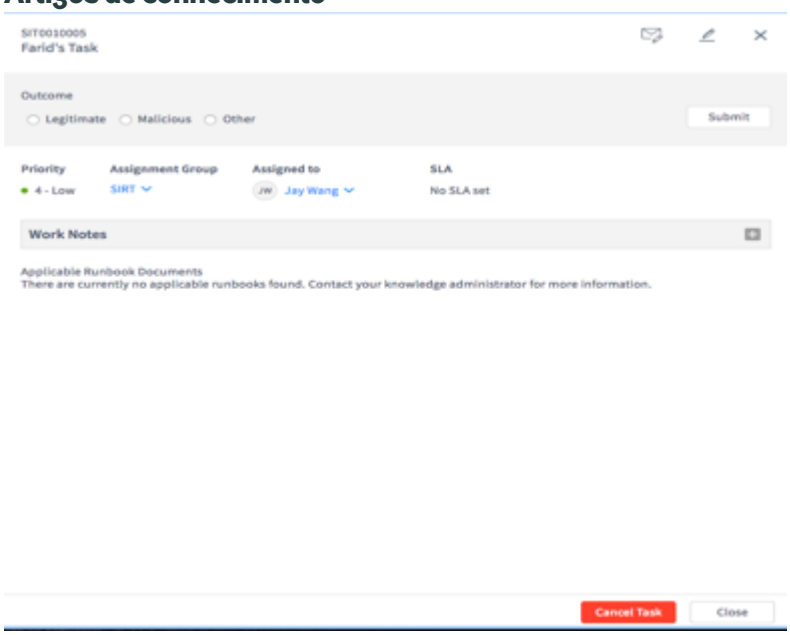
Playbook



Conforme você trabalha em cada tarefa, insira anotações de trabalho para ajudar a analisar ataques semelhantes no futuro. Depois que uma ameaça é identificada, você também pode usar as informações do playbook para colocar a ameaça em quarentena, isolar ativos afetados de forma semelhante e remover malware.

Os artigos de conhecimento, incluídos em cada tarefa, fornecem dicas e outras informações para ajudá-lo a executar as etapas necessárias.

Artigos de conhecimento



O sistema básico inclui artigos de conhecimento para cada uma das tarefas do playbook. Você pode, no entanto, escrever seus próprios artigos de conhecimento e associá-los a tarefas do playbook.

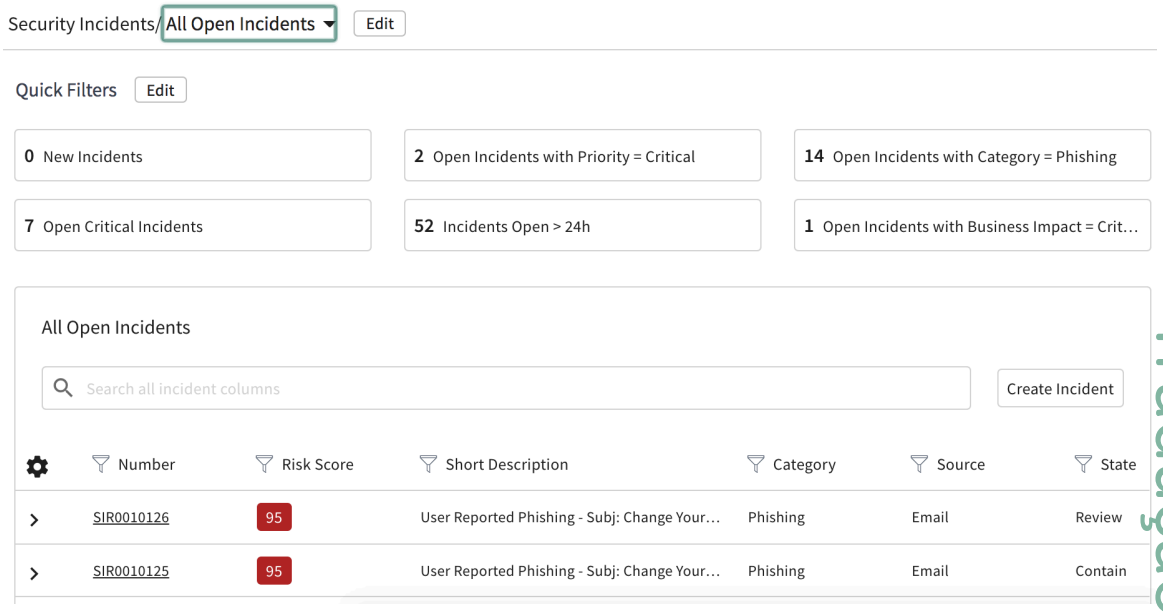
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Para obter um exemplo de como usar o playbook para analisar e resolver uma ameaça específica, consulte Resolver ataques de phishing relatados pelo usuário com o playbook.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes (Nova IU)**.
   A tela Incidentes de segurança mostra os incidentes de segurança que foram atribuídos a você.



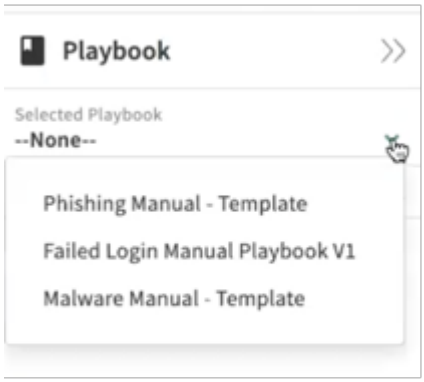
2. Você pode clicar na lista de seleção **Atribuído a mim** para selecionar um filtro diferente, como todos os incidentes abertos ou todos os incidentes não atribuídos.
   Como alternativa, você pode clicar em um dos Filtros rápidos para exibir incidentes de segurança de um tipo específico, como somente incidentes críticos.
3. Clique no incidente de segurança que você deseja analisar.

   Considere priorizar incidentes de segurança com pontuações altas de risco.

4. Se o painel do playbook na borda direita da tela estiver fechado, clique no ícone do playbook ( ) para abri-lo.
   Se nenhum playbook for atribuído ao incidente de segurança, você poderá selecionar um playbook na lista de seleção Playbook selecionado, conforme mostrado abaixo:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você também pode atribuir um playbook diferente ao incidente de segurança. Para incluir um playbook na lista de seleção Playbook selecionado ou para mudar o playbook para um incidente de segurança, consulte Habilitar playbooks para seleção do analista para obter detalhes.

O playbook específico para o tipo de ameaça à segurança é aberto. Ele é dividido em categorias de tarefas semelhantes. Por exemplo, você usa as tarefas no grupo de **análise** para determinar a validade e o escopo da ameaça. O grupo **Contêm** inclui tarefas para isolar a ameaça a um usuário ou ativo específico. As tarefas no grupo **Erradicar** orientam você no processo de remoção do malware ou recriação da imagem do host.

5. Clique no primeiro grupo (**Análise**) e na primeira tarefa no playbook.
6. Siga os avisos da tarefa.
   - Algumas tarefas fazem uma pergunta, como "O e-mail faz parte da campanha?" Realize a análise necessária para responder à pergunta e selecione **Sim** ou **Não**.
   - Se você definiu artigos de conhecimento e os associou a tarefas do playbook, os artigos serão exibidos quando você começar a trabalhar em uma tarefa.
   - Algumas tarefas são transicionais. Eles simplesmente instruem você a executar uma ação, como adicionar observáveis a um incidente de segurança. Depois de concluir a ação, clique em **Marcar como concluído**.

   Conforme você conclui as tarefas, as tarefas subsequentes são apresentadas a você com base nas escolhas feitas. Grupos esmaecidos (como **Recuperar**, **Revisar**e assim por diante) podem ser ativados por suas escolhas.
7. Continue trabalhando em cada tarefa apresentada a você até concluir todas as tarefas para resolver a ameaça e fechar o incidente de segurança.

Tópicos relacionados

Adicionar uma tarefa personalizada ao playbook

Resolver ataques de phishing relatados pelo usuário com o playbook

O playbook de Phishing orienta você nas tarefas necessárias para analisar e resolver um ataque de phishing relatado por um dos funcionários da sua empresa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

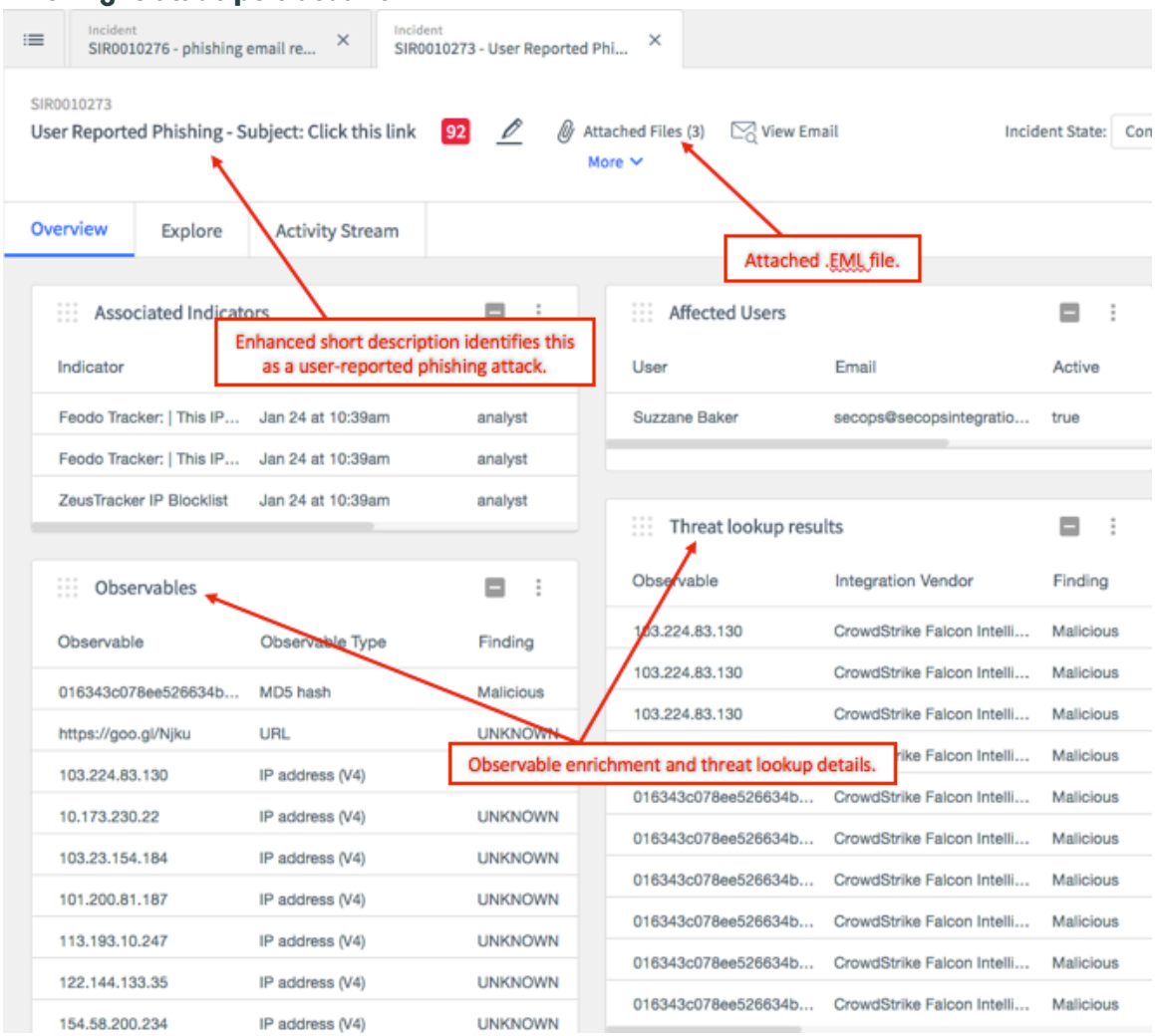
Como os incidentes de segurança são criados a partir de ataques de phishing relatados pelo usuário

Durante a configuração do Security Incident Response, o administrador do sistema cria uma série de regras de correspondência de e-mail que podem identificar e-mails que contêm sinais de um ataque de phishing. Quando os funcionários recebem um e-mail suspeito que contém os sinais comuns de um ataque de phishing (conforme definido por suas políticas de segurança), eles podem enviá-lo como um anexo .EML para o endereço de e-mail de phishing definido pela sua organização.

Quando o e-mail é recebido no endereço de e-mail de phishing, o anexo .EML é analisado e suas informações são comparadas com as regras de correspondência de e-mail. Se uma correspondência for encontrada, um incidente de segurança contendo as seguintes informações será criado:

- A descrição resumida inclui Phishing relatado pelo usuário, seguido pelo assunto real do e-mail de origem.
- O arquivo .EML é anexado ao incidente de segurança.
- Se o .EML contiver observáveis, eles serão analisados e as pesquisas de aprimoramento e ameaça serão realizadas automaticamente.

Phishing relatado pelo usuário

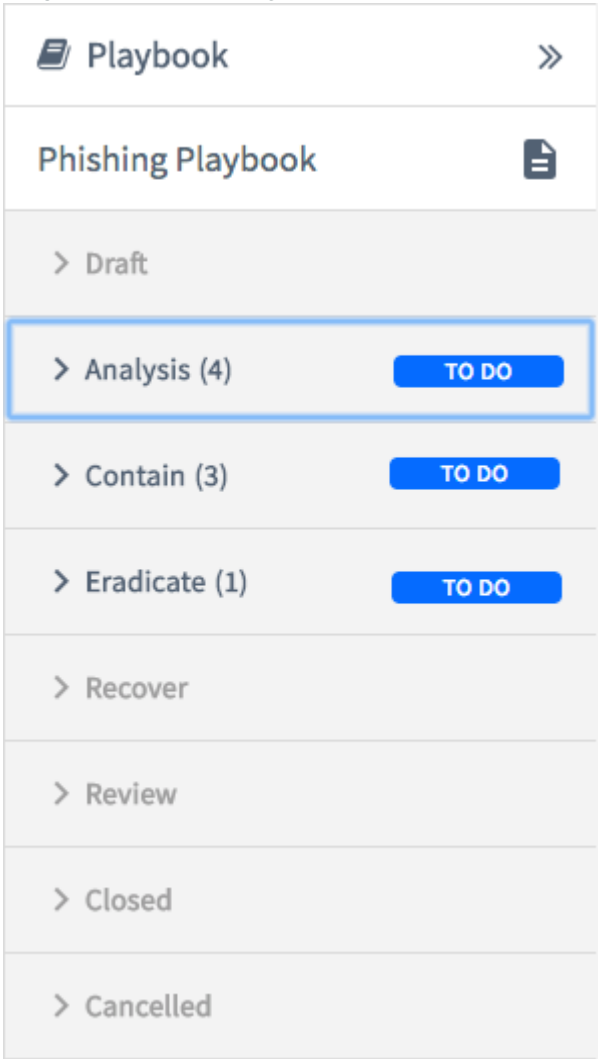


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando um incidente de segurança de categoria de phishing é aberto, o Playbook de phishing é disponibilizado automaticamente. Basta clicar no ícone do playbook ( ) para abrir o playbook.

Playbook de phishing



O playbook de Phishing contém tarefas para ajudá-lo a analisar, conter e erradicar uma ameaça de phishing. As tarefas são organizadas em estados (por exemplo, **Análise**, **Contêm**e assim por diante). Quando todas as tarefas de um estado forem concluídas, o playbook guiará você para o próximo estado.

Analisando detalhes do incidente de segurança

Quando o incidente de segurança está no estado Análise, você recebe tarefas para executar a investigação básica do incidente, incluindo:

- Determinar a validade do incidente.
- Estude o impacto da possível ameaça.
- Coordenar uma resposta eficaz ao incidente.

Conforme você trabalha nas tarefas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Familiarize-se com os artigos de conhecimento.
- Abra o anexo de e-mail e examine-o em busca de sinais de elementos de phishing comuns.
- Analise os resultados da pesquisa de ameaças.

Contendo o incidente de segurança

Quando o incidente de segurança está no estado **Contêm**, você recebe tarefas para revisar os detalhes do e-mail. Para garantir que as ameaças não possam entrar na sua organização, atualize as defesas da rede, na forma de assinaturas e regras do Sistema de defesa contra intrusão (IDS) e do Sistema de prevenção de intrusão (IPS).

Conforme você trabalha nas tarefas:

- Tome ações para limitar os impactos da ameaça, como isolar os dispositivos afetados.
- Examine os observáveis anexados ao e-mail.
- Determine se algum conteúdo de e-mail está associado a uma ameaça conhecida, incluindo:
  - URL
  - Remetente do e-mail
  - URL de phishing
  - Endereço IP do servidor SMTP do remetente

Erradicando o malware

Depois de implantar assinaturas e regras atualizadas em sua solução antivírus, use as tarefas no estado **Erradicar** para determinar se o malware está presente e trate-o de acordo.

Conforme você está trabalhando nas tarefas:

- Verifique os endpoints dos dispositivos afetados quanto à presença de malware.
- Remova qualquer malware encontrado.
- Como último recurso, limpe e crie novamente a imagem dos dispositivos host.

Revisando o incidente de segurança

Se você determinou que um ataque de phishing foi um alarme falso ao executar as tarefas de análise, o incidente de segurança passa para o estado **Revisar** e você precisa notificar os usuários para que eles saibam que é seguro abrir o anexo de e-mail.

Fechando o incidente de segurança

Quando todas as tarefas no playbook forem concluídas, o incidente de segurança será movido para o estado **Encerrado**. Você deve inserir comentários de encerramento antes que o incidente possa ser encerrado.

Como cancelar um incidente de segurança

Quando um incidente de segurança está no estado **Revisão** e você informou com sucesso os usuários de que o e-mail não é uma ameaça, o estado **Cancelado** se torna ativo e você pode cancelar o incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A tarefa de recuperação não é usada no playbook de phishing.

Associar um artigo de conhecimento a uma tarefa do playbook

Ao analisar as ameaças à segurança usando o playbook Security Incident Response, você pode exibir artigos de conhecimento para cada tarefa, se definida pela sua organização. Se os artigos de conhecimento não estiverem presentes, você poderá criá-los e associá-los a tarefas do playbook.

Antes de Iniciar

Ao usar o playbook em Security Incident Response, anote o texto associado a cada tarefa. Por exemplo, a primeira tarefa na categoria Phishing é **O alerta foi enviado pelo funcionário?** Esta é a descrição resumida da tarefa e você precisa deste texto (exatamente como ele aparece no playbook) para associar um artigo de conhecimento à tarefa.

Função necessária: sn_sir.knowledge_admin e sn_si.admin ou admin

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança** > **Catálogo e Conhecimento** > **Conhecimento**.
2. Crie e publique um artigo de conhecimento para uma tarefa específica do playbook.
3. Navegar até **Incidente de segurança** > **Runbook manual** > **Criar Novo Runbook**.
4. Crie um runbook, preenchendo as seguintes informações:

Campo	Descrição
Artigo de conhecimento	Selecione o artigo de conhecimento publicado que você deseja associar à tarefa do playbook.
Tabela	Selecione Security Incident Response Tarefa [sn_si_task].
Condição	Defina o construtor de condição como: ○ **Opção:** selecione **Descrição resumida**. ○ **Operador:**Selecione **é**. ○ **Valor de entrada:** insira a descrição resumida da tarefa, exatamente como ela aparece no playbook.

5. Clique em **Enviar**.
   Na próxima vez em que você executar o playbook e selecionar esta tarefa, o artigo de conhecimento associado será exibido.

Tópicos relacionados

Criar um artigo de conhecimento de incidente de segurança

Criar um runbook do Security Incident Response

Adicionar uma tarefa personalizada ao playbook

O sistema de base Espaço do analista de segurança inclui uma série de tarefas para cada categoria de ameaça. Você pode criar tarefas personalizadas que atendam às necessidades exclusivas do seu sistema ou dos clientes.

Tradução automática

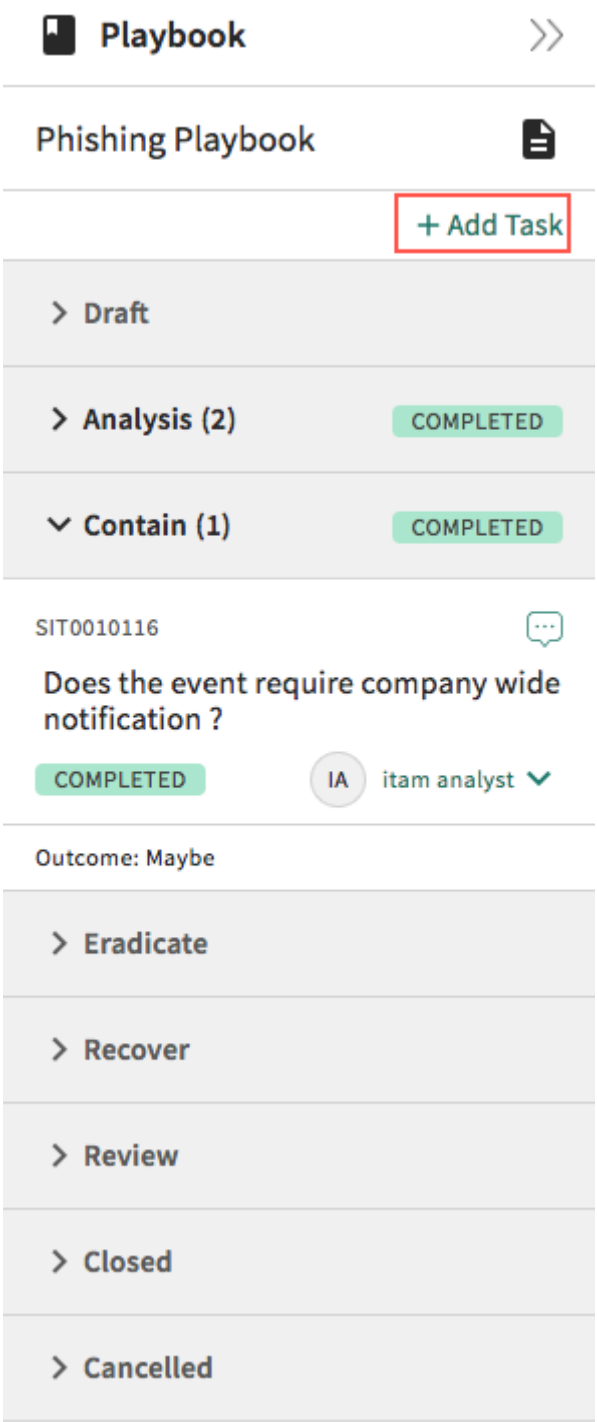
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.basic ou security_admin

Procedimento

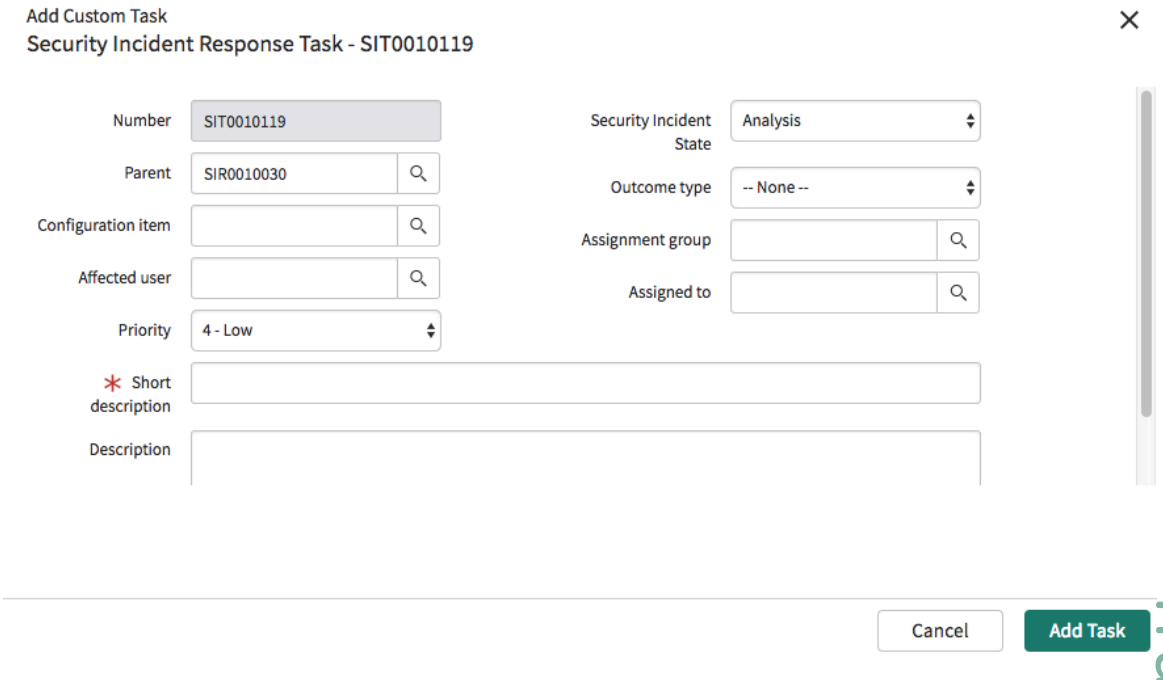
1. Com o playbook aberto, clique em **Adicionar tarefa**.



A tela Adicionar tarefa personalizada é aberta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Preencha os campos, conforme necessário.

Campo	Descrição
Número	[Somente leitura] O número da tarefa do incidente de segurança gerado automaticamente.
Primário	O número do incidente de segurança relacionado.
Item de configuração	O item de configuração afetado pelo problema de segurança, se houver.
Usuário afetado	O usuário afetado pelo problema de segurança, se houver.
Prioridade	Selecione a prioridade usada para determinar quando esta tarefa deve ser realizada.
Estado do Incidente de segurança	O estado atual da tarefa de resposta de segurança. Você pode selecionar um estado futuro, se necessário.
Tipo de resultado	Se você tiver a função sn_si.basic, selecione **Sim/Não** como o tipo de resultado. Se você tiver a função security_admin, poderá criar um tipo de resultado personalizado com vários valores de saída personalizados. Por exemplo, você pode definir uma tarefa com valores dependentes com base na categoria de ameaça. Para obter mais informações, consulte Listas de seleção
Grupo de atribuição	O grupo de atribuição do qual o trabalhador atribuído será selecionado.
Atribuído a	O indivíduo atribuído para executar a tarefa.
Descrição resumida	Uma descrição da tarefa do playbook de incidente de segurança.
Descrição	Insira uma descrição para a tarefa selecionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Ao concluir as entradas, clique em **Adicionar tarefa**.
   A tarefa é inserida no playbook seguindo a tarefa atual.

Pesquisas de detecções sobre ataques de phishing e malware relatados pelo usuário

Realize pesquisas de vistas em e-mails ou observáveis para determinar com que frequência determinados tipos de ataques, como ataques de phishing ou comunicações com um IP ou URL mal-intencionado, ocorrem em sua rede. Cada ocorrência é considerada uma vista. As pesquisas de vistas para observáveis devem ser configuradas para seus armazenamentos de log ou para a gestão de informações e eventos de segurança (SIEM).

Como usar o recurso de pesquisa de vista para localizar usuários com phishing e rastrear observáveis de phishing e malware no armazenamento de logs em sua rede.

Assista a este vídeo de três minutos para saber como usar o recurso de pesquisa de vista para localizar usuários phishing e rastrear observáveis de phishing e malware no armazenamento de logs em sua rede.

Os termos a seguir são usados para descrever ataques de phishing relatados pelo usuário:

- Usuário phishing: um usuário que recebeu um e-mail de phishing.
- Usuário vítima: um usuário que interagiu com o URL de phishing, normalmente clicando em um link no e-mail de phishing. Esta ação potencialmente expõe as credenciais ao invasor.

Ao começar a analisar um incidente de phishing, você pode Executar uma pesquisa de vistas de e-mail ou Executar uma pesquisa de vistas de observável para identificar outros usuários em sua organização que foram afetados pelo mesmo ataque de phishing. Pesquise seus armazenamentos de log para identificar usuários com phishing e vítimas. Depois de identificar a lista de usuários afetados, crie incidentes de segurança secundários para executar procedimentos de resposta do incidente abrangentes usando as ferramentas disponíveis em Security Incident Response.

Nota:
Você também pode usar a seguinte abordagem para executar uma pesquisa de vistas:

- Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes** e clique em um incidente de segurança.
- Clique em **Mostrar IoC** em Links relacionados. Uma lista de observáveis é exibida.
- Selecione um observável na lista e, na lista **Ações**, selecione uma das seguintes opções:
  - Executar pesquisa de detecções no tráfego da web
  - Executar pesquisa de detecções no tráfego de e-mail
- Especifique o intervalo de tempo e clique em **Pesquisar** para executar uma pesquisa de vistas.

Configurações de pesquisa de vista salvas

Configure pesquisas de vista e crie configurações salvas para SIEMs ou outros armazenamentos de log para instâncias de observáveis para determinar a presença de observáveis mal-intencionados em seu ambiente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Pesquisas salvas e consultas no local são compatíveis somente com a integração do Splunk.

Tópicos relacionados

Criar registros de configuração de pesquisa de vistas

Realizar uma pesquisa de detecções de e-mail para ataques de phishing relatados pelo usuário

Pesquise usuários que receberam e-mails de phishing com base em observáveis, como assunto do e-mail, nome do remetente ou ID da mensagem. Você pode conter e erradicar esses e-mails de phishing da sua organização.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Pesquise os logs de tráfego de e-mail do Splunk para coletar a lista de destinatários de um e-mail suspeito. A pesquisa pode ser realizada usando o remetente do e-mail, o ID da mensagem de e-mail ou o assunto do e-mail associado a um incidente de segurança como critério.

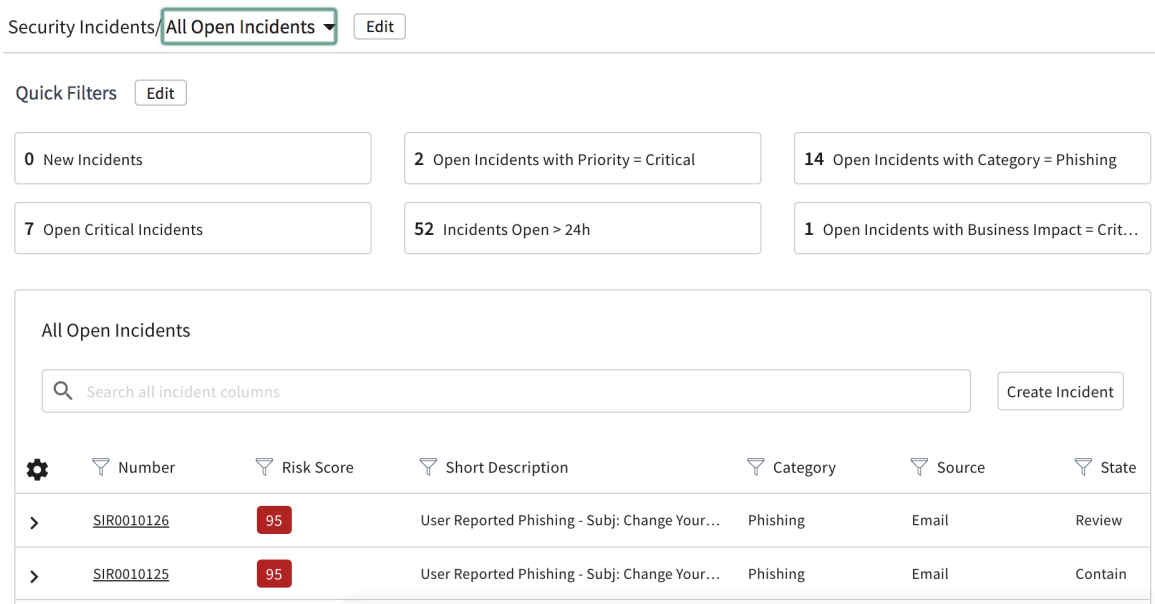
Nota:

- Esta implementação de pesquisa de vistas para observáveis baseados em e-mail foi testada somente com o armazenamento de log do Splunk Enterprise.
- Os eventos de log do Splunk devem ser compatíveis com o modelo de informação comum (CIM) para que a consulta de pesquisa de vistas retorne resultados precisos.

Procedimento

1. Para ver os incidentes de segurança atribuídos à sua equipe, navegue até **Incidente de segurança** > **Incidentes (Nova IU)**.
2. Na lista **Incidentes de segurança**, selecione um dos filtros, como todos **os incidentes abertos**, **todos os incidentes atribuídos a você**ou **todos os incidentes**.

   Para exibir incidentes de segurança de um tipo específico, como incidentes críticos ou e-mails de phishing, clique em um dos **Filtros rápidos**.

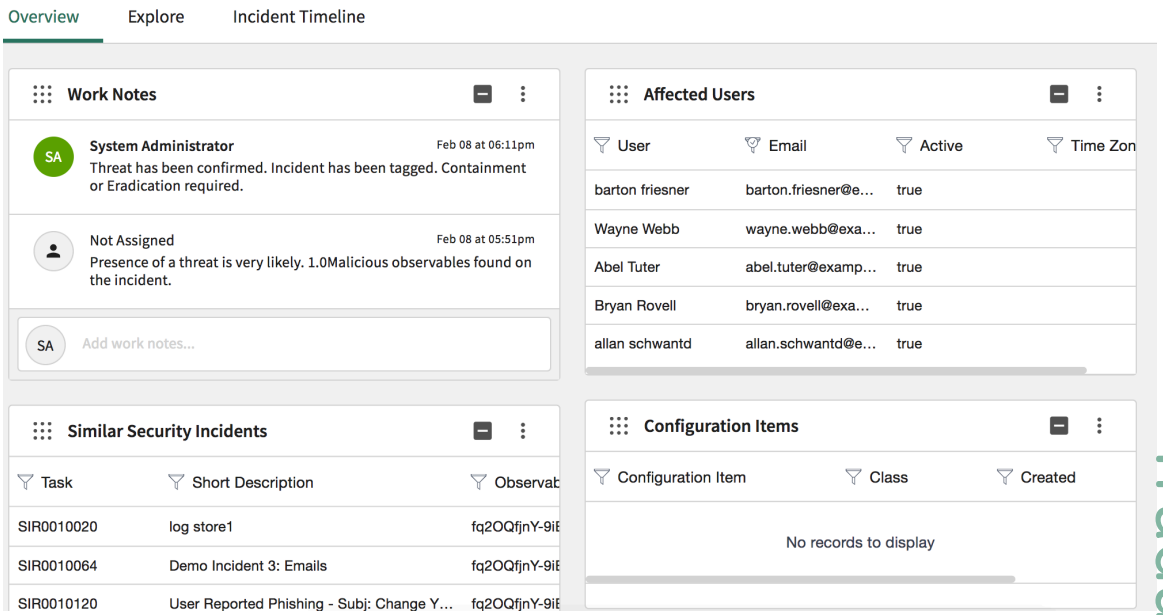


Tradução automática

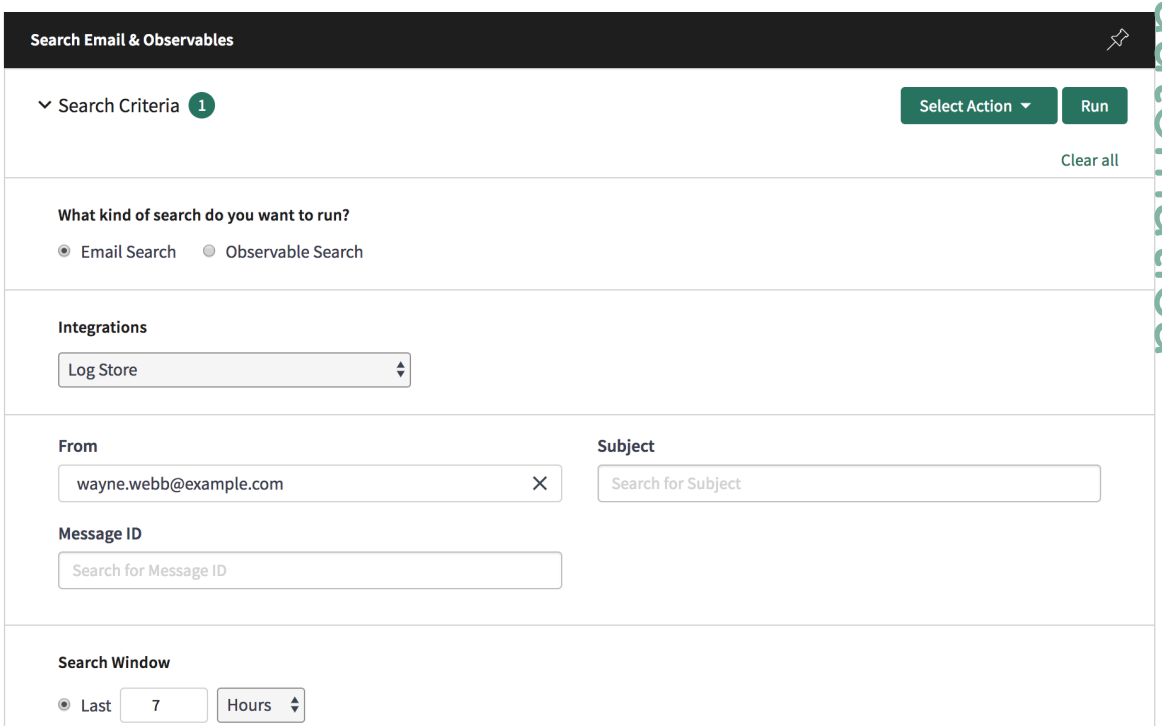
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique no incidente de segurança que você deseja analisar.

   A guia Visão geral fornece uma visão geral do incidente de segurança, incluindo uma lista de observáveis, usuários afetados e incidentes de segurança semelhantes.



4. Clique na guia **Explorar**.
5. Em **Dados do incidente**, navegue até **Investigação** > **Pesquisar e-mail e observáveis**.



6. Expanda a seção Critérios de pesquisa.
7. Selecione **Pesquisa de e-mail** como o tipo de pesquisa que você deseja executar e especifique o restante dos critérios de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de critérios de pesquisa

Campo	Descrição
Integrações	Tipo de integrações. Selecione **Armazenamento de logs** na lista. **Nota:** Este recurso é compatível somente com o armazenamento de log do Splunk.
De	Endereço de e-mail completo do remetente (por exemplo, jane.doe@example.com).
ID da Mensagem	ID da mensagem de e-mail do armazenamento de log.
Assunto	Assunto do e-mail de phishing.
Janela de Pesquisa	Janela de tempo para a pesquisa (por exemplo, as últimas 24 horas).

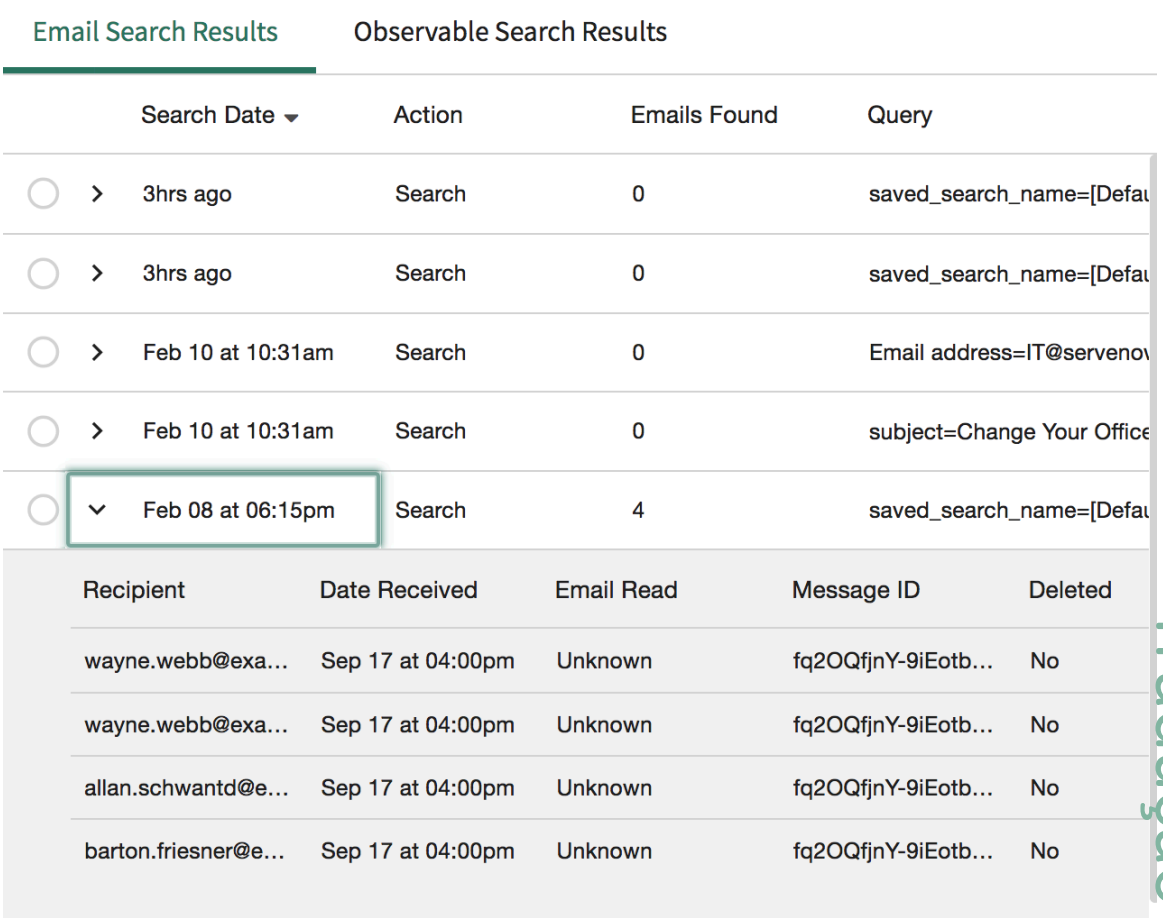
8. Na lista **Selecionar ação**, selecione **Pesquisar** e clique em **Executar**.

   O armazenamento de log do Splunk é pesquisado usando os critérios inseridos e os usuários visados pelo ataque de phishing são mostrados na guia **Resultados da pesquisa de e-mail**. O número total de e-mails de phishing e os detalhes de cada e-mail, incluindo a data de recebimento do e-mail, o destinatário e o ID da mensagem, são exibidos.

9. Para exibir a lista de usuários que receberam o e-mail de phishing, clique no símbolo **>** na coluna Data de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



10. Para exibir uma lista de usuários que receberam o e-mail, navegue até **Usuários** > **Usuários afetados**.

A coluna Usuário Phished identifica os destinatários do e-mail.

Nota:
A página Usuários afetados mostra somente os registros de usuário que estão presentes na instância da ServiceNow.

11. Para investigar melhor os usuários que são alvos do ataque de phishing, siga estas etapas:

a. Marque as caixas de seleção ao lado dos nomes de usuário.

b. Na lista, selecione **Criar incidente de segurança secundário**e clique em **Executar**.
Uma mensagem é exibida para mostrar que um incidente de segurança secundário foi criado. Para exibir os incidentes de segurança secundários associados a um incidente primário, clique na guia **Explorar** e navegue até **Incidentes** > **Incidentes de segurança secundários**.

Resultado
A lista de usuários com phishing é exibida.

Realizar uma pesquisa de vistas observáveis para ataques de phishing e malware relatados pelo usuário

Realize pesquisas de detecções em observáveis para descobrir quantos usuários visitaram um site mal-intencionado ou suspeito em um período específico.

Antes de Iniciar
Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você pode executar uma pesquisa de tráfego de rede em observáveis, como o URL, o host de destino ou o endereço IP de destino associado a um incidente de segurança.

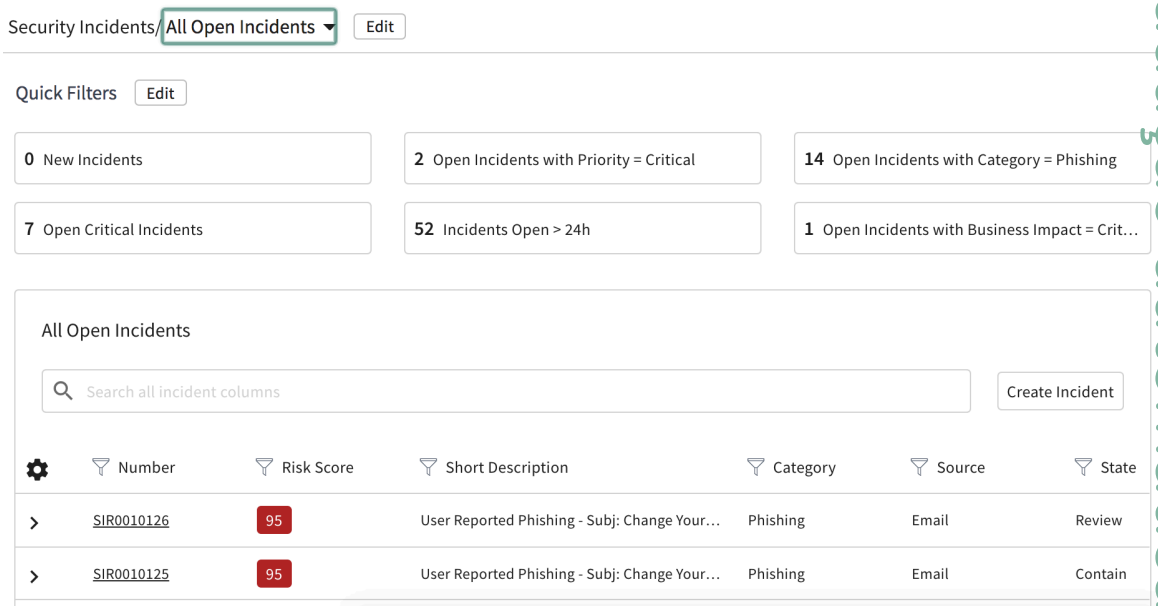
Nota:

- Esta implementação de pesquisa de vistas para observáveis foi testada somente com o armazenamento de log do Splunk Enterprise.
- Os eventos de log do Splunk devem ser compatíveis com o modelo de informação comum (CIM) para que a consulta de pesquisa de vistas retorne resultados precisos.

Procedimento

1. Para ver os incidentes de segurança atribuídos à sua equipe, navegue até **Incidente de segurança** > **Incidentes (Nova IU)**.
2. Na lista **Incidentes de segurança**, selecione um filtro diferente, como Todos os **incidentes atribuídos a mim**, **Todos os incidentes em aberto**ou **Todos os incidentes**.

   Para exibir incidentes de segurança de um tipo específico, como incidentes críticos ou e-mails de phishing, clique em um dos **Filtros rápidos**.

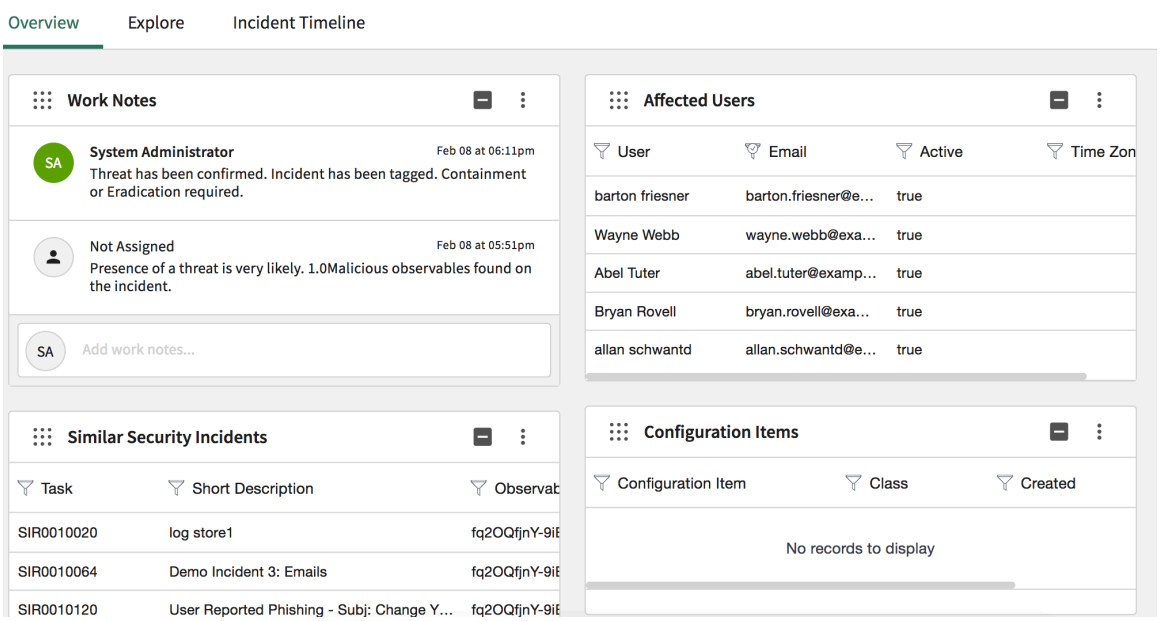


3. Clique no incidente de segurança que você deseja analisar.

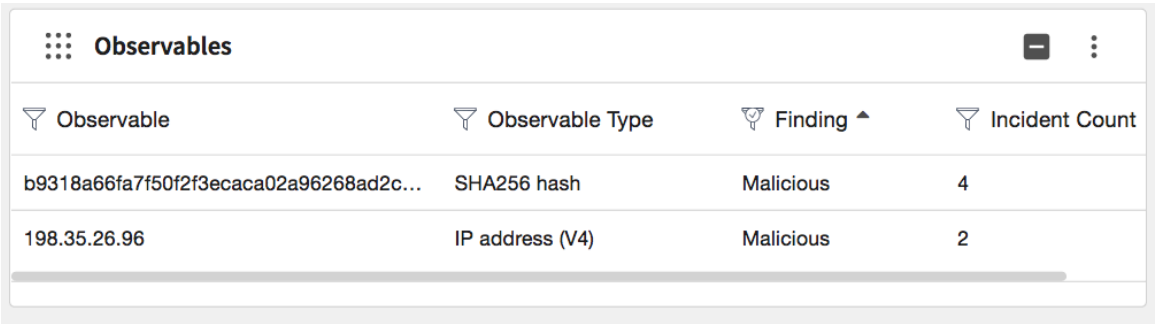
   Você pode ter uma visão geral do incidente de segurança, incluindo uma lista de observáveis, usuários afetados e incidentes de segurança semelhantes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



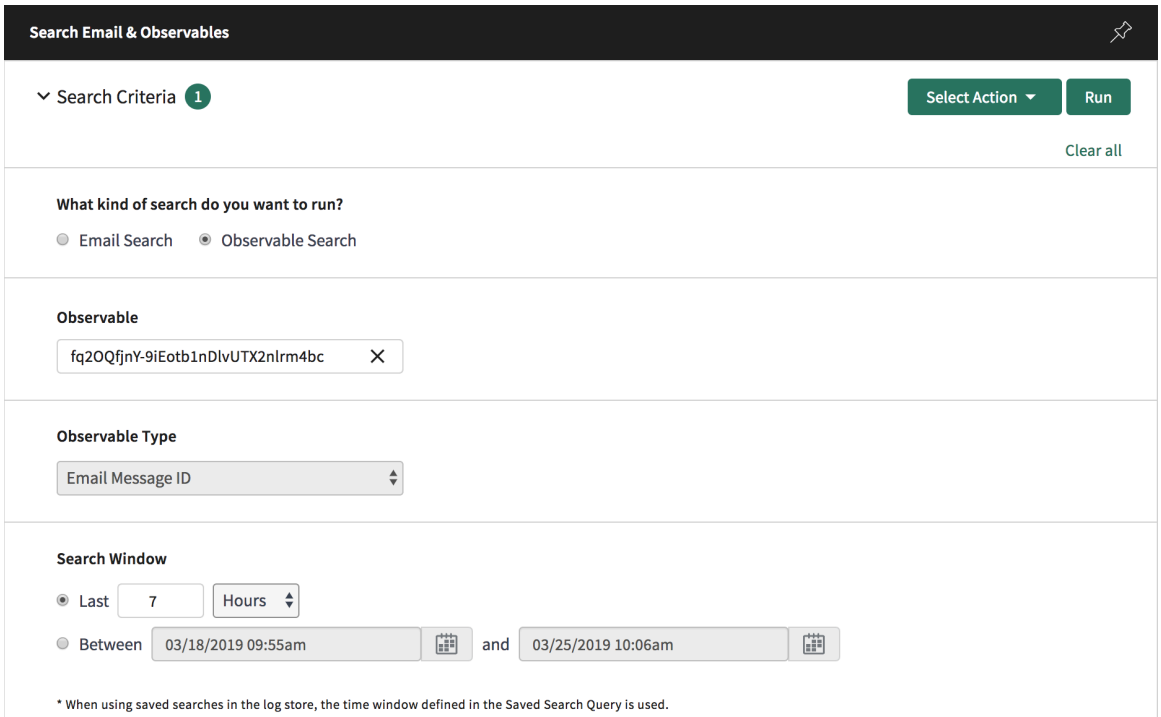
Na seção Observáveis, observe que a coluna Observável mostra o endereço de e-mail, o assunto e o URL. Observe também que a coluna Descoberta mostra que o URL foi verificado automaticamente quando o e-mail de phishing foi enviado e determinado como um URL malicioso conhecido. A coluna Contagem de incidentes mostra os outros incidentes que compartilham o mesmo observável. Esses artefatos indicam que você provavelmente está pronto para passar para procedimentos de contenção para este ataque de phishing, incluindo a determinação de quantos usuários na organização foram afetados.



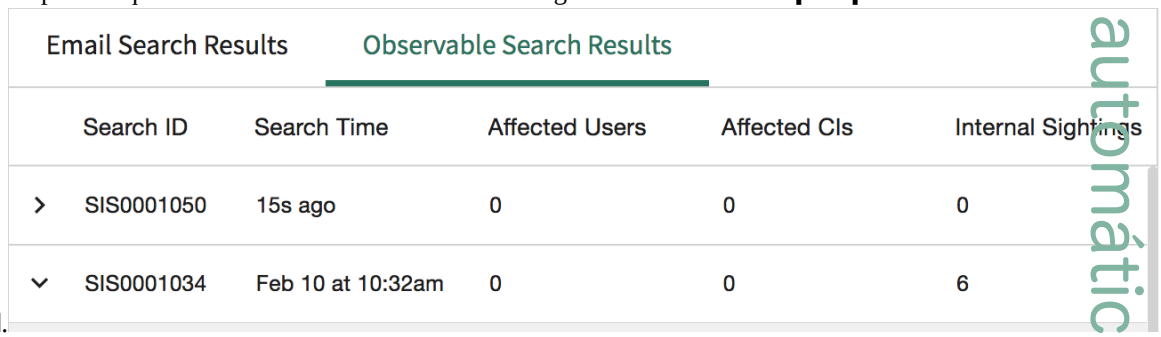
4. Navegar até **Explorar** > **Investigação** > **Pesquisar e-mail e observáveis**.
5. Expanda a seção Critérios de pesquisa e clique em **Pesquisa de observável**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Insira o observável que você está procurando e uma janela de tempo para a pesquisa (por exemplo, Últimas 24 horas).
7. Na lista **Selecionar ação**, selecione **Pesquisar**.
   O armazenamento de log do Splunk é pesquisado usando os critérios que você inseriu e os principais usuários visados pelo ataque mal-intencionado são mostrados na guia **Resultados da pesquisa do observável**.



8. Para exibir os usuários que receberam o e-mail, navegue até **Usuários** > **Usuários afetados**.

   A coluna Usuário Phished identifica os destinatários do e-mail de phishing e a coluna Interação do Usuário identifica os usuários que clicaram em um URL de phishing ou interagiram com um endereço de e-mail suspeito. A coluna Interação do usuário é definida como verdadeiro ou falso, dependendo se o usuário clicou no link mal-intencionado ou no IP.

   Nota:
   A página Usuários afetados mostra somente os registros de usuário que estão presentes na instância da ServiceNow.

9. Para investigar melhor os usuários que clicaram no e-mail de phishing e possivelmente comprometeram suas credenciais:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Nas colunas Usuário Phished e Interação do usuário, marque as caixas de seleção ao lado dos nomes de usuário que são **verdadeiros**.

b. Clique em **Criar incidente de segurança secundário** e em **Executar**.
Uma mensagem é exibida para mostrar que um incidente de segurança secundário foi criado. Para exibir os incidentes de segurança secundários associados a um incidente primário, clique na guia **Explorar** e navegue até **Incidentes** > **Incidentes de segurança secundários**.

Resultado
A lista de usuários com phishing é exibida.

Criar registros de configuração de pesquisa de vistas

Crie vários registros de configuração de pesquisa de vistas e use-os ao consultar vários armazenamentos de log ou variar os parâmetros de pesquisa.

Antes de Iniciar
Função necessária: sn_si.admin

- O complemento CIM deve ser instalado na instância do Splunk.
- Pesquisas salvas e consultas no local são compatíveis somente com a integração do Splunk.

Por Que e Quando Desempenhar Esta Tarefa
Você também pode criar registros de configuração de pesquisa de vistas para invocar pesquisas salvas no armazenamento de log do Splunk Enterprise.

Nota:
As consultas de configuração de pesquisa dependem dos dados de log do Splunk para serem compatíveis com o Splunk Common Information Model (CIM).

Com as configurações de pesquisa salvas, você pode:

- Crie pesquisas personalizadas que combinam vários registros de evento.
- Pesquisas eficazes e com design eficiente.
- Use entradas parametrizadas na pesquisa salva do Splunk.

O sistema de base inclui as configurações de amostra, conforme mostrado nesta imagem:

Configurações de pesquisa salvas

	Name	Observable type	Search	Is saved search
	Search	Search	Search	Search
	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

A pesquisa salva e as consultas de configuração Inplace são consultas de exemplo e podem ser substituídas por parâmetros apropriados para o seu ambiente. Crie configurações adicionais de pesquisa salva conforme necessário. Ao definir uma configuração de pesquisa salva, o nome e os parâmetros na consulta de pesquisa devem corresponder à

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

configuração salva definida na sua instância do Splunk. Se o nome e os parâmetros não forem os mesmos, talvez você não veja resultados precisos ao executar uma pesquisa de vistas.

Nota:
Na sua instância do Splunk, navegue até a página Pesquisas, relatórios e alertas e localize sua consulta de pesquisa salva. Clique no link **Permissões** para navegar até a página Permissões. Selecione o botão de opção **Todos os aplicativos** e habilite a opção **Permissão de leitura** para **Todos**. Isso mudará o valor da coluna Compartilhamento de Privado para Aplicação para sua consulta de pesquisa salva. Se isso não estiver definido, a consulta de pesquisa salva pode não retornar resultados.

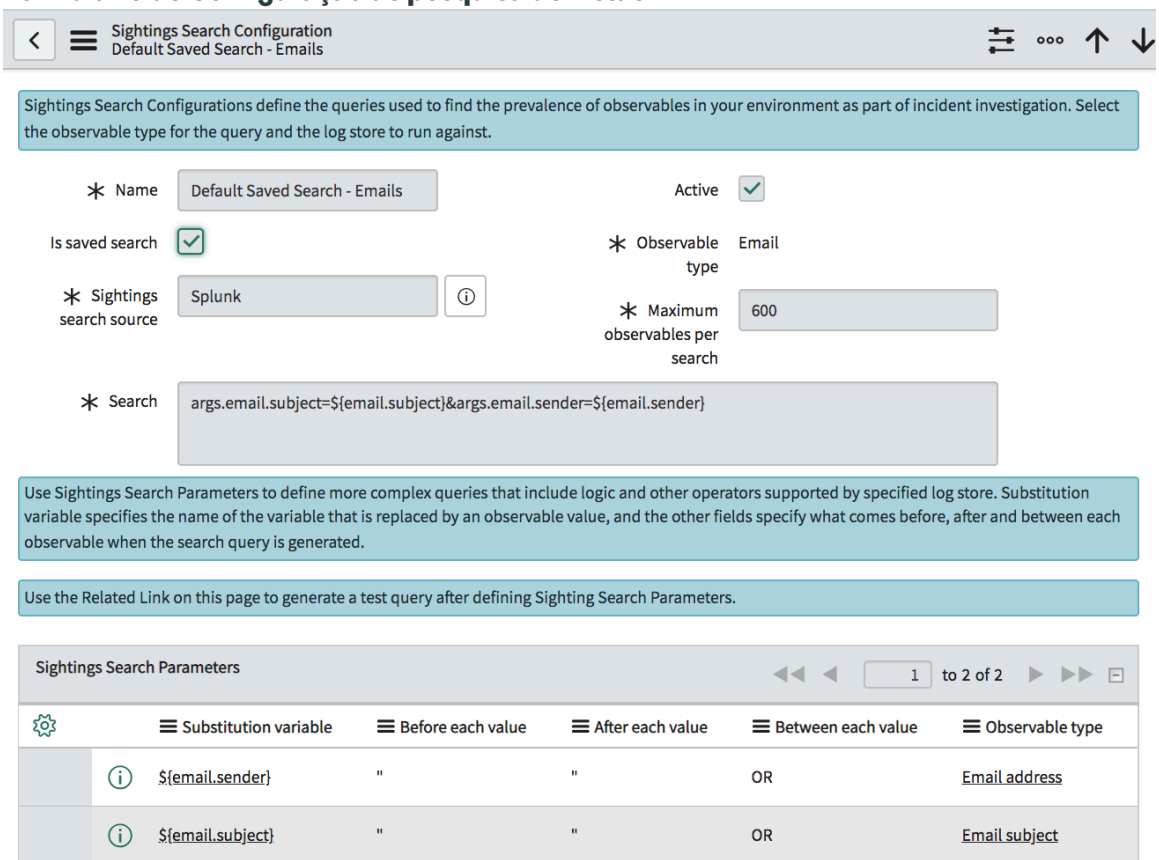
Para verificar se a configuração de pesquisa salva corresponde à configuração definida na sua instância do Splunk:

1. Navegar até **Configurações** > **Pesquisas, relatórios e alertas**.
2. Altere o **Contexto da aplicação** para **Todos**.

   Uma lista de relatórios de pesquisa será exibida.
3. Confirme se a consulta de pesquisa salva está presente na lista.

Por exemplo, o formulário Configuração de pesquisa de vistas contém o endereço de e-mail e o remetente do e-mail como parâmetros de pesquisa:

Formulário de Configuração de pesquisa de vistas



Na instância do Splunk, defina a pesquisa salva com o mesmo nome, Pesquisa salva padrão - e-mails e os mesmos parâmetros de pesquisa para o endereço e o assunto do e-mail. Se o nome e os parâmetros de pesquisa não forem iguais, a pesquisa de vistas não gerará um resultado preciso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Security Operations** > **Integrações** > **Configuração de Pesquisa de Vistas** e crie um novo registro (consulte a tabela para obter as descrições dos campos).

Formulário de Configuração de pesquisa de vistas

Campo	Descrição
Nome	Nome da configuração.
Pesquisa salva	A configuração de pesquisa salva será criada se você selecionar esta opção.
Origem de pesquisa de vistas	A origem da pesquisa de vistas. Selecione o armazenamento de log do Splunk como a origem.
Ativo	Opção para o status de pesquisa salvo. Somente configurações de pesquisa ativas podem ser usadas para executar uma pesquisa de vistas.
Tipo de observável	O tipo de observável pode ser qualquer tipo de observável, como IP, valor de hash, URL, nome de domínio e assim por diante.
Máximo de observáveis por pesquisa	Número máximo de observáveis a serem retornados da pesquisa.
Pesquisar	A cadeia de caracteres de pesquisa padrão é `$(observable)`, mas você pode definir sua própria consulta de pesquisa especificando parâmetros que são compatíveis com o armazenamento de log do Splunk.

2. Clique em **Enviar**.

Resultado
Você criou um registro de configuração de pesquisa de vistas.

O que Fazer Depois
Depois de definir a consulta de pesquisa, clique em **Gerar consulta de teste de pesquisa de detecções**e especifique uma lista de valores observáveis para gerar uma consulta de teste com base nesta configuração de pesquisa salva.

Recursos do Playbook

O Security Incident Response fornece um conjunto avançado de recursos de playbook que inclui uma biblioteca abrangente de playbooks, subfluxos e ações. Você pode criar ou configurar playbooks de forma rápida e fácil sem escrever código complicado. Você pode usar esses playbooks para resolver ameaças à segurança passo a passo.

Os recursos do Playbook incluem o seguinte:

Security Incident Response playbooks	Ações do playbook do Security Incident Response
Os playbooks fornecidos com o sistema básico foram projetados para acelerar o processo de investigação de incidentes de segurança, automatizando tarefas complexas e mundanas.	Ações complexas que são críticas para criar playbooks estão disponíveis como **Bibliotecas de ação**. Essas bibliotecas de ação permitem que os administradores de segurança criem playbooks sem escrever nenhum código complexo. Consulte Ações do playbook do Security Incident Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Security Incident Response playbooks	Ações do playbook do Security Incident Response
Os playbooks são altamente configuráveis e criados usando a tecnologia Flow Designer da ServiceNow. Para configurar, copie o playbook fornecido com o sistema de base e modifique-o usando a interface gráfica simples de arrastar e soltar. Consulte Security Incident Response playbooks.	

Ativar um fluxo Security Incident Response

Os administradores de segurança e designers de fluxo podem usar os fluxos Security Incident Response para automatizar o processo de resolução de incidentes de segurança na organização.

Antes de Iniciar

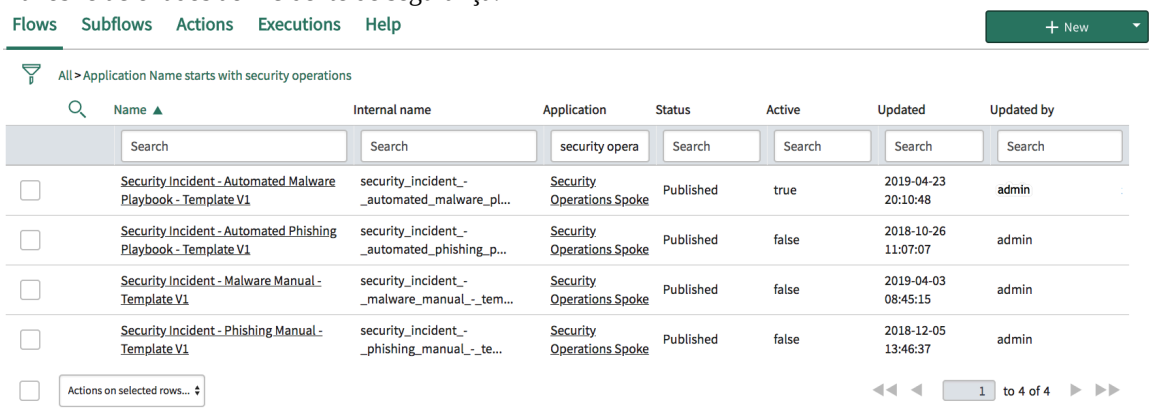
Função necessária: sn_si.admin, action_designer e flow_designer

Por Que e Quando Desempenhar Esta Tarefa

Os fluxos fornecidos com o sistema de base estão em um estado inativo. Ative esses fluxos antes de usá-los.

Procedimento

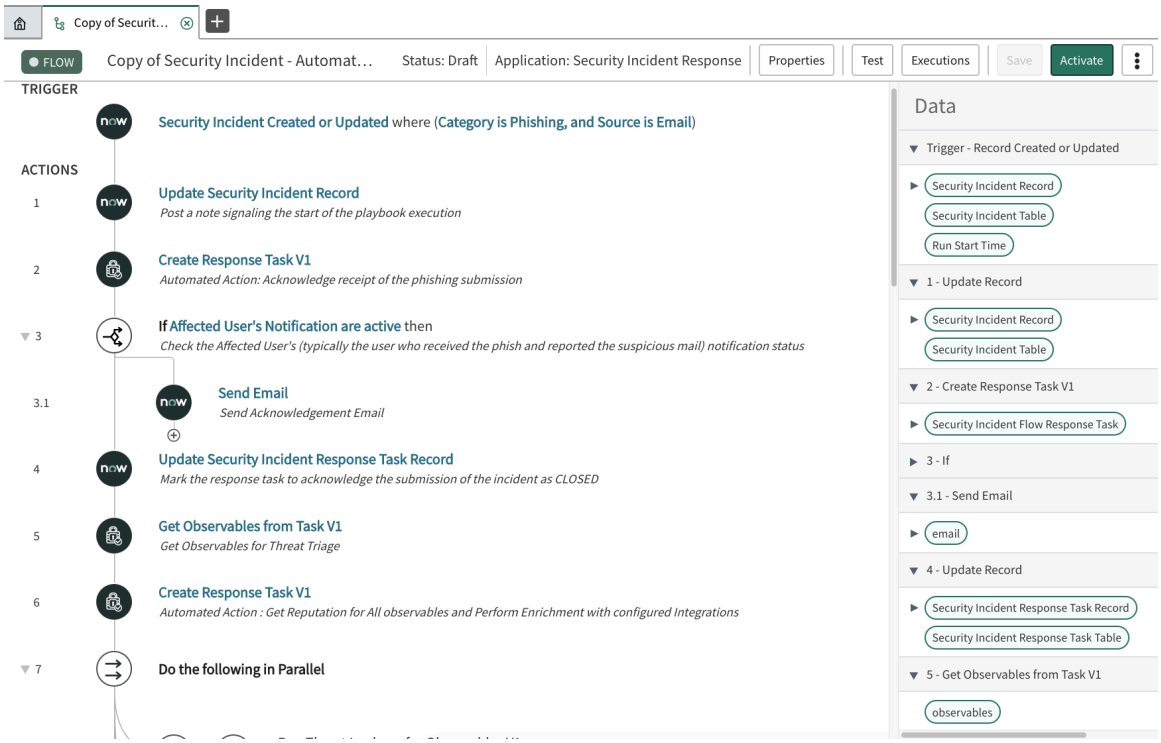
1. Baixe e instale a aplicação Security Operations Spoke.
   Esta aplicação Spoke fornece ações de operações de segurança que você pode usar ao definir fluxos Security Incident Response.
2. Navegar até **Flow Designer** > **Designer** e pesquise a aplicação Spoke Security Operations para exibir os fluxos relacionados ao incidente de segurança.



   Observe que os fluxos têm um status publicado e estão inativos.
3. Por exemplo, se você quiser ativar o fluxo do Automated Malware Playbook, clique no link **Incidente de segurança - Automated Phishing Playbook - Template V1** para exibir o fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:
Você não pode editar os fluxos fornecidos com o sistema de base, pois eles são somente leitura. Você pode usar esses fluxos como estão ou fazer uma cópia e modificá-los conforme necessário.

4. Clique em **Ativar** para ativar o fluxo.

Resultado
O fluxo do Automated Phishing Playbook está ativo e pronto para uso.

Security Incident Response playbooks

Você pode invocar o fluxo do playbook de incidente de segurança automaticamente ou manualmente.

Um Playbook ficará visível somente se pelo menos um playbook estiver associado a um incidente de segurança. O componente do playbook funciona somente para os processos criados pelo Designer de automação de processos (PAD) e não para os fluxos criados pelo Flow Designer. Para os fluxos habilitados para o Flow Designer existentes, ele continuará a funcionar e as atividades continuarão a ser renderizadas como tarefas de resposta.

Security Incident Response O oferece suporte a dois tipos de Playbooks:

- Playbooks baseados em processo
- Playbooks baseados em fluxo

Além dos playbooks listados, também há subfluxos no Security Operations Spoke que podem ser chamados do playbook de fluxos. O ransomware é um desses subfluxos.

Ative esses fluxos antes de usá-los. Para obter mais informações, consulte Ativação de um fluxo do Security Incident Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbooks baseados em processo

O componente do playbook funciona somente para os processos criados pelo Designer de automação de processos (PAD) e não para os fluxos criados pelo Flow Designer. Para os fluxos habilitados para o Flow Designer existentes, ele continuará a funcionar e as atividades continuarão a ser renderizadas como tarefas de resposta.

Security Incident Response fornece os seguintes playbooks com o sistema de base.

Playbook for Manual Phishing

O Manual de Phishing Playbook fornece orientação passo a passo para seus analistas sobre como eles podem resolver manualmente tipos específicos de ameaças à segurança em suas atividades de phishing.

Visão geral

O modelo de Playbook manual de phishing foi projetado para executar as tarefas de resposta de phishing manualmente e inclui uma sequência de ações que inclui condições do gatilho. Você pode usar os modelos de PAD para executar as etapas no playbook de resposta de phishing e resolver esses incidentes com eficiência.

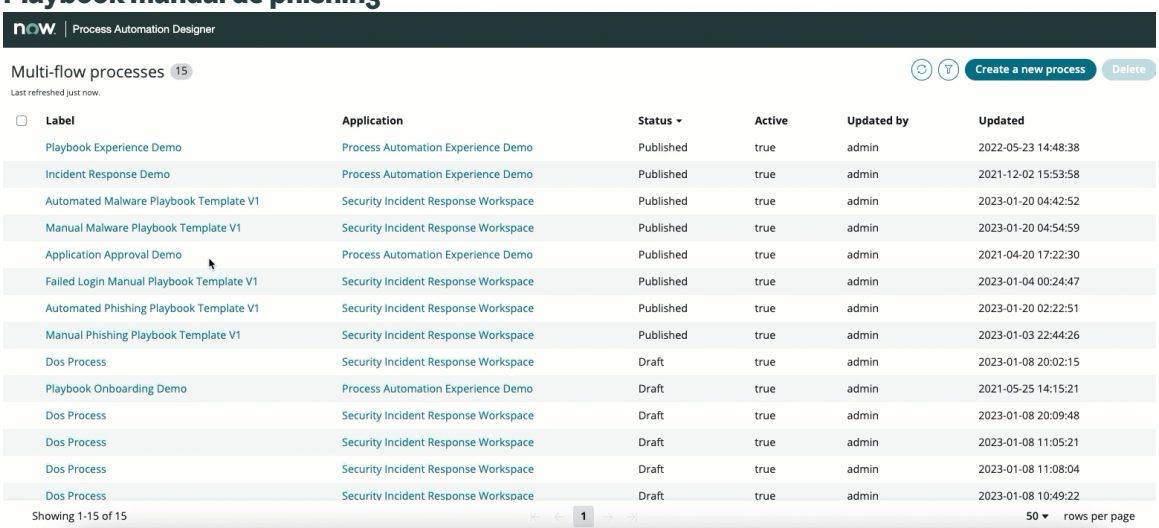
Este playbook pode ser usado se um incidente de segurança for criado ou atualizado. Você precisa ativar o Playbook de phishing manual no Designer de automação de processos (PAD) e executar todas as tarefas, como análise, contenção, erradicação e revisão.

A seguir estão as raias da definição do processo e correspondem ao estado do incidente de segurança:

- Análise
- Contém
- Erradicar
- Revisão

Cada raia tem atividades dentro dela.

Playbook manual de phishing



Depois de marcar uma tarefa como concluída em uma raia, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma raia, você

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

pode passar para a próxima raia. O status é refletido no painel esquerdo conforme você conclui as tarefas e as raias. Um log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as raias. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Criar processos para phishing manual no PAD

Use essas etapas para criar processos de phishing manual no Designer de automação de processos (PAD).

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

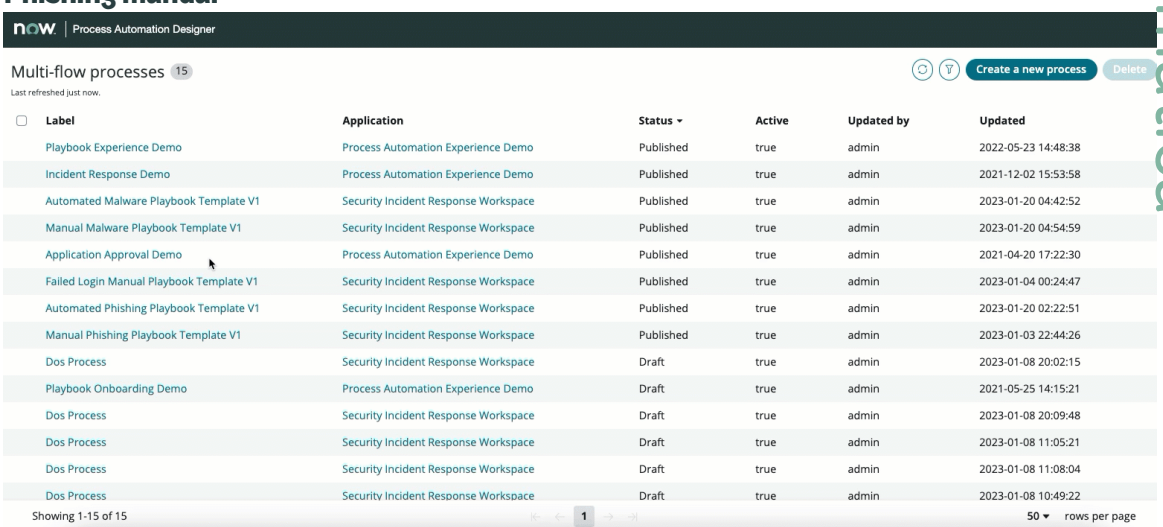
Procedimento

1. Clicar **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

   Por exemplo, Modelo de Playbook manual de phishing V1.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique **em Selecionar um gatilho**.
4. Selecione **Definir suas próprias condições para quando o processo for executado**e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique **em Definir condições do gatilho**.
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Phishing manual



7. Clique **em Ir para Designer**.
   A página do Process Automation Designer é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicionar uma nova raia**.
   O painel de propriedades da raia é aberto no lado direito da IU.
9. No painel de propriedades da raia, insira os seguintes detalhes: **Nome**, **Descrição**, **Condição de execução**e **Indicar quando iniciar**.

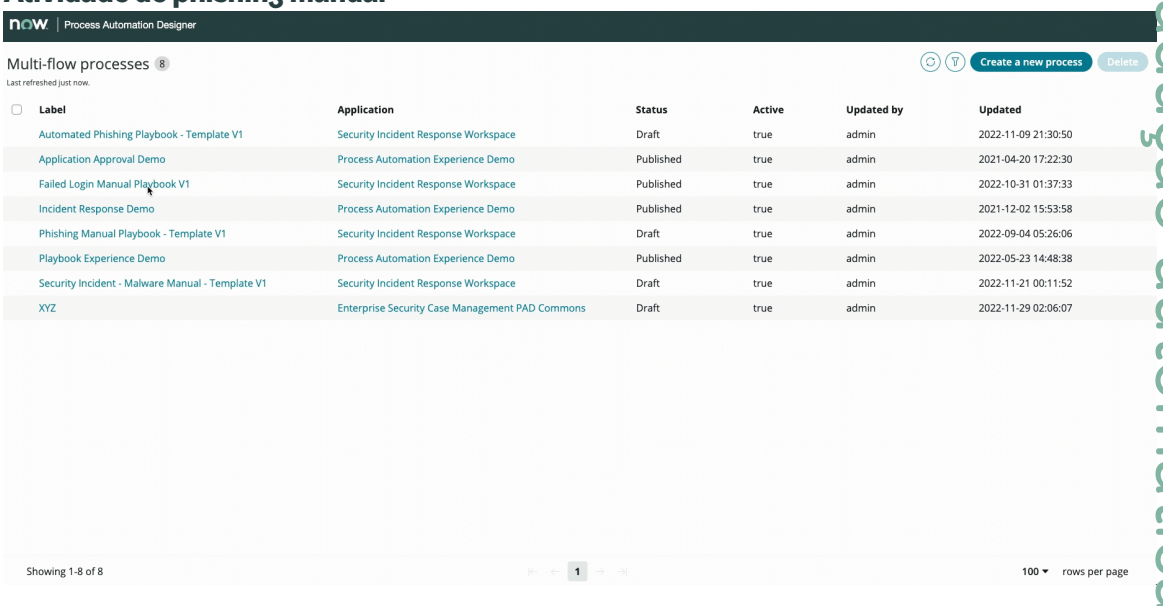
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os campos **Condição de execução** e **Indicar quando iniciar** indicam quando a raia deve ser executada.

10. Clique **em Salvar e fechar**.
11. Para adicionar outra raia, clique em **Adicionar outra raia**.
    Da mesma forma, você pode criar quantas raias quiser. Neste exemplo, você pode criar uma raia para Análise, Conter, Erradicar e Revisar, respectivamente. No exemplo a seguir, a raia de **análise** começa imediatamente e não tem condição de execução. **Contém** o início da raia após a conclusão da raia anterior e tem uma condição de execução que se baseia no resultado de uma atividade na raia anterior.
    Depois de adicionar as raias, você precisa adicionar atividades de processo para cada raia.
12. Clique em **Adicionar outra atividade de processo** em uma raia específica (por exemplo, Raia de análise).
    O pop-up Adicionar atividade é aberto.
    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.
13. Clique **em Criar uma nova atividade**.
    Depois que uma definição de atividade é adicionada, ela pode ser configurada de forma semelhante às raias. Da mesma forma, você pode criar outras atividades de processo em cada raia.

Atividade de phishing manual



14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique **em Exibir todas as propriedades** e habilite a alternância **Propriedades avançadas** para exibir todos os campos de experiência de atividade da definição da atividade.

Adicionar atividades paralelas

Se o campo **Quando iniciar** estiver definido como **Com o anterior**, as atividades paralelas poderão ser iniciadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para passar de uma raia para a próxima

Se nenhuma condição de execução for definida, as raias e as atividades serão executadas sequencialmente.

Você pode usar a condição de execução para ignorar atividades ou raias. Neste exemplo, **a raia Contêm começa quando o resultado de "O e-mail tem indicadores de ameaça?" é Sim**.

Para passar de uma raia para outra, você pode usar a **definição de atividade fornecida pela plataforma - Atualizar registro**. Isso atualizará o campo de estado do incidente de segurança e retomará a execução do playbook para a próxima raia.

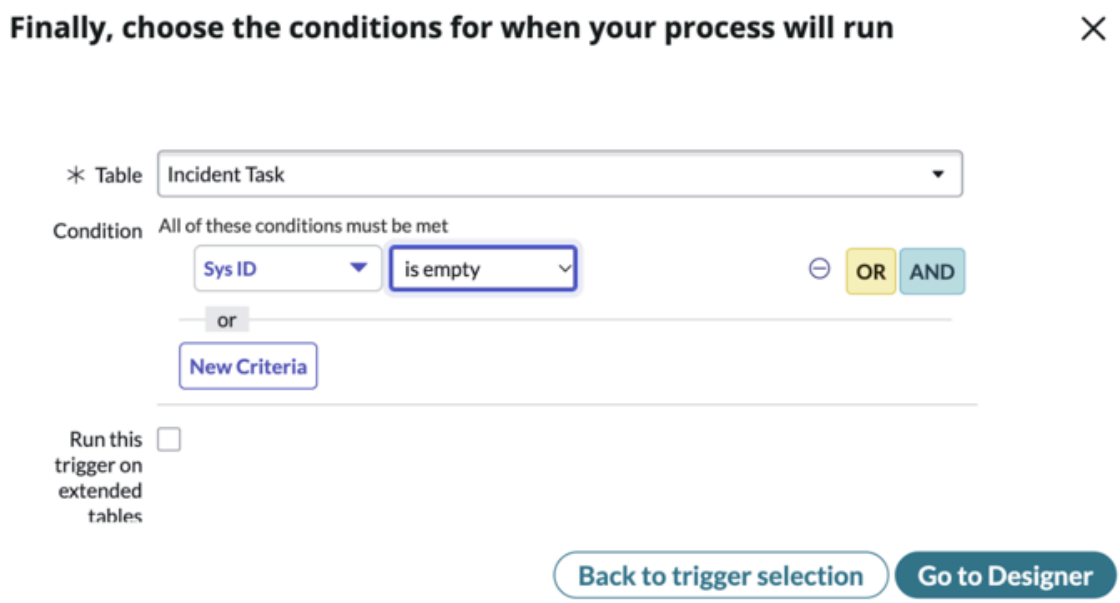
No entanto, o desafio com esta definição de atividade é que, se dizer que o playbook está na raia de análise e se o usuário tiver atualizado manualmente o estado para dizer revisão, a atividade Atualizar registro mudará novamente o estado para Conter para continuar o playbook execução. Isso substituirá a mudança manual feita.

Para superar isso, no sistema de base, uma definição de atividade chamada **Atualizar estado da tarefa** é fornecida. Esta atividade não substituirá o estado do incidente de segurança se o estado atual do estado da segurança estiver à frente da raia no playbook.

Criar uma definição de processo com condição de gatilho fictícia

Uma definição de processo sempre requer uma condição do gatilho. Mas, se você não tiver certeza de quando o processo deve ser acionado, ainda poderá criar uma definição de processo com uma condição de gatilho fictícia. Defina a condição do gatilho como **sys_id está vazio**. Esta condição nunca será atendida.

Condições do processo



Tradução automática

Usando o playbook manual de phishing

Use estas etapas para saber como você pode usar o playbook de phishing manual no Espaço do analista de SIR e seus recursos.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

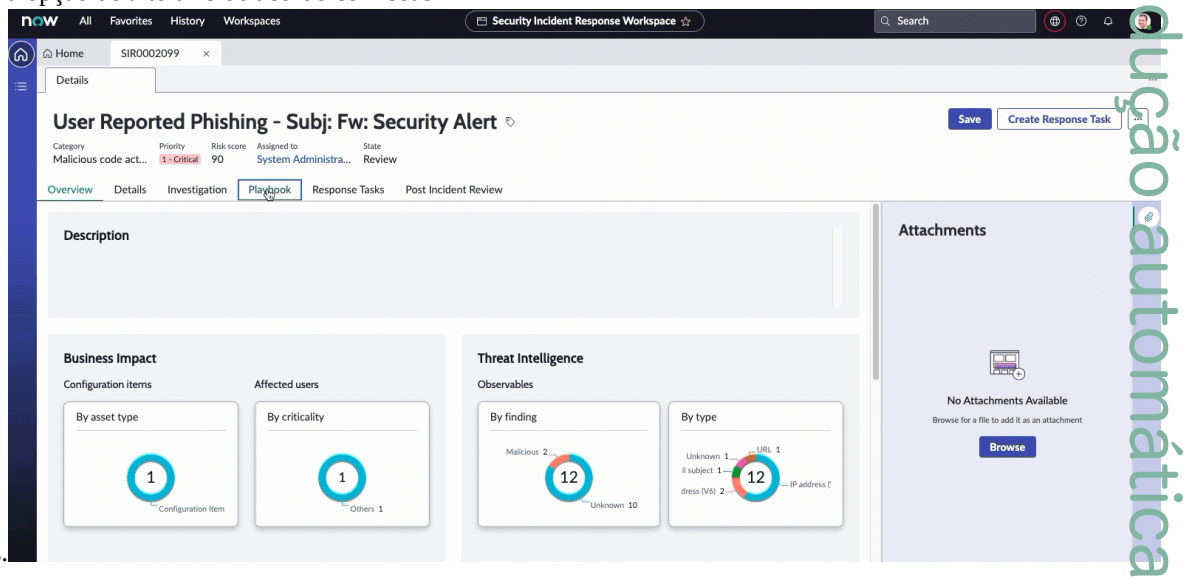
Procedimento

1. No espaço de SIR, abra um incidente de segurança.
2. Clique na guia **Playbook**.

   Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

   Nota:
   Se você não vir nenhum playbook listado, precisará ir para o PAD e permitir que ele o veja na guia **Playbook**.

3. Clique no **Playbook manual de phishing**.
4. Clique em cada raia para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** para ver a lista de atividades realizadas na fase de Análise.
   Você tem a opção de alterá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Erradicar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de alterá-los de acordo com seus requisitos. Se houver alguma atividade ou ação do usuário restante que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Resumo do Playbook do espaço

A seguir descreve o resumo do processo.

- Entenda o playbook legado baseado em fluxo.
- Liste as atividades possíveis, raias depois de analisar o fluxo. Procure as etapas em que a Orquestração verdadeira pode ser criada.
- Pegue cada atividade e verifique se a definição de atividade fornecida pelo sistema de base pode atender ao caso de uso ou não.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Listar os casos de uso de atividade inativos que precisam de novas definições de atividade para serem implementados. Classifique-os como interativos, não interativos ou automatizados. Para criar uma definição de atividade:
  - Crie um subfluxo ou uma ação para o caso de uso.
  - Decida se os dados associados devem ser capturados na tabela de dados de fluxo ou em uma tabela personalizada.
  - Se estiver usando a tabela de dados de fluxo, crie uma definição de dados de fluxo em **sys_flow_data_definition**. Ao criar um registro de dados de fluxo no subfluxo, selecione a definição de dados de fluxo criada.
  - Crie uma **definição de atividade**.
  - Mapeie o plano de automação.
  - Preencha as propriedades de **experiência da atividade**.
  - Crie uma ação em Ações do Playbook. Deve haver uma ação de atividade existente para atribuí-la à definição de atividade.
  - Para substituir a experiência do cartão padrão com base no tipo de experiência selecionado, adicione a substituição do playbook usando o conceito de IU de atividade.
- Algumas atividades podem ser feitas para lidar com automáticas e interativas usando o sinalizador aguardar entrada do usuário no subfluxo. Esta entrada pode ser passada ao configurar a atividade na definição do processo.
- Depois de ter todas as definições de atividade necessárias para o seu processo, comece a criar a definição do processo usando o PAD studio.

Playbook for Automated Phishing

O playbook de Phishing automatizado fornece orientação passo a passo para seus analistas sobre como eles podem resolver tipos específicos de ameaças à segurança em suas atividades de phishing automatizado.

Visão geral

O modelo de playbook de phishing automatizado foi projetado para automatizar as tarefas de resposta de phishing e contém uma sequência de ações que inclui condições do gatilho. Você pode usar os modelos de PAD para automatizar as etapas no playbook de resposta de phishing e resolver esses incidentes com eficiência. Este modelo de playbook contém uma sequência de ações reutilizáveis projetadas para responder a ataques de phishing. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos que você pode anotar.

Neste playbook, não haverá interação do usuário quando a categoria de um incidente de segurança estiver definida como phishing. Este playbook pode ser usado se um incidente de segurança for criado ou atualizado. Você precisa ativar o Automated Phishing Playbook no Designer de automação de processos (PAD), e esse playbook executa automaticamente todas as tarefas, como análise, contenção, erradicação e revisão.

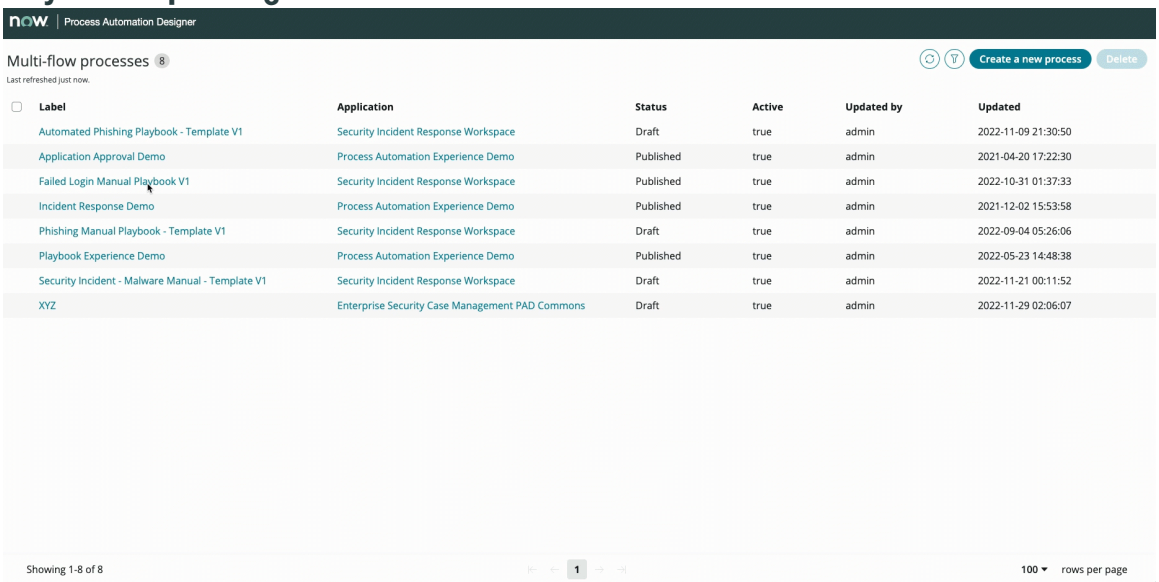
A seguir estão as raias da definição do processo e correspondem ao estado do incidente de segurança:

- Análise
- Contém
- Erradicar
- Revisão

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cada raia tem atividades dentro dela.

Playbook de phishing automatizado



Depois de marcar uma tarefa como concluída em uma raia, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma raia, você pode passar para a próxima raia. O status é refletido no painel esquerdo conforme você conclui as tarefas e as raias. Um log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as raias. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Criar processos para phishing automatizado no PAD

Use essas etapas para criar processos para Phishing automatizado no Designer de automação de processos (PAD).

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

Procedimento

1. Clicar **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

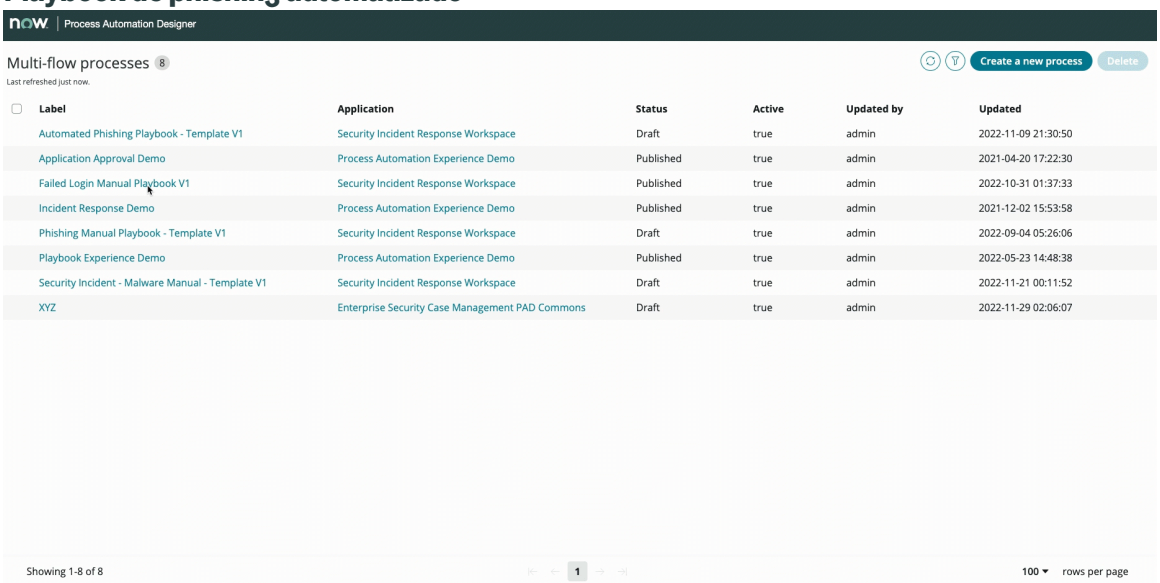
   Por exemplo, Automated Phishing Playbook Template V1.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique **em Selecionar um gatilho**.
4. Selecione **Definir suas próprias condições para quando o processo for executado**e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique **em Definir condições do gatilho**.
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de phishing automatizado

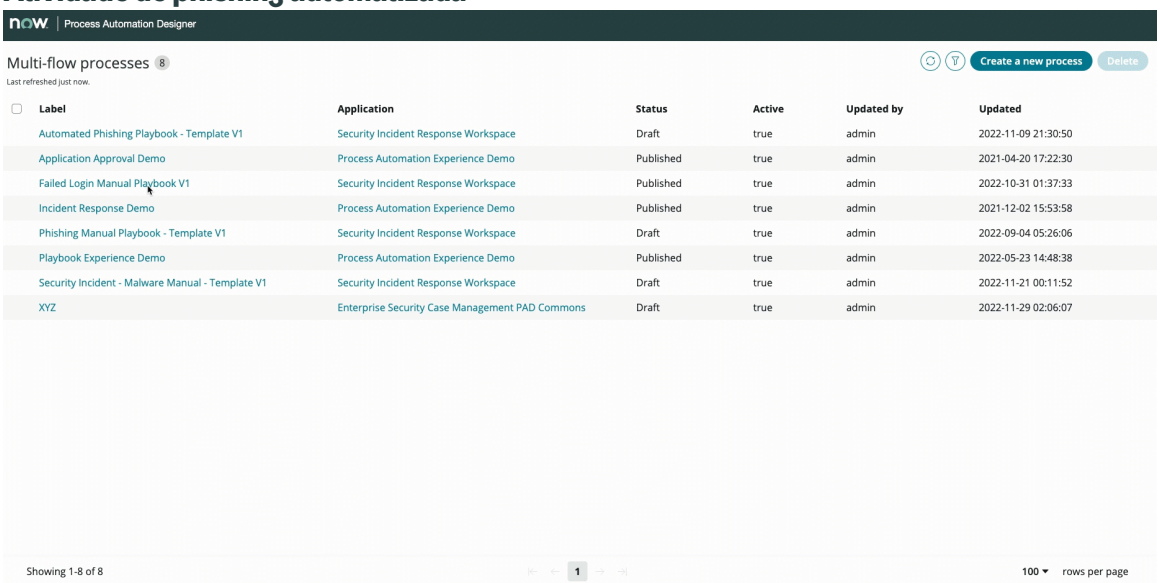


7. Clique **em Ir para Designer**.
   A página do Process Automation Designer é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicionar uma nova raia**.
   O painel de propriedades da raia é aberto no lado direito da IU.
9. No painel de propriedades da raia, insira os seguintes detalhes: **Nome**, **Descrição**, **Condição de execução**e **Indicar quando iniciar**.
   Os campos **Condição de execução** e **Indicar quando iniciar** indicam quando a raia deve ser executada.
10. Clique **em Salvar e fechar**.
11. Para adicionar outra raia, clique em **Adicionar outra raia**.
    Da mesma forma, você pode criar quantas raias quiser. Neste exemplo, você pode criar uma raia para Análise, Conter, Erradicar e Revisar, respectivamente. No exemplo a seguir, a raia de **análise** começa imediatamente e não tem condição de execução. **Contém** o início da raia após a conclusão da raia anterior e tem uma condição de execução que se baseia no resultado de uma atividade na raia anterior.
    Depois de adicionar as raias, você precisa adicionar atividades de processo para cada raia.
12. Clique em **Adicionar outra atividade de processo** em uma raia específica (por exemplo, Raia de análise).
    O pop-up Adicionar atividade é aberto.
    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.
13. Clique **em Criar uma nova atividade**.
    Depois que uma definição de atividade é adicionada, ela pode ser configurada de forma semelhante às raias. Da mesma forma, você pode criar outras atividades de processo em cada raia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade de phishing automatizada



14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique **em Exibir todas as propriedades** e habilite a alternância **Propriedades avançadas** para exibir todos os campos de experiência de atividade da definição da atividade.

Como usar o playbook de phishing automatizado

Use estas etapas para saber como você pode usar o playbook de phishing automatizado no Espaço do analista de SIR e seus recursos.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

Procedimento

1. No espaço de SIR, abra um incidente de segurança.
2. Clique na guia **Playbook**.

   Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

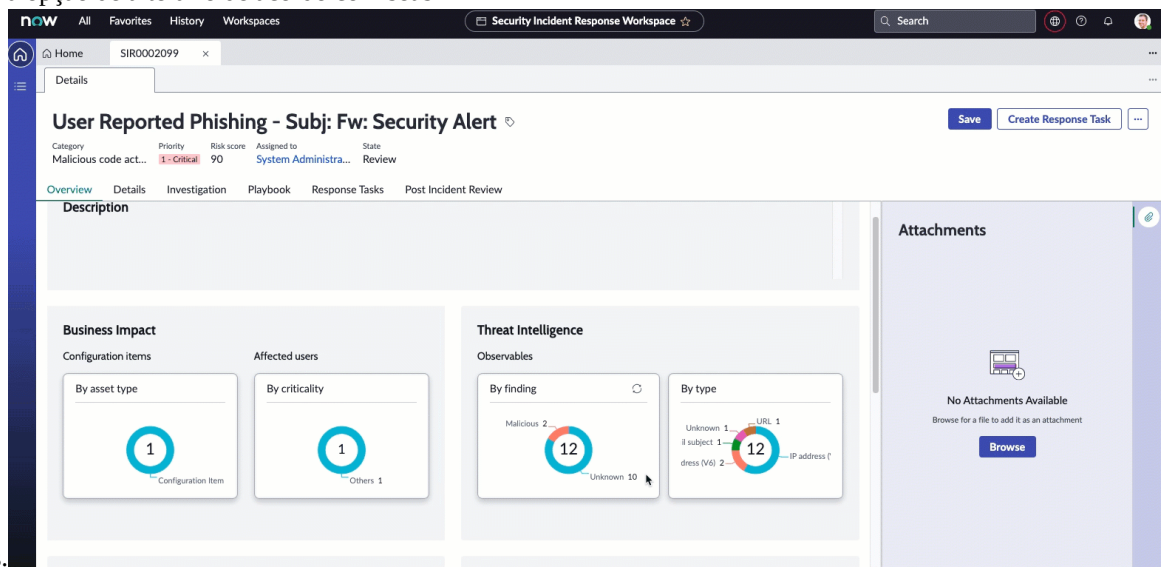
   Nota:
   Se você não vir nenhum playbook listado, precisará ir para o PAD e permitir que ele o veja na guia **Playbook**.

3. Clique no **Playbook de phishing automatizado**.
   Para phishing automatizado, as tarefas são realizadas automaticamente para o incidente de segurança.
4. Clique em cada raia para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** para ver a lista de atividades realizadas na fase de Análise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você tem a opção de alterá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Erradicar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de alterá-los de acordo com seus requisitos. Se houver alguma atividade ou ação do usuário restante que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Playbook para malware manual

O playbook manual de malware fornece orientação passo a passo sobre como os analistas podem resolver manualmente alertas de malware com mais eficiência.

O modelo de playbook manual de malware foi projetado para executar manualmente as etapas envolvidas no tratamento de alertas de malware do endpoint ou da rede. Você pode usar os modelos de PAD para executar as etapas no playbook de malware manual e resolver esses alertas com eficiência. Este playbook inclui condições do gatilho, uma sequência de ações e subfluxos que você pode anotar. Este playbook contém uma sequência de ações reutilizáveis projetadas para responder a ataques de malware. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos para anotação.

Este playbook pode ser usado se o malware for criado ou atualizado. Você precisa ativar o Playbook manual de malware no Designer de automação de processos (PAD) e criar todas as tarefas, como análise, contenção, erradicação e revisão.

A seguir estão as raias da definição do processo e correspondem ao estado de alerta de malware:

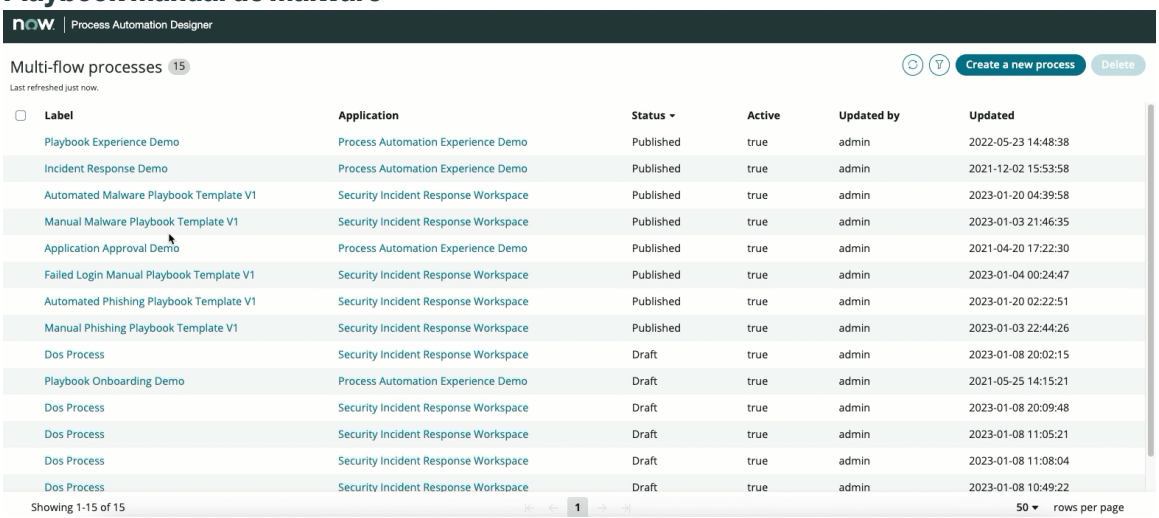
- Análise
- Contém
- Erradicar
- Revisão

Cada raia tem atividades dentro dela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook manual de malware



Depois de marcar uma tarefa como concluída em uma raia, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma raia, você pode passar para a próxima raia. O status é refletido no painel esquerdo conforme você conclui as tarefas e as raias. Um log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as raias. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Criar processos para malware manual no PAD

Use essas etapas para criar processos para malware manual no Designer de automação de processos (PAD).

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

Procedimento

1. Clicar **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

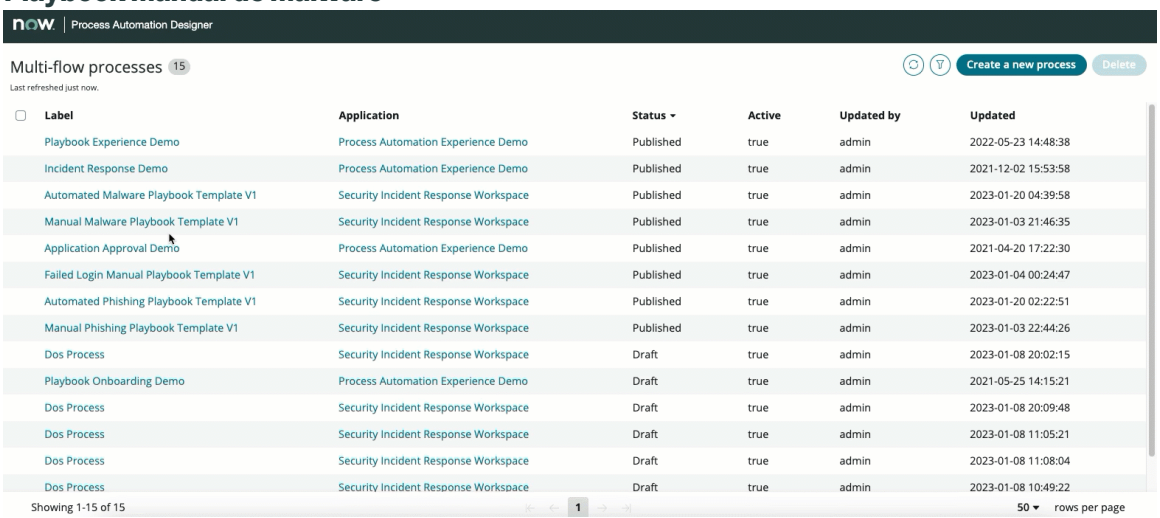
   Por exemplo, Manual Malware Playbook Template V1.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique **em Selecionar um gatilho**.
4. Selecione **Definir suas próprias condições para quando o processo for executado**e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique **em Definir condições do gatilho**.
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook manual de malware

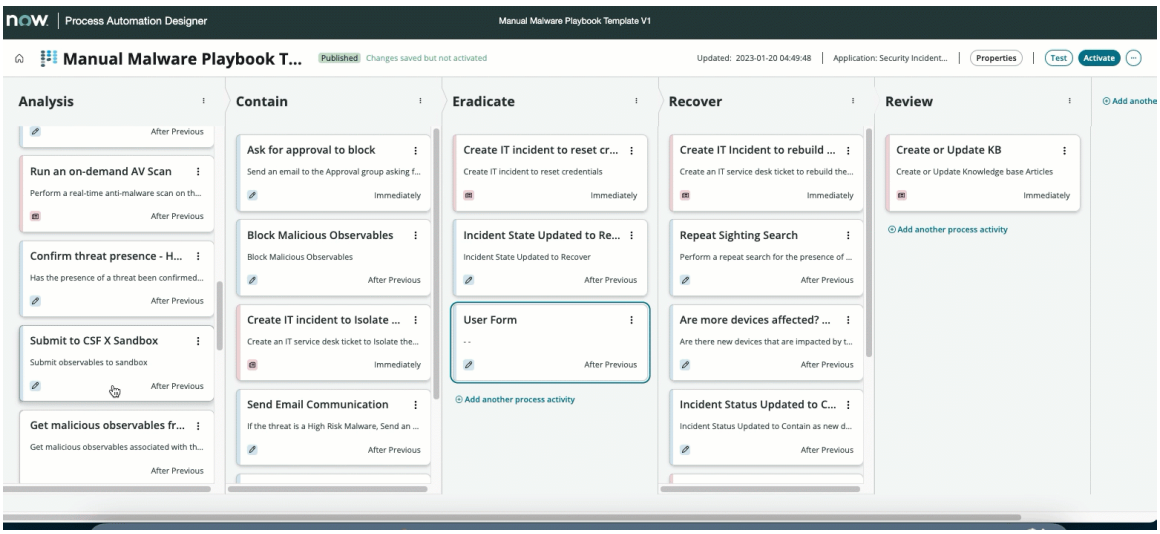


7. Clique **em Ir para Designer**.
   A página do Process Automation Designer é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicionar uma nova raia**.
   O painel de propriedades da raia é aberto no lado direito da IU.
9. No painel de propriedades da raia, insira os seguintes detalhes: **Nome**, **Descrição**, **Condição de execução**e **Indicar quando iniciar**.
   Os campos **Condição de execução** e **Indicar quando iniciar** indicam quando a raia deve ser executada.
10. Clique **em Salvar e fechar**.
11. Para adicionar outra raia, clique em **Adicionar outra raia**.
    Da mesma forma, você pode criar quantas raias quiser. Neste exemplo, você pode criar uma raia para Análise, Conter, Erradicar e Revisar, respectivamente. No exemplo a seguir, a raia de **análise** começa imediatamente e não tem condição de execução. **Contém** o início da raia após a conclusão da raia anterior e tem uma condição de execução que se baseia no resultado de uma atividade na raia anterior.
    Depois de adicionar as raias, você precisa adicionar atividades de processo para cada raia.
12. Clique em **Adicionar outra atividade de processo** em uma raia específica (por exemplo, Raia de análise).
    O pop-up Adicionar atividade é aberto.
    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.
13. Clique **em Criar uma nova atividade**.
    Depois que uma definição de atividade é adicionada, ela pode ser configurada de forma semelhante às raias. Da mesma forma, você pode criar outras atividades de processo em cada raia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade manual de malware



14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique **em Exibir todas as propriedades** e habilite a alternância **Propriedades avançadas** para exibir todos os campos de experiência de atividade da definição da atividade.

Como usar o playbook manual de malware

Use estas etapas para saber como você pode usar o playbook manual de malware no Espaço do analista de SIR e seus recursos.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

Procedimento

1. No espaço de SIR, abra um incidente de segurança.
2. Clique na guia **Playbook**.

   Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

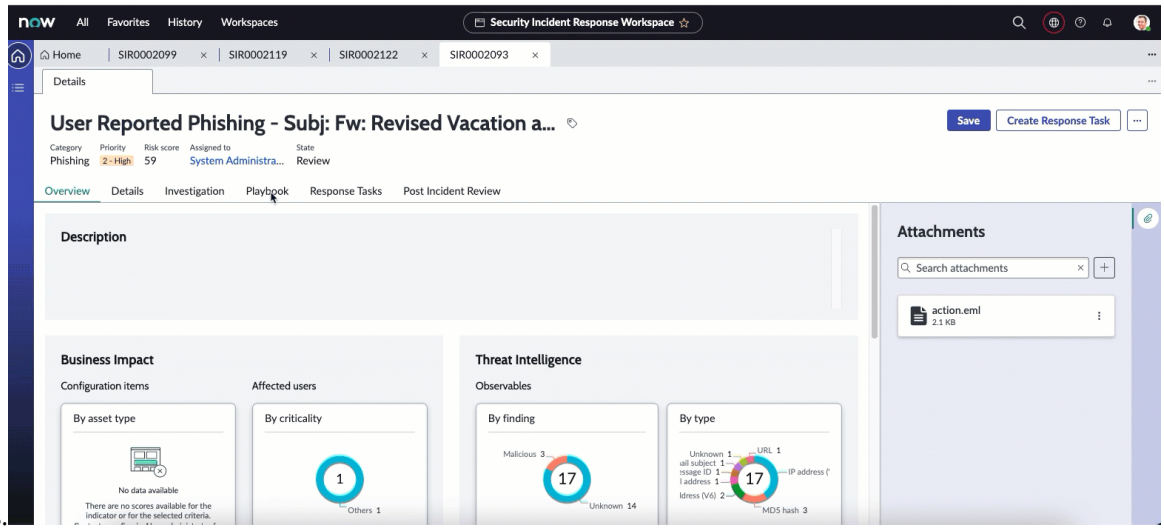
   Nota:
   Se você não vir nenhum playbook listado, precisará ir para o PAD e permitir que ele o veja na guia **Playbook**.

3. Clique no **Playbook manual de malware**.
   Para malware manual, as tarefas são realizadas automaticamente para o incidente de segurança.
4. Clique em cada raia para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** para ver a lista de atividades realizadas na fase de Análise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você tem a opção de alterá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Erradicar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de alterá-los de acordo com seus requisitos. Se houver alguma atividade ou ação do usuário restante que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Playbook for Automated Malware

O playbook de malware automatizado fornece uma sequência de etapas automatizadas que ajuda os analistas a resolver alertas de malware com mais eficiência.

O modelo de playbook de malware automatizado foi projetado para automatizar as etapas envolvidas no tratamento de alertas de malware do endpoint ou da rede. Você pode usar os modelos de PAD para automatizar as etapas no playbook de malware automatizado e resolver esses alertas com eficiência. Este playbook inclui condições do gatilho, uma sequência de ações e subfluxos que você pode anotar. Este playbook contém uma sequência de ações reutilizáveis projetadas para responder a ataques de malware. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos para anotação.

Este playbook pode ser usado se um incidente de segurança for criado ou atualizado. Você precisa ativar o playbook Automated Malware no Designer de automação de processos (PAD), e esse playbook executa automaticamente todas as tarefas, como análise, contenção, erradicação e revisão.

A seguir estão as raias da definição do processo e correspondem ao estado do incidente de segurança:

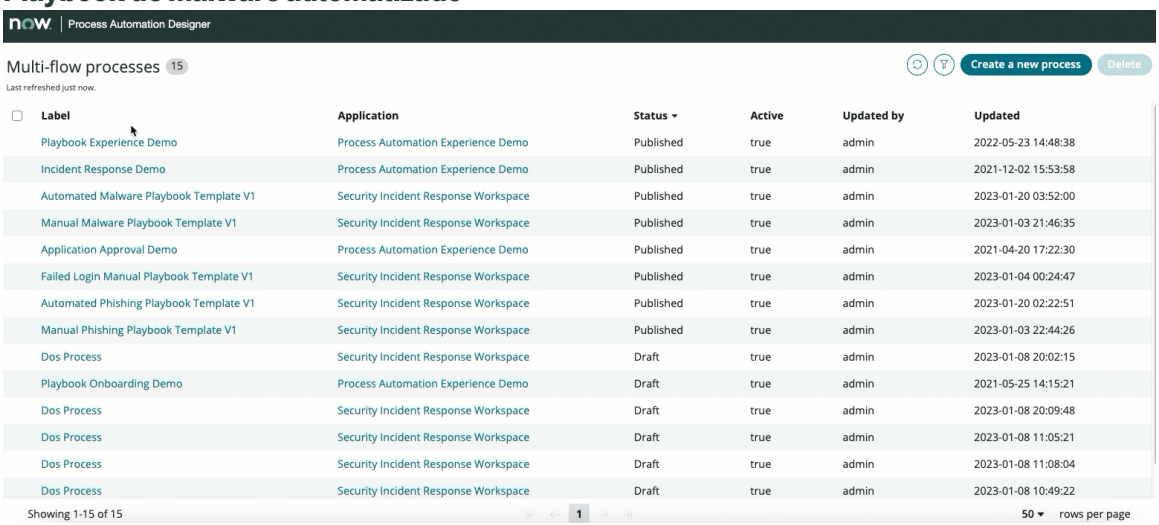
- Análise
- Contém
- Erradicar
- Revisão

Cada raia tem atividades dentro dela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de malware automatizado



Depois de marcar uma tarefa como concluída em uma raia, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma raia, você pode passar para a próxima raia. O status é refletido no painel esquerdo conforme você conclui as tarefas e as raias. Um log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as raias. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Criar malware automatizado de processos no PAD

Use estas etapas para criar processos para malware automatizado no Designer de automação de processos (PAD).

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

Procedimento

1. Clicar **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

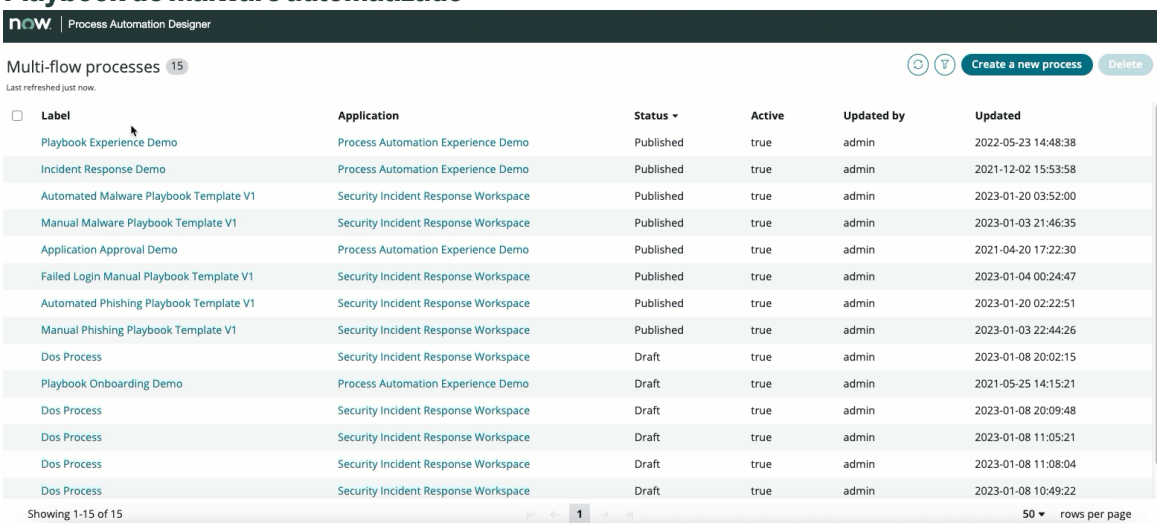
   Por exemplo, Automated Malware Playbook Template V1.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique **em Selecionar um gatilho**.
4. Selecione **Definir suas próprias condições para quando o processo for executado**e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique **em Definir condições do gatilho**.
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de malware automatizado

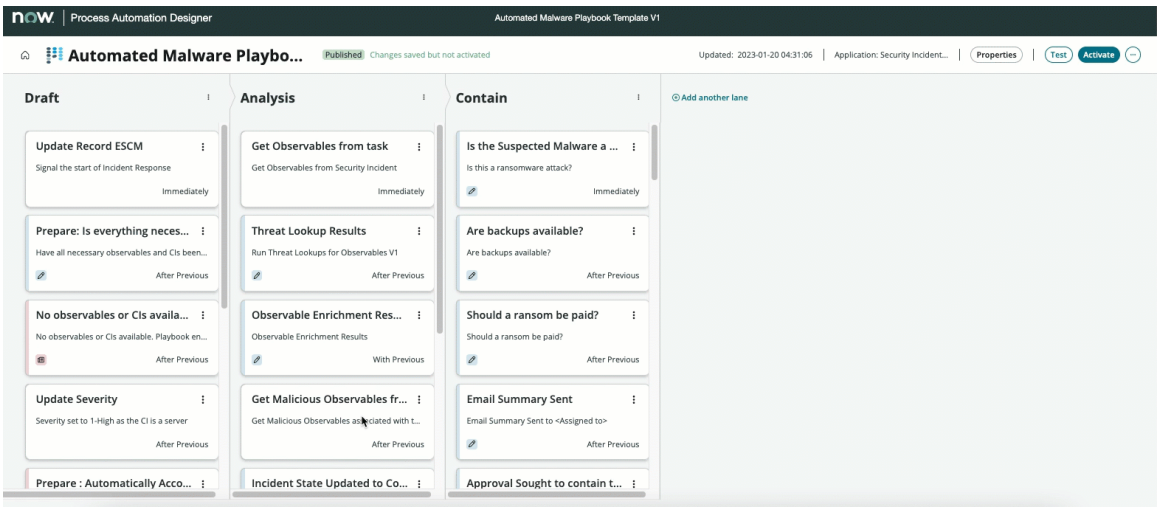


7. Clique **em Ir para Designer**.
   A página do Process Automation Designer é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicionar uma nova raia**.
   O painel de propriedades da raia é aberto no lado direito da IU.
9. No painel de propriedades da raia, insira os seguintes detalhes: **Nome**, **Descrição**, **Condição de execução**e **Indicar quando iniciar**.
   Os campos **Condição de execução** e **Indicar quando iniciar** indicam quando a raia deve ser executada.
10. Clique **em Salvar e fechar**.
11. Para adicionar outra raia, clique em **Adicionar outra raia**.
    Da mesma forma, você pode criar quantas raias quiser. Neste exemplo, você pode criar uma raia para Análise, Conter, Erradicar e Revisar, respectivamente. No exemplo a seguir, a raia de **análise** começa imediatamente e não tem condição de execução. **Contém** o início da raia após a conclusão da raia anterior e tem uma condição de execução que se baseia no resultado de uma atividade na raia anterior.
    Depois de adicionar as raias, você precisa adicionar atividades de processo para cada raia.
12. Clique em **Adicionar outra atividade de processo** em uma raia específica (por exemplo, Raia de análise).
    O pop-up Adicionar atividade é aberto.
    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.
13. Clique **em Criar uma nova atividade**.
    Depois que uma definição de atividade é adicionada, ela pode ser configurada de forma semelhante às raias. Da mesma forma, você pode criar outras atividades de processo em cada raia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade automatizada de malware



14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique **em Exibir todas as propriedades** e habilite a alternância **Propriedades avançadas** para exibir todos os campos de experiência de atividade da definição da atividade.

Como usar o playbook de malware automatizado

Use estas etapas para saber como você pode usar o playbook de malware automatizado no Espaço do analista de SIR e seus recursos.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

Procedimento

1. No espaço de SIR, abra um incidente de segurança.
2. Clique na guia **Playbook**.

   Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

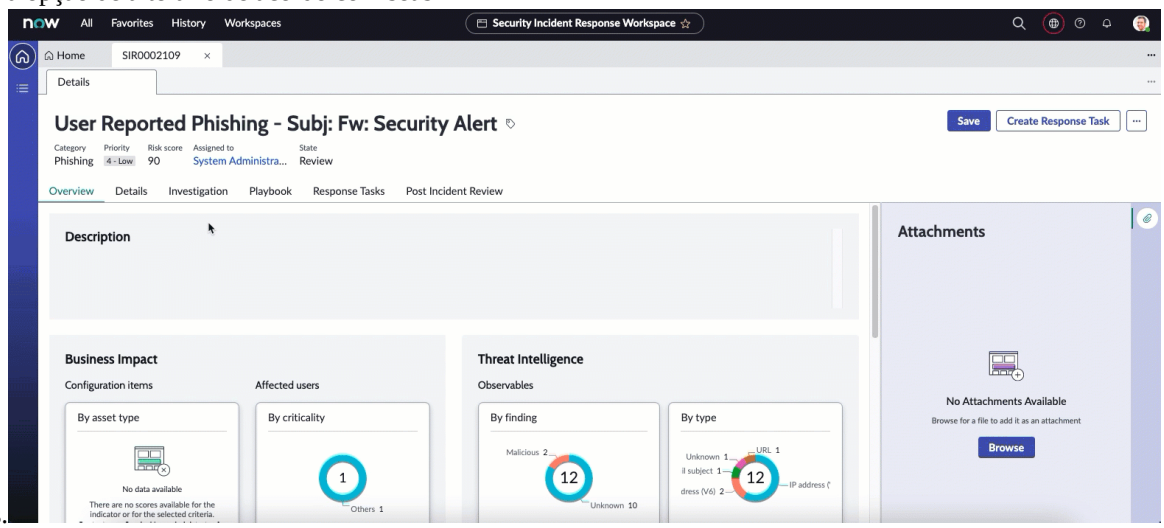
   Nota:
   Se você não vir nenhum playbook listado, precisará ir para o PAD e permitir que ele o veja na guia **Playbook**.

3. Clique no **Automated Malware Playbook**.
   Para malware automatizado, as tarefas são realizadas automaticamente para o incidente de segurança.
4. Clique em cada raia para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** para ver a lista de atividades realizadas na fase de Análise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você tem a opção de alterá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Erradicar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de modificá-los de acordo com seus requisitos. Se houver alguma atividade ou ação do usuário restante que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Playbook para falha de login manual

O playbook de login manual com falha fornece orientação e ajuda a otimizar a investigação de incidentes de segurança de login com falha.

Quando um usuário faz determinadas tentativas de login malsucedidas (de acordo com a configuração do SIM), um incidente de segurança é criado. Essas tentativas de login malsucedidas podem ser falsos positivos ou tentativas feitas por invasores de obter acesso às contas de e-mail do usuário.

Você pode usar os modelos de PAD para executar as etapas no playbook de login com falha e resolver incidentes de segurança de login com falha com eficiência. Este playbook inclui condições do gatilho, uma sequência de ações e subfluxos que você pode anotar. Este playbook contém uma sequência de ações reutilizáveis projetadas para responder a incidentes de segurança de login com falha. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos para anotação.

Este playbook pode ser usado se um incidente de segurança de login com falha for criado ou atualizado. Você precisa ativar o Playbook manual de login com falha no Designer de automação de processos (PAD) e criar todas as tarefas, como análise, contenção, erradicação e revisão.

A seguir estão as raias da definição do processo e correspondem ao estado do incidente de segurança:

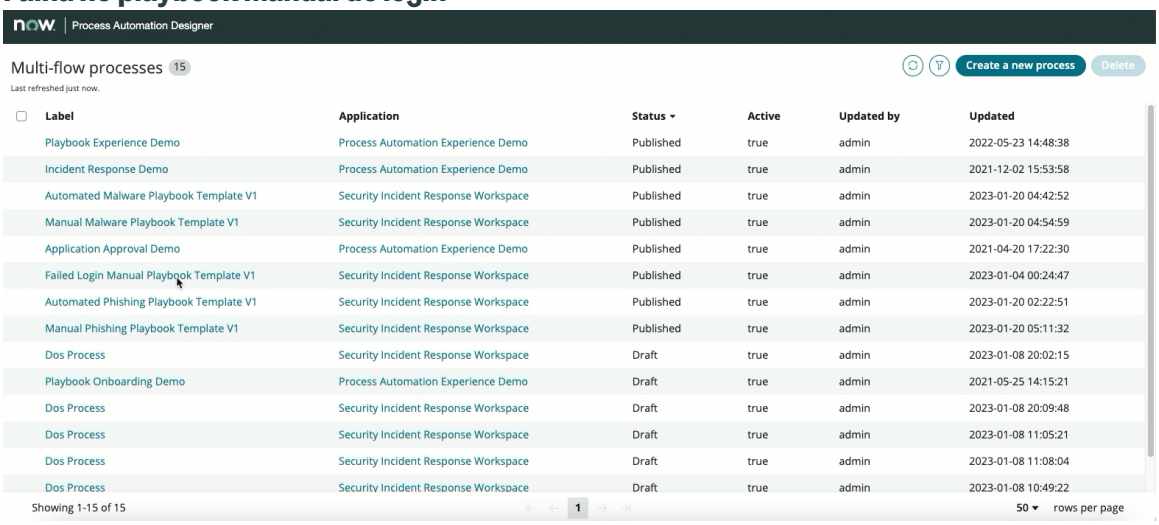
- Análise
- Contém
- Erradicar
- Revisão

Cada raia tem atividades dentro dela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Falha no playbook manual de login



Depois de marcar uma tarefa como concluída em uma raia, você pode passar para a próxima tarefa. Você pode salvar uma tarefa a qualquer momento e retornar ao playbook em uma data e hora posteriores. Depois de concluir todas as tarefas em uma raia, você pode passar para a próxima raia. O status é refletido no painel esquerdo conforme você conclui as tarefas e as raias. Um log de atividades no lado direito do playbook mostra todos os dados que você inseriu para cada tarefa.

Depois de concluir todas as tarefas, você será solicitado a revisar os detalhes inseridos em todas as raias. Você pode optar por editar qualquer campo ou clicar em Concluir para concluir o processo de criação do direito.

Criar processos para falha de login manual no PAD

Use essas etapas para criar processos para Falha no login manual no Designer de automação de processos (PAD).

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager

Procedimento

1. Clicar **TUDO** > **Designer de automação de processos** > > **Criar um novo processo** .

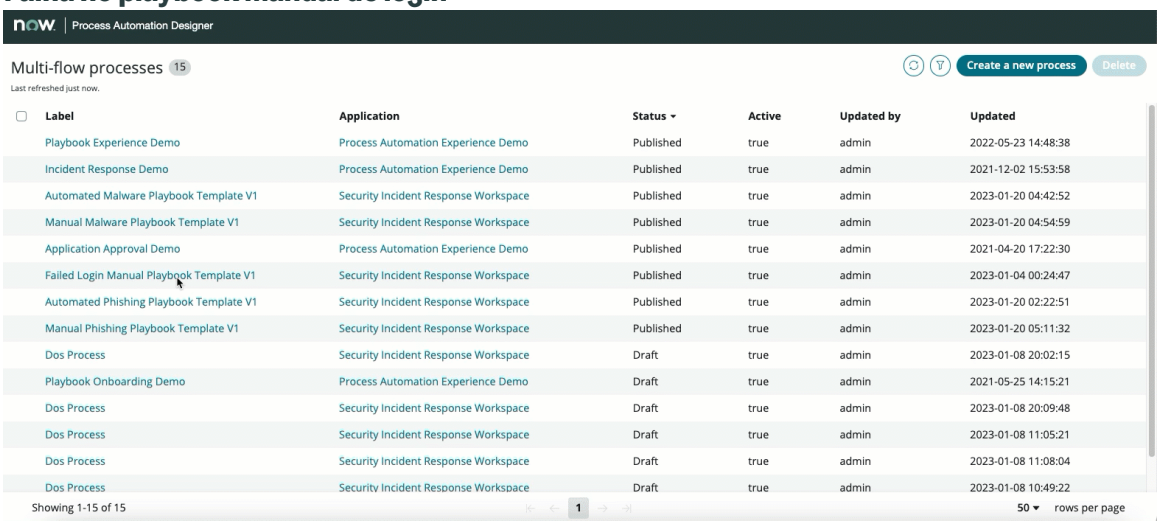
   Por exemplo, Falha no modelo de Playbook manual de login V1.

2. Insira um nome para o processo, a descrição e a aplicação para a qual o processo está sendo criado.
3. Clique **em Selecionar um gatilho**.
4. Selecione **Definir suas próprias condições para quando o processo for executado**e selecione a condição do gatilho para quando o processo deve ser executado.
5. Clique **em Definir condições do gatilho**.
6. Escolha as condições para definir quando o processo deve ser executado selecionando uma tabela e preenchendo as condições.
   Por exemplo, a condição do gatilho é quando um incidente de segurança da categoria Phishing é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Falha no playbook manual de login

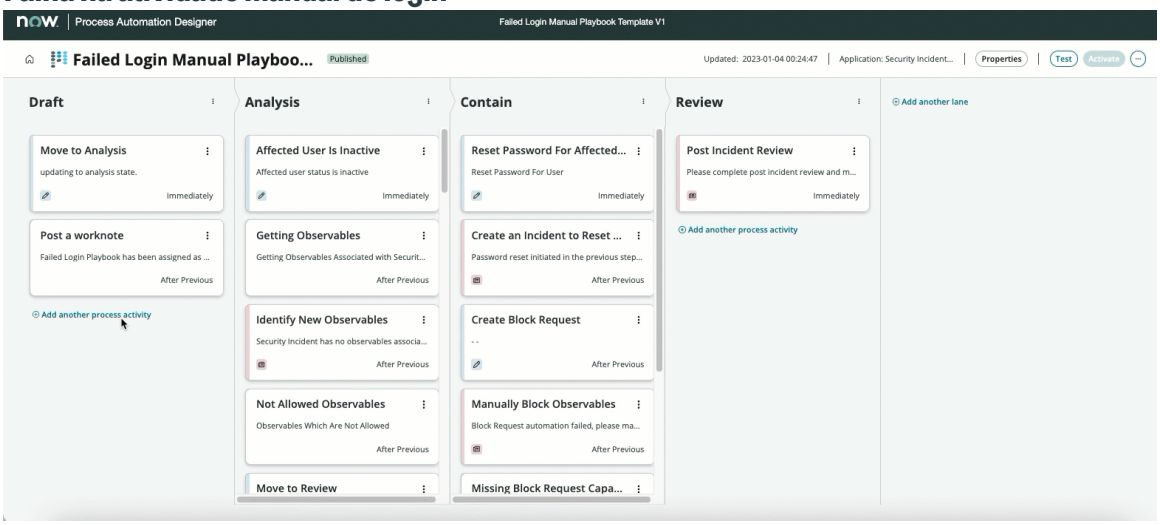


7. Clique **em Ir para Designer**.
   A página do Process Automation Designer é aberta.
8. Para começar a projetar seu processo automatizado, clique em **Adicionar uma nova raia**.
   O painel de propriedades da raia é aberto no lado direito da IU.
9. No painel de propriedades da raia, insira os seguintes detalhes: **Nome**, **Descrição**, **Condição de execução**e **Indicar quando iniciar**.
   Os campos **Condição de execução** e **Indicar quando iniciar** indicam quando a raia deve ser executada.
10. Clique **em Salvar e fechar**.
11. Para adicionar outra raia, clique em **Adicionar outra raia**.
    Da mesma forma, você pode criar quantas raias quiser. Neste exemplo, você pode criar uma raia para Análise, Conter, Erradicar e Revisar, respectivamente. No exemplo a seguir, a raia de **análise** começa imediatamente e não tem condição de execução. **Contém** o início da raia após a conclusão da raia anterior e tem uma condição de execução que se baseia no resultado de uma atividade na raia anterior.
    Depois de adicionar as raias, você precisa adicionar atividades de processo para cada raia.
12. Clique em **Adicionar outra atividade de processo** em uma raia específica (por exemplo, Raia de análise).
    O pop-up Adicionar atividade é aberto.
    a. No pop-up Adicionar atividade, selecione a definição de atividade necessária.
13. Clique **em Criar uma nova atividade**.
    Depois que uma definição de atividade é adicionada, ela pode ser configurada de forma semelhante às raias. Da mesma forma, você pode criar outras atividades de processo em cada raia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Falha na atividade manual de login



14. No painel Propriedades da atividade, adicione uma condição de execução e indique quando iniciar a atividade do processo.
15. Adicione uma condição de execução e indique quando iniciar.
    Todas as entradas necessárias para esta atividade (inclui entradas no plano de automação que estão configuradas) serão mostradas. Você pode substituir os valores ou usar os valores pré-configurados.
16. Clique **em Exibir todas as propriedades** e habilite a alternância **Propriedades avançadas** para exibir todos os campos de experiência de atividade da definição da atividade.

Como usar o playbook manual de login com falha

Use estas etapas para saber como você pode usar o playbook Manual de login com falha no Espaço do analista de SIR e seus recursos.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.manager ou sn_si.analyst

Procedimento

1. No espaço de SIR, abra um incidente de segurança.
2. Clique na guia **Playbook**.

   Você pode exibir os playbooks que foram habilitados para o incidente de segurança. Você também pode ver detalhes como a categoria do incidente de segurança e a pontuação de risco.

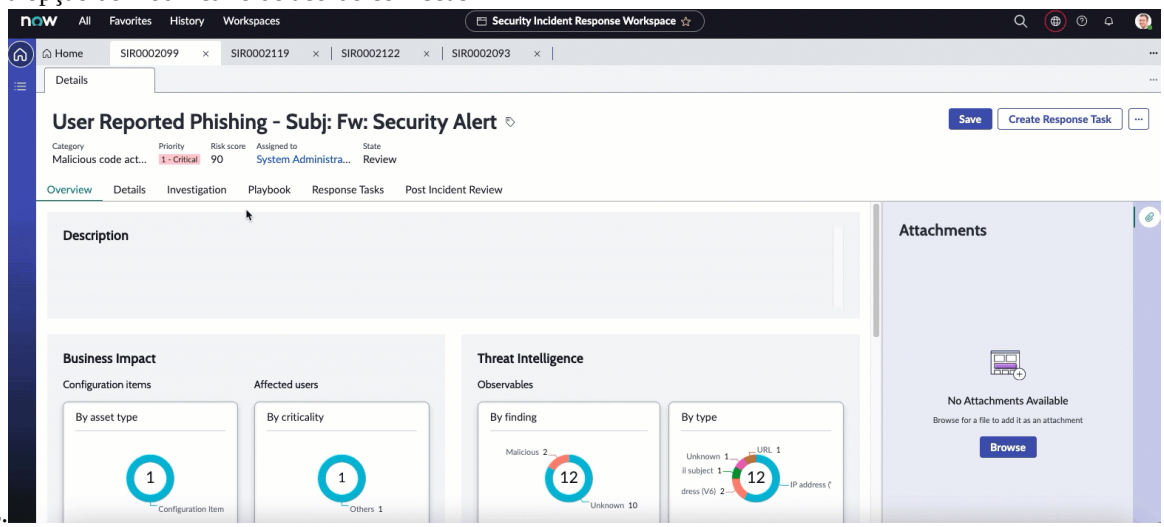
   Nota:
   Se você não vir nenhum playbook listado, precisará ir para o PAD e permitir que ele o veja na guia **Playbook**.

3. Clique no **Playbook manual de login com falha**.
   Para Falha no login manual, as tarefas são realizadas automaticamente para o incidente de segurança.
4. Clique em cada raia para saber quais tarefas foram realizadas por este playbook.
5. Clique em **Análise** para ver a lista de atividades realizadas na fase de Análise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você tem a opção de modificá-lo de acordo com seus requisitos.



6. Da mesma forma, você pode clicar em Conter, Erradicar e Revisar para exibir a lista de atividades que foram realizadas na respectiva fase.
   Você tem a opção de alterá-los de acordo com seus requisitos. Se houver alguma atividade ou ação do usuário restante que você precise executar, ela será exibida na respectiva fase.
7. Se houver alguma atividade restante ou ação do usuário necessária em qualquer uma das fases, clique na respectiva fase e execute a ação para concluir a atividade.

Playbooks baseados em fluxo

Usando o Flow Designer, os administradores de segurança e os autores de design de fluxo podem fazer a transição com mais facilidade de playbooks manuais ou não documentados para playbooks automatizados e repetíveis. O recurso de arrastar e soltar fornece flexibilidade ao mover objetos, verificações de condição, ramificação paralela, tabelas de decisão e muito mais.

Security Incident Response fornece os seguintes playbooks com o sistema de base.

Além dos playbooks listados, também há subfluxos no Security Operations Spoke que podem ser chamados do playbook de fluxos. O ransomware é um desses subfluxos.

Ative esses fluxos antes de usá-los. Para obter mais informações, consulte Ativação de um fluxo do Security Incident Response.

Playbook for Automated Phishing

O playbook de phishing automatizado ajuda a resolver determinados tipos de ameaças à segurança passo a passo. Com os modelos do Flow Designer, você pode automatizar as etapas do playbook de resposta de phishing e resolver incidentes de forma rápida e eficiente.

Você pode usar modelos criados com o Flow Designer para automatizar as tarefas no Playbook de resposta de phishing para analisar e resolver ataques de phishing em sua organização.

O playbook de resposta de phishing inclui os seguintes fluxos e subfluxos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Incidente de segurança - Modelo de resposta de phishing automatizado: este modelo foi projetado para automatizar as tarefas de resposta de phishing e contém uma sequência de ações, incluindo um gatilho.
- Incidente de segurança - Modelo manual de phishing: este modelo é o fluxo de trabalho de resposta de phishing manual existente. Defina a categoria como Phishing para ativar o fluxo.

Esses modelos contêm uma sequência de ações reutilizáveis projetadas para responder a ataques de phishing. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos que você pode anotar para facilitar a leitura. Para acessar esses fluxos, você deve instalar ospoke do Security Operations .

Nota:
Ative esses modelos antes de usá-los. Consulte Ativar um fluxo do Security Incident Response para obter detalhes.

- Executar pesquisas de ameaças para observáveis: executa pesquisas de ameaças de observáveis selecionados.
- Aprimorar observáveis: permite aprimorar observáveis com informações adicionais de várias fontes.
- Avaliar o impacto do e-mail de phishing: permite que você avalie o impacto do e-mail de phishing. Quando você recebe um e-mail no endereço de e-mail de phishing, este subfluxo analisa o anexo .EML e compara as informações com as regras de correspondência de e-mail.
- Erradicar e-mails de phishing: permite excluir ou erradicar e-mails de phishing para ajudar a reduzir a exposição a um ataque específico.
- Executar pesquisa de detecções em observáveis: determina a predominância de uma ameaça ao longo do tempo ou testa os esforços de correção ou erradicação.
- Criar solicitações de bloqueio: bloqueia a comunicação com observáveis associados ao incidente.

Esses subfluxos representam um conjunto de operações reutilizáveis que você pode usar em vários playbooks. Você pode usar esses subfluxos para definir modelos personalizados (fluxos) de acordo com seus requisitos.

Para criar modelos personalizados (fluxos), siga as instruções em Fluxos .

Executar o fluxo do playbook de resposta de phishing automatizado

Usando o Flow Designer, você pode definir e automatizar tarefas no playbook para analisar e resolver ataques de phishing contra sua organização.

Antes de Iniciar

- Função necessária: sn_si.admin, flow_designer e action_designer
- Instale e configure as seguintes integrações com as credenciais corretas:
  - Solicitação de bloqueio (Security Operations Integração de NGFW da Palo Alto Networks)
  - Aprimoramento de Observável
  - Pesquisa de vista
  - Pesquisa de ameaças
  - Microsoft Office Exchange

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

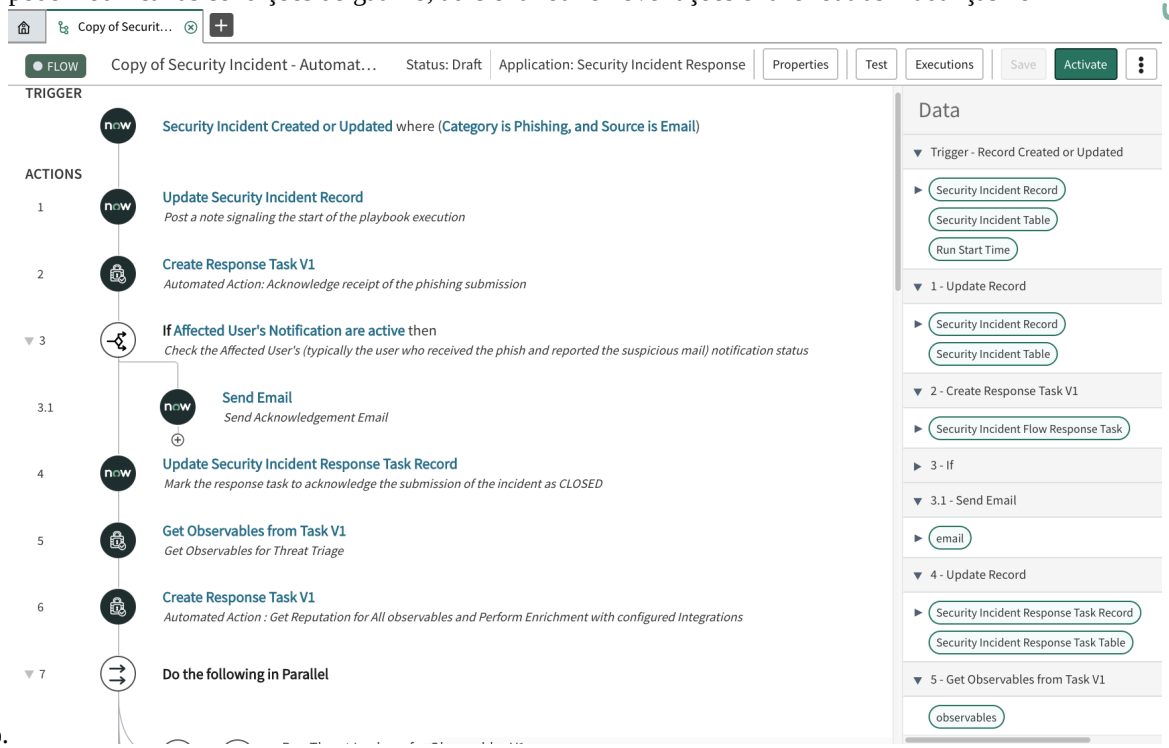
Quando os funcionários recebem um e-mail suspeito que contém os sinais comuns de um ataque de phishing (conforme definido por suas políticas de segurança), eles podem enviá-lo como um anexo .EML para o endereço de e-mail de phishing definido pela sua organização. Usando as tarefas definidas no fluxo do playbook automatizado de phishing, você pode fazer a triagem, analisar, conter e erradicar uma ameaça de phishing. Essas tarefas podem ser invocadas como parte de diferentes estados de incidente (por exemplo, Análise, Contêm e assim por diante). Quando um incidente de segurança de phishing é criado, o fluxo de phishing automatizado pode ser acionado automaticamente. Usando o Flow Designer, você pode exibir os detalhes das várias ações de resposta do incidente conforme elas são invocadas.

Nota:
O fluxo do playbook Incidente de segurança - Modelo de resposta de phishing automatizado V1 é Somente leitura. Você pode fazer uma cópia do fluxo e fazer mudanças conforme necessário.

As etapas a seguir descrevem como fazer uma cópia do modelo de playbook de phishing e orientam você em algumas das tarefas no fluxo.

Procedimento

1. Navegar até **Todos** > **Flow Designer** > **Designer** para exibir os fluxos disponíveis com o Security Operations Spoke.
2. Clique no link **Incidente de segurança - IV de modelo de resposta de phishing automatizado**.
3. Na página Fluxo, clique no ícone mais ícone , faça uma cópia do fluxo e abra-o para uso.
   Você pode modificar as condições do gatilho, adicionar ou remover ações e fazer outras mudanças no fluxo.



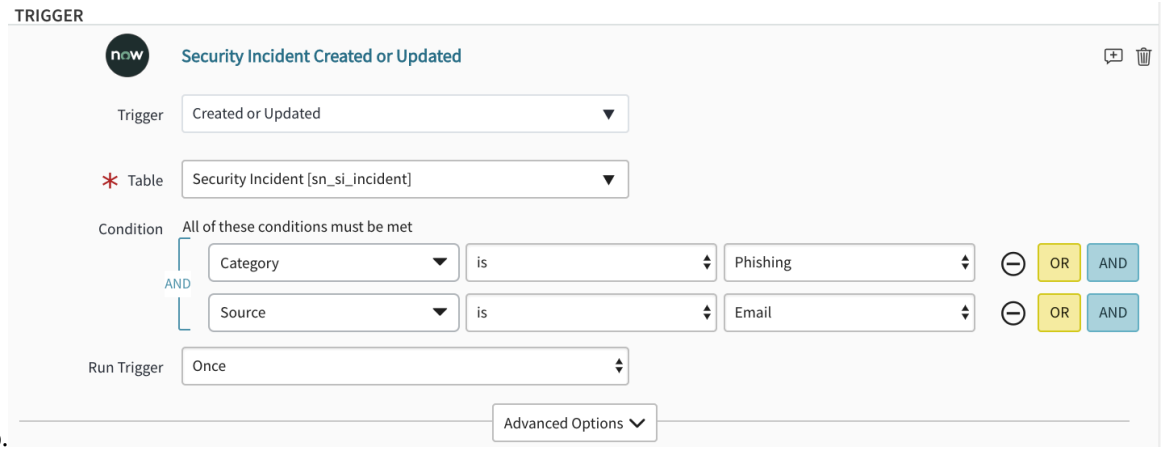
   Esta imagem mostra as condições do gatilho e as etapas que o fluxo executa. O painel à direita mostra o fluxo de dados. Clique em um ícone para expandir a etapa e exibir os detalhes.

4. Clique no ícone **Gatilho**.

Tradução automática

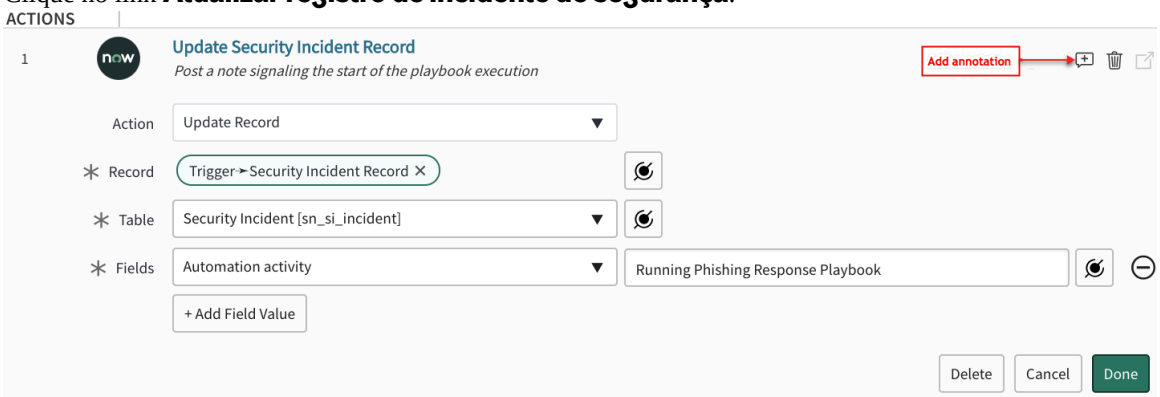
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na primeira etapa, você define ou define o gatilho do fluxo. Especifique as condições do gatilho e com que frequência você deseja que o fluxo execute o gatilho.



Quando as condições definidas no fluxo (a categoria é Phishing e a origem é e-mail) são atendidas no registro do incidente, as tarefas no fluxo de phishing automatizado começam a ser executadas sequencialmente. Você pode modificar o gatilho, adicionar anotações, adicionar ou excluir condições e assim por diante.

5. Clique no link **Atualizar registro de incidente de segurança**.



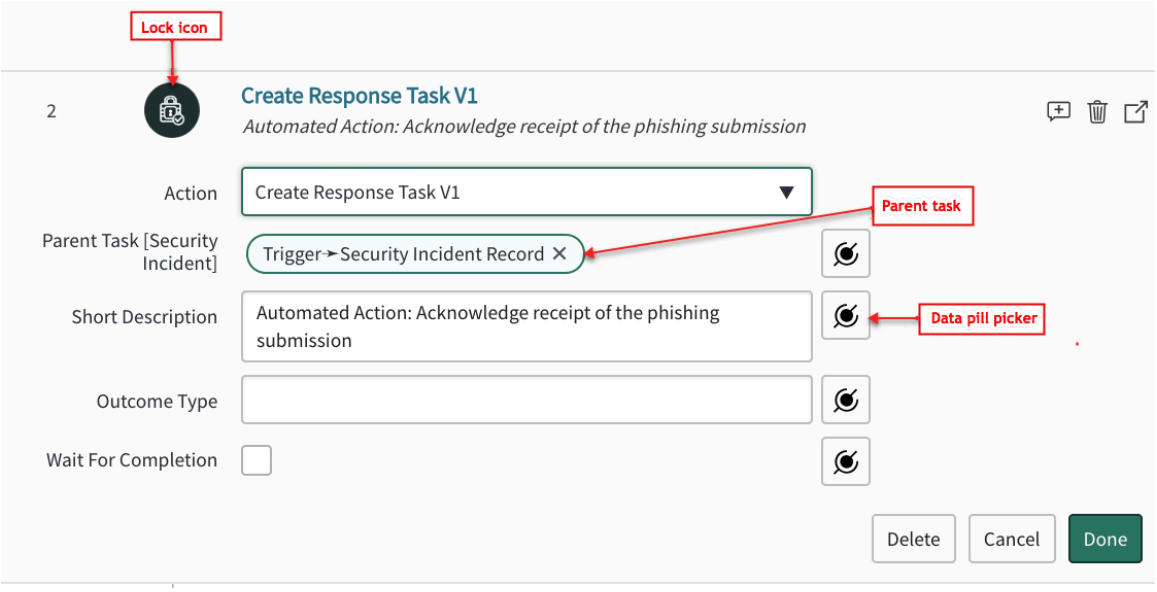
Atualizar registro de incidente de segurança é a primeira etapa do fluxo. Clique no ícone de anotação Ícone de para adicionar uma anotação ao analista de segurança indicando que ocorreu um incidente de phishing e que o fluxo do playbook de phishing automatizado começou a ser executado.

6. Prossiga com a etapa 2 no fluxo e clique no link **Criar tarefa de resposta**.

Nesta etapa, o fluxo cria uma tarefa de resposta automatizada para confirmar o recebimento ao remetente do incidente ou ao usuário afetado.

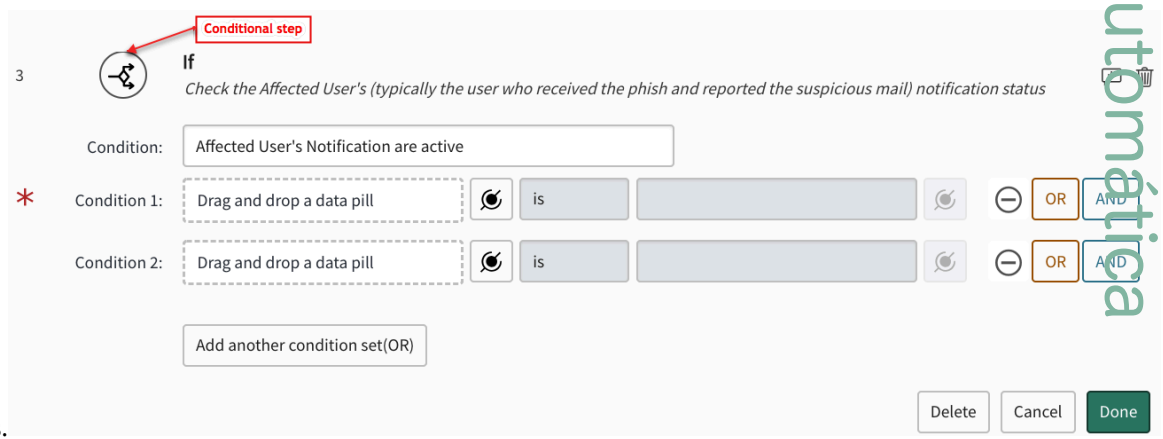
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Observe que o campo **Tarefa primária [Incidente de segurança]**faz referência ao registro primário associado a esta etapa. Você pode escolher qualquer registro de referência usando o ícone do selecionador de cápsula de ou arrastar o item de referência relevante do painel direito. Observe o ícone de cadeado Ícone de . O ícone de cadeado indica que a etapa não requer nenhuma intervenção do usuário.

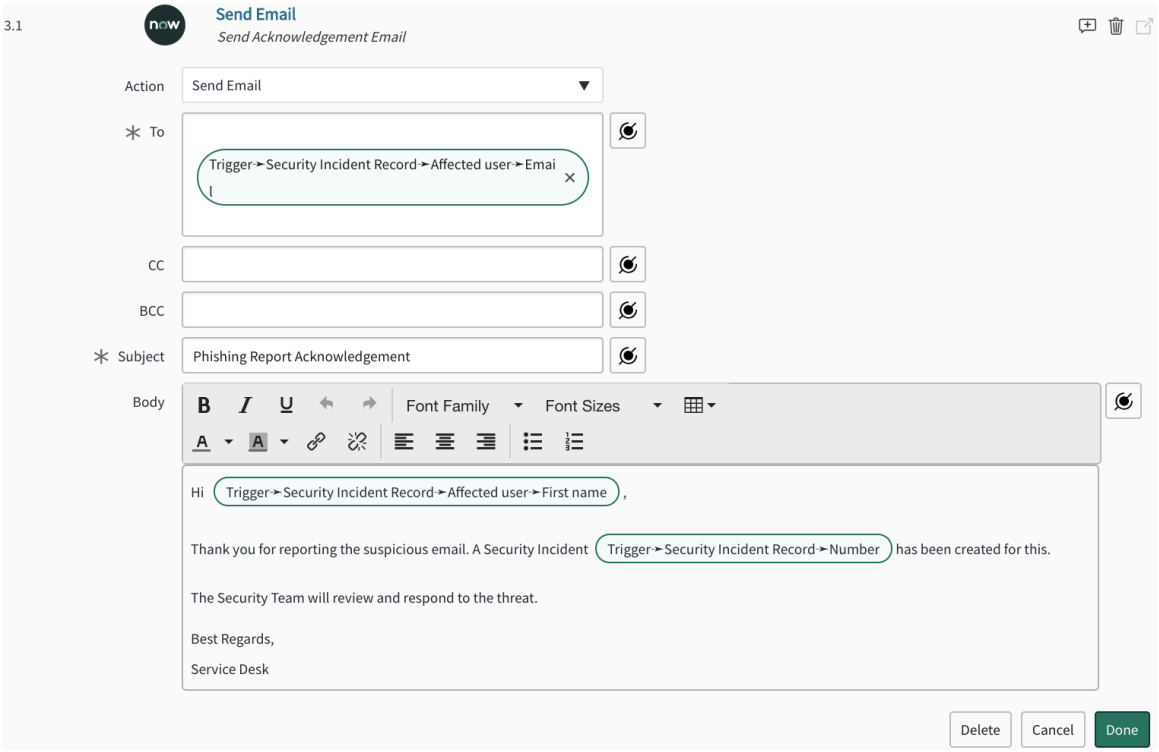
7. Na etapa 3, o fluxo coleta detalhes adicionais do usuário afetado (normalmente o usuário que enviou o incidente) para garantir que ele possa enviar uma notificação com sucesso.
Você pode especificar condições para verificar se o status do usuário afetado está ativo e se o usuário pode receber notificações.



Observe o ícone de etapa na etapa 3. O fluxo executa a próxima etapa (3.1) somente se as condições especificadas forem atendidas.

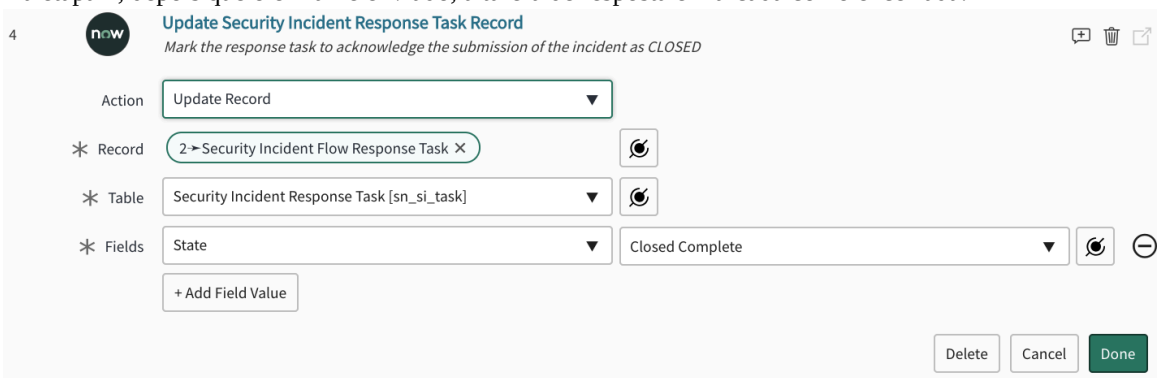
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

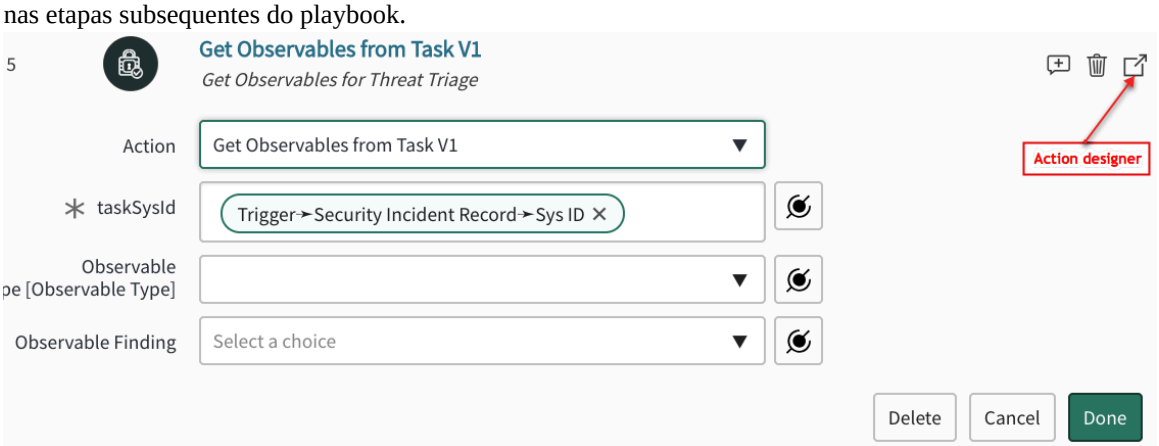


Quando as condições definidas na etapa 3 forem atendidas com sucesso, o e-mail será enviado.

8. Na etapa 4, depois que o e-mail é enviado, a tarefa de resposta é marcada como encerrada.



9. Na etapa 5, todos os observáveis envolvidos no incidente (como assunto do e-mail, endereço de e-mail do qual o e-mail de phishing foi enviado, URL de phishing) ou observáveis pertencentes a uma categoria selecionada (hash, arquivo ou domínio) são coletados para executar tarefas automatizadas adicionais ações nas etapas subsequentes do playbook.



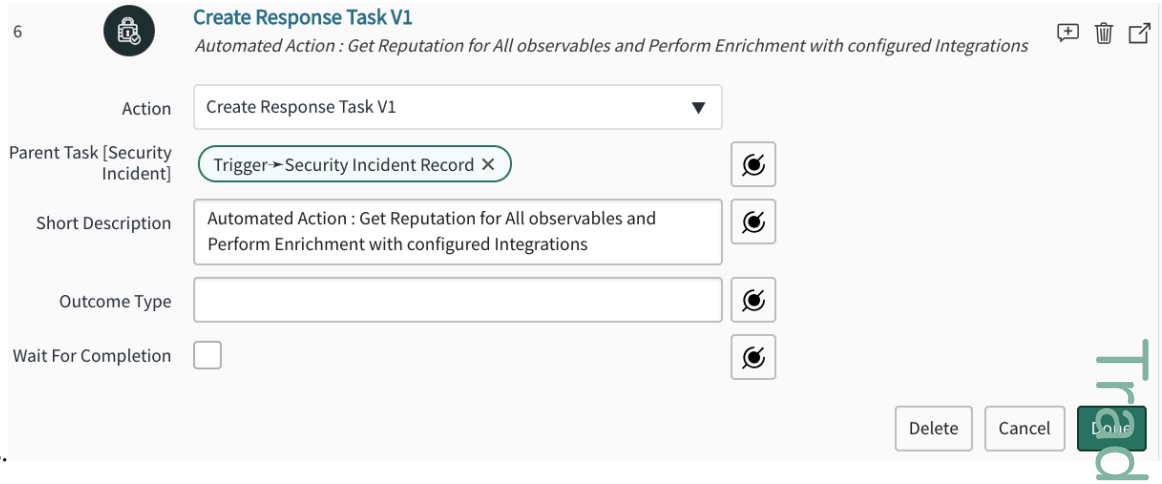
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

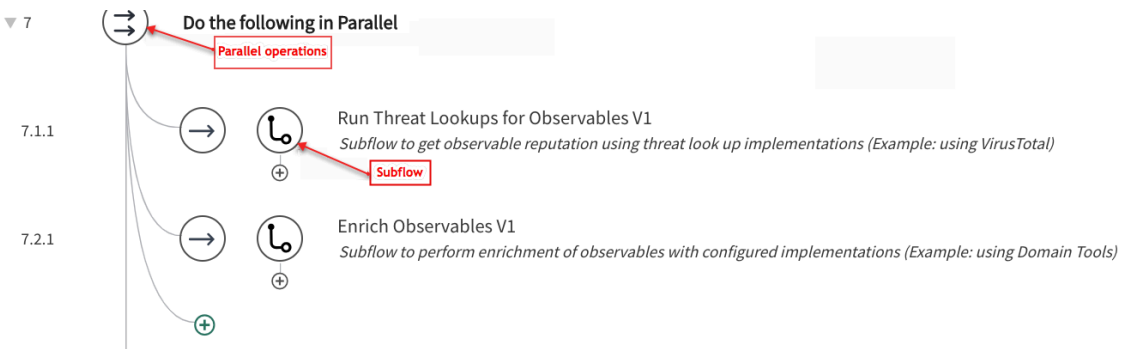
Clique no ícone do designer de ação Ícone para obter uma exibição detalhada da ação.

Para exibir a página do Designer de ações, expanda uma etapa no fluxo e clique no ícone do designer de ações.

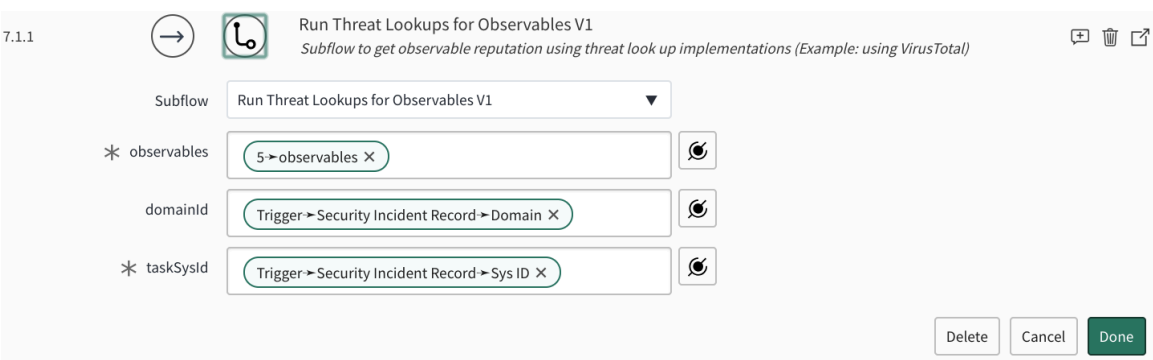
10. Na etapa 6, uma tarefa de resposta automatizada é criada.
Esta tarefa captura o início do processo de obtenção da reputação de todos os observáveis e execução do aprimoramento com integrações configuradas.



11. Na etapa 7, dois subfluxos são chamados:
    - Executar pesquisas de ameaças para observáveis: este subfluxo é usado para obter a reputação de todos os observáveis usando implementações de pesquisa de ameaças.
    - Aprimorar observáveis: este subfluxo é usado para executar o aprimoramento de observáveis com implementações configuradas.



Observe os ícones para esta tarefa. O ícone de operações indica que ambas as tarefas serão realizadas em paralelo e o ícone de subfluxo de subfluxo indica que a tarefa que está sendo executada é um subfluxo conforme mostrado abaixo:

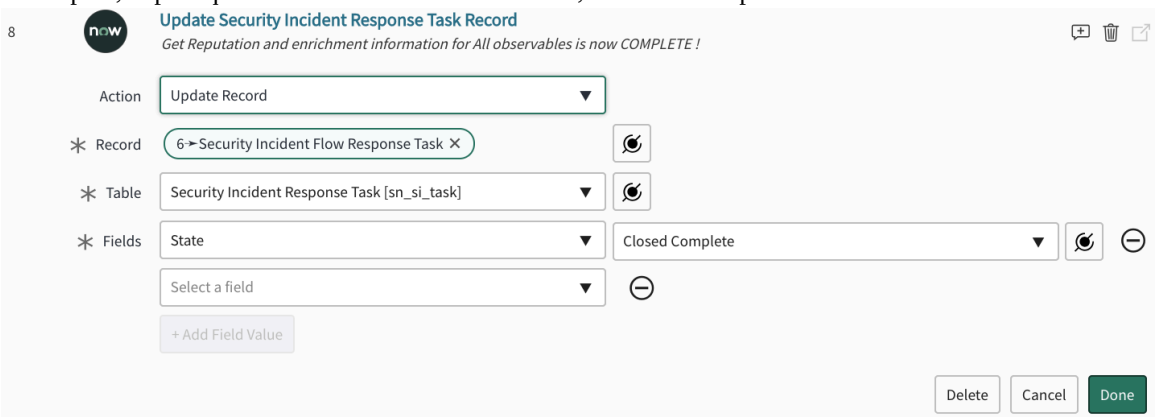


Tradução automática

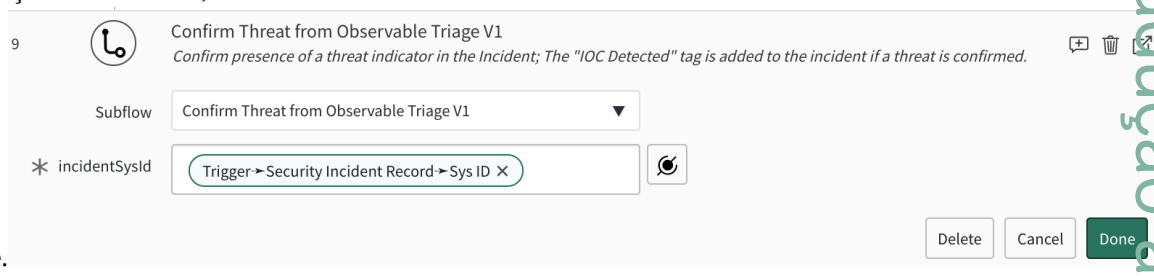
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Observe o número 5 no campo de observáveis. Isso indica que a pesquisa de ameaças será executada nos observáveis recuperados na etapa 5. Esse subfluxo, por sua vez, chama fluxos de trabalho e ações existentes, conforme mostrado no Designer de subfluxos.

12. Na etapa 8, depois que os subfluxos forem concluídos, a tarefa de resposta será marcada como Encerrada.

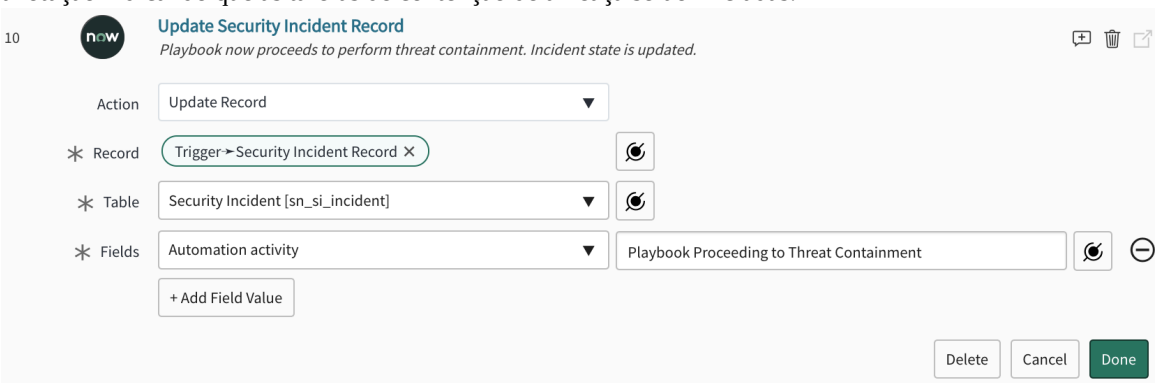


13. Na etapa 9, o subfluxo Confirmar ameaça da triagem observável é chamado.
Este subfluxo é usado para confirmar a presença de um indicador de ameaça no incidente.
Se a ameaça for confirmada, um sinalizador "IOC detectado" será adicionado ao



incidente.

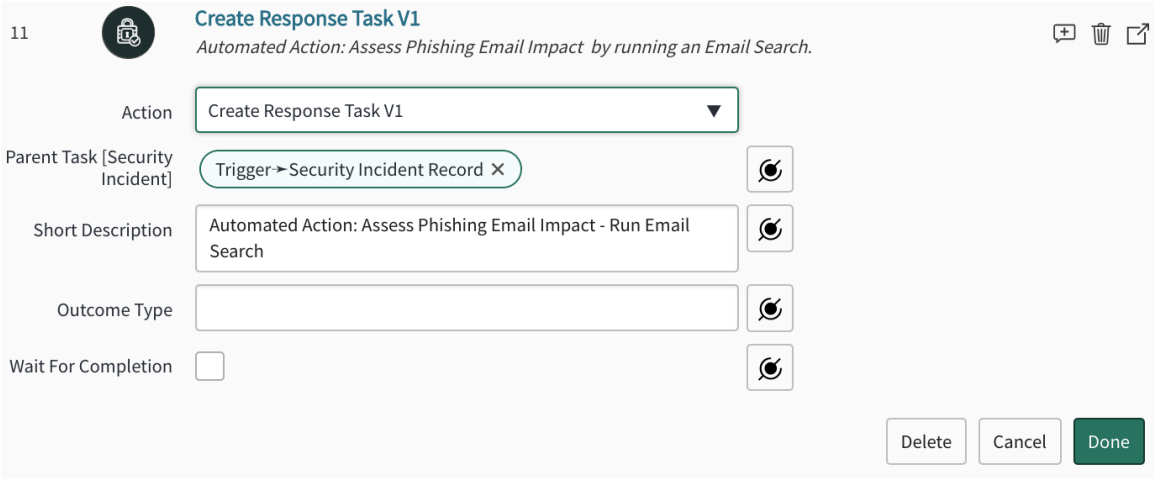
14. Quando a ameaça for confirmada, na etapa 10, você atualiza o incidente de segurança e adiciona uma anotação indicando que as tarefas de contenção de ameaça serão iniciadas.



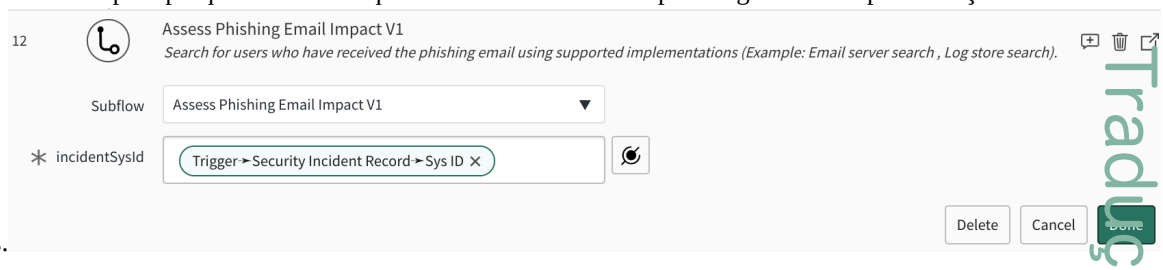
15. A etapa 11 é uma tarefa de resposta automatizada que captura o início e a conclusão da tarefa usada para avaliar o impacto dos e-mails de phishing.

Tradução automática

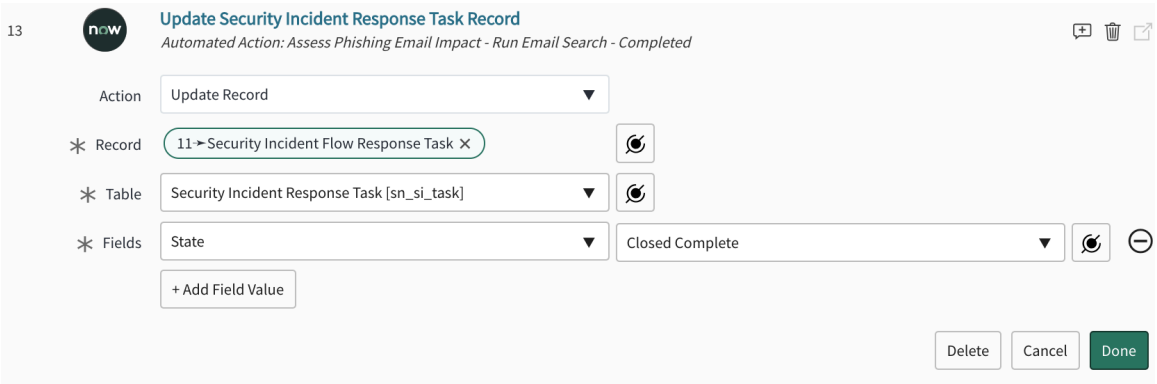
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



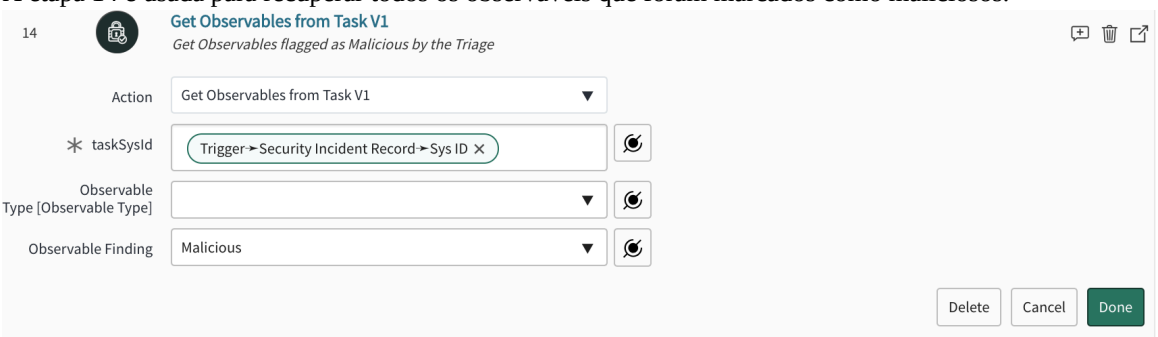
16. Na etapa 12, o subfluxo Avaliar o impacto do e-mail de phishing é chamado.
Este subfluxo é usado para pesquisar usuários que receberam o e-mail de phishing usando implementações compatíveis.



17. Na etapa 13, a tarefa é marcada como encerrada para indicar que o subfluxo Avaliar o impacto do e-mail de phishing foi executado.



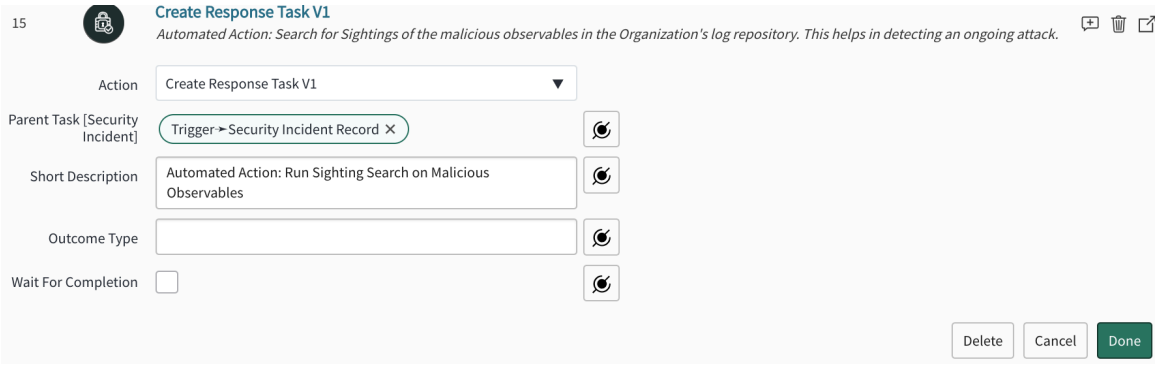
18. A etapa 14 é usada para recuperar todos os observáveis que foram marcados como maliciosos.



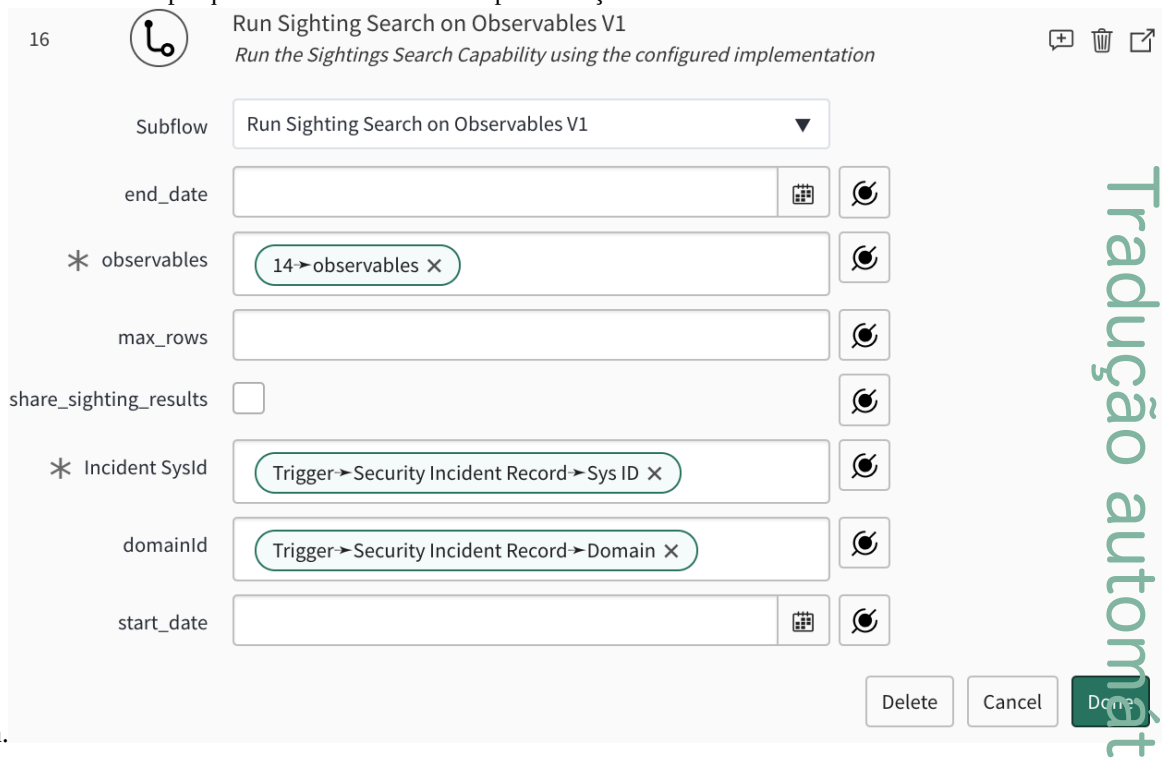
19. A etapa 15 é uma tarefa de resposta automatizada que captura o início e a conclusão da tarefa de pesquisa de vista de observáveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

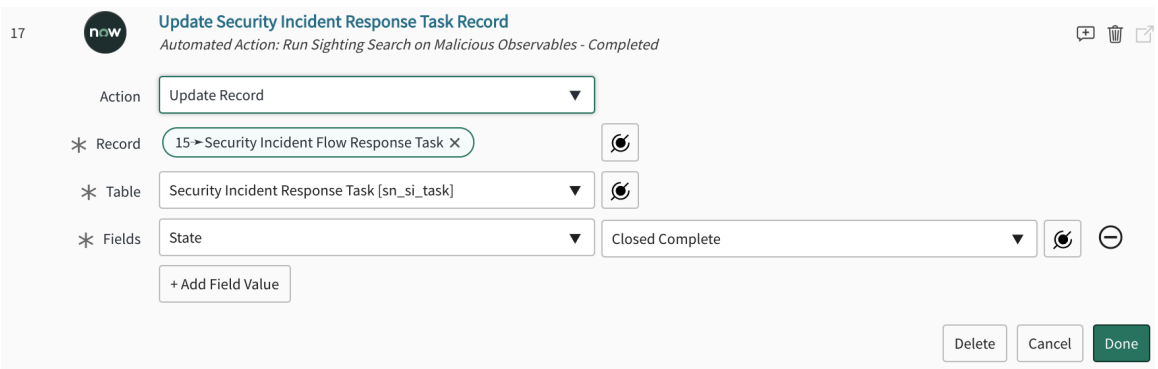


20. Na etapa 16, o subfluxo Executar pesquisa de detecções em observáveis é chamado. Este subfluxo executa uma pesquisa de vistas usando a implementação



configurada.

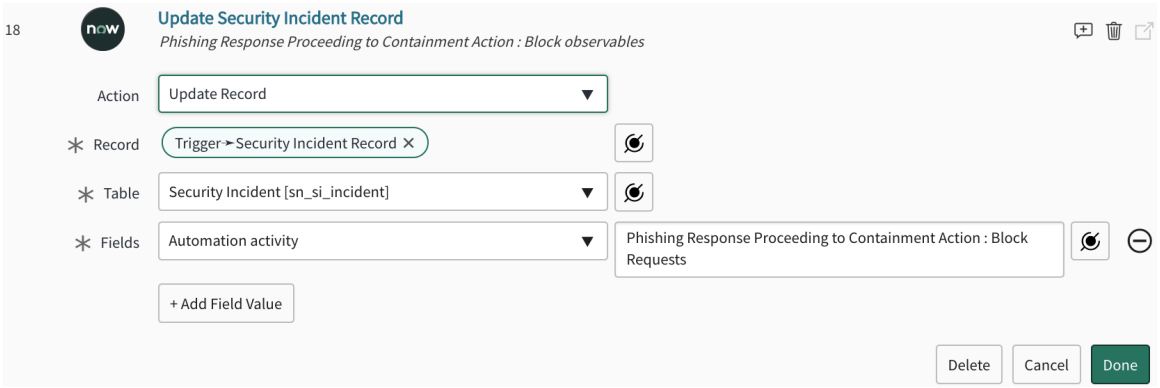
21. Na etapa 17, a tarefa é marcada como encerrada para indicar que o subfluxo Executar pesquisa de vistas em observáveis foi concluído.



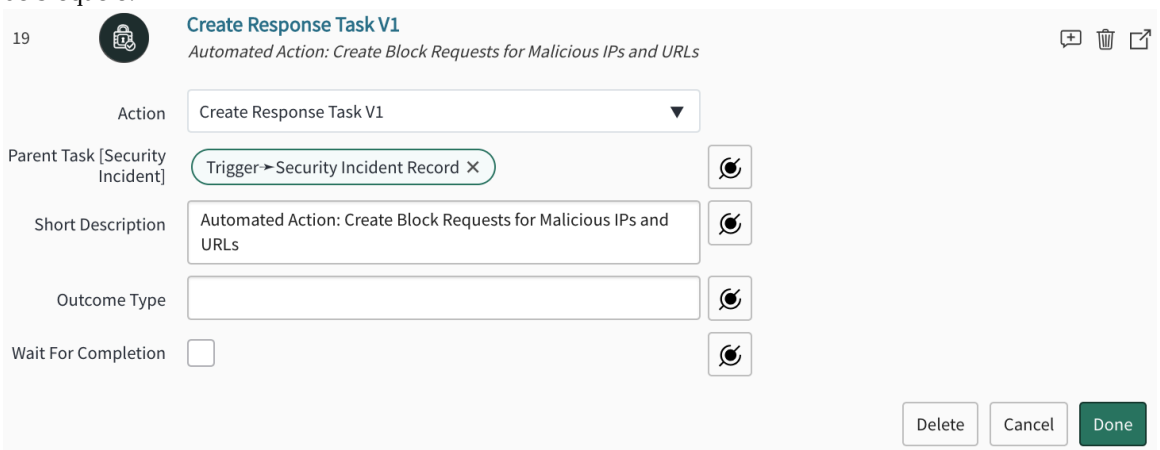
22. Depois de identificar os observáveis maliciosos, na etapa 18, você atualiza o registro de incidente de segurança para indicar que as ações de contenção serão iniciadas agora.

Tradução automática

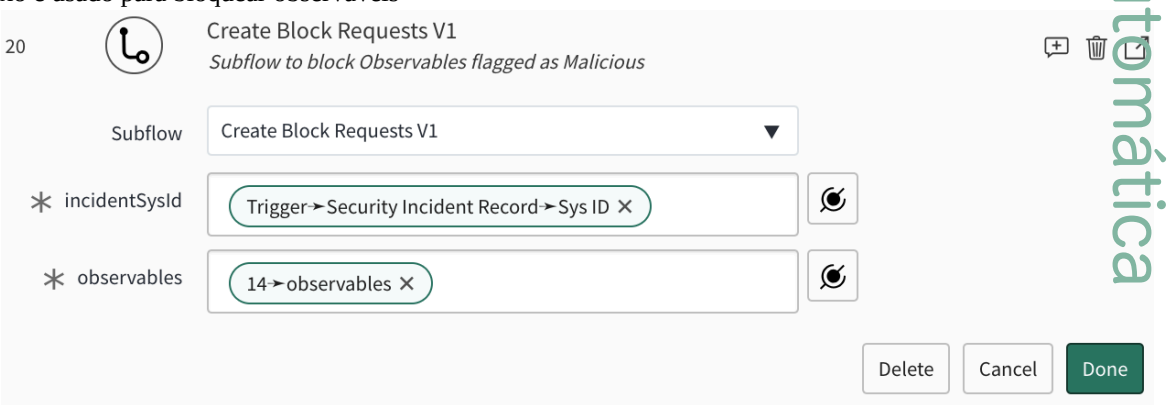
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



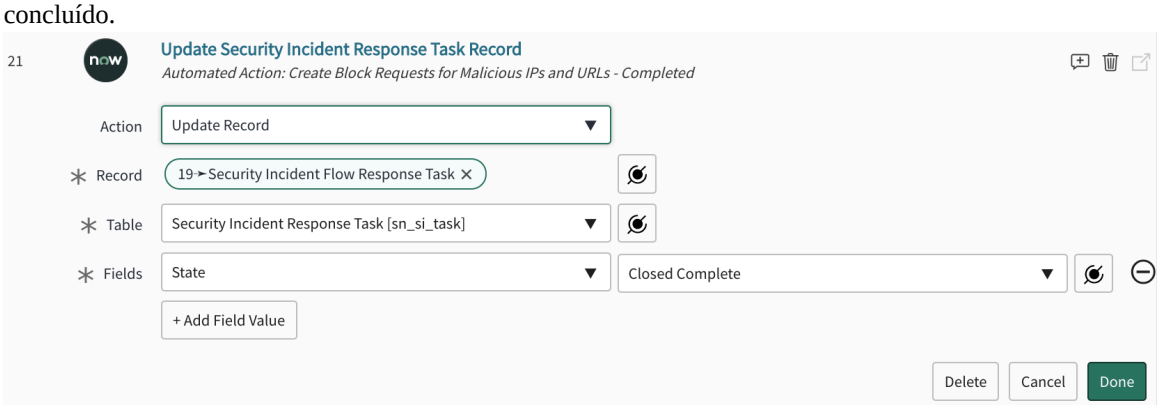
23. A etapa 19 é uma tarefa de resposta automatizada que captura o início e a conclusão da tarefa de solicitações de bloqueio.



24. Na etapa 20, o subfluxo Criar solicitações de bloqueio é chamado. Este subfluxo é usado para bloquear observáveis maliciosos.



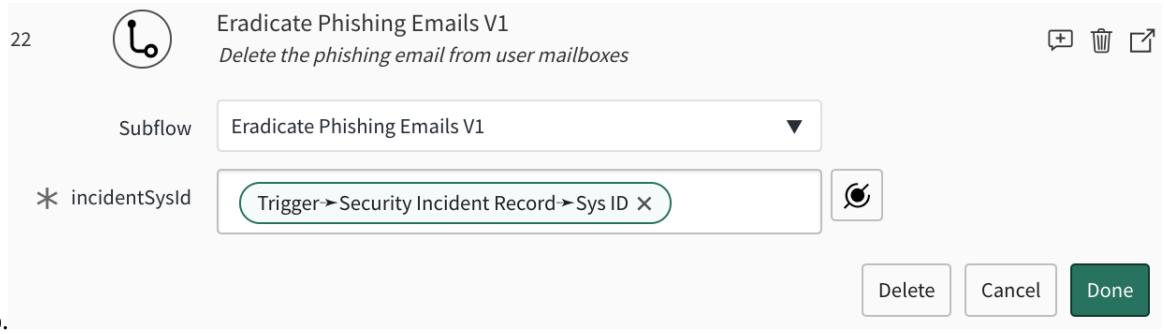
25. Na etapa 21, a tarefa é marcada como encerrada para indicar que o subfluxo Criar solicitações de bloqueio foi concluído.



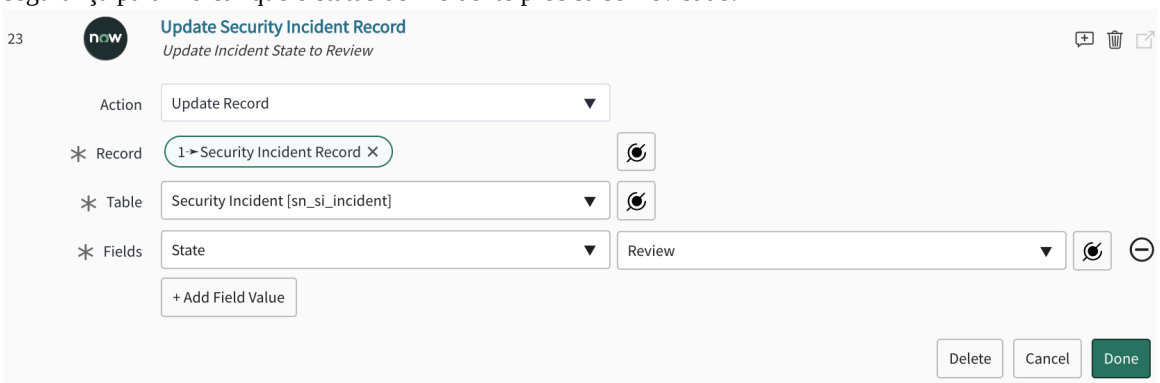
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

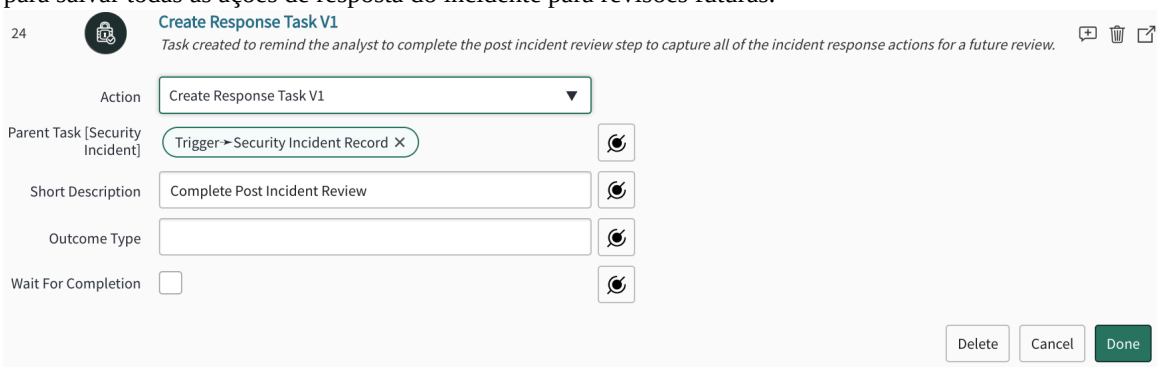
26. Na etapa 22, o subfluxo Erradicar e-mails de phishing é chamado.
Este subfluxo é usado para excluir e-mails de phishing das caixas de correio do usuário.



27. Depois que os e-mails de phishing forem excluídos, na etapa 23, você atualizará o registro do incidente de segurança para indicar que o status do incidente precisa ser revisado.



28. Na última etapa, o fluxo cria uma tarefa de resposta automatizada.
Esta tarefa é usada para enviar um lembrete ao analista de segurança para salvar todas as ações de resposta do incidente para revisões futuras.



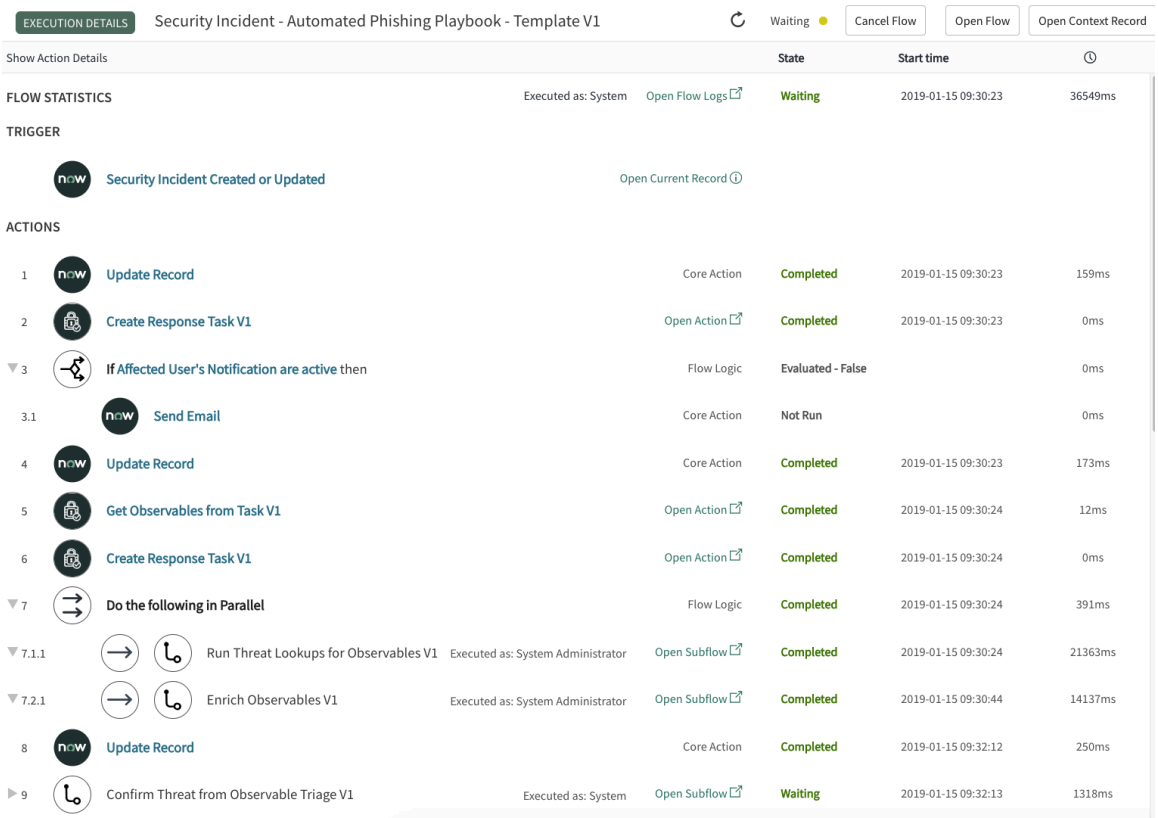
O que Fazer Depois

Você pode clicar em **Testar** para simular as ações no fluxo antes de publicá-lo. Depois de testar o fluxo, clique em **Ativar** para ativar o fluxo e executá-lo.

Clique em **Execuções** para exibir os detalhes da execução do fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



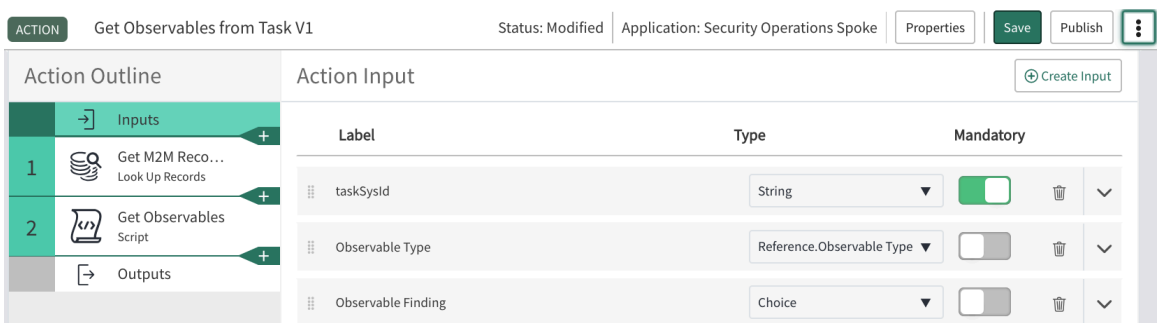
Exibir designer de ação de fluxo do playbook de resposta de phishing automatizado

Você pode fazer uma busca detalhada no Designer de ações para exibir informações detalhadas sobre as ações que estão sendo realizadas para uma etapa específica no fluxo do playbook de resposta de phishing automatizada.

Esta página descreve a página do Designer de ações para a etapa Obter observáveis da tarefa. Clique em uma tarefa no painel Contorno da ação para exibir os detalhes.

Ação de entrada

Esta seção mostra detalhes sobre como a ação foi criada, incluindo o ID do incidente, o tipo de observável (hash ou IP) e a descoberta do observável (somente e-mails maliciosos).

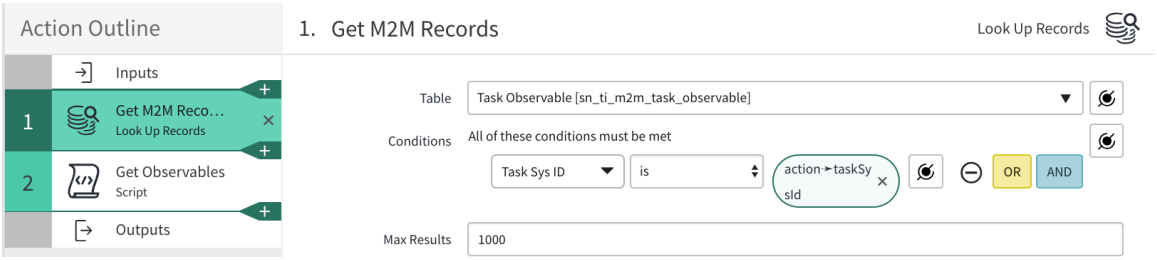


Obter registros M2M

Esta seção mostra as condições que foram definidas para pesquisar observáveis em uma tabela especificada.

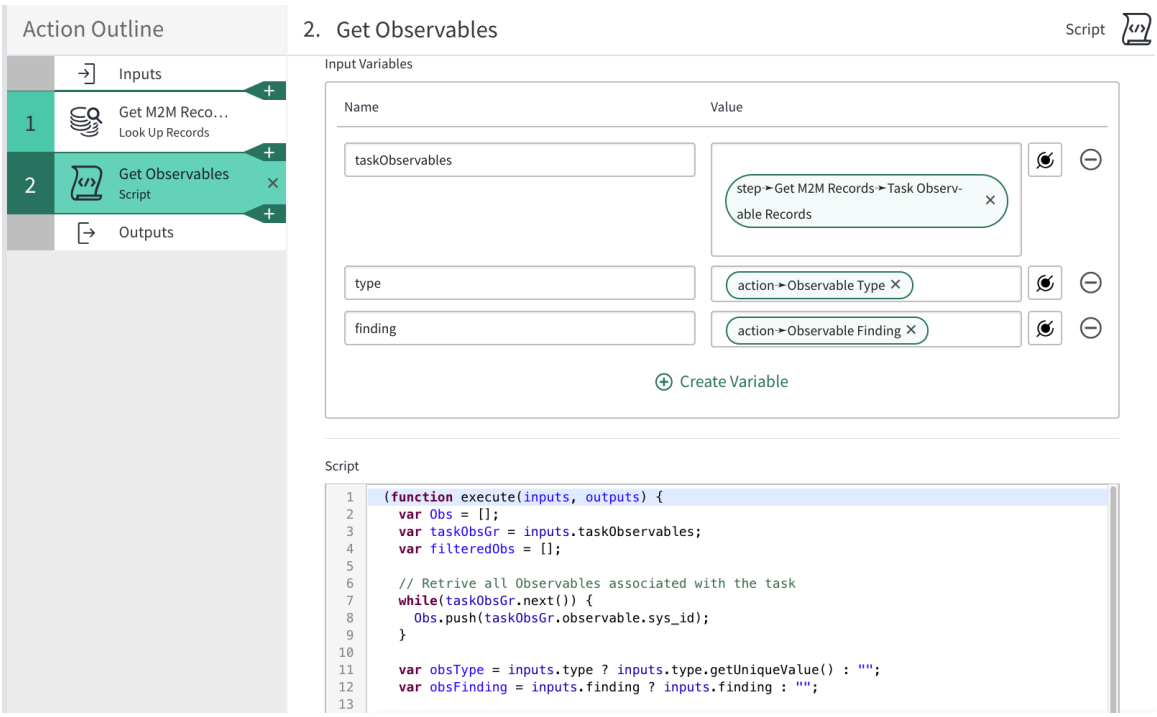
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Obter observáveis

Esta seção mostra o script usado para recuperar observáveis com base nas condições de filtro especificadas. Por fim, os observáveis que atendem a esses critérios e a contagem são exibidos.



Nota:
Todas as ações definidas neste fluxo são reutilizáveis e podem ser modificadas de acordo com seus requisitos.

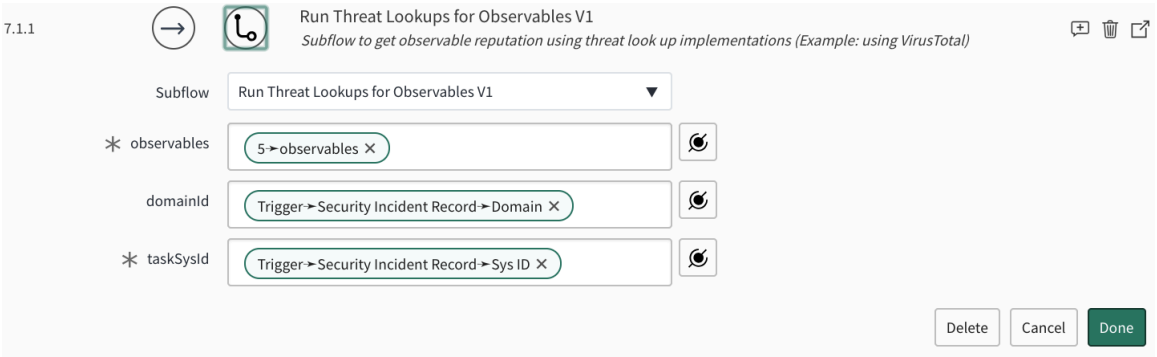
Exibir o designer de subfluxo do playbook de resposta de phishing automatizado

É possível fazer uma busca detalhada no Designer de subfluxos para exibir informações detalhadas sobre o subfluxo que está sendo executado como parte do fluxo do playbook de resposta de phishing automatizado.

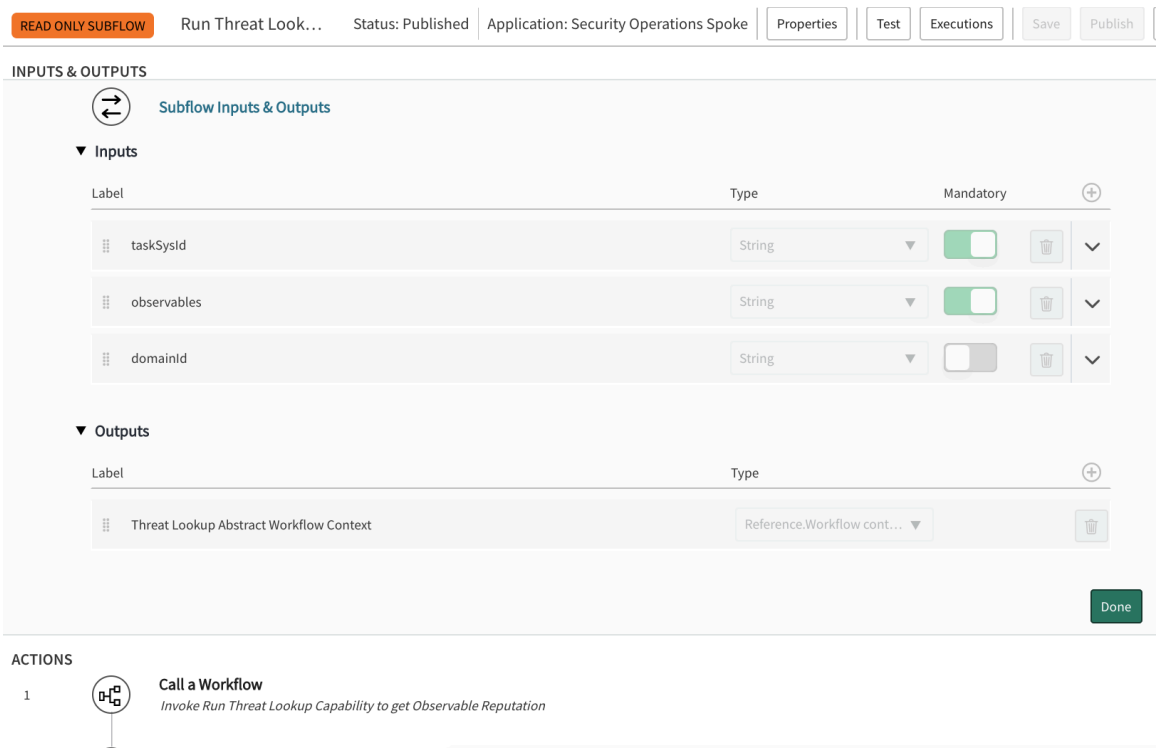
Você pode iniciar o Designer de subfluxos para exibir detalhes adicionais de um subfluxo. A página do Designer de subfluxos para o subfluxo Executar pesquisas de ameaças para observáveis é mostrada aqui. Clique no ícone do na imagem abaixo para exibir o Designer de subfluxos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Na página do Subflow Designer, você pode ver as entradas e saídas deste subfluxo e as ações de fluxo de trabalho subjacentes que estão sendo executadas.



Nota:
Este subfluxo é somente leitura e não pode ser editado. Você pode adicionar ou excluir subfluxos da etapa, mas não pode modificar o subfluxo.

Playbook for Automated Malware

O playbook de malware automatizado fornece uma sequência de etapas automatizadas que ajudam a resolver alertas de malware de forma rápida e eficiente.

Use o fluxo do playbook de malware para automatizar as etapas envolvidas no tratamento de alertas de malware do endpoint ou da rede. O modelo de fluxo inclui condições do gatilho, uma sequência de ações e subfluxos que são anotados para facilitar a leitura.

Esses modelos contêm uma sequência de ações reutilizáveis projetadas para responder a ataques de phishing. Cada fluxo tem um gatilho (condição), uma sequência de ações e subfluxos que são anotados para facilitar a leitura. Para acessar esses fluxos, você deve instalar ospoke do Security Operations e o aplicativo Security Operations Palo Alto Networks - WildFire da ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Você deve ativar esses modelos antes de usá-los.

Os seguintes fluxos e subfluxos estão incluídos:

- Security Incident - Automated Malware Playbook Template: este modelo foi projetado para automatizar as respostas a alertas de malware e contém uma sequência de ações, incluindo um gatilho.
- Incidente de segurança - Modelo manual de malware: este modelo é o fluxo de trabalho de resposta de malware manual existente que é ativado quando a categoria é definida como Atividade de código malicioso.

Subfluxos

- Confirmar ameaça do observável: verifica se os observáveis são mal-intencionados e precisam ser resolvidos.
- Definir severidade do incidente: define um status de severidade para o incidente.
- Playbook de ransomware: determina se é um ataque de ransomware.

Esses subfluxos representam um conjunto de operações reutilizáveis que podem ser usados em vários playbooks. Você pode usar esses subfluxos para definir modelos personalizados (fluxos) de acordo com seus requisitos.

Para criar modelos personalizados (fluxos), siga as instruções em Fluxos .

Executar o fluxo automatizado do playbook de malware

Use este fluxo para automatizar tarefas no playbook para analisar e resolver ataques de malware contra sua organização.

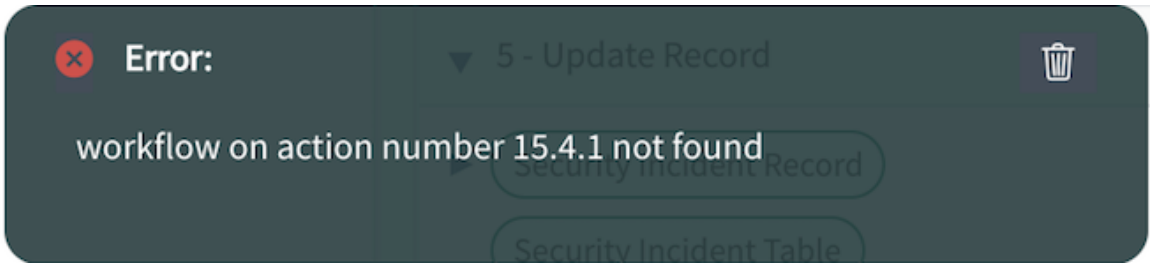
Antes de Iniciar

- Função necessária: sn_si.admin, flow_designer e action_designer
- Instale e configure as seguintes integrações com as credenciais corretas:
  - Palo Alto Networks WildFire for Security Operations
  - Pesquisa de detecções (Splunk)
  - Solicitações de bloqueio
  - Pesquisa de ameaças
  - Aprimorar observáveis

  Verifique se essas integrações estão funcionando corretamente antes de ativar o Security Incident - Automated Malware Playbook Template.
- Aplicativo Security Operations Palo Alto Networks Wildfire: para acessar o fluxo do playbook automatizado de malware, você deve instalar o Security Operations Spoke e o aplicativo Security Operations Palo Alto Networks - WildFire da ServiceNow Store. Se o aplicativo Security Operations Palo Alto Networks Wildfire não estiver instalado, você verá um erro "fluxo de trabalho na ação número 15.4.1 não encontrado", conforme mostrado abaixo:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se você não quiser instalar este aplicativo, exclua as etapas **15.2, 15.3 e 15.4** do fluxo do playbook automatizado de malware.

- Certifique-se de que as seguintes condições foram atendidas:
  - O incidente de segurança foi atribuído a um analista de segurança que pertence ao grupo de aprovação apropriado.
  - O analista de segurança que lida com o incidente deve ter um endereço de e-mail válido.
  - Os itens de configuração e observáveis necessários foram adicionados ao incidente de segurança.
- Para **a etapa 21 (Solicitar aprovação)**, altere o Grupo de **Atribuição de incidente de segurança** para o grupo de sua preferência.
- A etapa 21 do fluxo é uma etapa de aprovação de tarefa obrigatória em que uma solicitação de aprovação é enviada ao administrador. Para aprovar a solicitação, o administrador deve navegar até a página Aprovações de tarefa e definir o campo Estado como **Aprovado**. Se a tarefa não for aprovada, o Flow Designer não poderá prosseguir e o processo será encerrado.

Por Que e Quando Desempenhar Esta Tarefa

Quando uma atividade de código mal-intencionado é detectada na rede, um incidente de segurança é criado e o fluxo automatizado do playbook de malware é iniciado. Você pode usar as tarefas definidas no fluxo do playbook automatizado de malware para fazer triagem, analisar, conter e erradicar a ameaça.

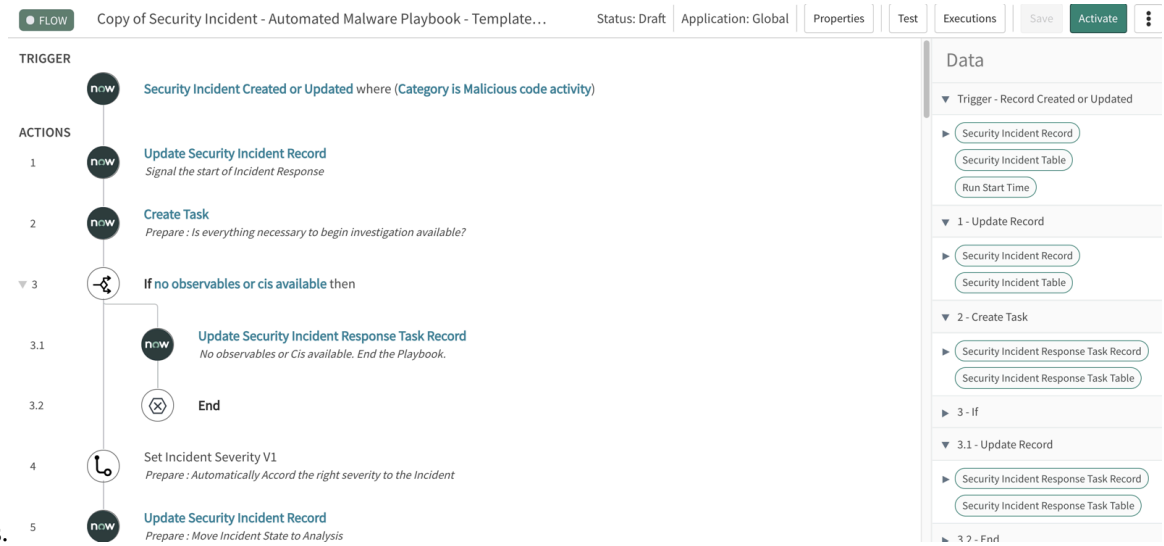
Procedimento

1. Navegar até **Todos** > **Flow Designer** > **Designer** para exibir os fluxos disponíveis com o spoke do Security Operations.
2. Clique no link **Incidente de segurança - IV Modelo de malware automatizado**.
3. Na página Fluxo, clique no ícone mais ícone , faça uma cópia do fluxo e abra-o para uso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

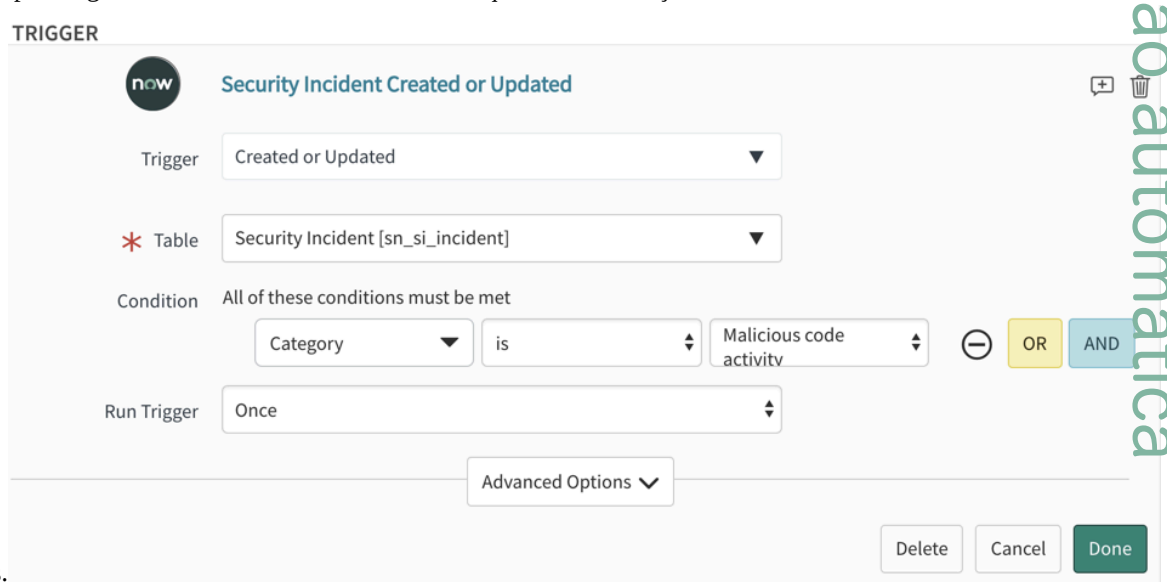
Agora você pode fazer mudanças no fluxo, como modificar condições ou ações do gatilho, ou adicionar e remover



ações.

Isso mostra o gatilho e as etapas que serão executadas com o fluxo. O painel à direita mostra o fluxo de dados. Clique em um ícone para expandir a etapa e exibir os detalhes.

4. Clique no ícone **Gatilho**.
Na primeira etapa, você define ou define o gatilho do fluxo. Especifique as condições para o gatilho e a tarefa a serem executadas quando as condições forem



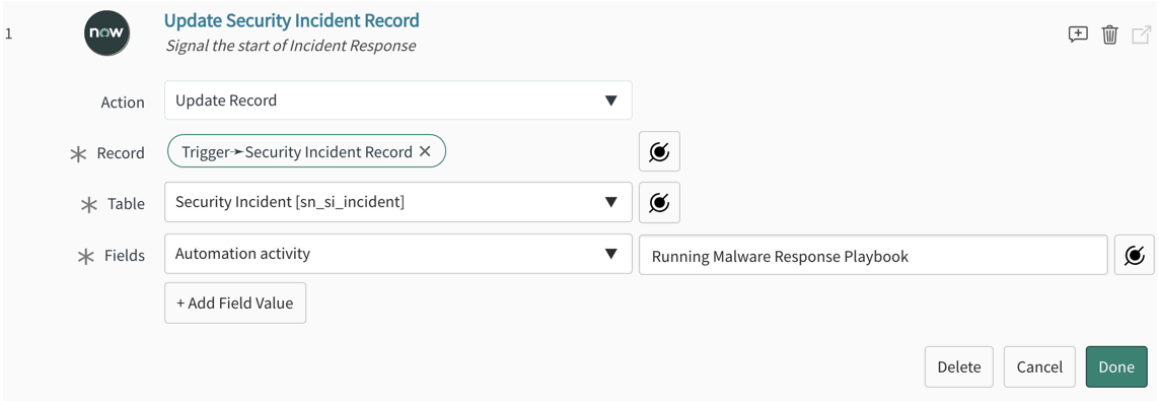
atendidas.

Quando a condição definida no fluxo (a categoria é atividade de código malicioso) é atendida no registro do incidente, as tarefas no fluxo de phishing automatizado começam a ser executadas sequencialmente. Você pode modificar o gatilho, adicionar anotações, adicionar ou excluir condições e assim por diante.

5. A primeira etapa no fluxo é **Atualizar registro de incidente de segurança**.

Tradução automática

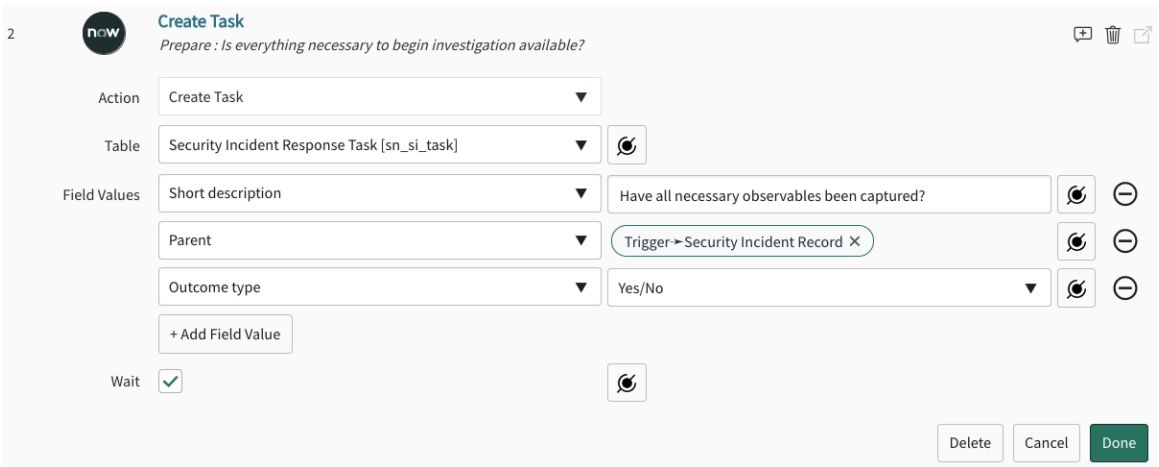
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Clique no link e clique no ícone de anotação Ícone de para adicionar uma anotação ao analista de segurança indicando que houve alguma atividade de código mal-intencionado e que o fluxo do playbook de resposta automatizada de malware começou a ser executado.

6. Prossiga com a etapa 2 no fluxo e clique no link **Criar tarefa**.

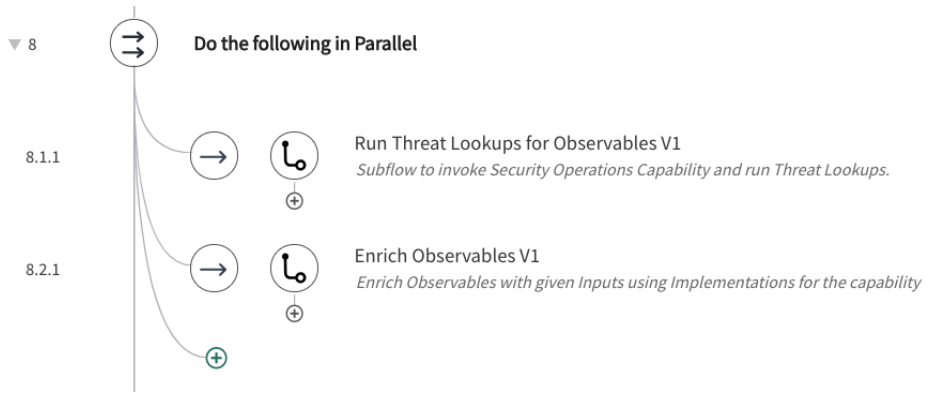
   Nesta etapa, uma tarefa de resposta automatizada é criada para verificar se todos os observáveis necessários foram capturados e se a investigação pode começar.



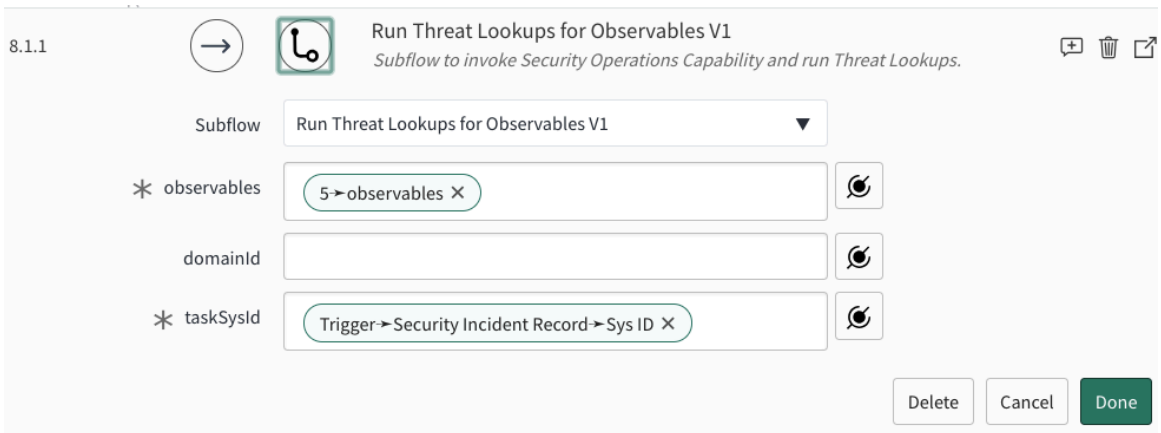
7. Se o tipo de resultado for **Não**, isso indica que não há observáveis e ICs disponíveis para iniciar a investigação.
   Atualize o registro de incidente de segurança para indicar que o playbook não pode prosseguir.
8. Se o tipo de resultado for **Sim**, o subfluxo Definir severidade do incidente atribuirá automaticamente a severidade correta ao incidente de segurança.
9. Na próxima etapa, o registro do incidente de segurança é atualizado.
10. Na próxima etapa, todos os observáveis envolvidos no incidente ou em uma categoria selecionada são coletados para executar ações automatizadas adicionais nas etapas subsequentes do playbook.
11. Na próxima etapa, uma tarefa de resposta automatizada será criada.
    Esta tarefa captura o início do processo de obtenção da reputação de todos os observáveis e execução do aprimoramento com integrações configuradas.
12. Na etapa 8, dois subfluxos são chamados:

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Executar pesquisas de ameaças para observáveis: este subfluxo é usado para obter a reputação de todos os observáveis usando implementações de pesquisa de ameaças.
- Aprimorar observáveis: este subfluxo é usado para executar o aprimoramento de observáveis com implementações configuradas.



Observe os ícones para esta tarefa. O ícone de operações indica que ambas as tarefas serão realizadas em paralelo e o ícone de subfluxo de subfluxo indica que a tarefa que está sendo executada é um subfluxo conforme mostrado abaixo:



Observe o número 5 no campo de observáveis. Isso indica que a pesquisa de ameaças será executada nos observáveis recuperados na etapa 5. Esse subfluxo, por sua vez, chama fluxos de trabalho e ações existentes.

13. Na próxima etapa, a ação Executar a pesquisa de registros é executada.
Esta ação é usada para pesquisar registros de contexto de fluxo de trabalho em que os fluxos de trabalho primários podem ser um dos seguintes.

- Contexto de fluxo de trabalho abstrato de Pesquisa de ameaças
- Contexto de Fluxo de Trabalho Abstrato de Aprimoramento de Observável

14. Na próxima etapa, os resultados de reputação e aprimoramento são revisados para cada oito registros.

15. Continue revisando as próximas etapas:

a. Atualizar registro de incidente de segurança: atualiza o registro de incidente de segurança para indicar que a pesquisa de reputação e as atividades de aprimoramento foram concluídas.

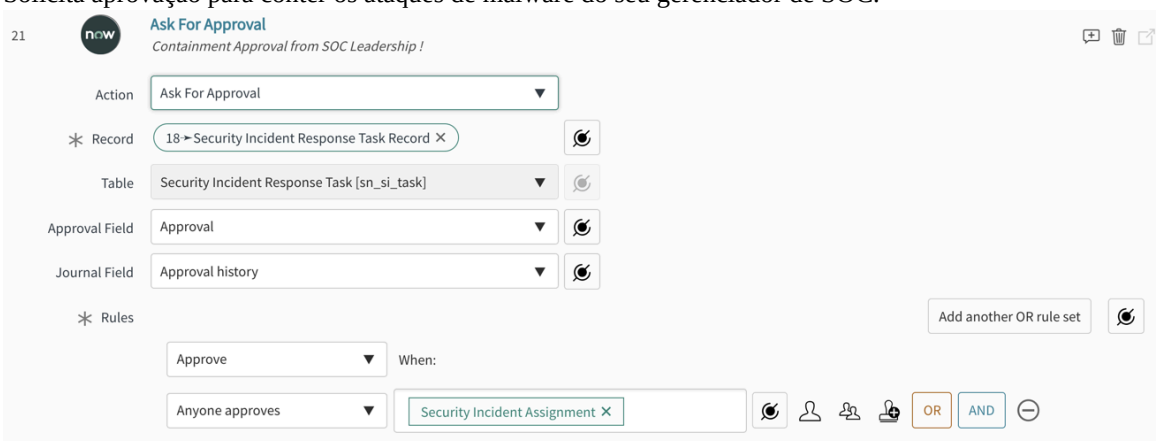
b. Obter observáveis da tarefa: recupera todos os observáveis maliciosos associados ao incidente de segurança.

c. Criar tarefa: verifica e confirma se as execuções de triagem automatizadas foram bem-sucedidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

16. Se houver observáveis que foram sinalizados como maliciosos:
    a. Atualizar registro de incidente de segurança: publique uma anotação de trabalho indicando que uma ameaça foi detectada.
    b. Criar consulta de entrada a partir de observáveis: se mais de dez observáveis forem sinalizados como mal-intencionados, o subfluxo Pesquisa de detecções em observáveis (em Splunk ou Carbon Black) será executado.
17. Se os observáveis não forem sinalizados como maliciosos, o fluxo continuará com as seguintes etapas:
    a. Atualizar registro de incidente de segurança: publique uma anotação de trabalho indicando que nenhuma ameaça foi detectada
    b. Obter observáveis da tarefa: identifica todos os IDs de hash SHA256 do incidente.
    c. Pesquisar registros observáveis: pesquisa registros que atendem a esses critérios.
18. Continue revisando as próximas etapas:
    a. Para cada observável malicioso, o fluxo de trabalho **Security Operations Palo Alto Networks - Obter aprimoramento de dados do Wildfire** é executado.
    b. Revisa os resultados da investigação para ver se eles são satisfatórios.
    Uma tarefa de resposta é criada para verificar se o malware suspeito é um ataque de ransomware. Em caso afirmativo, o subfluxo do Ransomware Playbook será executado.
    c. Na próxima etapa, um e-mail é enviado com um resumo da análise e uma solicitação de aprovação para iniciar os procedimentos de contenção.
    d. Uma tarefa é criada para capturar detalhes da aprovação solicitada.
    e. A próxima etapa é atualizar o registro do incidente de segurança.
    Publique uma anotação de trabalho informando ao analista de segurança que a solicitação de aprovação foi feita.
    f. Solicita aprovação para conter os ataques de malware do seu gerenciador de SOC.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Quando uma solicitação de aprovação for gerada pelo fluxo, a anotação de trabalho será atualizada com a seguinte mensagem:

Uma solicitação de aprovação foi feita para<task id> prosseguir com a contenção. Para aprovar esta tarefa, como gerente do SOC, siga estas etapas manualmente:

- Navegue até a página Aprovações de tarefas.
- Você verá a lista de aprovações. Clique no<task id> que deve ser aprovado.
- Mude o Estado para **Aprovar** e Salvar o atualizado<task id> .

g. Na próxima etapa, o registro do incidente de segurança é atualizado para rastrear o status de aprovação.

h. Em seguida, uma tarefa é criada para iniciar procedimentos de contenção.

i. O subfluxo Executar Criar solicitações de bloqueio para observáveis maliciosos é executado e um registro de incidente é criado com uma solicitação para recriar o dispositivo infectado e seus ativos.

j. Em seguida, uma tarefa é criada para executar a pesquisa de vistas para confirmar se o ambiente é seguro. A pesquisa de vistas é repetida até que nenhuma vista seja encontrada.

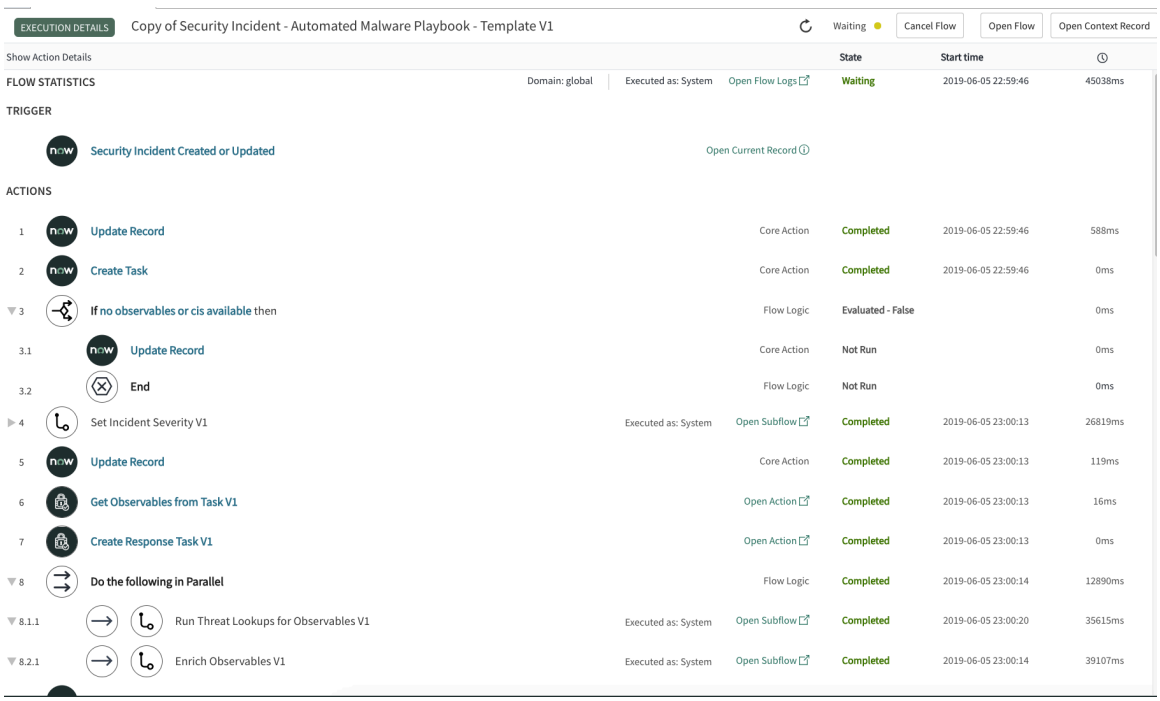
k. Em seguida, uma tarefa é criada para indicar que o registro do incidente de segurança está pronto para revisão.

l. Por fim, o registro é atualizado e movido para a fase Revisar.

O que Fazer Depois

Você pode clicar em **Testar** para simular as ações no fluxo antes que ele seja publicado. Depois de testar o fluxo, clique em **Ativar** para ativar o fluxo para que ele possa ser executado.

Clique em **Execuções** para exibir os detalhes da execução do fluxo.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook para falha de login manual

Quando um usuário faz determinadas tentativas de login malsucedidas (de acordo com a configuração do SIM), um incidente de segurança é criado.

Essas tentativas de login malsucedidas podem ser falsos positivos ou tentativas feitas por invasores de obter acesso às contas de e-mail do usuário. Nesses cenários, o playbook de login manual com falha pode fornecer orientação e ajudar a otimizar a investigação de incidentes de segurança de login com falha.

Pré-requisitos

Função necessária:

- sn_si.admin
- flow_designer

Spoke: instale o Security Operations Spoke (sn_sec_spoke)

Capacidades-chave

O playbook de login com falha abrange os seguintes recursos para investigar incidentes de segurança:

1. Verifica se o usuário afetado é um usuário ativo/inativo
2. Filtra observáveis da lista de permissões
3. Aprimora os observáveis
4. Executa pesquisa de ameaça automatizada.
5. Envia e-mail automatizado ao usuário para confirmar a falha na tentativa de login.
6. Atribui tarefas ao analista para investigar o acesso do usuário
7. Identifica observáveis maliciosos e bloqueia IPs e URLs.
8. Redefine a senha do usuário.
9. Atualiza o status do incidente de segurança
10. Atribui tarefas a um analista de segurança para lidar com a revisão pós-incidente.

Capacidades necessárias

- Pesquisa de ameaças (total de vírus, análise híbrida)
- Aprimoramento de observável (Whois, ReverseWhois)
- Pesquisa de detecções (Splunk, QRadar)
- Bloqueio de observável (CheckPoint, Palo Alto)

Para obter mais informações, consulte a ServiceNow Store .

Experiência do analista de segurança

Para entender como resolver ameaças de segurança passo a passo, consulte Resolver ameaças à segurança com o playbook.

Tradução automática

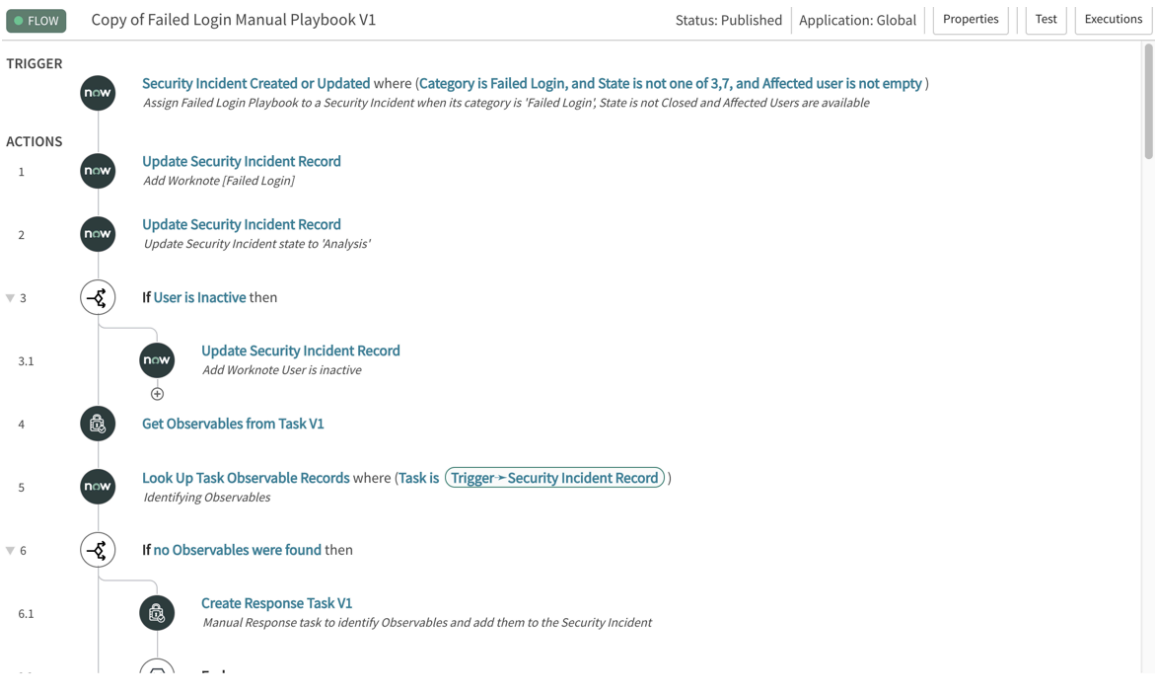
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como usar o playbook de falha de login com recursos do Flow Designer

Introdução

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Flow Designer** > **Designer** e clique no playbook **Falha no login**.
3. Faça uma cópia dos fluxos a seguir para copiar o Playbook de login com falha e faça as modificações necessárias. (Esta é uma etapa opcional. Siga esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.
   - Falha no Playbook manual de login V1
   - Falha no login - Analisar a resposta do usuário e atualizar a tarefa de resposta V1
4. Faça as modificações necessárias de acordo com seus requisitos. (Esta é uma etapa opcional. Siga esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.
5. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível com o sistema de base.
   - Ative os fluxos copiados depois de fazer modificações de acordo com seus requisitos.

A imagem a seguir mostra uma cópia do playbook de Login manual com falha. Revise as etapas abaixo para entender as várias ações no playbook.

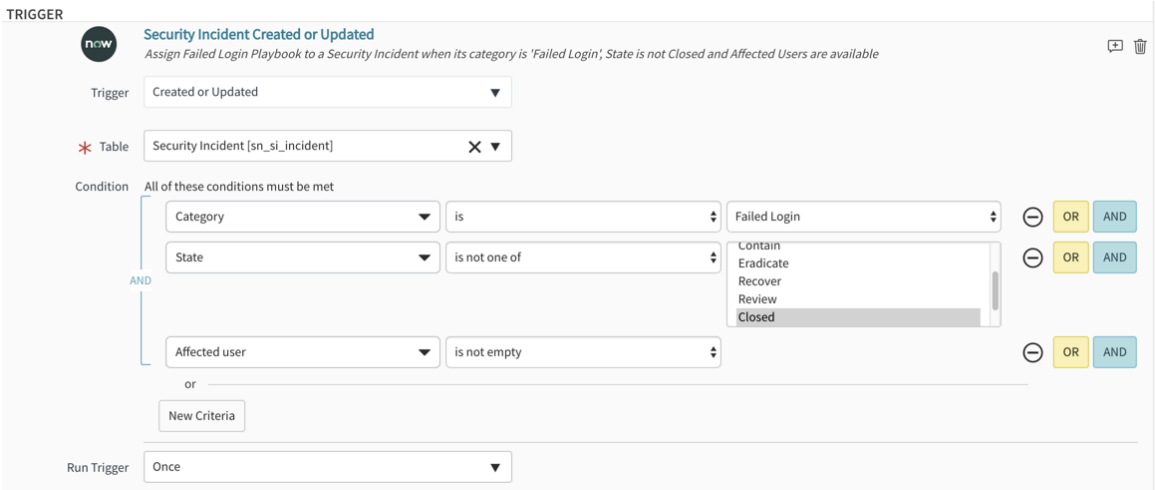


Este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:

- A categoria é Falha no login
- Tem um ou mais usuários afetados
- O incidente de segurança não foi encerrado ou cancelado

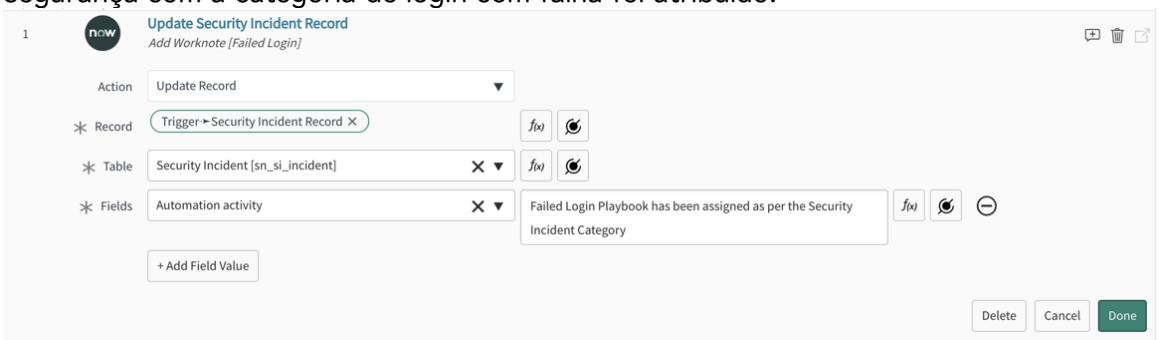
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

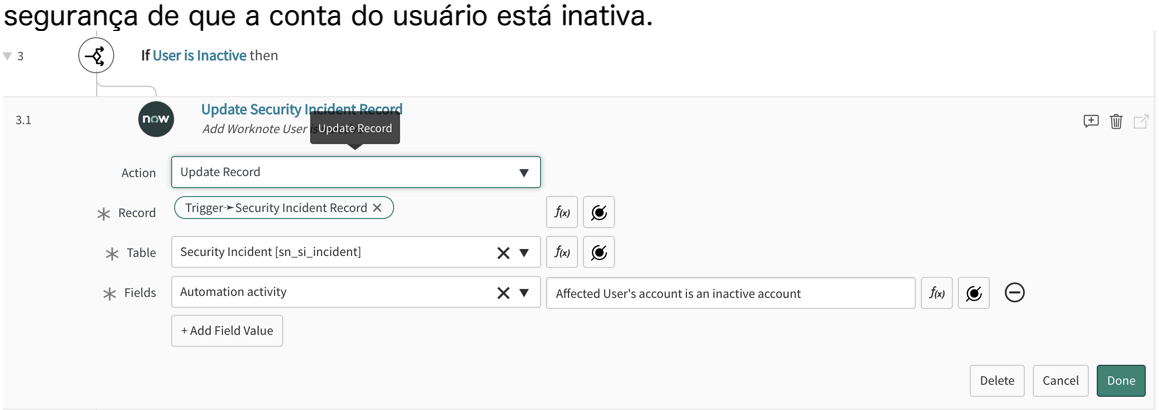


As etapas a seguir orientam você nas ações, tarefas e subfluxos que estão disponíveis no playbook de login manual com falha.

1. Quando o playbook começa a ser executado, na Etapa 1, ele é atualizado automaticamente com uma anotação de trabalho mostrando que o incidente de segurança com a categoria de login com falha foi atribuído.



2. Na Etapa 2, o playbook é atualizado e movido para o estado Análise.
3. Na etapa 3, o playbook verifica se o usuário afetado é um usuário ativo ou inativo. Se o usuário estiver inativo, uma anotação de trabalho será adicionada ao incidente de segurança de que a conta do usuário está inativa.



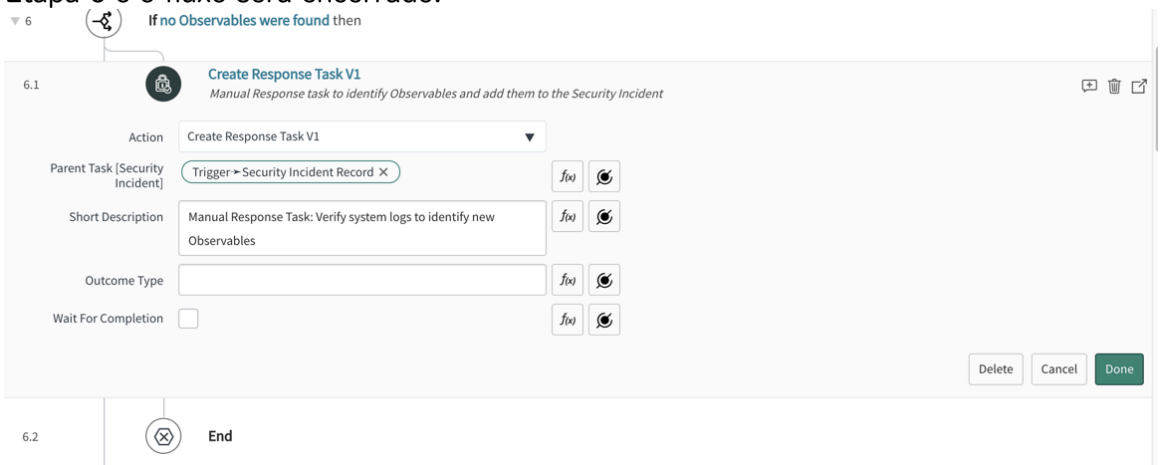
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

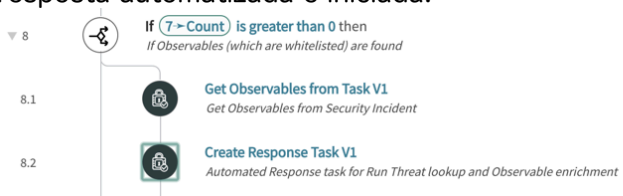
Nota:
Na etapa 3 do fluxo, o fluxo verifica os usuários inativos na tabela `sn_si_incident` disponível em ServiceNow. Esta etapa é fornecida como uma diretriz e deve ser modificada para seu ambiente específico. Se você quiser usar esta funcionalidade, recomendamos que você tenha uma integração do Active Directory configurada em seu ambiente. Você pode verificar com a integração do Active Directory para encontrar o status do usuário e, dependendo da resposta, pode projetar as próximas etapas para o seu playbook.

Se você não tiver uma integração do Active Directory, substitua esta etapa por uma tarefa manual para o analista de segurança trabalhar com a equipe de TI para bloquear o usuário e seguir em frente com o restante das etapas no playbook.

4. Na Etapa 4, os observáveis do incidente de segurança são recuperados.
5. Na Etapa 5, os observáveis são identificados.
6. Se nenhum observável for encontrado, uma tarefa de resposta manual será criada na Etapa 6 e o fluxo será encerrado.

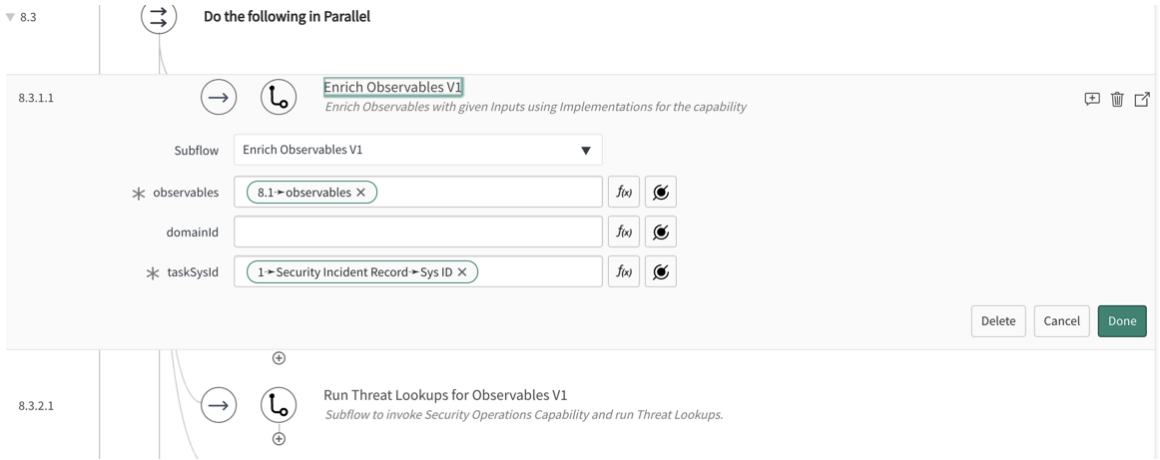


7. Se os observáveis forem encontrados na Etapa 7, os observáveis que não estão na lista de permitidos serão identificados.
8. Se pelo menos um dos observáveis não estiver na lista de observáveis, as seguintes etapas serão realizadas:
   a. As etapas 8.1 e 8.2 são executadas. Os observáveis são recuperados e uma tarefa de resposta automatizada é iniciada.



   b. Depois que a tarefa automatizada tiver sido criada, a etapa 8.3 (8.3.1.1 e 8.3.2.1) será executada e as integrações Aprimorar observáveis e Pesquisa de ameaças serão executadas. Observe que esses são subfluxos que foram incluídos no playbook.

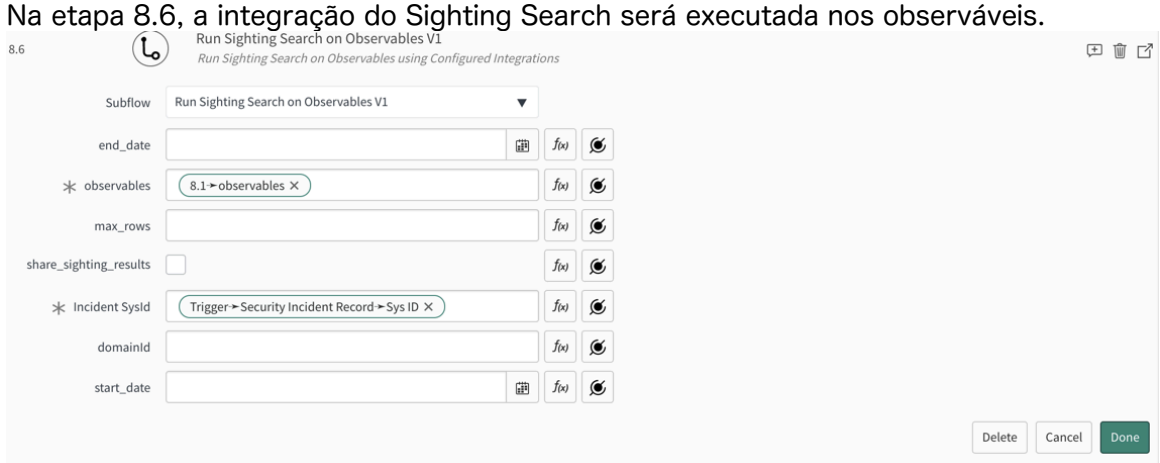
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Na Etapa 8.4, depois que as integrações forem concluídas, o registro de incidente de segurança será atualizado.

d. Na Etapa 8.5, uma nova tarefa de resposta é criada para indicar a próxima tarefa automatizada que ocorrerá.

e. Na etapa 8.6, a integração do Sighting Search será executada nos observáveis.



f. Depois que o subfluxo Pesquisa de detecções for concluído, na etapa 8.7, o incidente de segurança será atualizado.

g. Na Etapa 8.8, os observáveis são verificados para ver se são mal-intencionados.

h. Se os observáveis não forem maliciosos e se a conta do usuário estiver ativa, um e-mail automatizado será enviado ao usuário para reconfirmar as tentativas de login malsucedidas. Uma tarefa de resposta manual é criada para identificar os observáveis e adicioná-los ao incidente de segurança. O playbook termina nesta fase.

i. Se os observáveis forem maliciosos, três tarefas de resposta serão criadas:

  i. Um e-mail automatizado é enviado ao usuário para confirmar **(Sim ou Não)** as tentativas de login malsucedidas. Se o usuário responder Sim:

    1. O status do incidente de segurança é atualizado para **Contêm**.

    2. Um e-mail automatizado é enviado ao usuário para redefinir a senha.

    3. O subfluxo Redefinir senha é iniciado e um e-mail é enviado ao usuário quando a tarefa é concluída.

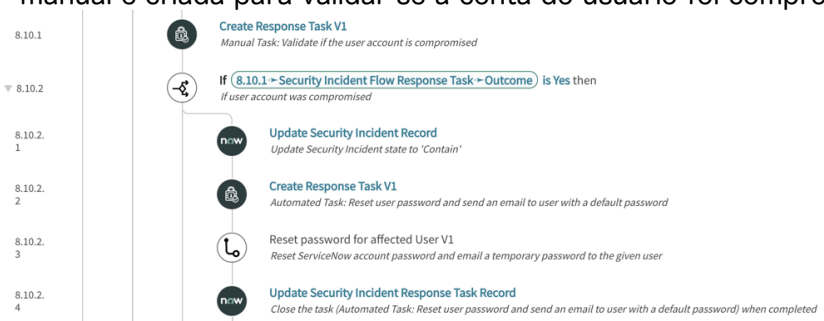
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A etapa Redefinir senha é fornecida como uma diretriz. As etapas no fluxo redefinem a senha da conta do usuário no sistema ServiceNow. Mas o processo para redefinir a senha pode ser diferente dependendo do seu ambiente. Você pode verificar com a integração do Active Directory para redefinir a senha dos usuários automaticamente. Se você não tiver uma integração do Active Directory, substitua esta etapa por uma tarefa manual para que o analista de segurança trabalhe com a respectiva equipe de TI para redefinir a senha dos usuários e siga em frente com o restante das etapas do playbook ao concluir o respectivo tarefa.

ii. Se o usuário responder Não, um e-mail automatizado será enviado ao usuário para reconfirmar a resposta. O analista de segurança deve executar as ações apropriadas manualmente.

iii. Se o usuário não responder ao e-mail automatizado, o analista de segurança deverá atualizar o incidente de segurança manualmente e fornecer uma resposta. Uma tarefa manual é criada para validar se a conta do usuário foi comprometida.



9. Na Etapa 8.10.3, o estado do incidente de segurança é atualizado.

10. Na Etapa 8.10.4, uma tarefa automatizada é criada para verificar se a implementação do recurso Criar solicitações de bloqueio para IPs e URLs maliciosos está disponível. Se a implementação da funcionalidade estiver disponível, o subfluxo Criar solicitações de bloqueio será executado. Se não estiver disponível, o incidente de segurança será atualizado e uma anotação de trabalho será publicada para indicar que a implementação da capacidade não está disponível.

11. Na Etapa 9, o incidente de segurança é atualizado e o estado é definido como **Revisar**.

12. Na Etapa 10, uma tarefa de resposta é criada para que o usuário conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para automação de incidente de segurança secundário

Incidentes de segurança duplicados são categorizados como incidentes de segurança secundários e são acumulados para os incidentes de segurança primários.

O playbook de automação de incidentes de segurança secundários ajuda a reduzir o tempo necessário para investigar e fechar incidentes de segurança duplicados. Este playbook acumula automaticamente artefatos exclusivos específicos do incidente de segurança secundário (observáveis, usuários afetados, ICs) para o incidente de segurança primário.

Pré-requisitos

Função necessária:

- sn_si.admin
- flow_designer

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Spoke: instale o Security Operations Spoke (sn_sec_spoke)

Capacidades-chave

O playbook de automação secundária abrange os seguintes recursos:

1. Move o incidente de segurança para a fase de **Análise**.
2. Elimina duplicatas e adiciona (acúmulos) os usuários e ICs afetados ao incidente de segurança primário.
3. Adiciona observáveis do incidente secundário ao incidente de segurança primário.
4. Fecha ou cancela o incidente de segurança secundário quando o incidente de segurança primário é encerrado.

Capacidades necessárias

Para obter mais informações, consulte a ServiceNow Store .

Experiência do analista de segurança

Para entender como resolver ameaças de segurança passo a passo, consulte Resolver ameaças à segurança com o playbook.

Compreensão mais profunda do playbook de automação de incidente de segurança secundário com recursos do Flow Designer

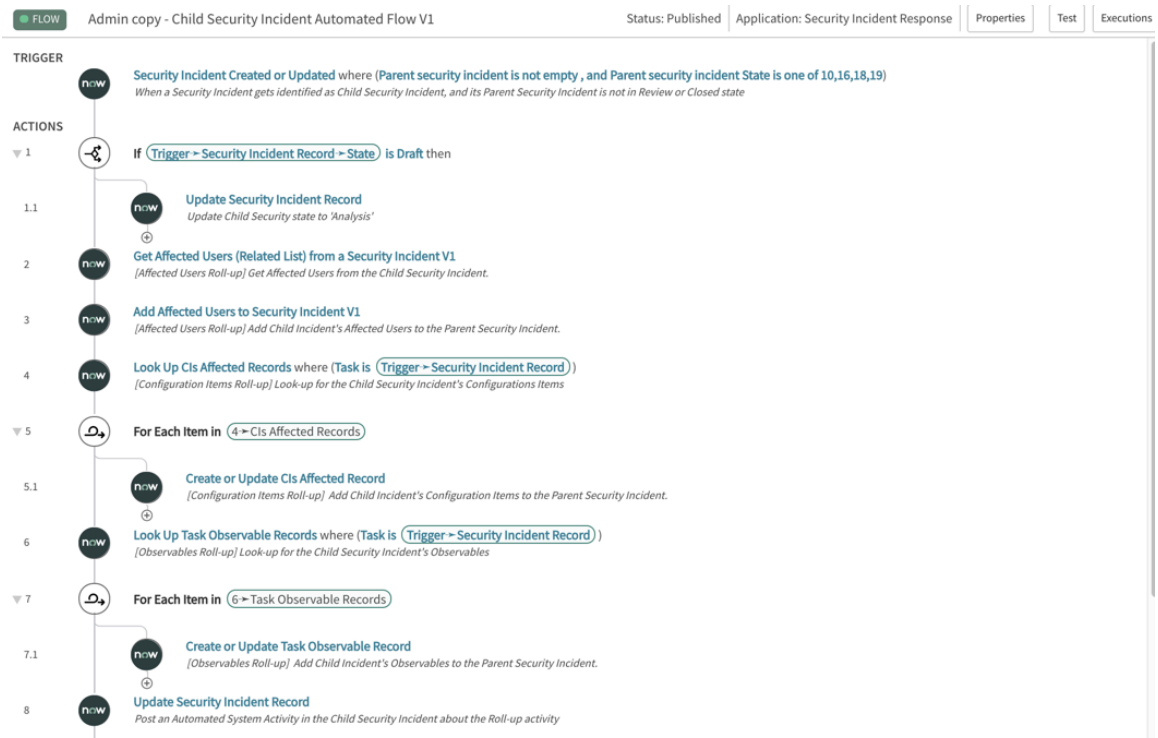
Introdução

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Flow Designer** > **Designer** e clique no playbook Falha no login.
3. Faça uma cópia do playbook de automação de incidente de segurança secundário e faça as modificações necessárias. (Esta é uma etapa opcional. Siga esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.
4. Faça as modificações necessárias de acordo com seus requisitos. (Esta é uma etapa opcional. Siga esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.
5. Ative o playbook.
   - Ative o fluxo principal para usar o playbook disponível com o sistema de base.
   - Ative o fluxo copiado depois de fazer modificações de acordo com seus requisitos.

A imagem a seguir mostra uma cópia do playbook de automação de incidente de segurança secundário. Revise as etapas abaixo para entender as várias ações no playbook.

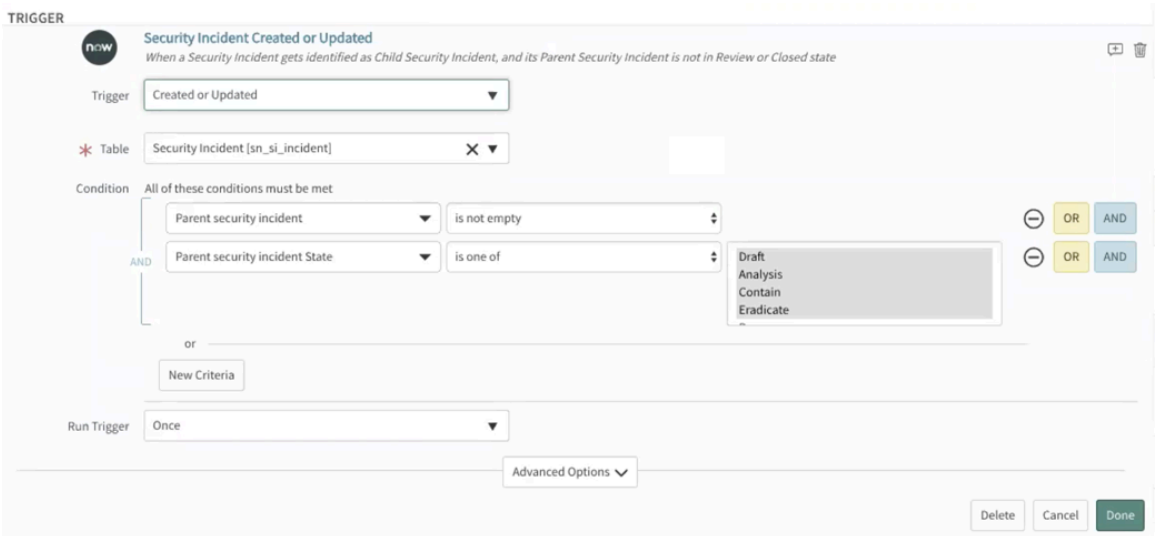
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Este playbook é acionado quando:

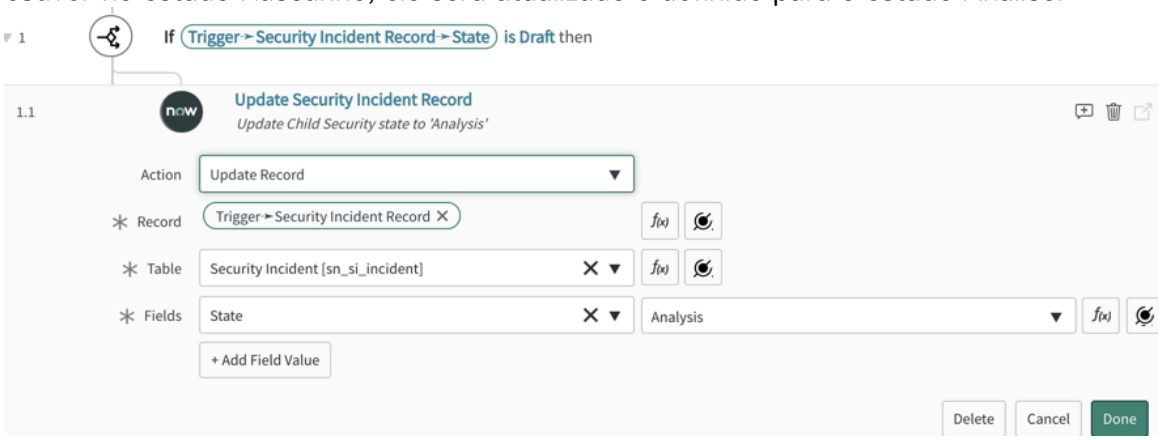
- O campo de incidente de segurança primário não está vazio.
- O incidente de segurança primário está no estado Rascunho, Análise, Conter ou Erradicar.



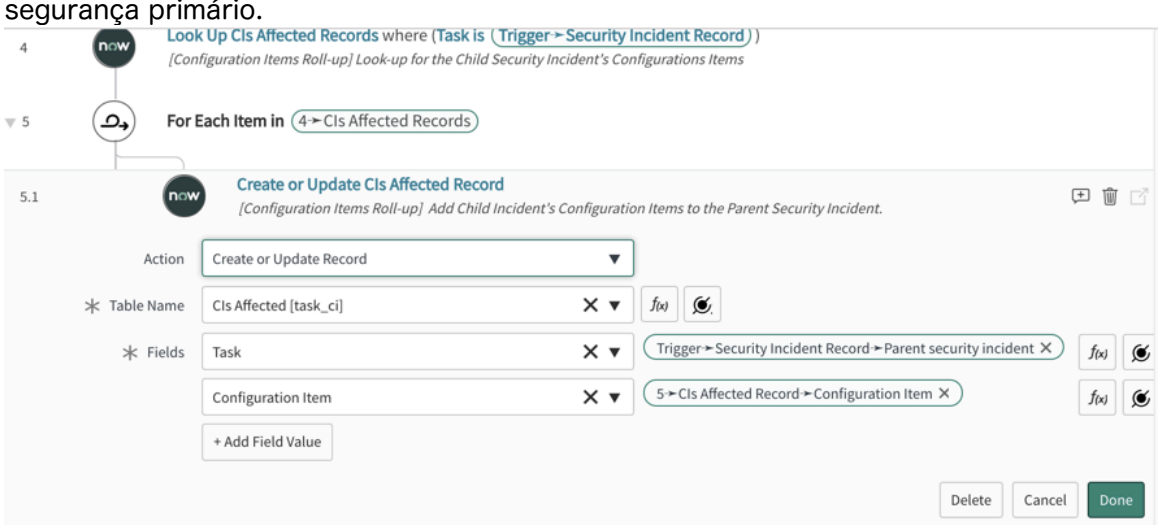
As etapas a seguir orientam você nas ações e tarefas que estão disponíveis no playbook de automação de incidentes de segurança secundários.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

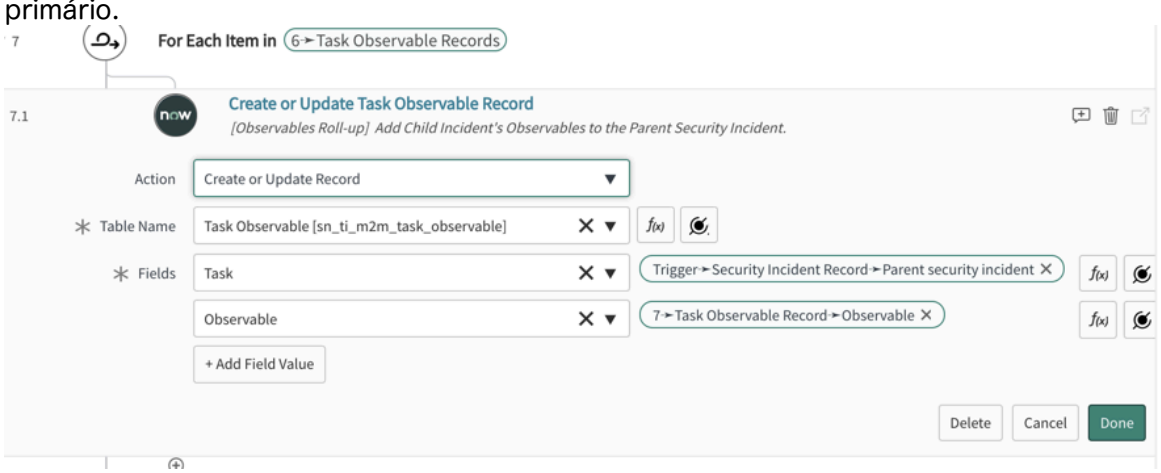
1. Quando o playbook começar a ser executado, na Etapa 1, se o incidente de segurança estiver no estado Rascunho, ele será atualizado e definido para o estado Análise.



2. Nas etapas 2 e 3, os usuários afetados pelo incidente de segurança são recuperados e acumulados no incidente de segurança primário. Todos os usuários duplicados serão eliminados.
3. Nas etapas 4 e 5, os itens de configuração associados ao incidente de segurança secundário são recuperados e os ICs exclusivos são acumulados para o incidente de segurança primário.



4. Nas etapas 6 e 7, os observáveis associados ao incidente de segurança secundário são recuperados e os observáveis exclusivos são acumulados para o incidente de segurança primário.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Nas etapas 8 e 9, anotações de trabalho automatizadas são publicadas nos incidentes de segurança primários e secundários, indicando que os usuários afetados, itens de configuração e observáveis foram acumulados do incidente de segurança secundário para o incidente de segurança primário.

Playbook for Office 365 - Arquivo malicioso detectado

Este playbook fornece etapas de correção sistemática para investigar arquivos mal-intencionados detectados no Office 365

Quando arquivos mal-intencionados são detectados no Office 365, você pode usar o playbook 365 - Arquivo mal-intencionado detectado no Flow Designer para obter orientação e ajudar a otimizar a investigação desses arquivos mal-intencionados.

O fluxo de trabalho é criado com base em um playbook existente que fornece uma abordagem consistente e eficiente para investigação de incidentes. Cada ponto de decisão no playbook foi convertido em uma tarefa orientada por resultado e o fluxo muda de direção com base no resultado dessas tarefas.

Introdução ao Office 365 - Playbook de arquivo malicioso detectado

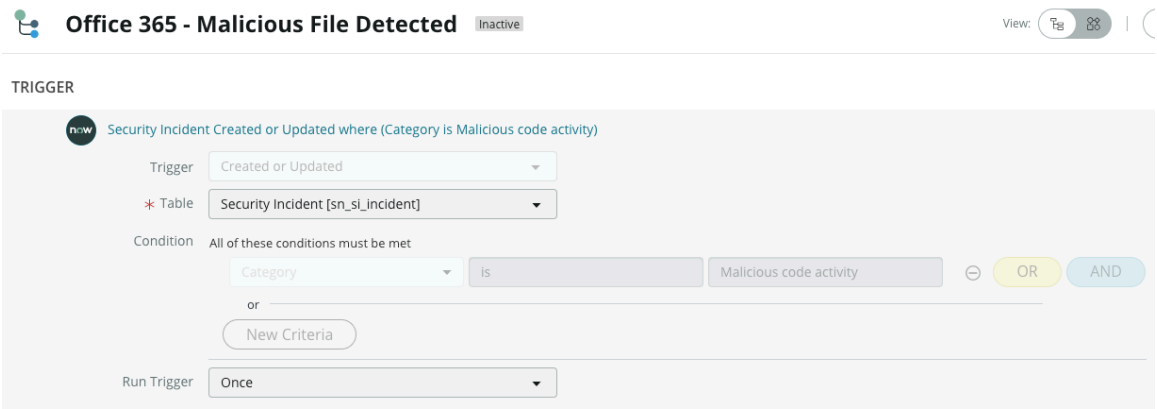
1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione o playbook **Office 365 - Arquivo mal-intencionado detectado**.
3. (Opcional) Você pode criar uma cópia do fluxo do playbook Office 365 - Arquivo mal-intencionado detectado e fazer as modificações necessárias. Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.

Condição do gatilho: este playbook é acionado e associado ao incidente de segurança quando a **categoria** é **atividade de código malicioso**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Configurar arquivo malicioso do Office detectado

Use as etapas a seguir para configurar o playbook Falhas de login do usuário do Okta de vários IPs.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

Navegar até **Todos** > > .

Use o playbook do arquivo malicioso detectado do Office 365

As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook do Office 365 Arquivo malicioso detectado.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Etapa 1, você precisa extrair o arquivo mal-intencionado do console do Office 365.
2. Na etapa 2, você precisa analisar se o arquivo ou o hash foi adicionado como um observável na plataforma de inteligência de ameaça.
3. Na Etapa 3, você precisa investigar o nome e o caminho do arquivo para determinar se é um arquivo/aplicação conhecido ou não malicioso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Na Etapa 4, você precisa enviar o arquivo para Sandbox para analisar os resultados.
5. Na etapa 5, com base na investigação feita até o momento, você precisa verificar se o arquivo ou o hash é malicioso ou não.
   Se o arquivo ou o hash não for mal-intencionado, uma tarefa de resposta manual será criada na Etapa 5 e o fluxo será encerrado.
6. Na etapa 6, se o arquivo ou hash for mal-intencionado, as etapas 7 e 8 serão executadas.
7. Na etapa 7, você precisa entrar em contato com o usuário final para obter uma justificativa comercial válida sobre o motivo pelo qual ele tem um arquivo mal-intencionado no dispositivo.
   Se o arquivo ou o hash forem mal-intencionados, você poderá usar o modelo de e-mail preexistente no playbook para enviar um e-mail ao usuário final solicitando esclarecimentos.
8. Na etapa 8, você precisa verificar se o usuário final forneceu uma justificativa comercial válida ou não.
   Se o usuário final forneceu uma justificativa de negócios válida, uma tarefa de resposta manual será criada na Etapa 5 e o fluxo será encerrado.
9. Na etapa 9, se o usuário não forneceu uma justificativa de negócios válida, as etapas 10, 11 e 12 serão executadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

10. Na etapa 10, como não havia justificativa comercial válida, você pode encaminhar o arquivo mal-intencionado ou o hash para a equipe de inteligência contra ameaças para revisão.

11. Na Etapa 11, você precisa executar o script do scanner de bytes de malware para verificar se o arquivo ou o hash são mal-intencionados.

12. Na Etapa 12, você precisa executar uma análise forense para verificar se o arquivo ou o hash são mal-intencionados.

13. Na Etapa 13, uma tarefa de resposta é criada para que o usuário conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para detecção de repetição

Este playbook ajuda a determinar se a resposta do incidente foi fornecida em um relatório de phishing exato ou semelhante no passado e funciona automaticamente no novo relatório de forma semelhante.

O playbook de detecção de repetição verifica se o incidente de phishing recém-relatado se parece com um incidente anterior. Quando a detecção de repetição é identificada, o incidente de segurança correspondente e os detalhes da resolução são fornecidos ao analista, que pode usá-los no incidente recém-relatado, resultando em uma correção rápida do incidente de segurança.

O fluxo de trabalho é criado com base em um playbook existente, que fornece uma abordagem consistente e eficiente para investigação de incidentes. Cada ponto de decisão no playbook foi convertido em uma tarefa orientada por resultado e o fluxo muda de direção com base no resultado dessas tarefas.

Introdução ao playbook de detecção de repetição

1. Faça login como um usuário com as funções sn_si.user e flow_designer.

2. Navegar até **Tudo** > **Flow Designer** e selecione o playbook de **detecção de repetição**.

3. (Opcional) Você pode criar uma cópia do fluxo do playbook de detecção de repetição e fazer as modificações necessárias. Para criar uma cópia do fluxo do playbook, clique no

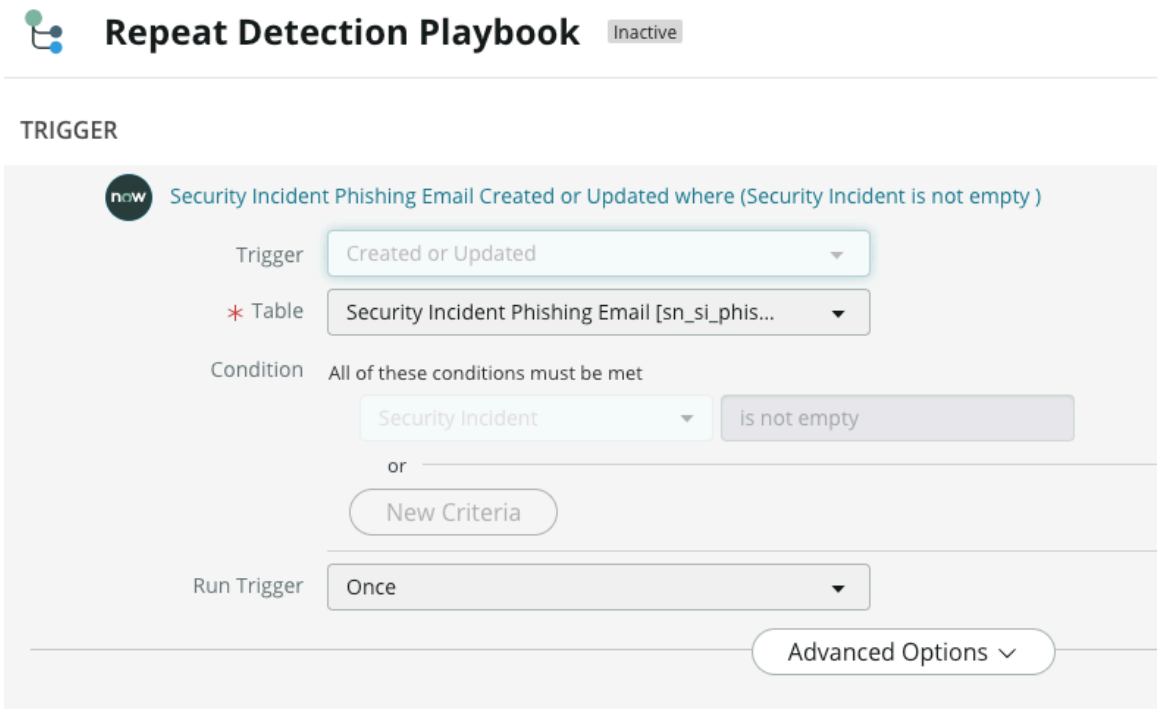
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.

Condição do gatilho: este playbook é acionado quando o **incidente de segurança não está vazio**.



Configurar playbook de detecção de repetição

Use as etapas a seguir para configurar o playbook Falhas de login do usuário do Okta de vários IPs.

Antes de Iniciar
Função necessária:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

Navegar até **Todos** > > .

Usar o playbook de detecção de repetição

As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook de detecção de repetição.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

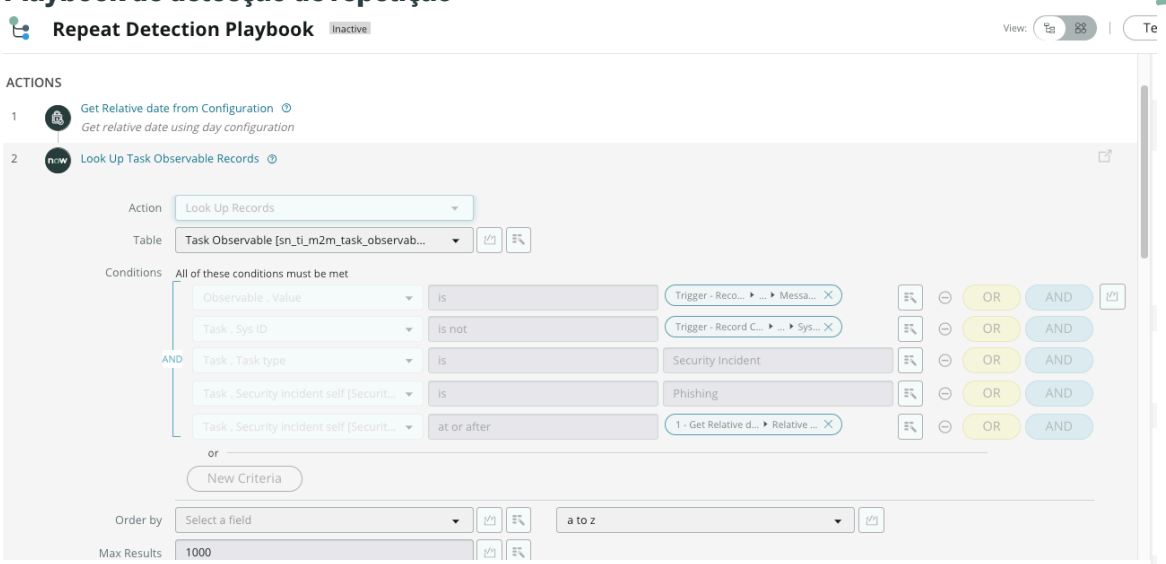
Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*). Você tem a opção de modificar as seguintes propriedades do sistema:

- *sn_sec_spoke.similarphish.earlytermificationspontuação*
- *sn_sec_spoke.similarphish.lookbackdays*
- *sn_sec_spoke.similarphish.maxcomparsonsize*
- *sn_sec_spoke.similarphish.minmatchscore*

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Etapa 1, o playbook recupera a data relativa do incidente de segurança usando a configuração de dia.
2. Na etapa 2, o playbook pesquisa os registros do observável de tarefa na tabela *sn_ti_m2m_task_observable* que correspondem ao incidente com base no ID da mensagem.

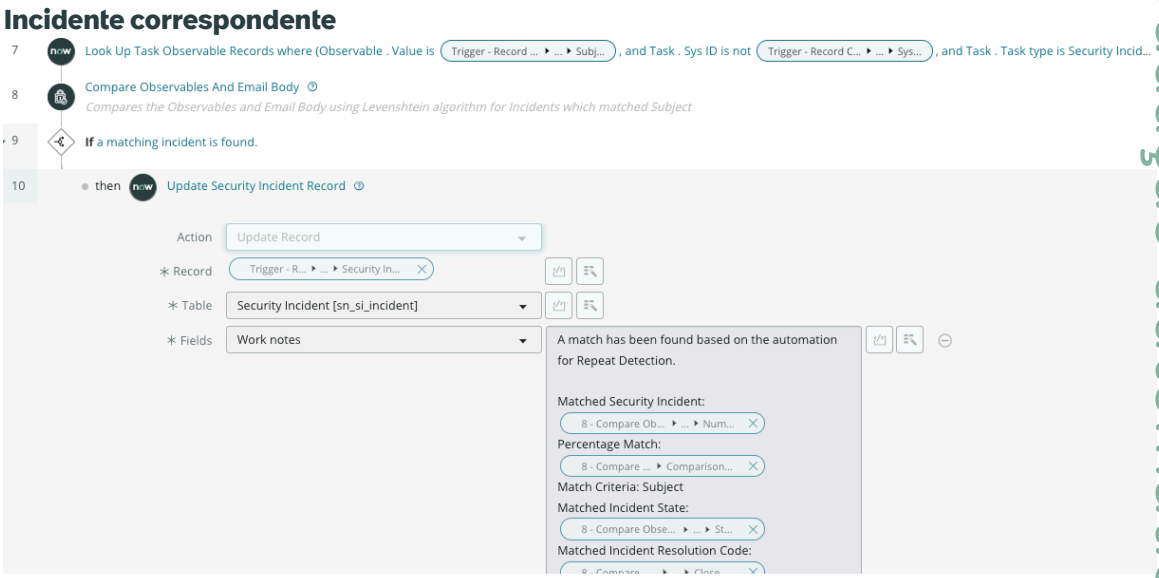
Playbook de detecção de repetição



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na etapa 3, o playbook compara os observáveis da tarefa e o corpo do e-mail usando o algoritmo Levenshtein para incidentes que correspondem ao ID da mensagem.
4. Na etapa 4, com base na investigação feita até o momento, o playbook verifica se o incidente correspondente foi encontrado com base no ID da mensagem ou não.
   Na etapa 5, se o incidente correspondente for encontrado, o playbook atualizará automaticamente a anotação de trabalho de que uma correspondência foi encontrada com base na automação da detecção de repetição. Na Etapa 6, o fluxo termina.
5. Se o incidente correspondente não for encontrado, na etapa 7, o playbook pesquisará os registros do observável de tarefa na tabela `sn_ti_m2m_task_observable` que correspondem ao incidente com base no assunto.
6. Na etapa 8, o playbook compara os observáveis da tarefa e o corpo do e-mail usando o algoritmo Levenshtein para incidentes que correspondem ao assunto.
7. Na Etapa 9, o playbook verifica se o incidente correspondente foi encontrado ou não.
   Na etapa 10, se o incidente correspondente for encontrado, o playbook atualizará automaticamente a anotação de trabalho de que uma correspondência foi encontrada com base na automação da detecção de repetição. Na Etapa 11, o fluxo termina.



8. Na etapa 12, o playbook pesquisa os registros do observável de tarefa na tabela `sn_ti_m2m_task_observable` que correspondem ao incidente com base no endereço.
9. Na etapa 13, o playbook compara os observáveis da tarefa e o corpo do e-mail usando o algoritmo Levenshtein para incidentes que correspondem ao endereço.
10. Na Etapa 14, o playbook verifica se o incidente correspondente foi encontrado com base no Endereço ou não.
    Na etapa 15, se o incidente correspondente for encontrado, o playbook atualizará automaticamente a anotação de trabalho de que uma correspondência foi encontrada com base na automação da detecção de repetição. Na Etapa 16, o fluxo termina.

Playbook para e-mails falsificados (usando o mesmo nome de exibição)

Este playbook fornece etapas de correção sistemática para investigar e-mails falsificados, que são acionados quando nomes falsificados de e-mails são enviados para os funcionários da organização.

O fluxo de trabalho é criado com base em um playbook existente, que fornece uma abordagem consistente e eficiente para investigação de incidentes. Cada ponto de decisão

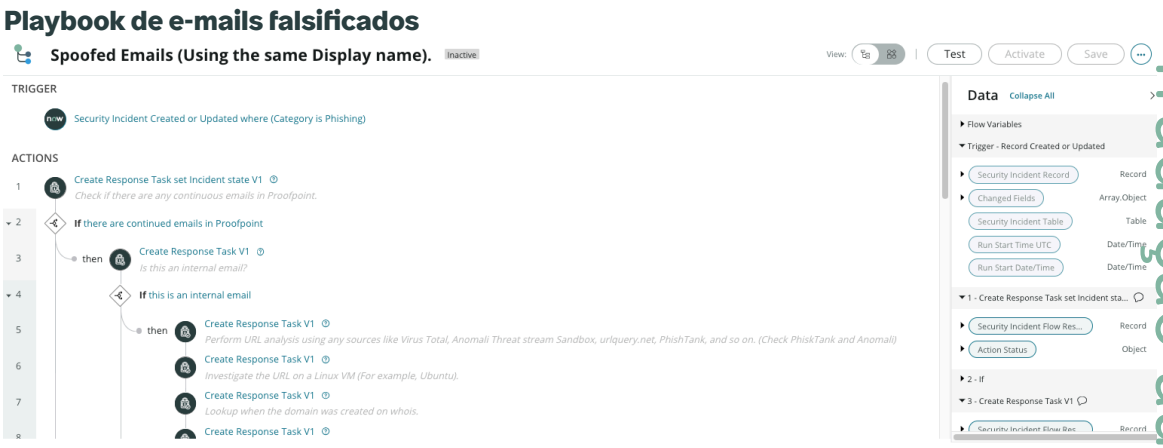
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

no playbook foi convertido em uma tarefa orientada por resultado e o fluxo muda de direção com base no resultado dessas tarefas.

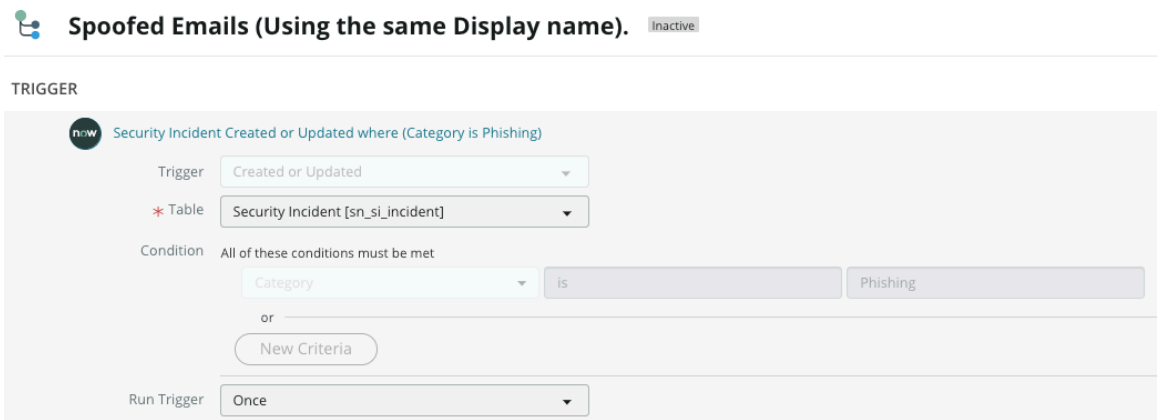
Introdução ao playbook de e-mails falsificados (usando o mesmo nome de exibição)

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione o playbook **E-mails falsificados (usando o mesmo nome de exibição)**.
3. (Opcional) Você pode criar uma cópia do fluxo do playbook de detecção de repetição e fazer as modificações necessárias. Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.



4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.

Condição do gatilho: este playbook é acionado e associado ao incidente de segurança quando a **categoria** é **Phishing**.



Configurar e-mails falsificados

Use as etapas a seguir para configurar o playbook Falhas de login do usuário do Okta de vários IPs.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

Navegar até **Todos** > > .

Usar o playbook de e-mails falsificados (usando o mesmo nome de exibição)

As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook de e-mails falsificados (usando o mesmo nome de exibição).

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

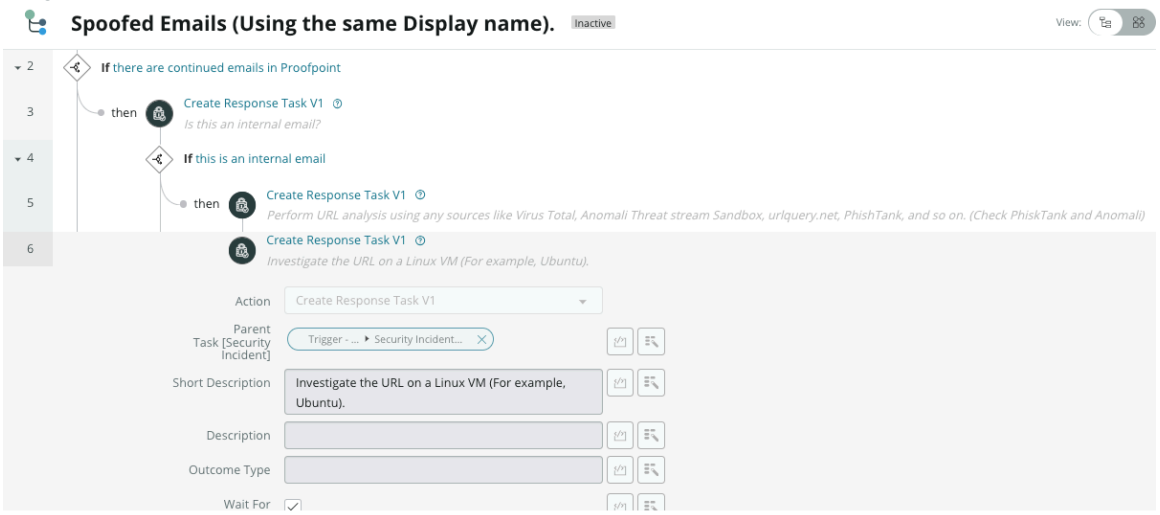
Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Etapa 1, você precisa verificar se há e-mails falsificados contínuos no Proofpoint.
2. Na Etapa 2, se houver e-mails contínuos no Proofpoint, verifique se este é um e-mail interno falsificado ou não.
3. Na Etapa 3, se este for um e-mail interno falsificado, execute as seguintes etapas:

   a. Na etapa 5, você precisa executar a análise de URL usando fontes como Total de vírus, Sandbox de fluxo de ameaças de Anomalia, urlquery.net, PhishTank (por exemplo, verifique PhiskTank e Anomali).

   b. Na etapa 6, você precisa investigar o URL em uma VM Linux (por exemplo, Ubuntu).

Playbook de e-mails falsificados (usando o mesmo nome de exibição)

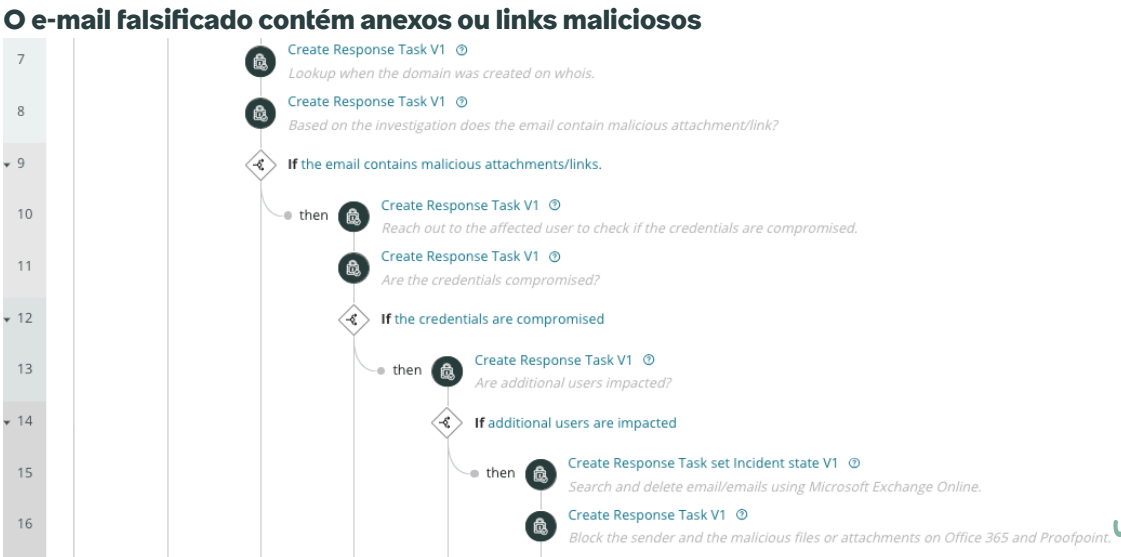


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Na etapa 7, você precisa pesquisar quando o domínio foi criado no WHOIS.
Procure domínios registrados recentemente (na última semana) que sejam suspeitos e tenham uma alta probabilidade de ataques de phishing.

d. Na etapa 8, com base na investigação feita até o momento, você precisa verificar se este e-mail contém um anexo ou link malicioso.
Se este e-mail não contiver um anexo ou link malicioso, o fluxo será encerrado.



e. Na Etapa 9, se o e-mail contiver anexos ou links maliciosos, execute as etapas a seguir.

i. Na Etapa 10, você precisa entrar em contato com o usuário afetado para verificar se as credenciais foram comprometidas. Você pode usar o modelo de e-mail fornecido para entrar em contato com o usuário afetado.

ii. Na Etapa 11, você precisa verificar se as credenciais estão comprometidas com base na resposta do e-mail. Se as credenciais não foram comprometidas, o fluxo será encerrado.

1. Na Etapa 12, se as credenciais forem comprometidas, na Etapa 13, você precisará verificar se usuários adicionais foram afetados. Se nenhum usuário adicional for afetado, o fluxo será encerrado.

2. Na Etapa 14, se usuários adicionais forem afetados, execute as seguintes etapas:

a. Na Etapa 15, você precisa pesquisar e excluir e-mails usando o Microsoft Exchange Online.

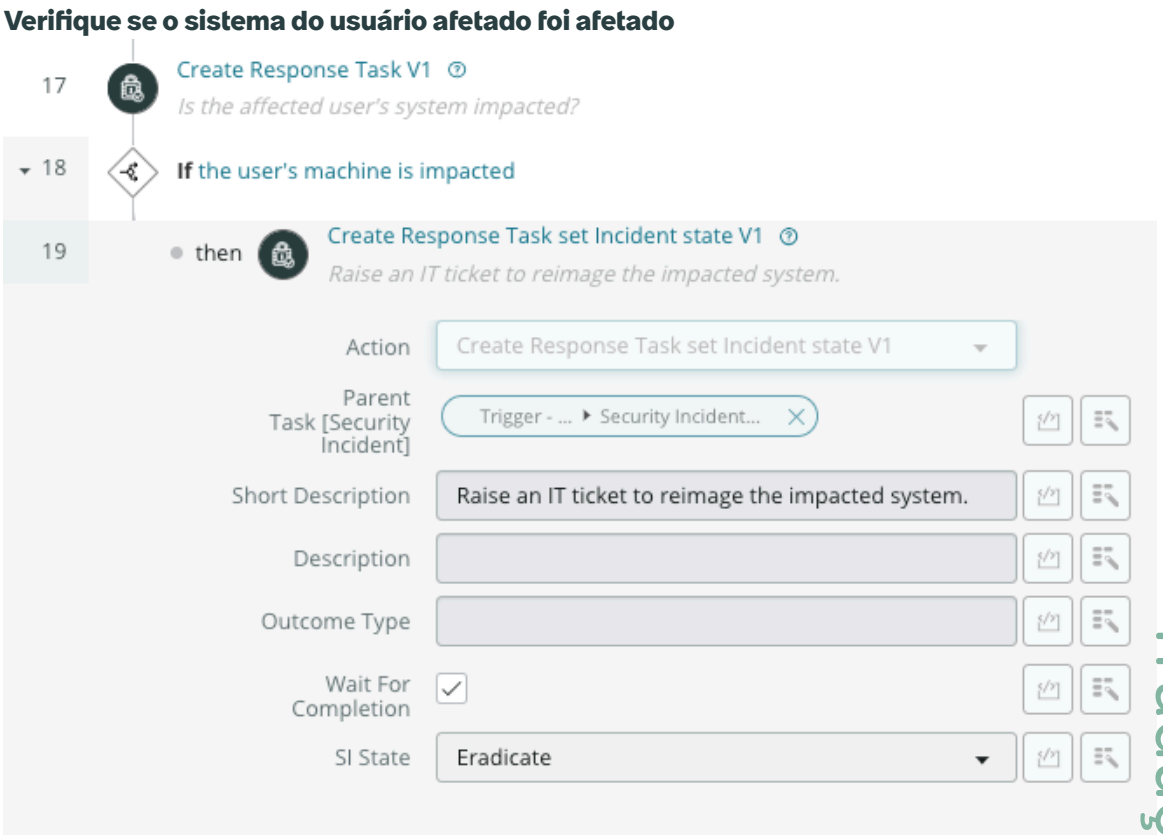
b. Na Etapa 16, você precisa bloquear o remetente e os arquivos ou anexos mal-intencionados no Office 365 e no Proofpoint.

4. Na Etapa 17, se este não for um e-mail interno falsificado, será necessário verificar se o sistema do usuário afetado foi afetado.

5. Na Etapa 18, se o sistema do usuário for afetado, na Etapa 19, gere um tíquete de TI para recriar a imagem do sistema afetado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Na Etapa 20, uma tarefa de resposta é criada para você concluir a revisão pós-incidente antes de fechar a tarefa.

Playbook for Endpoint Detection

Este playbook fornece etapas de correção sistemática para investigar alertas de malware acionados em um host ou endpoint (por exemplo, uma detecção de arquivo mal-intencionado).

Quando os alertas do CrowdStrike são acionados em um host ou endpoint, você pode usar o playbook de detecção de endpoint no Flow Designer para obter orientação e ajudar a otimizar a investigação desses arquivos maliciosos.

O fluxo de trabalho é criado com base em um playbook existente, que fornece uma abordagem consistente e eficiente para investigação de incidentes. Cada ponto de decisão no playbook foi convertido em uma tarefa orientada por resultado e o fluxo muda de direção com base no resultado dessas tarefas.

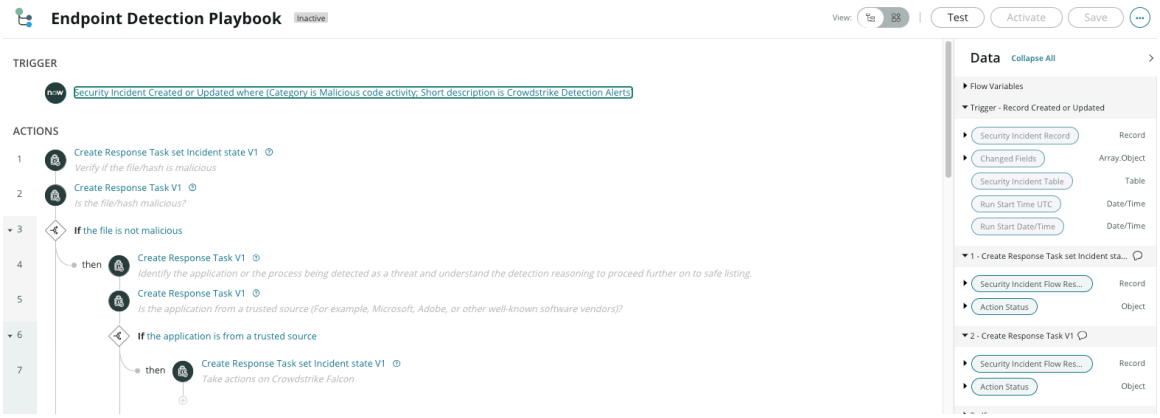
Introdução ao playbook de detecção de endpoint

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione o playbook de **detecção de endpoint**.
3. (Opcional) Você pode criar uma cópia do fluxo do playbook de detecção de endpoint e fazer as modificações necessárias. Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

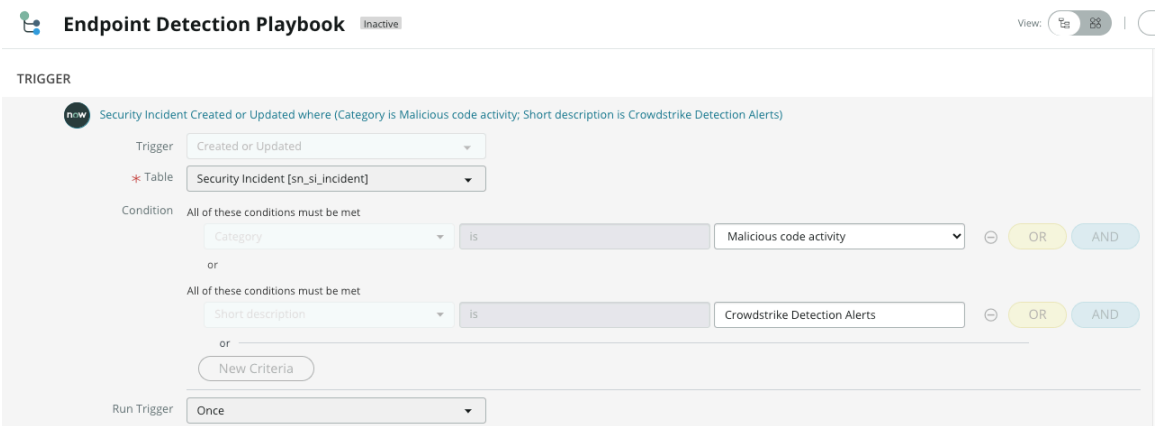
Playbook de detecção de endpoint



4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.

Condição do gatilho: este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:

- A**categoria** é **Atividade de código malicioso**.
- **A descrição resumida** é **CrowdStrike Detection Alerts**.



Configurar detecção de endpoint

Use as etapas a seguir para configurar o playbook Falhas de login do usuário do Okta de vários IPs.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

Navegar até **Todos** > > .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use o playbook de detecção de endpoint

As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook de detecção de endpoint.

Antes de Iniciar

Função necessária:

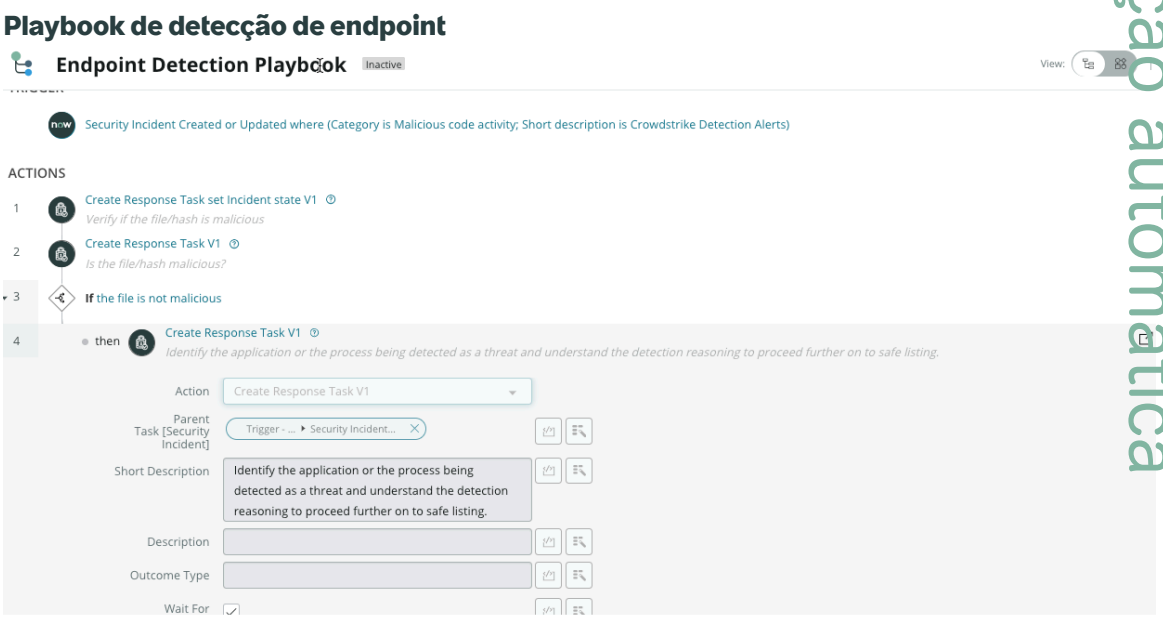
- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Etapa 1, você precisa verificar se o arquivo ou o hash é malicioso analisando os resultados da pesquisa de ameaças no SIR e coletando informações do VirusTotal, WildFire, ThreatCrowd etc.
2. Na Etapa 2, você precisa verificar se o arquivo ou o hash é mal-intencionado ou não.
3. Na Etapa 3, se o arquivo ou hash for mal-intencionado, execute as seguintes etapas:

   a. Na Etapa 4, você precisa identificar a aplicação ou o processo que está sendo detectado como uma ameaça e coletar informações sobre o motivo da detecção para prosseguir para a listagem segura.

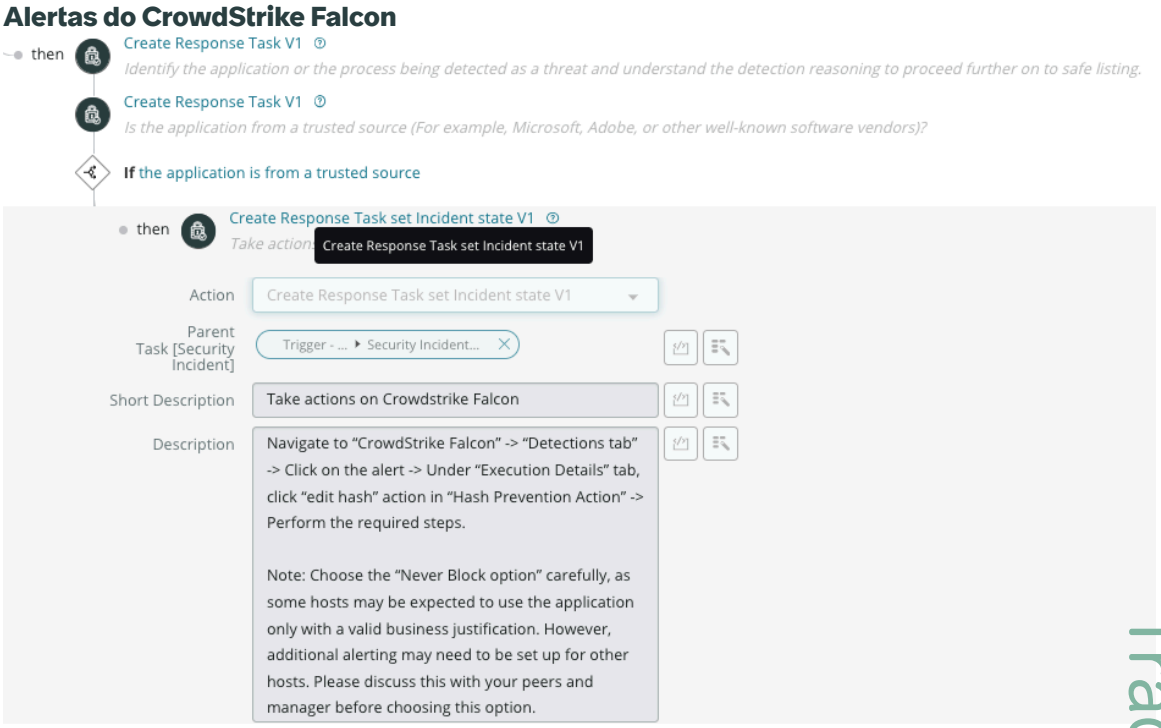


   b. Na Etapa 5, você precisa verificar se a aplicação é de uma fonte confiável (por exemplo, Microsoft, Adobe ou outros fornecedores de software conhecidos).

   c. Na Etapa 6, se a aplicação for de uma fonte confiável, você precisará agir nos alertas do CrowdStrike Falcon.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. Na Etapa 7, execute as seguintes etapas:

i. Navegar até **CrowdStrike Falcon** > **Detecções** guia.

ii. Clique no alerta do CrowdStrike Falcon.

iii. Na guia Detalhes da execução, clique em **Editar** ação de hash em Ação de prevenção de hash.

iv. Execute as etapas necessárias.

> **Nota:**
> Escolha a opção **Nunca bloquear** com cuidado, pois somente determinados hosts podem ter permissão para usar a aplicação com uma justificativa de negócios válida. No entanto, alertas adicionais podem precisar ser configurados para outros hosts.

e. Na Etapa 8, se a aplicação não for de uma fonte confiável, você precisará escolher se deseja dispensar o arquivo ou a aplicação do dispositivo localmente.
Na Etapa 10, se você quiser dispensar o arquivo ou a aplicação do dispositivo localmente, execute as seguintes etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

i. Na Etapa 11, navegue até a guia **Arquivos em quarentena** e filtre o endpoint pesquisando o nome do dispositivo.

ii. Selecione o arquivo que precisa ser suspenso localmente e clique em **Liberar**.

Nota:

- O arquivo ainda é executado neste endpoint específico. No entanto, a detecção e a quarentena continuam acontecendo em todos os outros hosts.
- Para liberar em massa o arquivo de quarentena em vários hosts, selecione os nomes de arquivo e o status apropriados. Clique em **Selecionar**e em **Liberar**.

Na Etapa 12, se você não quiser dispensar o arquivo ou a aplicação do dispositivo localmente, poderá redirecionar o usuário para o suporte de TI para solicitar a instalação das aplicações aprovadas.

4. Na Etapa 14, se o arquivo ou o hash não for malicioso, execute as seguintes etapas:

a. Na Etapa 15, você precisa determinar se o arquivo/hash é de alto risco ou baixo risco com base na função do usuário (departamento ou cargo que lida com informações confidenciais), no tipo de aplicação (ransomware, root kit etc.) e no impacto da aplicação (quantos usuários foram afetados).

b. Na Etapa 16, se o arquivo for de alto risco, execute as seguintes etapas:

i. Na Etapa 17, revise os resultados com a equipe de informações sobre ameaças.

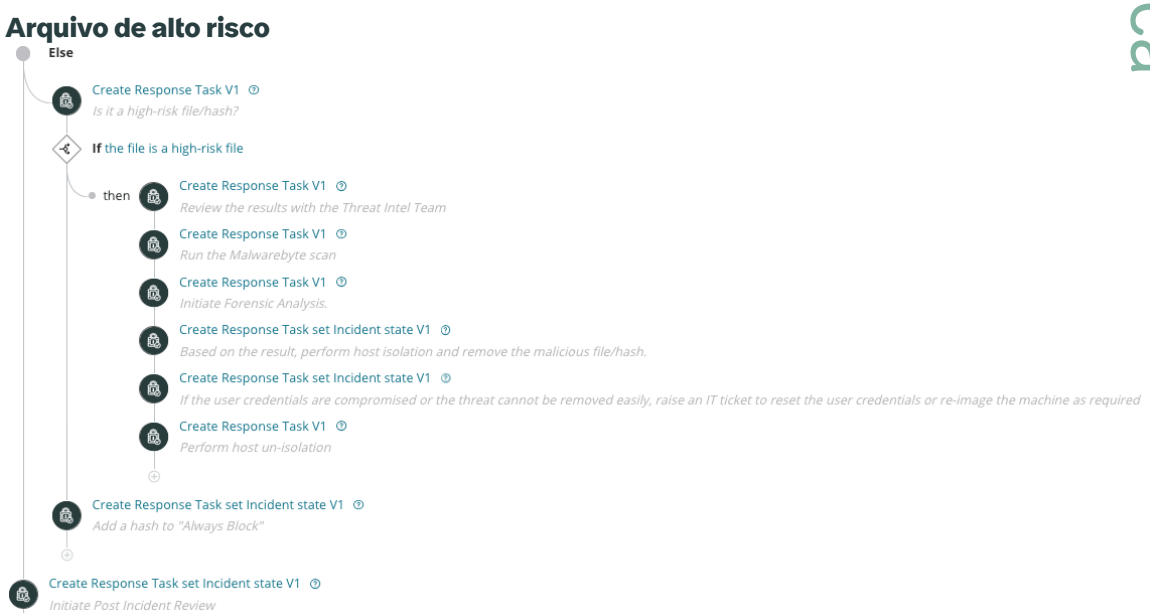
ii. Na Etapa 18, execute a verificação do Malwarebyte no arquivo.

iii. Na Etapa 19, inicie a Análise forense.

iv. Na etapa 20, com base no resultado da análise forense, execute o isolamento de host e remova o arquivo/hash mal-intencionado.

v. Na Etapa 21, se as credenciais do usuário forem comprometidas ou a ameaça não puder ser removida facilmente, gere um tíquete de TI para redefinir as credenciais do usuário ou recriar a imagem da máquina conforme necessário.

vi. Na Etapa 22, execute o cancelamento do isolamento do host.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Na Etapa 23, se o arquivo não for um arquivo de alto risco, execute as seguintes etapas:

i. Navegar até **CrowdStrike Falcon** > **Configurações** guia.

ii. Na guia Configurações, navegue até **Hashes de prevenção** > > **Carregar hash** > **Adicionar o hash**.

iii. Escolha o SO necessário e selecione **Sempre bloquear**.

5. Na Etapa 24, uma tarefa de resposta é criada para que o usuário conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para Possível PasswordSpray

Este playbook fornece etapas de correção sistemática para investigar alertas de aplicação de senha acionados por vários logins com falha (muitas falhas de autenticação de mais de um endereço IP para o mesmo usuário).

O fluxo de trabalho é criado com base em um playbook existente, que fornece uma abordagem consistente e eficiente para investigação de incidentes. Cada ponto de decisão no playbook foi convertido em uma tarefa orientada por resultado e o fluxo muda de direção com base no resultado dessas tarefas.

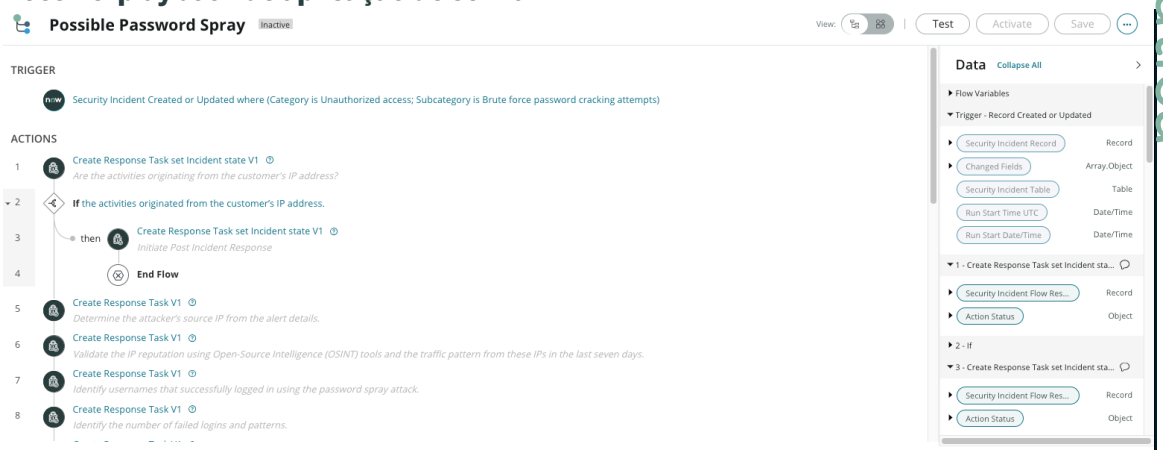
Introdução ao playbook de possível aplicação de senha

1. Faça login como um usuário com as funções sn_si.user e flow_designer.

2. Navegar até **Tudo** > **Flow Designer** e selecione o playbook de **Possível aplicação de senha**.

3. (Opcional) Você pode criar uma cópia do fluxo do playbook de possível aplicação de senha e fazer as modificações necessárias. Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

Possível playbook de aplicação de senha



4. Ative os playbooks.

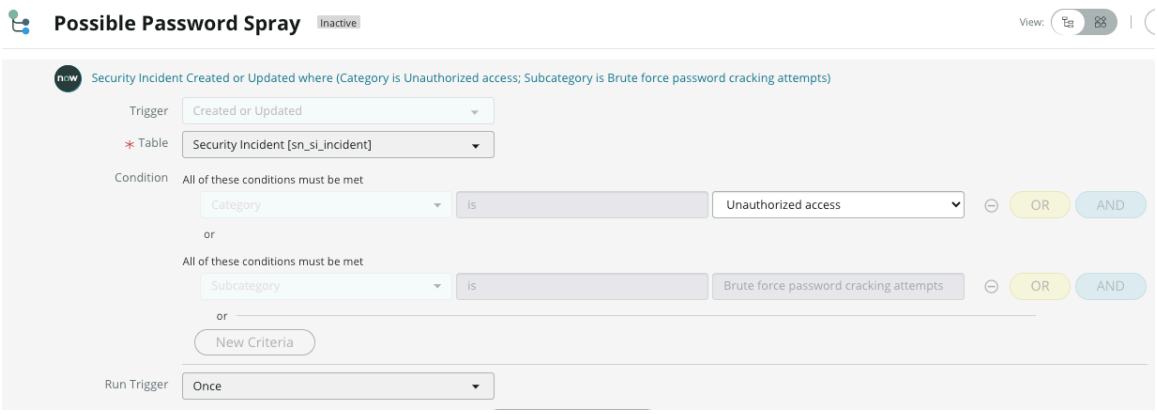
- Ative o fluxo principal para usar o playbook disponível no sistema de base.
- Ative os fluxos copiados depois de fazer as mudanças necessárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condição do gatilho: este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:

- A**categoria** é **Acesso não autorizado**.
- **A subcategoria** é **Tentativas de quebra de senha de força bruta**.



Configurar possível aplicação de senha

Use as etapas a seguir para configurar o playbook Falhas de login do usuário do Okta de vários IPs.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

Navegar até **Todos** > > .

Use o playbook de Possível aplicação de senha

As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook de Possível aplicação de senha.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Etapa 1, você precisa verificar se as atividades são originadas do endereço IP do cliente.
   Identifique os endereços IP que executam o ataque do PasswordSpray. Por exemplo, use os TXIDs (IDs de transação) do alerta e pesquise-os nos logs F5.
2. Na Etapa 2, se as atividades se originaram do endereço IP do cliente, execute as seguintes etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

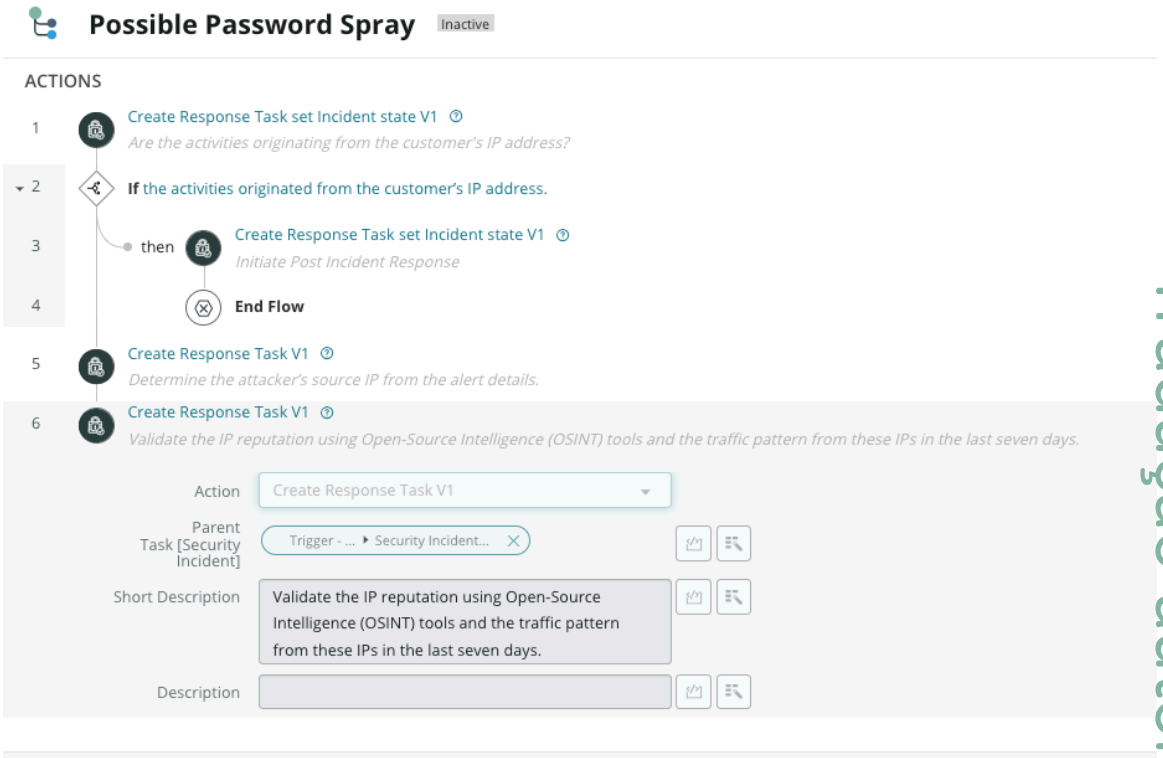
a. Na Etapa 3, você precisa iniciar uma revisão pós-incidente do possível ataque de PasswordSpray.

b. Na Etapa 4, o fluxo termina.

3. Na etapa 5, se as atividades não se originaram do endereço IP do cliente, determine o IP de origem do invasor a partir dos detalhes do alerta.

4. Na etapa 6, você precisa validar a reputação do IP usando as ferramentas da Inteligência de código aberto (OSINT) e o padrão de tráfego desses IPs nos últimos sete dias.

Possível playbook de aplicação de senha



5. Na Etapa 7, você precisa identificar os nomes de usuário que fizeram login com sucesso usando o ataque de PasswordSpray.

6. Na Etapa 8, você precisa identificar o número de logins e padrões com falha.

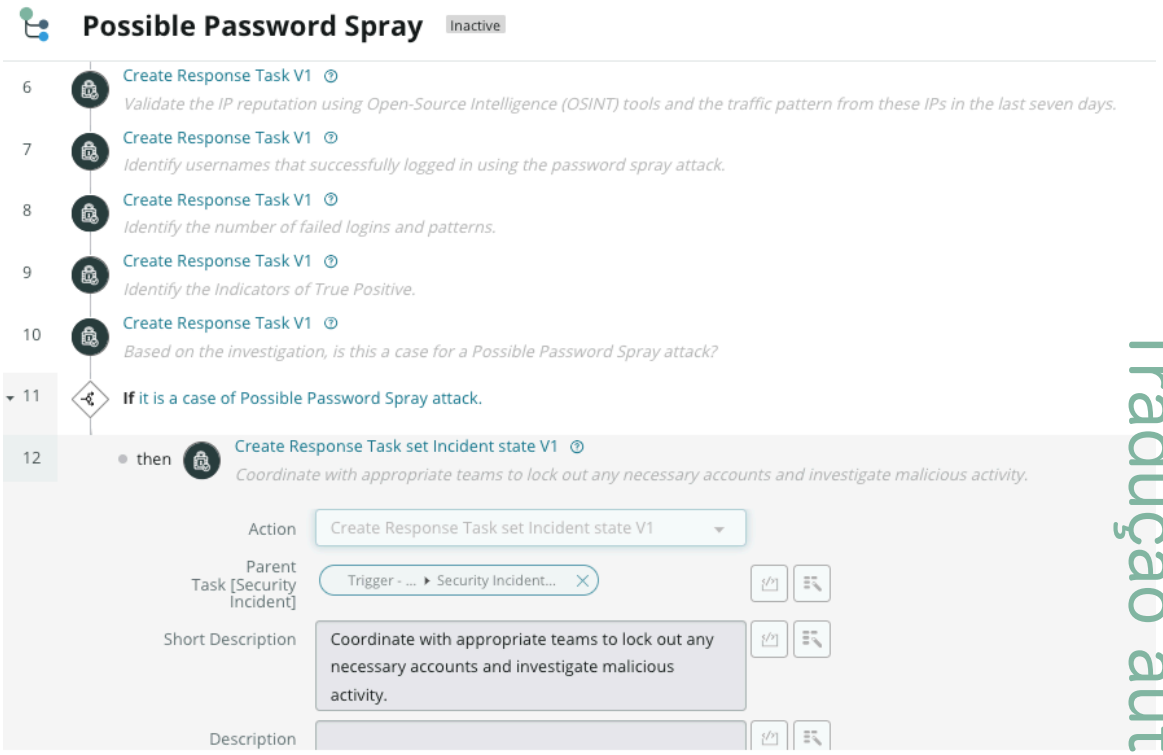
7. Na Etapa 9, você precisa identificar os indicadores de verdadeiro positivo.

- Verifique o tráfego dos IPs de origem nos últimos 60 dias. Nenhum tráfego histórico pode ser uma indicação de um verdadeiro positivo.
- Verifique os padrões de nome de usuário com falhas de autenticação e a contagem. Quanto maior a contagem, maior a probabilidade de ser um verdadeiro positivo.
- O nome de usuário se parece com uma base de dicionário (começando de A a Z) e pode ter nomes de administrador comuns, como admin, sysadmin, root e assim por diante
- O mesmo nome de usuário pode ter padrões diferentes no ataque de dispersão, como o mesmo alerta, pode ter falhas para john.doe, johnd, jdoe, john_doe, jdoe7 etc., indicando que os invasores adivinham o padrão de nome de usuário com base em casos de uso comuns.
- Observe o agente do usuário e os URIs dos logs F5 na etapa acima e veja se os IOCs estão relacionados aos alertas do Red Condor. Se eles corresponderem, será um evento verdadeiro positivo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Na Etapa 10, com base na investigação feita até o momento, você precisa verificar se este é um caso de possível ataque de PasswordSpray ou não.
9. Na Etapa 11, se este for o caso de um possível ataque de Pulverização de Senha, execute as seguintes etapas:
    a. Na Etapa 12, você precisa coordenar com as equipes apropriadas para bloquear todas as contas necessárias e investigar atividades mal-intencionadas.



    b. Na Etapa 13, você precisa iniciar uma revisão pós-incidente do possível ataque do PasswordSpray.
    c. Na Etapa 14, o fluxo termina.
10. Na Etapa 15, você precisa verificar se este não é um caso de possível ataque de PasswordSpray.
11. Na Etapa 16, se este não for um caso de possível ataque de Aplicação de senha, execute as seguintes etapas:
    a. Na Etapa 17, você precisa documentar as descobertas até o momento.
    b. Na Etapa 18, você precisa iniciar uma revisão pós-incidente do possível ataque do PasswordSpray.
    c. Na Etapa 19, o fluxo termina.
12. Na etapa 20, você precisa consultar os colegas e o gerente de GIR para obter orientação.
13. Na Etapa 21, uma tarefa de resposta é criada para concluir a revisão pós-incidente antes de fechar a tarefa.

Playbook for T1003 - Detectar ferramentas de despejo de credencial

Este playbook ajuda na triagem de fase inicial dos envios de phishing relatados pelo usuário, alertando o analista para a possibilidade de um domínio semelhante no endereço de e-mail do Phisher.

O fluxo de trabalho é criado com base em um playbook existente, que fornece uma abordagem consistente e eficiente para investigação de incidentes. Cada ponto de decisão

Tradução automática

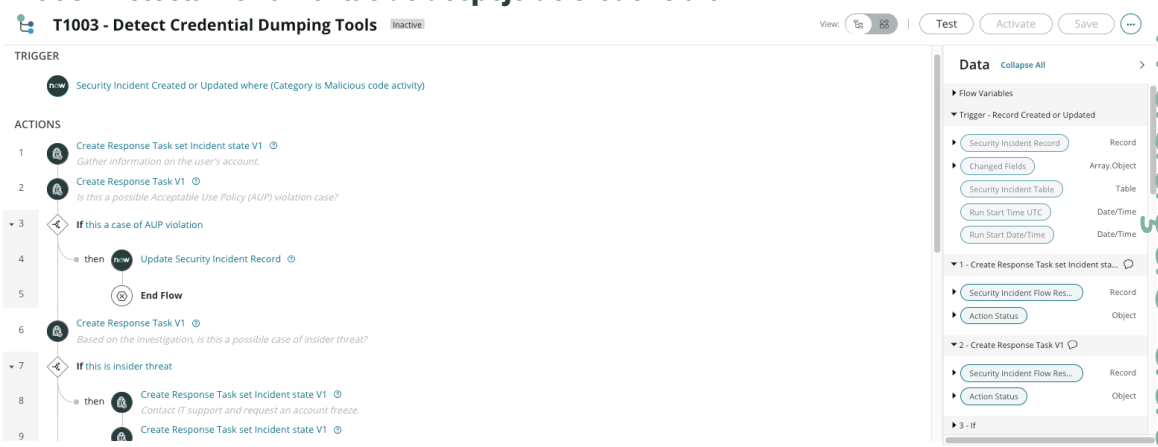
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

no playbook foi convertido em uma tarefa orientada por resultado e o fluxo muda de direção com base no resultado dessas tarefas.

Introdução ao T1003 - Detectar playbook de ferramentas de despejo de credencial

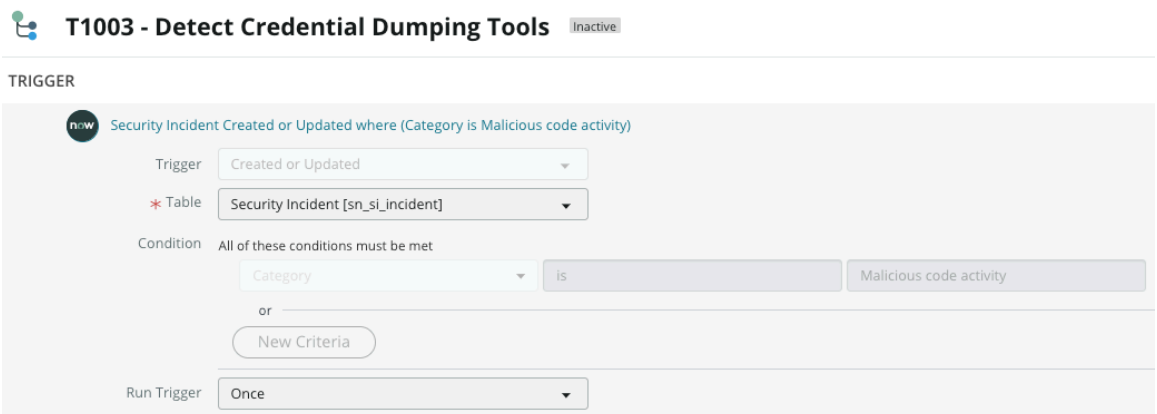
1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione o **playbook T1003 - Detectar ferramentas de despejo de credencial**.
3. (Opcional) Você pode criar uma cópia do fluxo do playbook T1003 - Detectar ferramentas de despejo de credencial e fazer as modificações necessárias. Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

T1003 - Detectar ferramentas de despejo de credenciais



4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.

Condição do gatilho: este playbook é acionado e associado ao incidente de segurança quando a **categoria** é **atividade de código malicioso**.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar despejo de credencial de detecção

Use as etapas a seguir para configurar o playbook Falhas de login do usuário do Okta de vários IPs.

Antes de Iniciar
Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

Navegar até **Todos** > > .

Use o playbook T1003 - Detectar ferramentas de despejo de credenciais

As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook T1003 - Detectar ferramentas de despejo de credencial.

Antes de Iniciar
Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

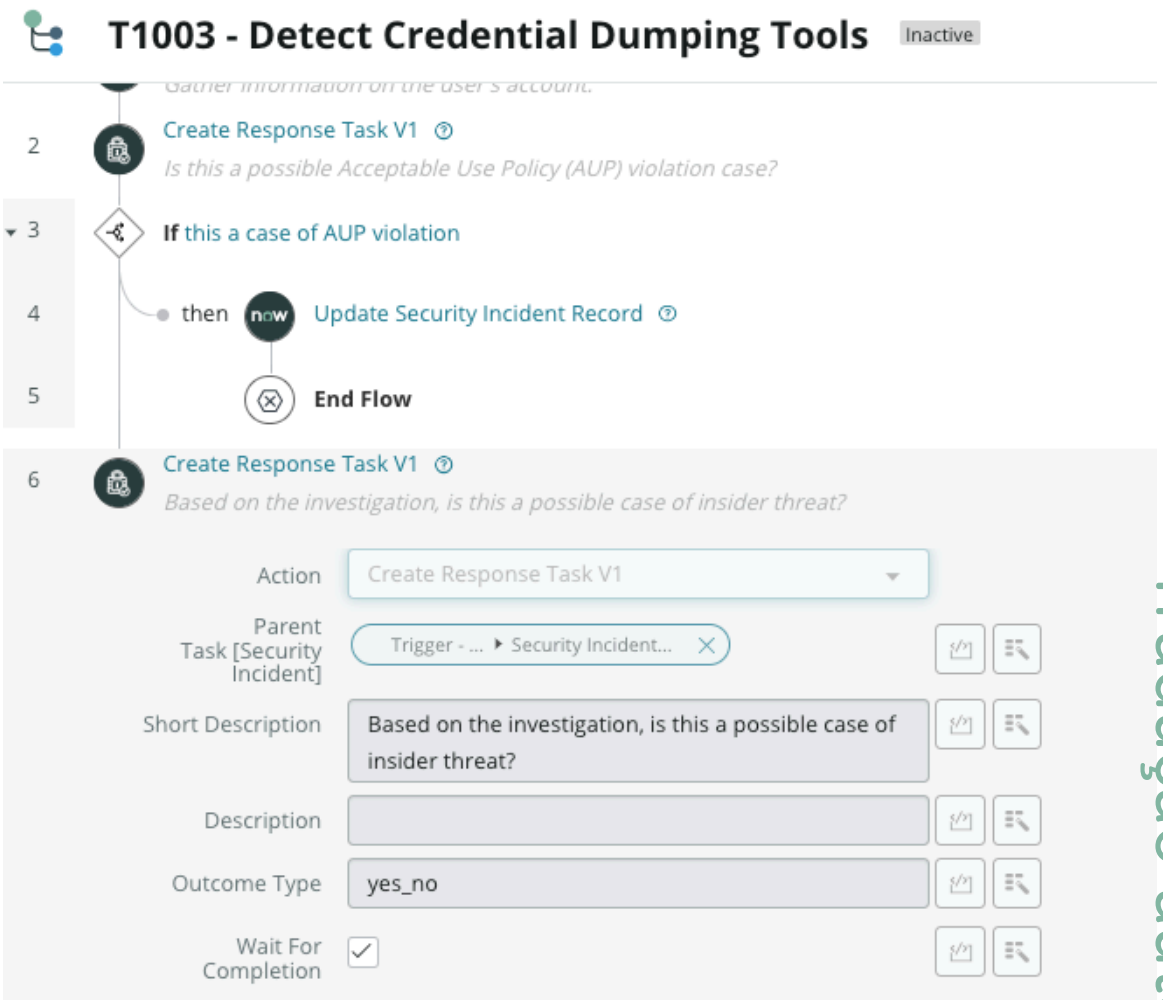
Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Etapa 1, você precisa coletar informações sobre a conta do usuário.
   - Você precisa verificar a atividade do host para procurar atividades suspeitas.
   - Você precisa identificar o proprietário do servidor/endpoint/VM e capturar os dados correlacionados à ferramenta.
   - Você precisa coletar informações sobre as outras contas do usuário.
2. Na etapa 2, você precisa verificar se este é um possível caso de violação da Política de uso aceitável (AUP). Você pode fazer uma revisão por pares com as evidências coletadas e consultar o gerente de incidentes regional para saber se deve entrar em contato com o usuário.
3. Na etapa 3, se este for um caso de violação da Política de uso aceitável (AUP), execute as seguintes etapas:
   a. Na Etapa 4, você precisa atualizar o incidente de segurança de que este é um caso de violação de AUP
   b. Na Etapa 5, o fluxo termina.
4. Na etapa 6, com base na investigação feita até o momento, você precisa verificar se este é um possível caso de ameaça interna ou não.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

T1003 - Detectar ferramentas de despejo de credenciais



5. Na Etapa 7, se este for um caso de ameaça interna, execute as seguintes etapas:

a. Na Etapa 8, você precisa entrar em contato com o suporte de TI e solicitar um congelamento de conta.

b. Na Etapa 9, você precisa bloquear IPs mal-intencionados.

c. Na Etapa 10, você precisa entrar em contato com os funcionários internos por meio de um e-mail. Você pode usar o modelo de e-mail fornecido para entrar em contato com seus funcionários internos.

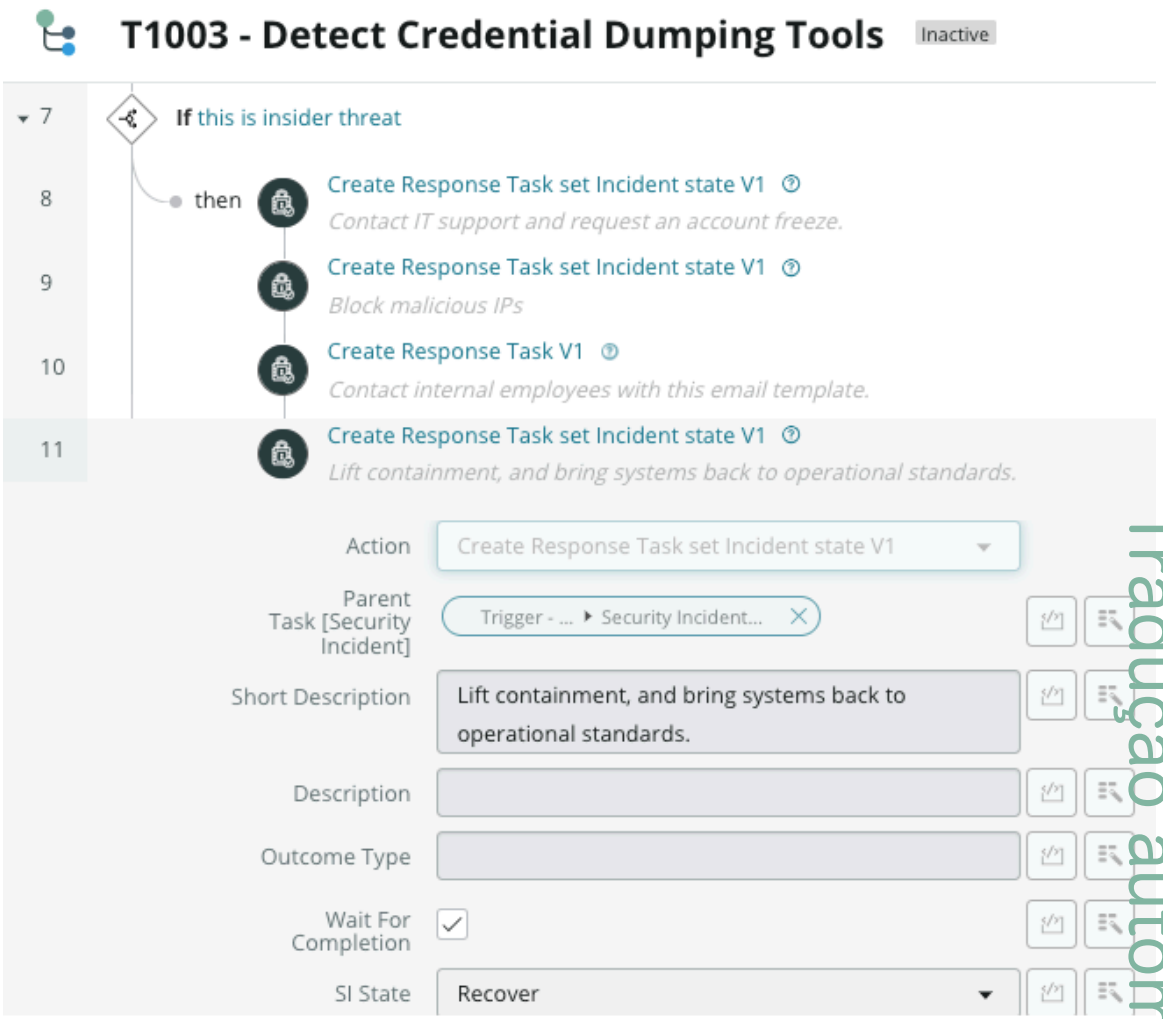
d. Na Etapa 11, você precisa suspender a contenção e trazer os sistemas de volta aos padrões operacionais.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O fluxo termina.

Tarefas de resposta para retirar a contenção



6. Na Etapa 12, se este não for um caso de ameaça interna, na Etapa 13, você precisará executar uma revisão por pares para determinar se isso precisa ser adicionado à lista de exclusões.
   O fluxo termina.
7. Na Etapa 14, uma tarefa de resposta é criada para concluir a revisão pós-incidente antes de fechar a tarefa.

Playbook para detecção de falsificação de domínio de e-mail

Este playbook ajuda na triagem de fase inicial dos envios de phishing relatados pelo usuário, alertando o analista para a possibilidade de um domínio semelhante no endereço de e-mail do Phisher.

O playbook de detecção de falsificação de domínio de e-mail procura encontrar uma correspondência de semelhança entre o domínio de e-mail do remetente do Phisher com um nome de domínio confiável existente no repositório do observável. Quando uma correspondência de domínio de e-mail do remetente falsificada for identificada pelo playbook, os analistas serão alertados com um marcador.

O fluxo de trabalho é criado com base em um playbook existente, que fornece uma abordagem consistente e eficiente para investigação de incidentes. Cada ponto de decisão no playbook foi convertido em uma tarefa orientada por resultado e o fluxo muda de direção com base no resultado dessas tarefas.

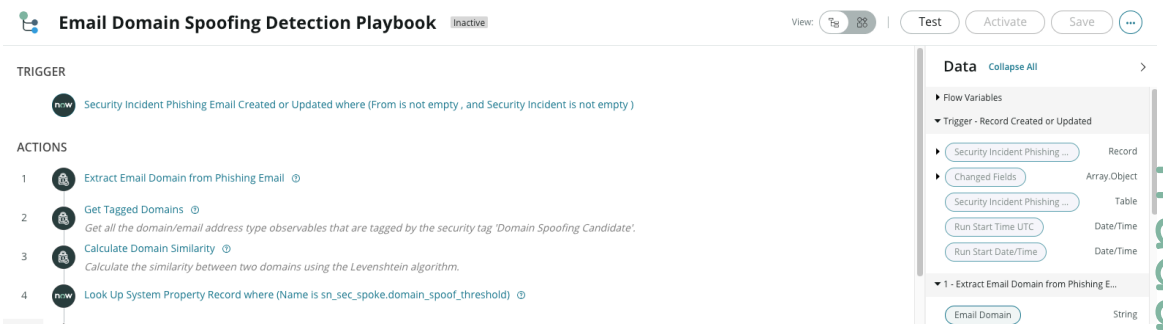
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Introdução ao playbook de detecção de falsificação de domínio de e-mail

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione o **playbook de detecção de falsificação de domínio de e-mail**.
3. (Opcional) Você pode criar uma cópia do fluxo do playbook de detecção de falsificação de domínio de e-mail e fazer as modificações necessárias. Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

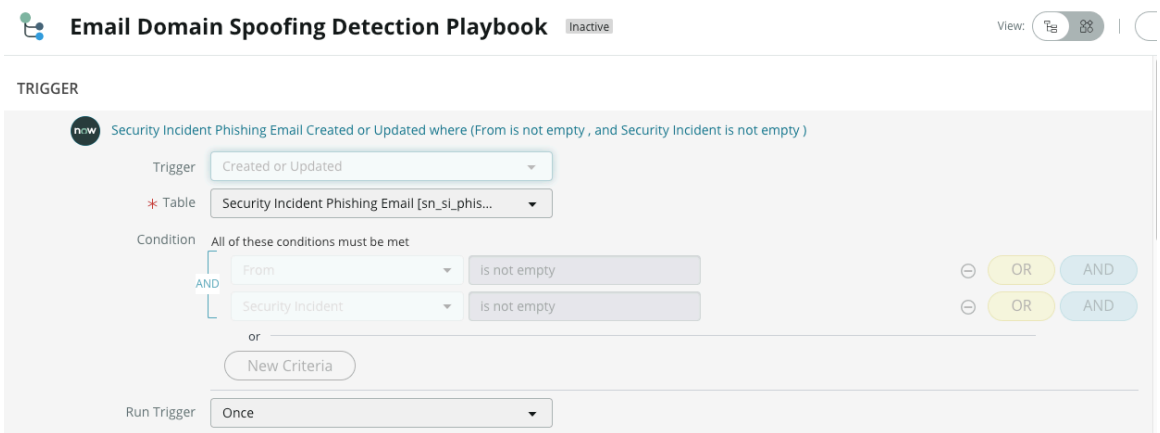
Playbook de detecção de falsificação de domínio de e-mail



4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.

Condição do gatilho: este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:

- **De não está vazio**.
- **O incidente de segurança não está vazio**.



Configurar detecção de falsificação de e-mail

Use as etapas a seguir para configurar o playbook Falhas de login do usuário do Okta de vários IPs.

Antes de Iniciar

Função necessária:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

Navegar até **Todos** > > .

Usar o playbook de detecção de falsificação de domínio de e-mail

As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook de detecção de falsificação de domínio de e-mail.

Antes de Iniciar

Função necessária:

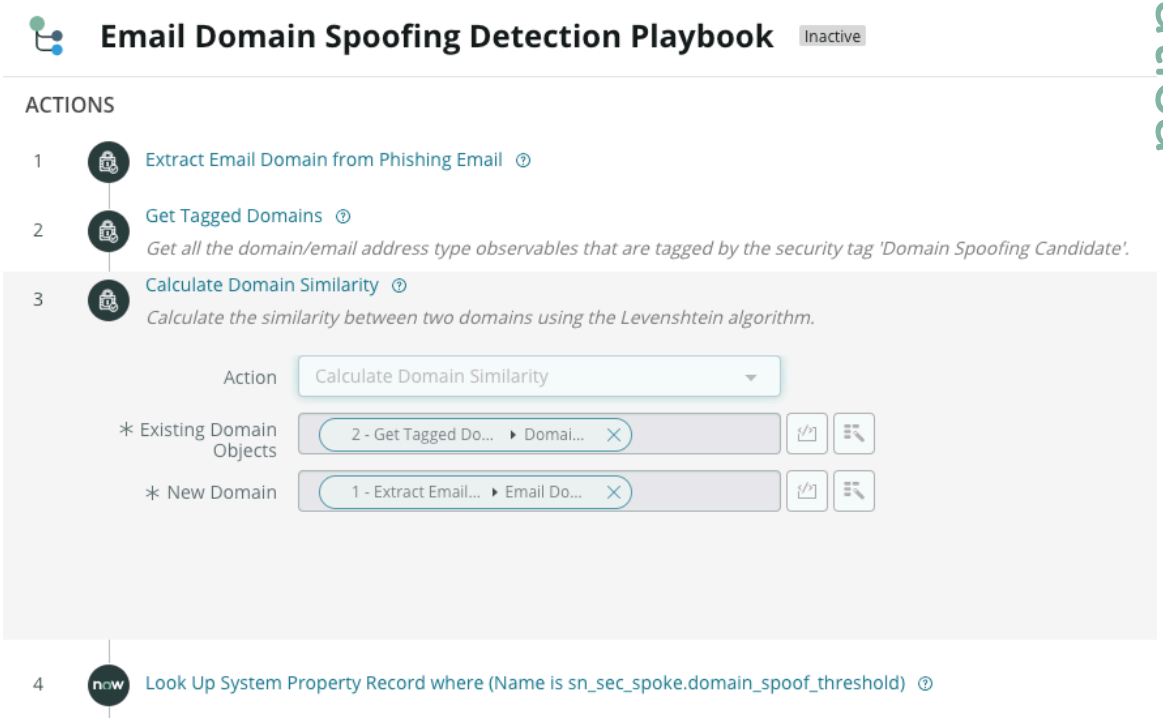
- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Etapa 1, o playbook extrai o domínio de e-mail do e-mail de phishing.
2. Na etapa 2, o playbook recupera todos os observáveis de tipo de domínio/endereço de e-mail marcados pelo marcador de segurança "Candidato a falsificação de domínio".
3. Na etapa 3, o playbook calcula a semelhança entre o domínio Obter marcador e o domínio E-mail usando o algoritmo Levenshtein.

Playbook de detecção de falsificação de domínio de e-mail



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Na etapa 4, o playbook pesquisa o registro de propriedade do sistema com base nas seguintes condições:
   - O nome é sn_sec_spoke.domain_spoof_threshold, (OR)
   - O nome vai de A a Z e, se vários registros forem encontrados, retornará somente o primeiro registro.
5. Na etapa 5, com base na investigação feita até o momento, o playbook verifica se a semelhança dos dois domínios excede o limite ou não.
   Se a semelhança dos dois domínios não exceder o limite, uma tarefa de resposta manual será criada na Etapa 5 e o fluxo será encerrado. Se a semelhança dos dois domínios exceder o limite, as etapas 6 e 7 serão executadas.

A semelhança excede o limite

6. Na etapa 6, o playbook adiciona o marcador de segurança de falsificação de domínio de e-mail ao incidente de segurança.
7. Na etapa 7, o playbook adiciona um link de anotação de trabalho ao contexto usando a opção de script.
8. Na Etapa 8, o fluxo termina.

Playbook para domínio com erro de digitação

Domínios com erro de digitação são nomes de domínio intencionalmente incorretos que se parecem muito com nomes legítimos. Os invasores aproveitam os erros de ortografia para direcioná-los a um site mal-intencionado para fins de exploração financeira ou outras atividades mal-intencionadas.

Os domínios com erro de digitação são relatados para a equipe de operações de segurança de diferentes fontes, como soluções de proteção de risco digital (Sombras digitais) e plataformas de inteligência contra ameaças (Anomali Threatstream). Depois que um incidente de segurança é criado, esta solução ajuda a identificar se o domínio é realmente um domínio com erro de digitação. Se for um domínio com erro de digitação, o analista poderá relatá-lo para a equipe jurídica para que outras ações possam ser tomadas.

Tradução automática

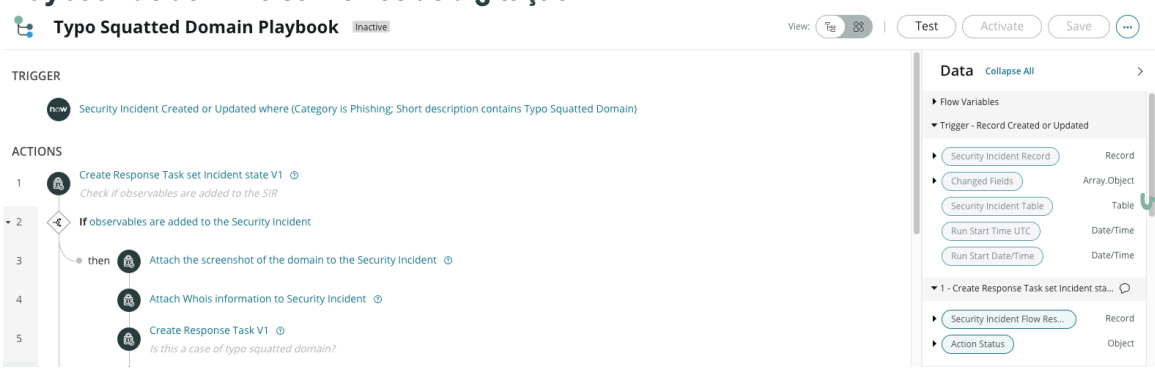
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O fluxo de trabalho é criado com base em um playbook existente, que fornece uma abordagem consistente e eficiente para investigação de incidentes. Cada ponto de decisão no playbook foi convertido em uma tarefa orientada por resultado e o fluxo muda de direção com base no resultado dessas tarefas.

Introdução ao playbook de domínio com erro de digitação

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione o playbook **Domínio** com erros de digitação.
3. (Opcional) Você pode criar uma cópia do fluxo do playbook de domínio com erro de digitação e fazer as modificações necessárias. Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

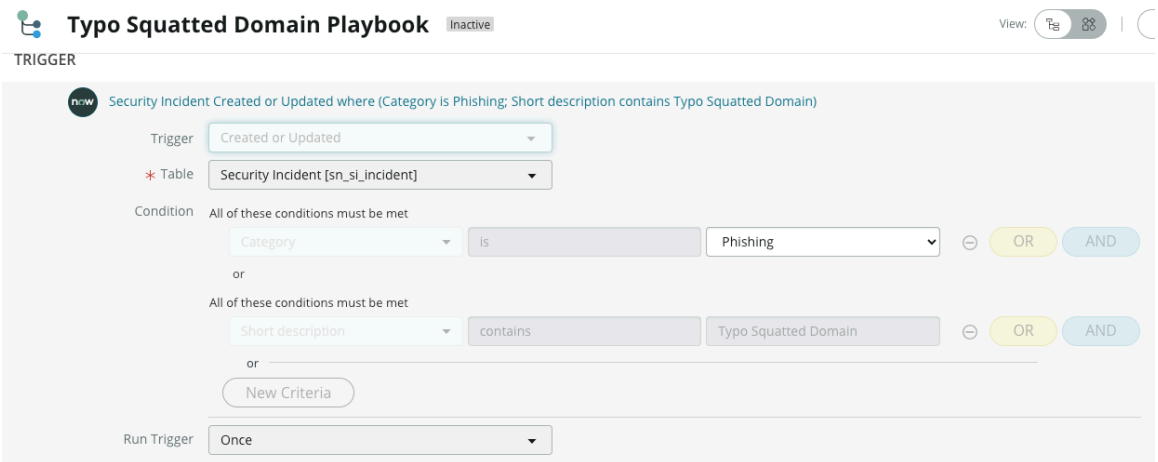
Playbook de domínio com erros de digitação



4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.

Condição do gatilho: este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:

- A**categoria** é **Phishing**.
- **A descrição resumida** contém **domínio com erro**de digitação.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar playbook de domínio com erro de digitação

Use as etapas a seguir para configurar o playbook Falhas de login do usuário do Okta de vários IPs.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

Navegar até **Todos** > > .

Usar o playbook de domínio com erros de digitação

As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook de domínio de erro de digitação.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

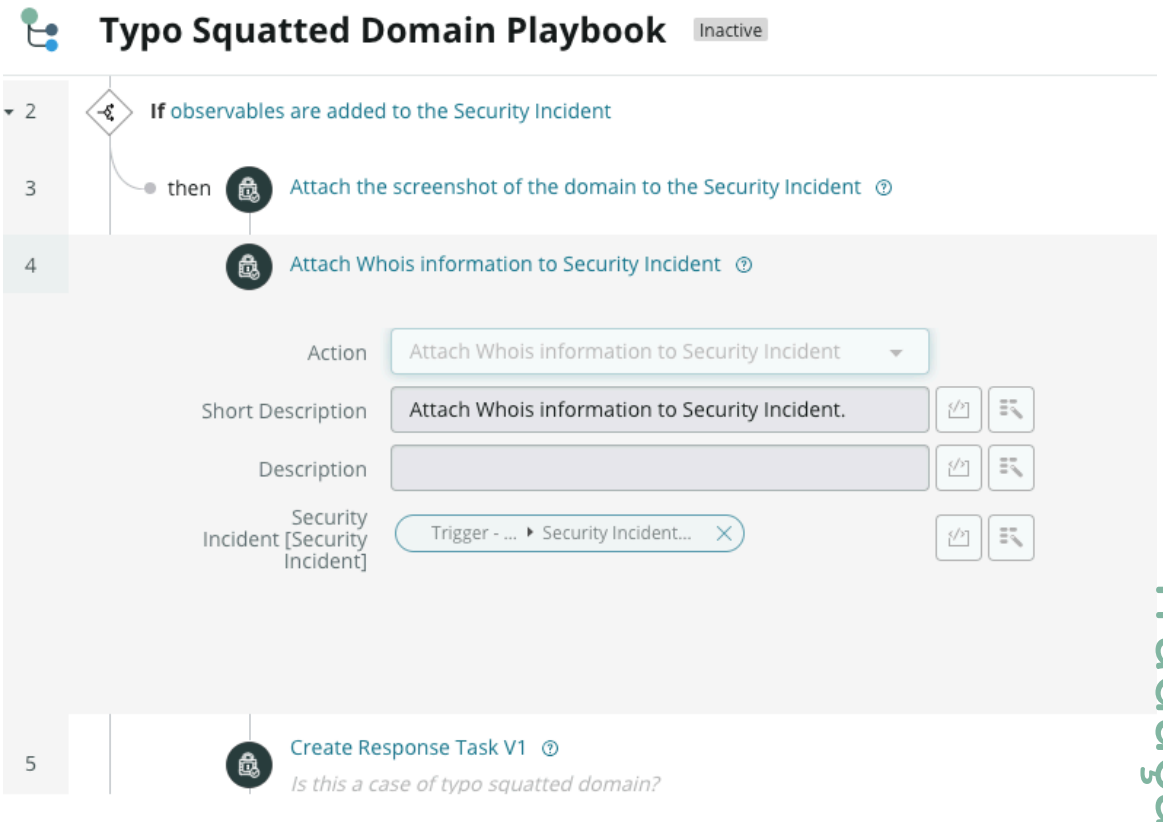
Procedimento

1. Quando o playbook é acionado e começa a ser executado, na Etapa 1, você precisa verificar se os observáveis foram adicionados ao Security Incident Response (SIR).
   Se os observáveis não forem adicionados ao SIR, adicione os observáveis antes de prosseguir. Se os observáveis não estiverem disponíveis, a Etapa 10 será executada e o incidente de segurança será encerrado.
2. Na Etapa 2, se os observáveis forem adicionados ao incidente de segurança, as etapas a seguir serão executadas.
3. Na etapa 3, você precisa anexar a captura de tela do domínio de erro de digitação ao incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de domínio com erros de digitação

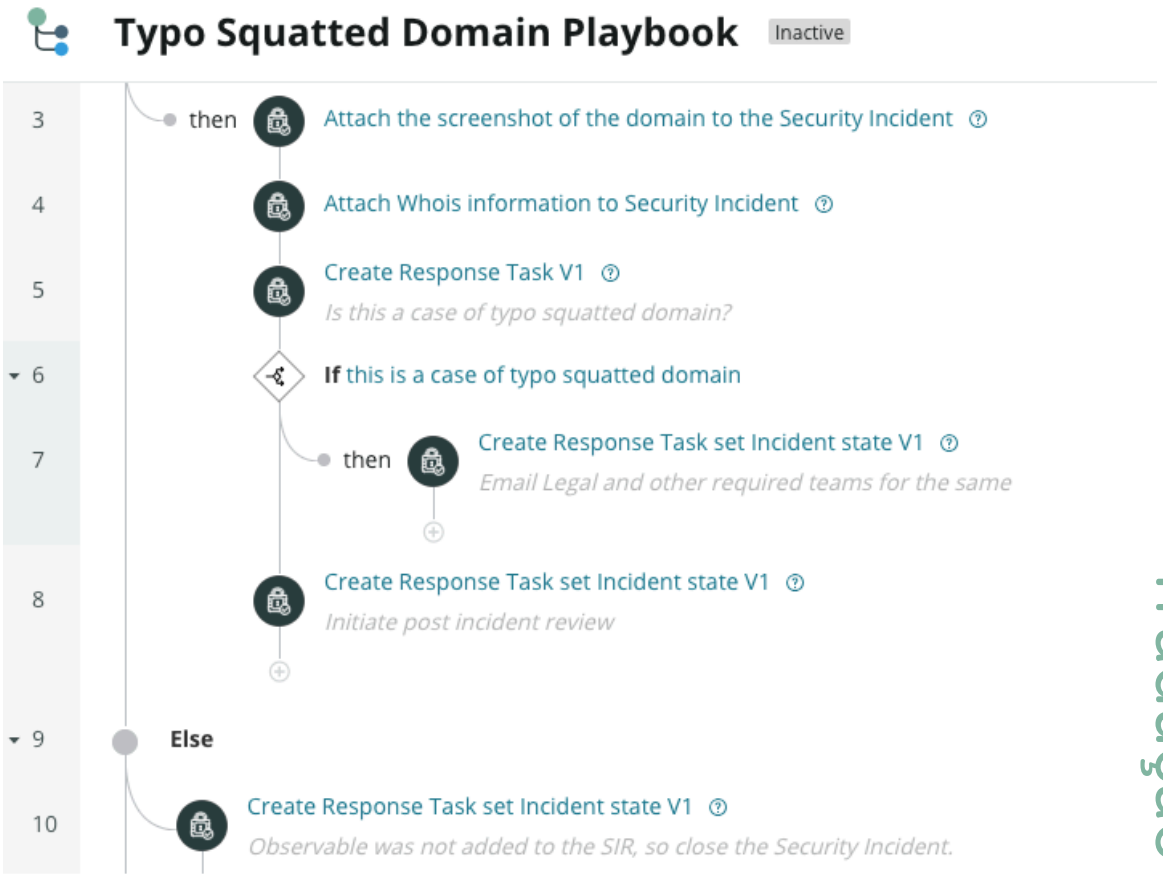


4. Na Etapa 4, você precisa anexar as informações de Whois ao incidente de segurança.
5. Na etapa 5, com base na investigação feita até o momento, o playbook verifica se este é um caso de domínio com erro de digitação ou não.
   Se este não for um caso de domínio de erro de digitação, uma tarefa de resposta manual será criada na etapa 5 e o fluxo será encerrado.
6. Na etapa 6, se este for um caso de domínio com erro de digitação, a etapa 7 será executada.
7. Na Etapa 7, você precisa enviar um e-mail e informar as equipes jurídicas e outras necessárias que este é um caso de domínio com erro de digitação e tomar as medidas necessárias para erradicá-lo.
   Se este não for um caso de domínio de erro de digitação, uma tarefa de resposta manual será criada na etapa 5 e o fluxo será encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caso de domínio com erro de digitação



8. Na Etapa 9, uma tarefa de resposta é criada para você concluir a revisão pós-incidente antes de fechar a tarefa.

Playbook for Credential Snifting

Este playbook fornece etapas de correção do sistema para investigar um incidente envolvendo atividades de detecção de credenciais realizadas por meio da tabela `sys_installation_exit` em uma instância da ServiceNow.

O playbook de detecção de credenciais fornece um campo de script para processar os logins do banco de dados (DB), Single Sign-on (SSO) e LDAP (Lightweight Directory Access Protocol) usando os registros na tabela `sys_installation_exit`. Esses campos de script privilegiados permitem ouvir solicitações e parâmetros do usuário para as instâncias durante o login, incluindo credenciais do usuário, como nome de usuário e senha.

Um usuário mal-intencionado pode criar um script para ouvir as solicitações do usuário e registrar essas solicitações na instância. A tabela `sys_installation_exit` em uma instância define as regras de processamento das atividades de login e logout de todos os usuários nessa instância.

Configurar o playbook de detecção de credenciais

Use as etapas a seguir para configurar o playbook de detecção de credenciais.

Antes de Iniciar
Função necessária:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_si.admin
- flow_designer

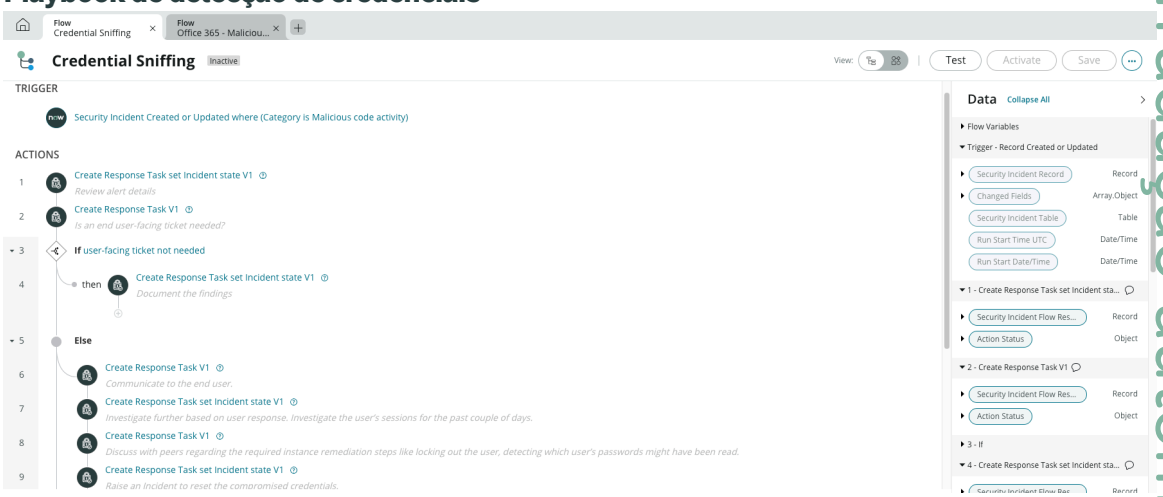
Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o playbook **de Farefação de credencial**.
3. Crie uma cópia do fluxo do playbook de detecção de credenciais e faça as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

Playbook de detecção de credenciais



4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. **Condição do gatilho** para o playbook: este playbook é acionado e associado ao incidente de segurança quando a **Categoria** é **Atividade de código malicioso**.

Condição do gatilho do Playbook de detecção de credenciais

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usar o playbook de detecção de credenciais

Use este playbook para investigar um incidente envolvendo atividades de detecção de credenciais realizadas por meio da tabela *sys_installation_exit* em uma instância da ServiceNow. As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook de detecção de credenciais.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Procedimento

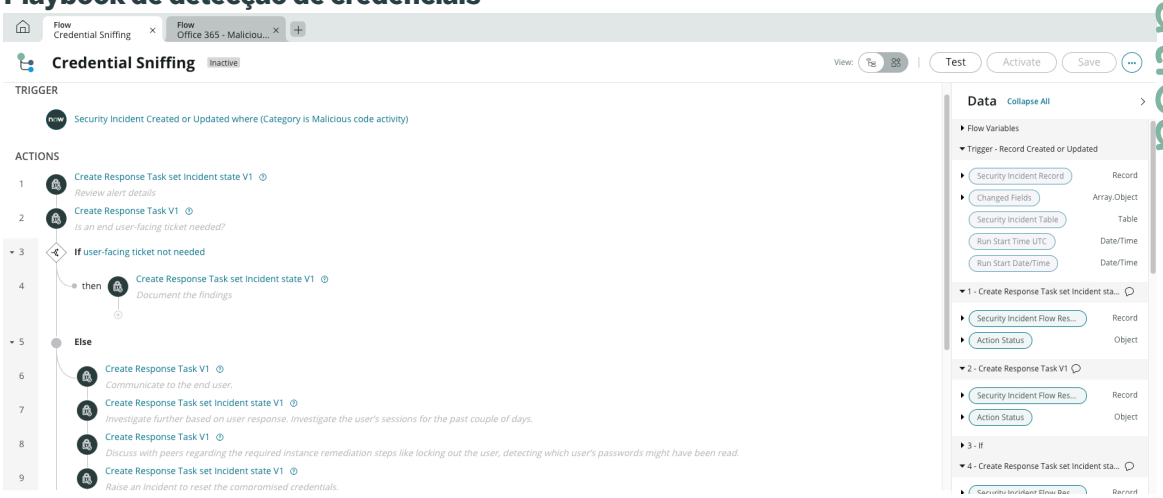
1. Quando o playbook for acionado e começar a ser executado, na Ação 1, revise os detalhes do alerta a seguir.
   - Instância
   - ID da sessão
   - ID de Transação
   - _raw: fornece o script inteiro.

   Script de exemplo:

   ```
   Var pass= request.getParameter("user_password");
   Gs.log(pass);
   ```

2. Na Ação 2, com base nos dados coletados até o momento, verifique se um tíquete de usuário final é necessário para este alerta ou não.
3. Na Ação 3, se o alerta não exigir um tíquete de usuário final, na Ação 4, documente as descobertas até o momento.
   O fluxo termina.

Playbook de detecção de credenciais



4. Na Ação 5, se o alerta exigir um tíquete de usuário final, execute as seguintes etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na Ação 6, informe ao usuário final que o alerta requer um tíquete de usuário final.

b. Na Ação 7, investigue mais com base na resposta do usuário e nas sessões do usuário durante os últimos dias.

c. Na Ação 8, discuta com colegas sobre as etapas de correção da instância, como bloquear o usuário e detectar quais senhas de usuário podem ter sido lidas.

d. Na Ação 9, gere um incidente ou tíquete para redefinir as credenciais de usuário comprometidas.

e. Na Ação 10, suspenda a contenção e retorne os sistemas aos padrões operacionais
O fluxo termina.

5. Na Ação 11, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook for T1070 - Logs de eventos do Windows limpos

Este playbook fornece etapas de correção para investigar incidentes que rastreiam tipos de evento em que o usuário remove logs de segurança. Sempre que o log de segurança é limpo, os eventos 517 e 1102 são registrados, independentemente do status da política de evento do sistema de auditoria.

Este alerta pode rastrear os seguintes tipos de eventos:

- **Evento 517**: os campos Nome de usuário primário e Nome de usuário do cliente identificam o usuário que limpou o log. O nome de usuário primário corresponde ao sistema e o nome de usuário do cliente indica o usuário que limpou o log.
- **Evento 1102**: os campos Nome da conta e Nome do domínio identificam o usuário que limpou o log. O ID de logon permite que você correlacione para trás o evento de logon e outros eventos registrados durante a mesma sessão de logon.

Configurar o playbook T1070 - Logs de eventos do Windows limpos

Use as etapas a seguir para configurar o playbook T1070 - Logs de eventos do Windows limpos.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.

2. Navegar até **Todos** > **Flow Designer** e selecione o **playbook T1070 - Logs de eventos do Windows limpos**.

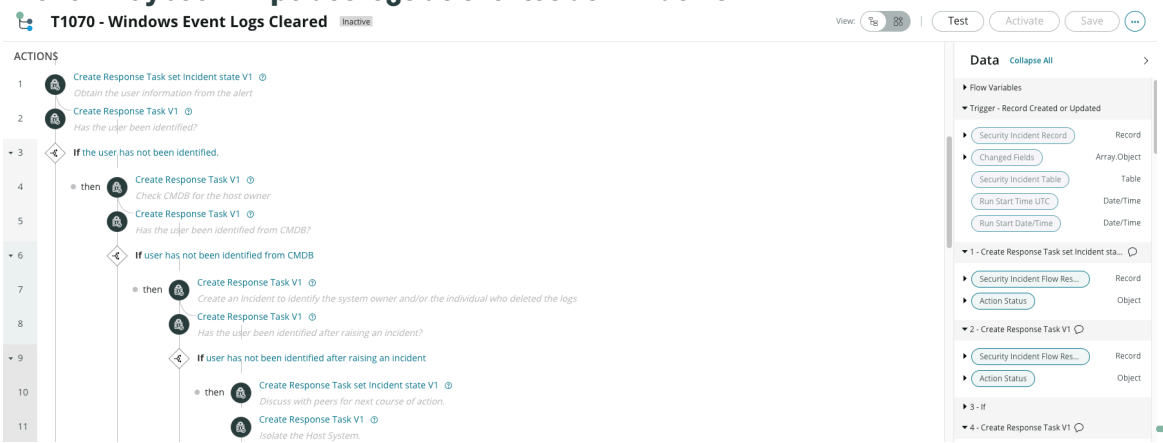
3. Crie uma cópia do fluxo do playbook T1070 - Logs de eventos do Windows limpos e faça as modificações necessárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

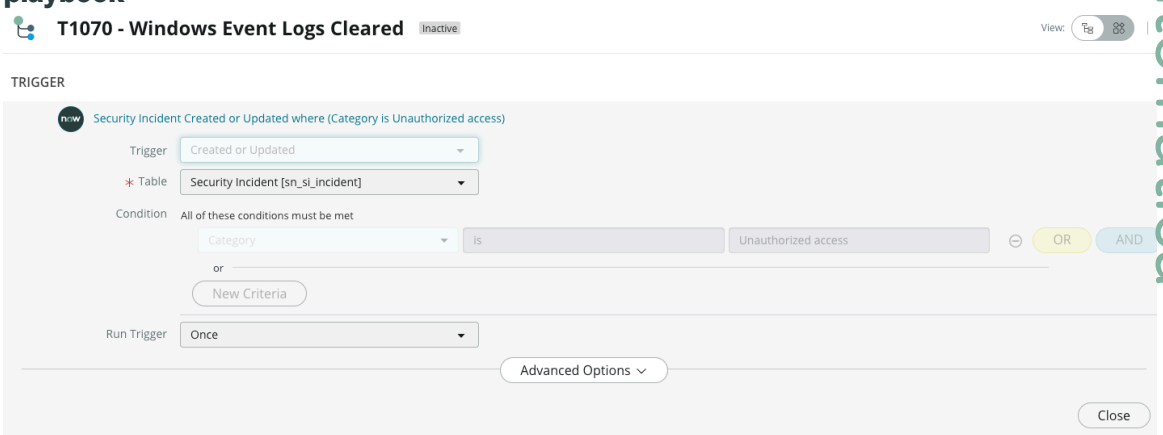
Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

T1070 - Playbook limpo dos logs de eventos do Windows



4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. **Condição do gatilho** para o playbook: este playbook é acionado e associado ao incidente de segurança quando a **Categoria** é **Acesso não autorizado**.

T1070 - Logs de eventos do Windows limpos da condição do gatilho do playbook



Use o playbook T1070 - Logs de eventos do Windows limpos

Use este playbook para investigar incidentes que rastreiam tipos de evento em que o usuário remove logs de segurança. As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook T1070 - Logs de eventos do Windows limpos.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

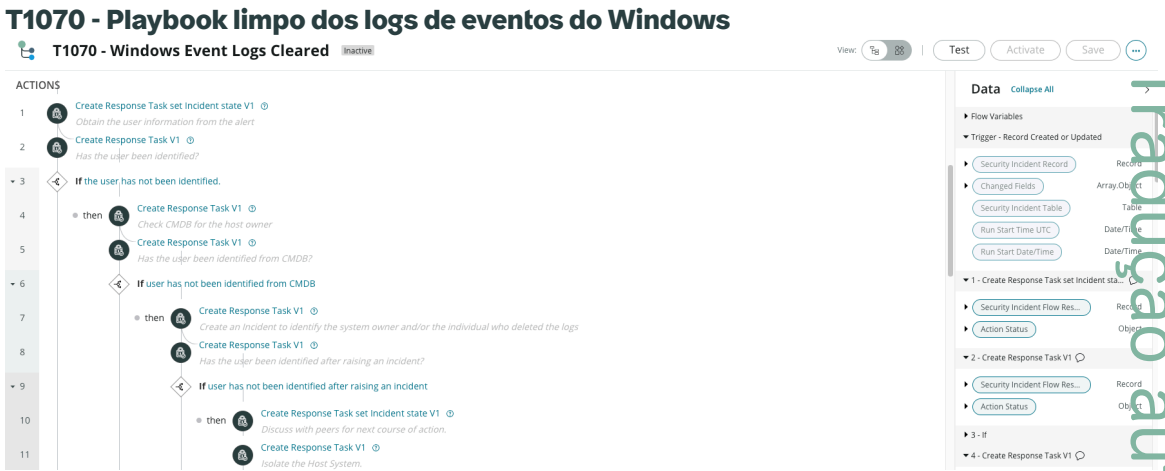
Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, obtenha os detalhes do usuário do alerta.
2. Na Ação 2, verifique se o usuário foi identificado ou não.
3. Na Ação 3, se o usuário não tiver sido identificado, execute as seguintes etapas:

   a. Na Ação 4, verifique o CMDB (Configuration Management Database) para obter os detalhes do proprietário do host.

   b. Na Ação 5, verifique se o usuário foi identificado no CMDB ou não.

      Se o usuário tiver sido identificado no CMDB, uma tarefa de resposta manual será criada na Ação 5 e o fluxo será encerrado.



   c. Na Ação 6, se o usuário não tiver sido identificado no CMDB, execute as seguintes etapas:

      i. Na Ação 7, crie um incidente para identificar o proprietário do sistema e o indivíduo que excluiu os logs.

      ii. Na Ação 8, verifique se o usuário foi identificado após gerar um incidente ou não.

      Se o usuário tiver sido identificado após gerar um incidente, uma tarefa de resposta manual será criada na Ação 8 e o fluxo será encerrado.

      iii. Na Ação 9, se o usuário não tiver sido identificado após gerar um incidente, execute as seguintes etapas:

         1. Na Ação 10, discuta o próximo curso de ação com colegas.
         2. Na Ação 11, isole o sistema host.
         3. Na Ação 12, remova todos os arquivos indesejados que possam ter sido criados e exclua as contas não autorizadas.
         4. Na Ação 13, suspenda a contenção e traga os sistemas de volta aos padrões operacionais.
         5. Na Ação 14, conclua a revisão pós-incidente antes de fechar a tarefa.

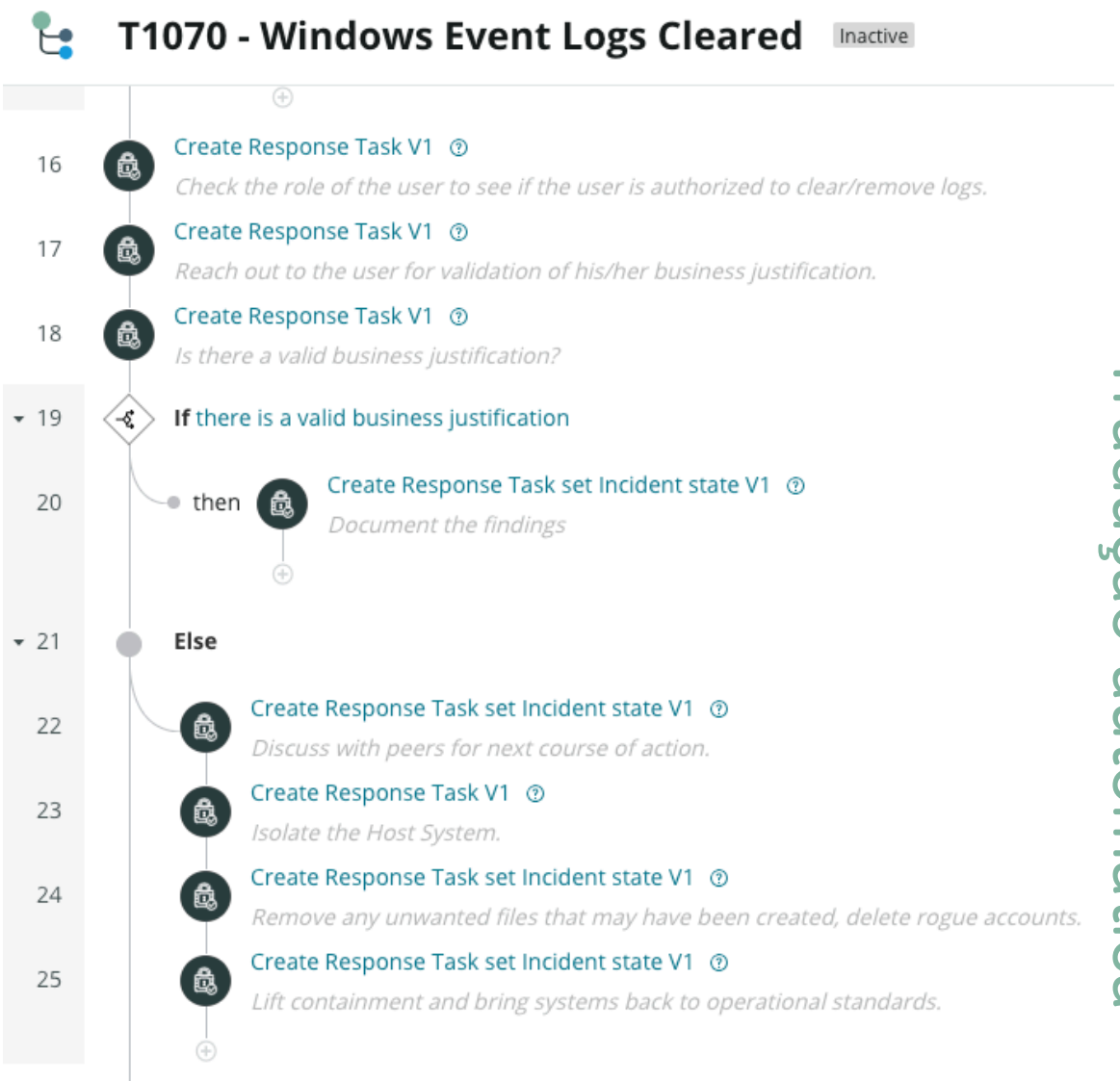
         Na Ação 15, o fluxo termina.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Na Ação 16, se o usuário tiver sido identificado, verifique a função do usuário para ver se ele está autorizado a limpar ou remover logs.
5. Na Ação 17, entre em contato com o usuário para validação de sua justificativa comercial.
   Você pode usar o modelo de e-mail fornecido para entrar em contato com o usuário.

Usando o playbook T1070 - Logs de eventos do Windows limpos



6. Na Ação 18, verifique se uma justificativa de negócios válida foi fornecida ou não.
7. Na Ação 19, se houver uma justificativa de negócios válida fornecida, na Ação 20, documente as descobertas até o momento.
   O fluxo termina.
8. Na Ação 21, se nenhuma justificativa de negócios válida for fornecida, execute as seguintes etapas:
   a. Na Ação 22, discuta o próximo curso de ação com colegas.
   b. Na Ação 23, isole o sistema host.
   c. Na Ação 24, remova todos os arquivos indesejados que possam ter sido criados e exclua as contas não autorizadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Na Ação 25, suspenda a contenção e traga os sistemas de volta aos padrões operacionais.
O fluxo termina.

9. Na Ação 26, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para consulta do SO de endereço externo no arquivo /etc/hosts

Este playbook fornece etapas de correção sistemática para investigar incidentes que indicam que um nome de host interno ou domínio foi atribuído a um endereço IP externo no DNS local (/etc/hosts) de um servidor Linux.

Configure o OSquery do endereço externo no playbook do arquivo /etc/hosts

Use as etapas a seguir para configurar o OSquery do endereço externo no playbook do arquivo /etc/hosts.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

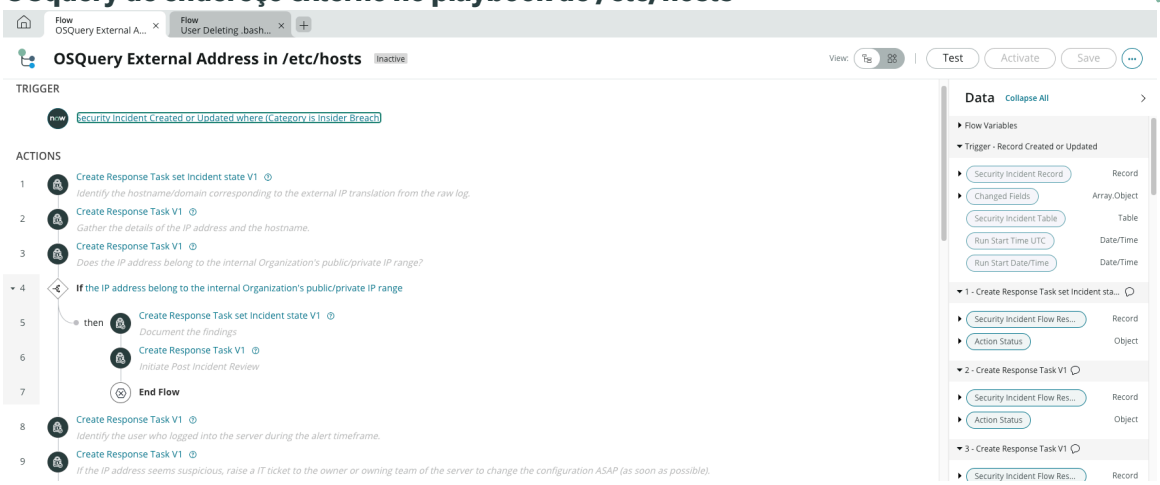
1. Faça login como um usuário com as funções sn_si.user e flow_designer.

2. Navegar até **Todos** > **Flow Designer** e selecione o **endereço externo do OSquery no playbook de /etc/hosts**.

3. Crie uma cópia do endereço externo do OSquery no fluxo do playbook /etc/hosts e faça as modificações necessárias.

Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

OSquery de endereço externo no playbook de /etc/hosts



4. Ative os playbooks.

Tradução automática

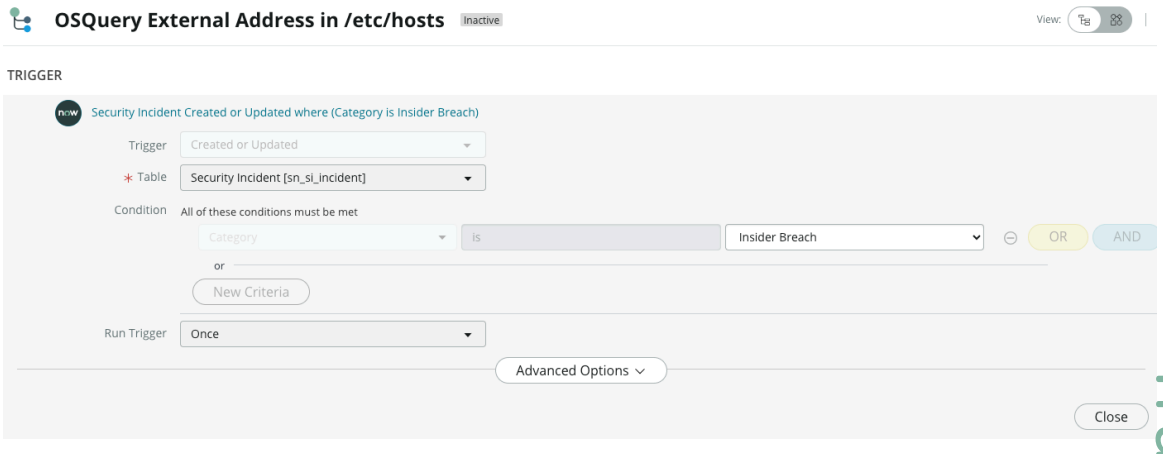
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Ative o fluxo principal para usar o playbook disponível no sistema de base.

b. Ative os fluxos copiados depois de fazer as mudanças necessárias.

5. **Condição do gatilho** para o playbook: este playbook é acionado e associado ao incidente de segurança quando a **Categoria** é **Violação**interna.

OSquery do endereço externo na condição do gatilho do playbook /etc/hosts



Use o OSquery do endereço externo no playbook do arquivo /etc/hosts

Use este playbook para investigar incidentes que indicam que um nome de host ou domínio interno foi atribuído a um endereço IP externo no DNS local (/etc/hosts) de um servidor Linux. As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no OSquery do endereço externo no playbook do arquivo /etc/hosts.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

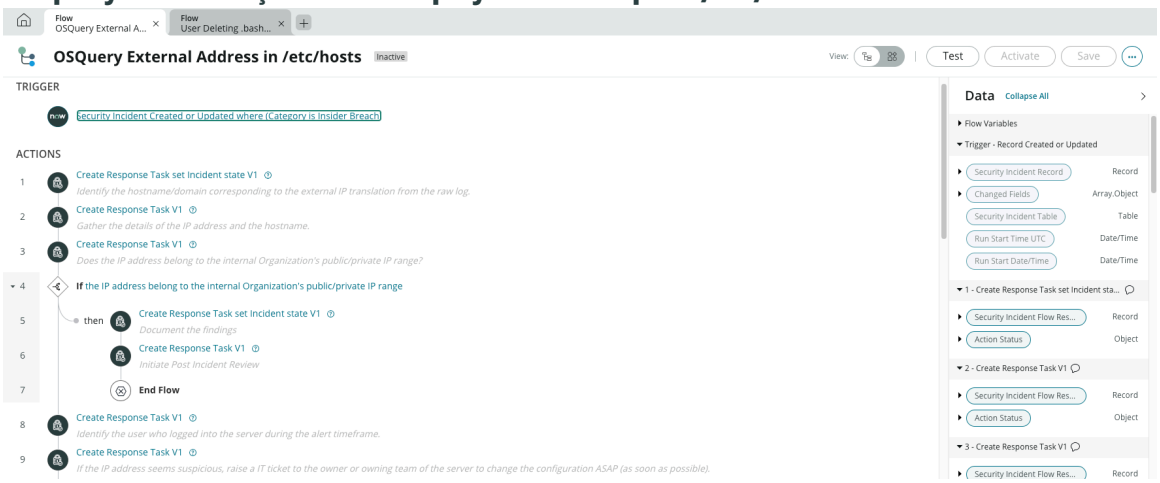
Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, identifique o nome do host ou do domínio correspondente à tradução do IP externo do log bruto.
2. Na Ação 2, reúna os detalhes do endereço IP e o nome do host.
3. Na Ação 3, verifique se este endereço IP pertence ao intervalo IP público/privado da organização interna ou não.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

OSquery do endereço externo no playbook do arquivo /etc/hosts



4. Na Ação 4, se o endereço IP pertencer ao intervalo IP público/privado da organização interna, execute as seguintes etapas:

   a. Na Ação 5, documente as descobertas até o momento.

   b. Na Ação 6, inicie uma análise pós-incidente.
   Na Ação 7, após a revisão pós-incidente, o fluxo termina.

5. Se o endereço IP não pertencer ao intervalo IP público/privado da organização interna, na Ação 8, identifique o usuário que fez login no servidor durante o intervalo de tempo do alerta.
6. Na Ação 9, se o endereço IP parecer suspeito, gere um tíquete de TI para o proprietário ou a equipe do servidor para mudar a configuração o mais rápido possível.
7. Na Ação 10, verifique se houve alguma atividade mal-intencionada no servidor antes e depois de adicionar a entrada DNS.
8. Na Ação 11, verifique se há conexões com o endereço IP externo do servidor.
9. Na Ação 12, documente as descobertas até o momento.
10. Na Ação 13, verifique se as informações do proprietário ou da equipe estão disponíveis ou não.
11. Na Ação 14, se as informações do proprietário ou da equipe estiverem disponíveis, execute as seguintes etapas:

    a. Na Ação 15, entre em contato com o proprietário ou a equipe do servidor para ver se eles reconhecem a atividade.
    Você pode usar o modelo de e-mail fornecido para entrar em contato com o proprietário ou a equipe do servidor.

    b. Na Ação 16, verifique se o proprietário ou a equipe forneceu uma justificativa comercial válida ou não.

    c. Na Ação 17, se o proprietário ou a equipe fornecida não fornecer uma justificativa comercial válida, o fluxo será encerrado.
    Mas, se o proprietário ou a equipe forneceu uma justificativa comercial válida, execute as seguintes etapas:

Tradução automática

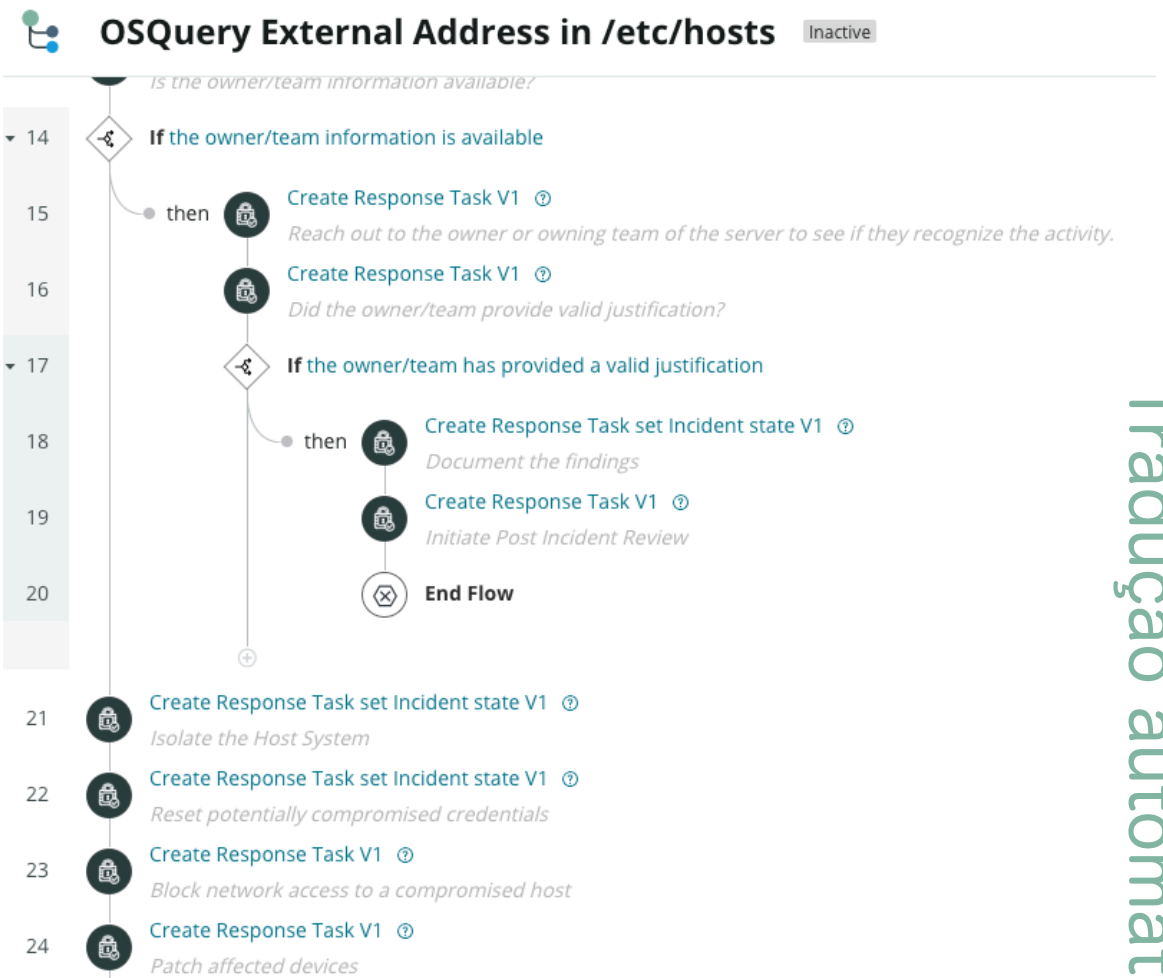
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

i. Na Ação 18, documente as descobertas até o momento.

ii. Na Ação 19, inicie uma revisão pós-incidente.

Na Ação 20, após a revisão pós-incidente, o fluxo termina.

Usando o OSquery do endereço externo no playbook do arquivo /etc/hosts



12. Na Ação 21, se as informações do proprietário ou da equipe não estiverem disponíveis, isole o sistema host.
13. Na Ação 22, redefina as credenciais potencialmente comprometidas.
14. Na Ação 23, bloqueie o acesso à rede do host comprometido.
15. Na Ação 24, corrija os dispositivos afetados.
16. Na Ação 25, suspenda a contenção e traga os sistemas de volta aos padrões operacionais.
17. Na Ação 26, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para usuário que está excluindo histórico de bash - Nuvem

Este playbook fornece etapas de correção sistemática para investigar incidentes que indicam se alguém estava tentando remover o arquivo de histórico do bash (`.bash_history`) de um servidor Linux.

Nota:
Você precisa atenuar este alerta com cuidado, pois ele raramente é acionado e pode indicar uma ameaça interna.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar o playbook de histórico de bash de exclusão de usuário

Use as etapas a seguir para configurar o playbook de histórico de bash de exclusão de usuário.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

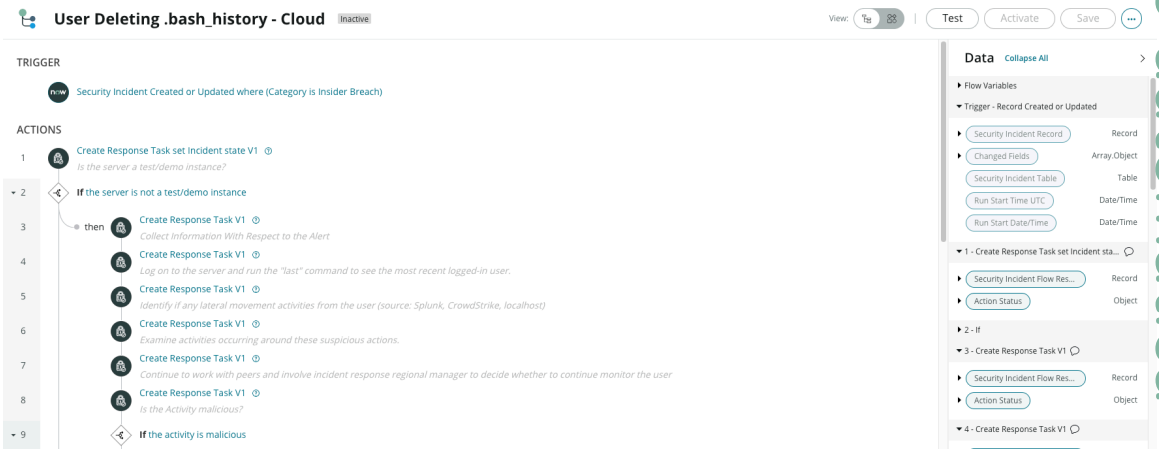
Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o playbook **User Excluting .bash_history - Cloud**.
3. Crie uma cópia do fluxo do Playbook de exclusão de usuário .bash_history - Nuvem e faça as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

   Histórico de exclusão de usuário do Bash - Playbook de nuvem

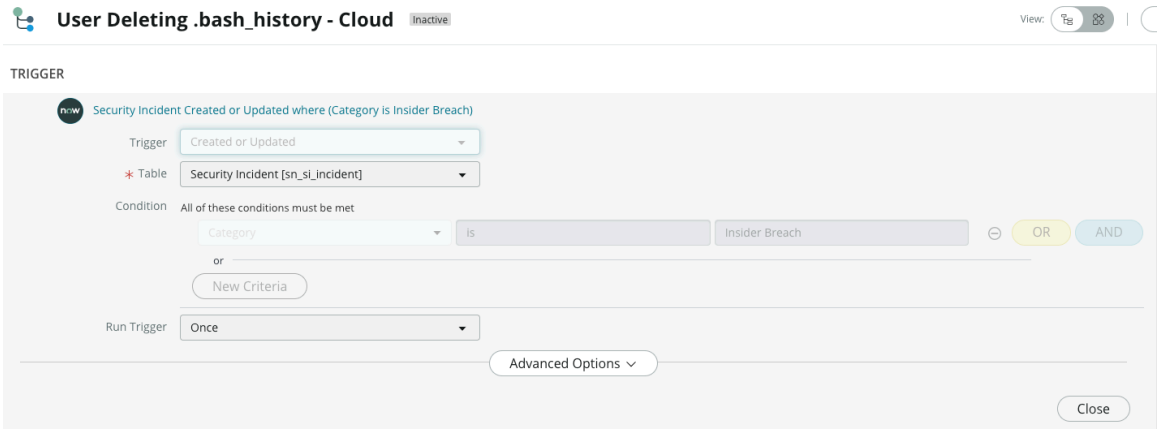
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. **Condição do gatilho** para o playbook: este playbook é acionado e associado ao incidente de segurança quando a **Categoria** é **Violação**interna.

Usuário excluindo histórico de bash - Condição do gatilho do playbook em nuvem



Use o playbook de histórico de bash de exclusão de usuário

use este playbook para investigar incidentes que indicam se alguém estava tentando remover o arquivo de histórico do bash de um servidor Linux. As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook do usuário que exclui o histórico do Bash (`.bash_history`).

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, verifique se o servidor é uma instância de teste ou de demonstração.
2. Na Ação 2, se o servidor não for uma instância de teste ou de demonstração, execute as seguintes etapas:

   a. Na Ação 3, colete as seguintes informações para o alerta:
      - Nome do usuário
      - Endereço IP
      - Comandos maliciosos que tentam excluir o histórico do bash
      - Todos os comandos executados pelo usuário, se disponíveis nos logs do CrowdStrike.

   b. Na Ação 4, faça login no servidor e execute o `último` comando para exibir o usuário conectado mais recentemente.

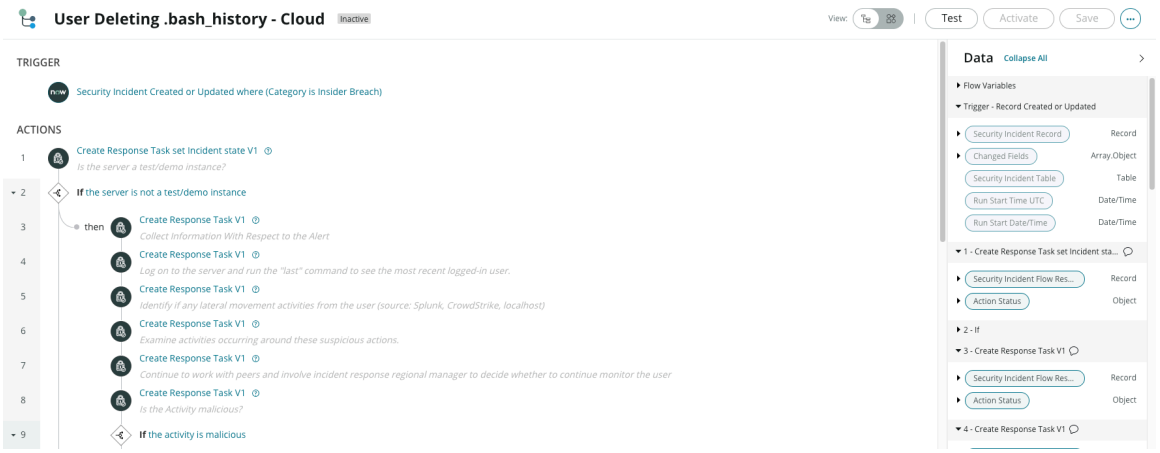
   c. Na Ação 5, identifique se houve alguma atividade de movimento lateral do usuário (Origem: Splunk, CrowdStrike, localhost).

   d. Na Ação 6, examine as atividades que ocorrem em torno dessas ações suspeitas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook de histórico de bash para exclusão de usuário



e. Na Ação 7, continue trabalhando com colegas e envolva o gerente regional de resposta do incidente para decidir se deve continuar monitorando o usuário.

f. Na Ação 8, determine se a atividade é mal-intencionada ou não.

g. Na Ação 9, se a atividade for mal-intencionada, execute as seguintes etapas:

i. Na Ação 10, durante a investigação, entre em contato com o Suporte de TI e solicite um congelamento de conta.

ii. Na Ação 11, certifique-se de que a instância seja restaurada para um estado normal livre de atividades mal-intencionadas.

iii. Na Ação 12, suspenda a contenção e traga os sistemas de volta aos padrões operacionais.

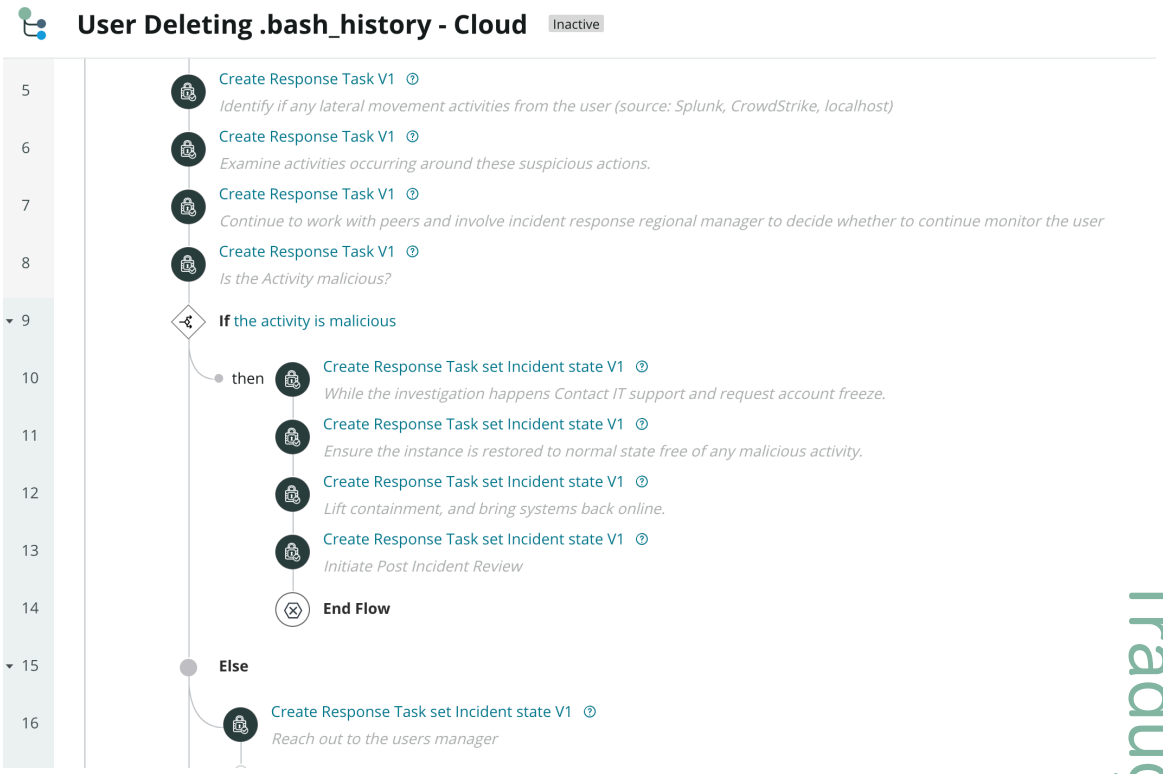
iv. Na Ação 13, inicie uma revisão pós-incidente.

Na Ação 14, após a revisão pós-incidente, o fluxo termina.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando o playbook de histórico de bash de exclusão de usuário



h. Na Ação 15, se a atividade não for mal-intencionada, na Ação 16, entre em contato com o gerente do usuário.
Você pode usar o modelo de e-mail fornecido para entrar em contato com o gerente do usuário e informá-lo sobre a abordagem recomendada.

3. Na Ação 17, documente as descobertas até o momento.

4. Na Ação 18, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para tentativas bem-sucedidas de VPN das contas de serviço - Corp/Cloud

Este playbook forneceu etapas de correção sistemática para investigar incidentes que rastreiam tentativas de login bem-sucedidas de contas de serviço por meio de VPN. As contas de serviço não devem ter eventos de login de uma VPN, e esses eventos podem ser indicadores de força bruta ou possível exposição das credenciais da conta.

Configurar as tentativas de VPN bem-sucedidas no playbook de contas de serviço

Use as etapas a seguir para configurar as tentativas de VPN bem-sucedidas no playbook de contas de serviço.

Antes de Iniciar
Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Tradução automática

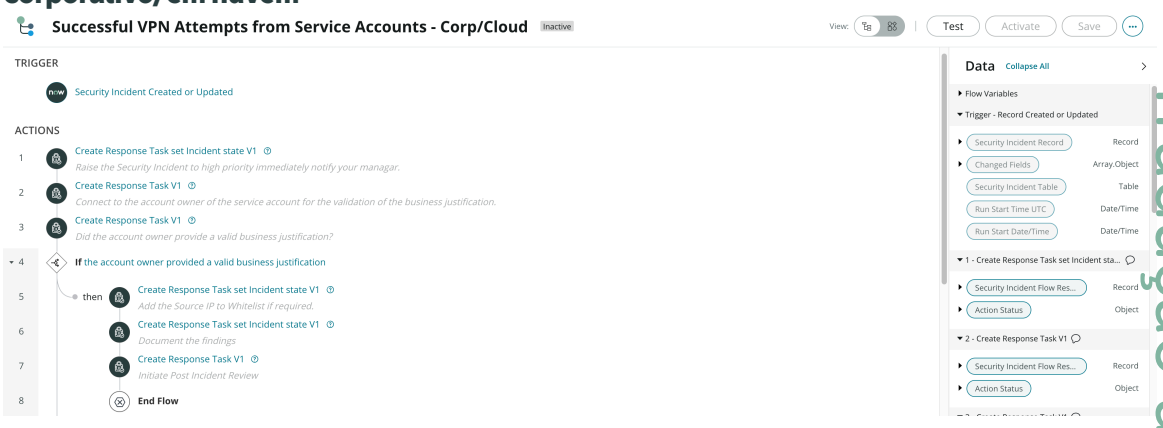
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione **Tentativas de VPN bem-sucedidas no playbook de Contas de serviço**.
3. Crie uma cópia do fluxo de tentativas de VPN bem-sucedidas do playbook de contas de serviço e faça as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

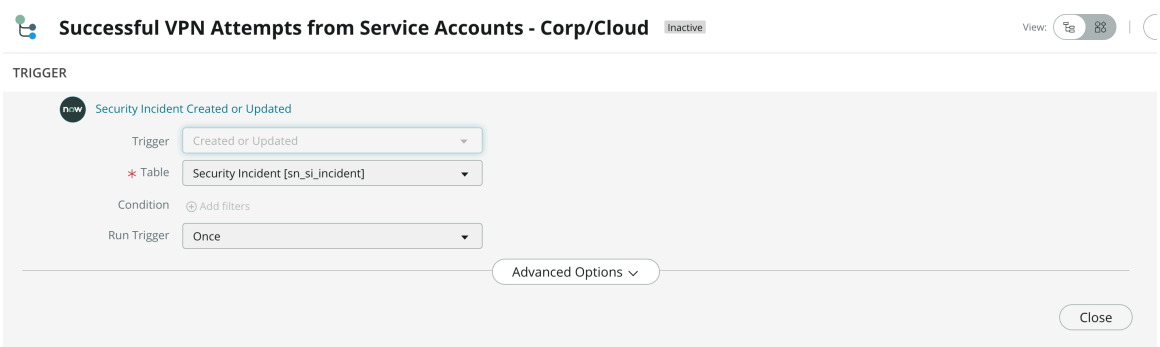
   Tentativas de VPN bem-sucedidas das Contas de serviço - Playbook corporativo/em nuvem

4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. **Condição do gatilho** para o playbook: este playbook é acionado e associado ao incidente de segurança quando ele é criado ou atualizado com base nas condições necessárias.

   Por exemplo, quando **Categoria** for **Violação interna**.

   Tentativas de VPN bem-sucedidas das contas de serviço - Playbook de empresa/nuvem

Usar tentativas de VPN bem-sucedidas do playbook de contas de serviço

Use este playbook para investigar incidentes que rastreiam tentativas de login bem-sucedidas de contas de serviço por meio de VPN. As etapas a seguir fornecem instruções

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

sobre as ações, tarefas e subfluxos que estão disponíveis no playbook Tentativas de VPN bem-sucedidas do Service Accounts.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, eleve o incidente de segurança para alta prioridade e notifique imediatamente seu gerente.
2. Na Ação 2, entre em contato com o proprietário da conta de serviço para validar a justificativa comercial. Você pode usar o modelo de e-mail fornecido para entrar em contato com o proprietário da conta de serviço para validar a justificativa comercial.
3. Na ação 3, verifique se o proprietário da conta de serviço forneceu uma justificativa comercial válida.

4. Na Ação 4, se o proprietário da conta de serviço forneceu uma justificativa comercial válida, execute as seguintes etapas:

   a. Na Ação 5, adicione o IP de origem à lista de permissões, se necessário.

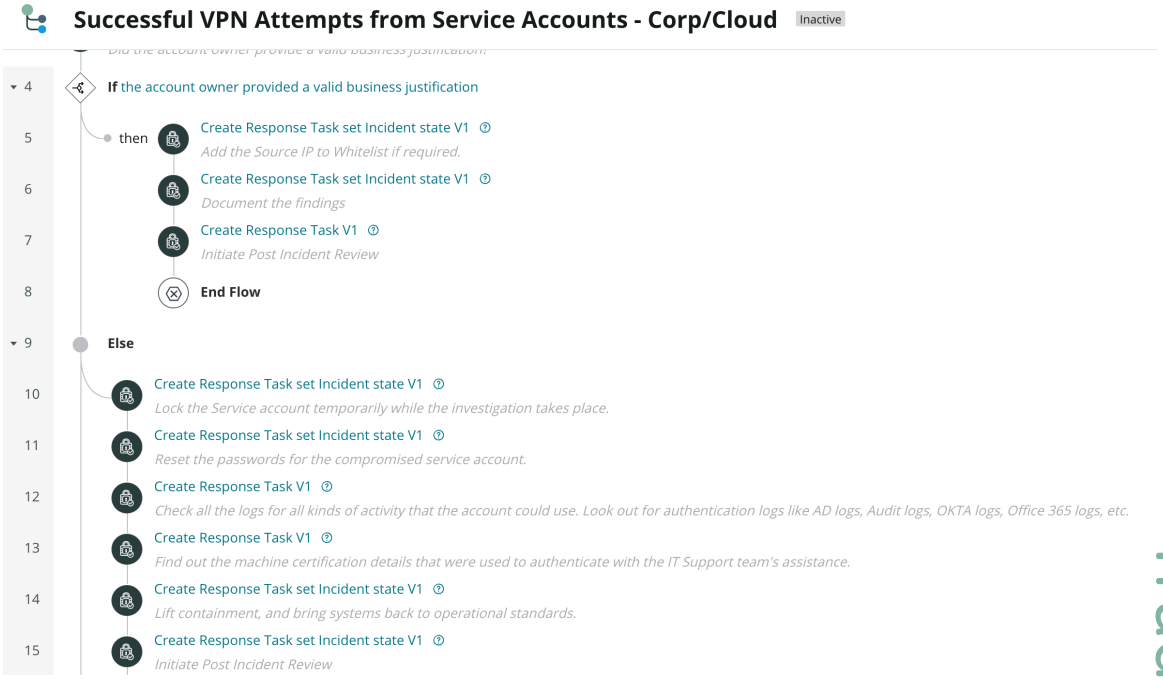
   b. Na Ação 6, documente as descobertas até o momento.

   c. Na Ação 7, inicie uma revisão pós-incidente.
   Na Ação 8, após a revisão pós-incidente, o fluxo termina.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como usar as tentativas de VPN bem-sucedidas do playbook Contas de serviço - Corp/Cloud



5. Na Ação 9, se o proprietário da conta de serviço não forneceu uma justificativa comercial válida, execute as seguintes etapas:

a. Na Ação 10, bloqueie temporariamente a conta de serviço enquanto a investigação ocorre.

b. Na Ação 11, redefina as senhas da conta de serviço comprometida.

c. Na Ação 12, verifique os logs para todos os tipos de atividade que a conta pode usar.
Procure logs de autenticação, como logs do Active Directory, logs de auditoria, logs do Okta, logs do Office 365 e assim por diante.

d. Na Ação 13, encontre os detalhes de certificação da máquina usados para autenticar com a assistência da equipe de suporte de TI.

e. Na Ação 14, suspenda a contenção e traga os sistemas de volta aos padrões operacionais.

f. Na Ação 15, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para tentativa de acesso a contas desativadas

Este playbook é acionado quando um funcionário cuja conta foi encerrada, desabilitada ou separada tenta fazer login com suas credenciais. O estado de identidade do usuário no ponto de navegação geralmente é atualizado para desabilitado na data de término.

30 dias é o tempo ideal a partir da data de rescisão para que ele seja atualizado para um estado separado. Você pode usar a lógica de negócios no ponto de navegação para excluir as contas RSA e remover as associações de grupo do Active Directory (AD) após 30 dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar o playbook de conta desativada de tentativa de acesso

Use as etapas a seguir para configurar o playbook de conta desativada de tentativa de acesso.

Antes de Iniciar

Função necessária:

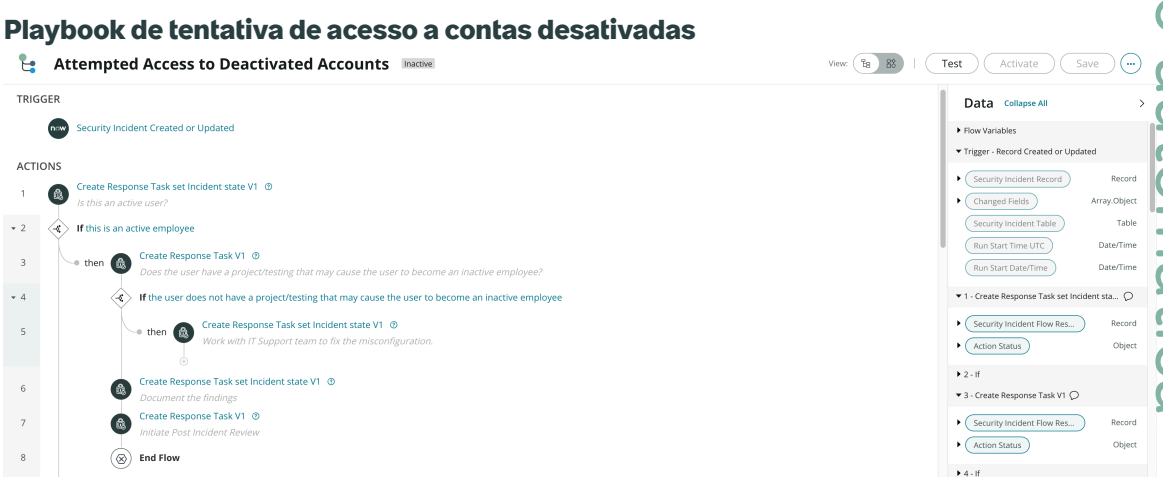
- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o playbook **de conta desativada de tentativa de acesso**.
3. Crie uma cópia do fluxo do playbook de Conta Desativada de Tentativa de Acesso e faça as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.



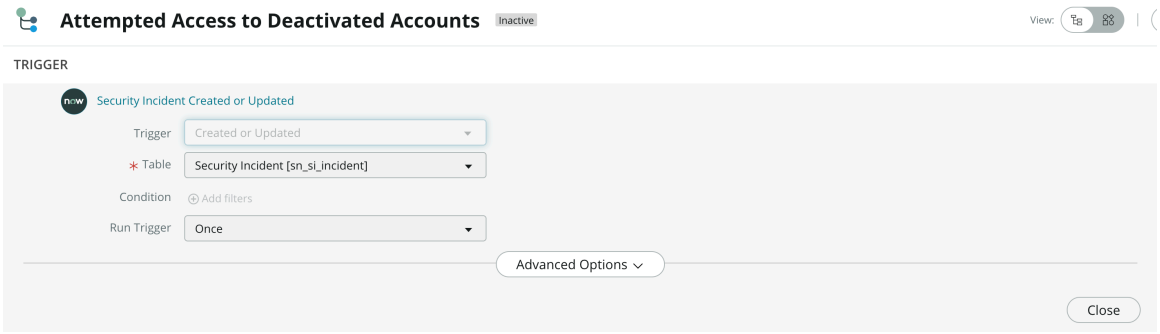
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. **Condição do gatilho**: este playbook é acionado quando o incidente de segurança é criado ou atualizado com base nas condições necessárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, quando **Categoria** for **Violação interna**

Condição do gatilho do playbook de tentativa de acesso a contas desativadas



Usar o playbook de Tentativa de acesso a contas desativadas

Use este playbook quando um funcionário cuja conta foi encerrada, desabilitada ou separada tentar fazer login com suas credenciais. As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook Tentativa de acesso a contas desativadas.

Antes de Iniciar

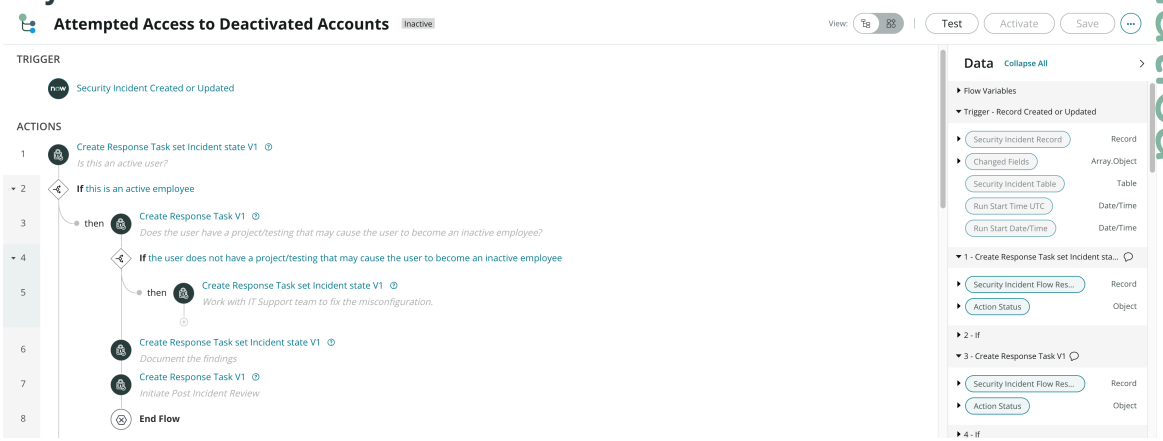
Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, verifique se a tentativa de acesso às contas desativadas foi feita por um usuário ativo.
2. Na Ação 2, verifique se a tentativa de acesso às contas desativadas foi feita por um funcionário ativo.

Playbook de tentativa de acesso a contas desativadas



3. Se a tentativa de acesso às contas desativadas foi feita por um funcionário ativo, execute as seguintes etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na Ação 3, verifique se o usuário tinha um projeto ou caso de teste que fez com que o usuário se tornasse um funcionário inativo.

b. Na Ação 4, se o usuário não tiver um projeto ou caso de teste que fez com que o usuário se tornasse um funcionário inativo, trabalhe com a equipe de suporte de TI para corrigir o erro de configuração.
O fluxo termina.

c. Na Ação 5, se o usuário tiver um projeto ou caso de teste que fez com que o usuário se tornasse um funcionário inativo, execute as seguintes etapas:

i. Na Ação 6, documente as descobertas até o momento.

ii. Na Ação 7, inicie uma revisão pós-incidente.

Na Ação 8, após a revisão pós-incidente, o fluxo termina.

4. Na Ação 9, se a tentativa de acesso à conta desativada não tiver sido feita por um funcionário ativo, execute as seguintes etapas:

a. Na Ação 10, verifique se o usuário fez logins bem-sucedidos.

b. Na Ação 11, verifique quando o funcionário foi desligado.

c. Na Ação 12, investigue os eventos no Splunk para examinar as atividades do usuário durante o período.

d. Na Ação 13, com base na investigação até o momento, determine se o usuário exfiltrou algum dado.

e. Na Ação 14, se o usuário não exfiltrar nenhum dado, execute as seguintes etapas:

i. Na Ação 15, trabalhe com a equipe de suporte de TI para encerrar todas as sessões ativas e desabilitar as contas.

ii. Na Ação 16, documente as descobertas até o momento.

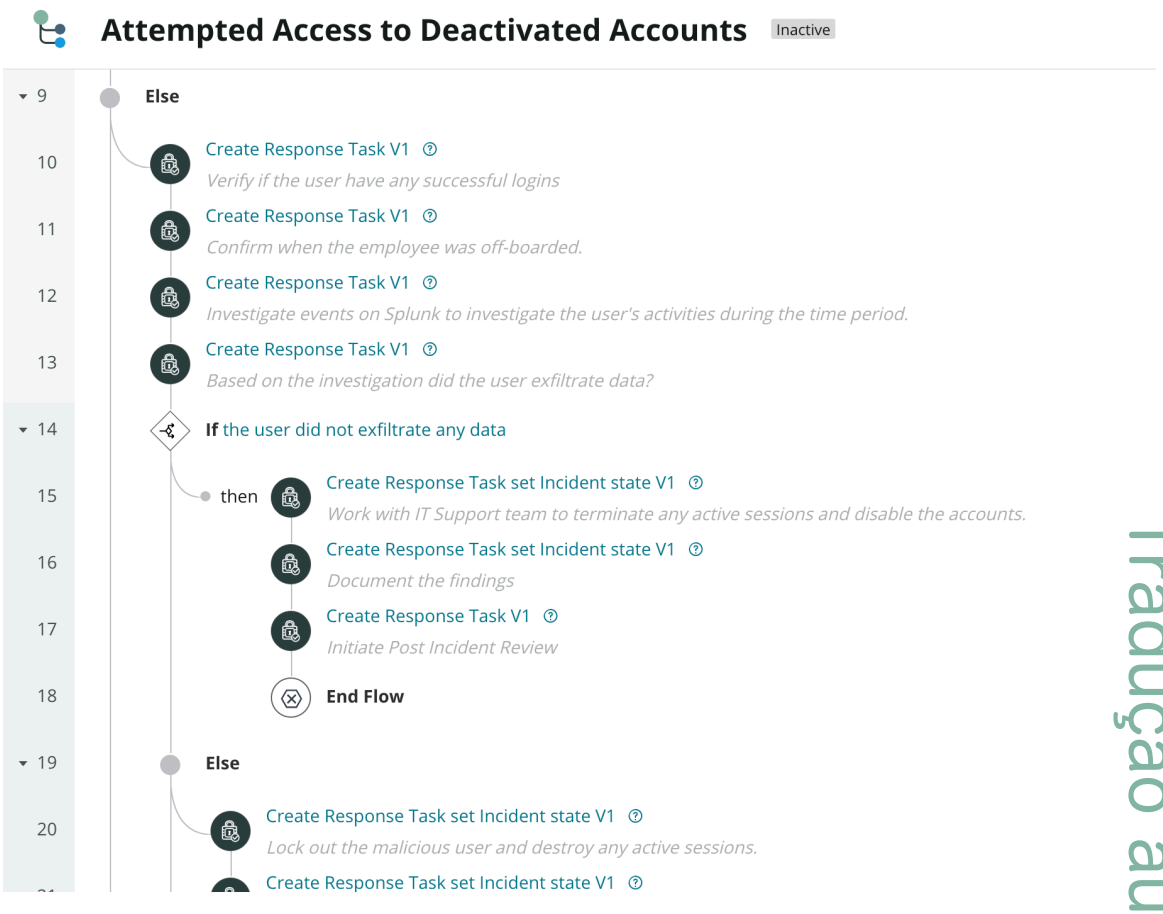
iii. Na Ação 17, inicie uma revisão pós-incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na Ação 18, após a revisão pós-incidente, o fluxo termina.

Como usar o playbook de Tentativa de acesso a contas desativadas



5. Na Ação 19, se o usuário exfiltrar algum dado, execute as seguintes etapas:

a. Na Ação 20, bloqueie o usuário mal-intencionado e destrua todas as sessões ativas.

b. Na Ação 21, trabalhe com a equipe de suporte de TI para desabilitar todas as contas.

c. Na Ação 22, certifique-se de que os recursos sejam restaurados ao estado normal e livres de qualquer atividade mal-intencionada.
Você pode recriar a imagem dos recursos, se necessário.

d. Na Ação 23, suspenda a contenção e traga os sistemas de volta aos padrões operacionais.

e. Na Ação 24, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook for T1003 - Evasão de defesa - Mimakatz DCSombra

Este playbook fornece etapas de correção sistemática para investigar incidentes suspeitos de serem causados pelo Mimkatz DCShendow. DCSombra é um recurso do Mimakatz que simula o comportamento de um controlador de domínio (um servidor que controla o Active Directory) para injetar seus próprios dados, ignorando a maioria dos controles de segurança padrão (incluindo SIEMs).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O MIMIKATZ DC SHADOW ajuda o invasor a estabelecer um controlador de domínio (DC) desonesto que se torna parte do Active Directory (AD). Depois de registrado, ele pode atuar como um DC legítimo e causar danos.

Configurar o playbook T1003 - Evasão de defesa - Mimakatz DCSombra

Use as etapas a seguir para configurar o playbook T1003 - Defesa evasão - Mimakatz DCSombra.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

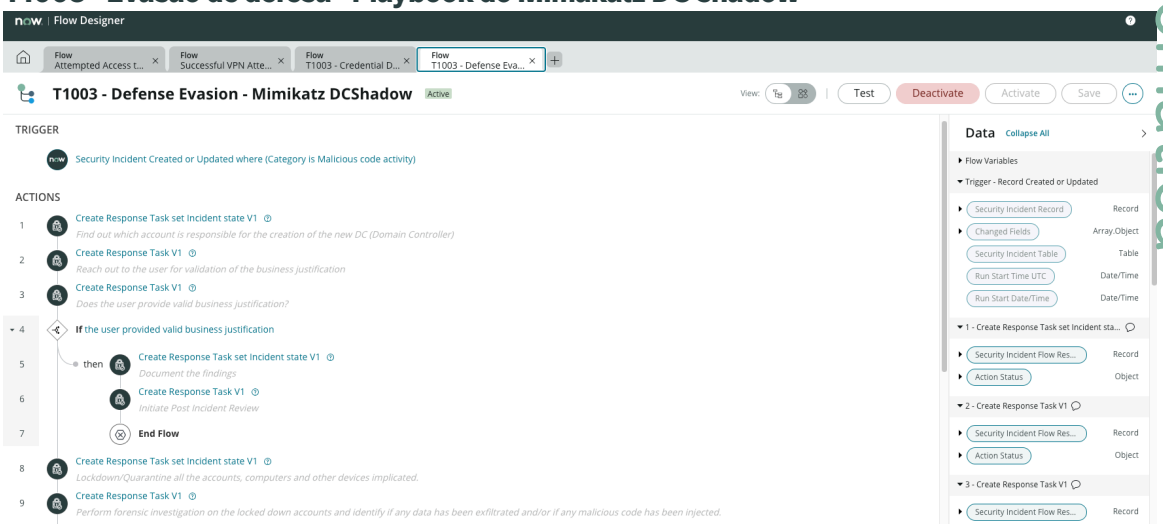
Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o **playbook T1003 - Evasão de defesa - Mimakatz DCSombra**.
3. Crie uma cópia do fluxo do playbook T1003 - Evasão de defesa - Mimkatz DCSombra e faça as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

   T1003 - Evasão de defesa - Playbook do Mimakatz DC shadow

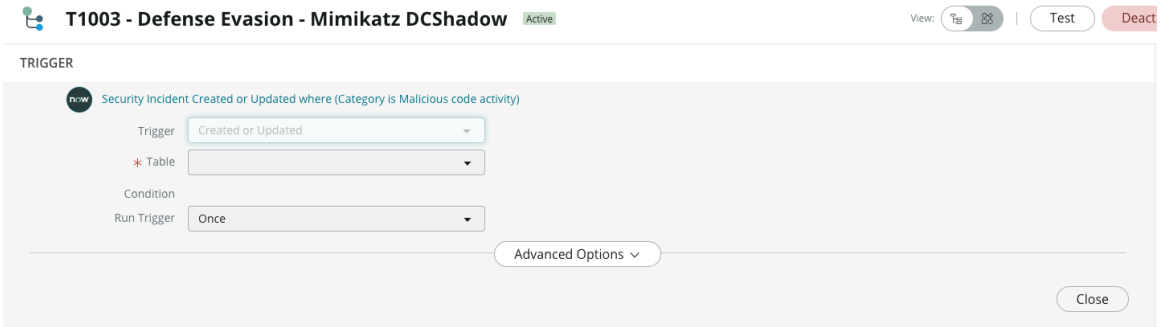
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. **Condição do gatilho** para o playbook: este playbook é acionado e associado ao incidente de segurança quando a **Categoria** é **Atividade de código malicioso**.

T1003 - Evasão de defesa - Condição do gatilho do playbook de Mimakatz DC Shadow



Use o playbook T1003 - Evasão de defesa - Mimakatz DCSombra

Use este playbook para investigar incidentes de segurança suspeitos de serem causados pelo Mimkatz DCShendow. As etapas a seguir fornecem um passo a passo das ações, tarefas e subfluxos que estão disponíveis no playbook T1003 - Defesa evasão - Mimkatz DCSombra.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, descubra qual conta é responsável pela criação do novo DC (Controlador de domínio).
2. Na Ação 2, entre em contato com o usuário para validar a justificativa de negócio.
   Você pode usar o modelo de e-mail fornecido para entrar em contato com o usuário.
3. Na Ação 3, verifique se o usuário forneceu uma justificativa comercial válida.
4. Na Ação 4, se o usuário forneceu uma justificativa comercial válida, execute as seguintes etapas:

T1003 - Evasão de defesa - Playbook do Mimakatz DC shadow

Tradução automática

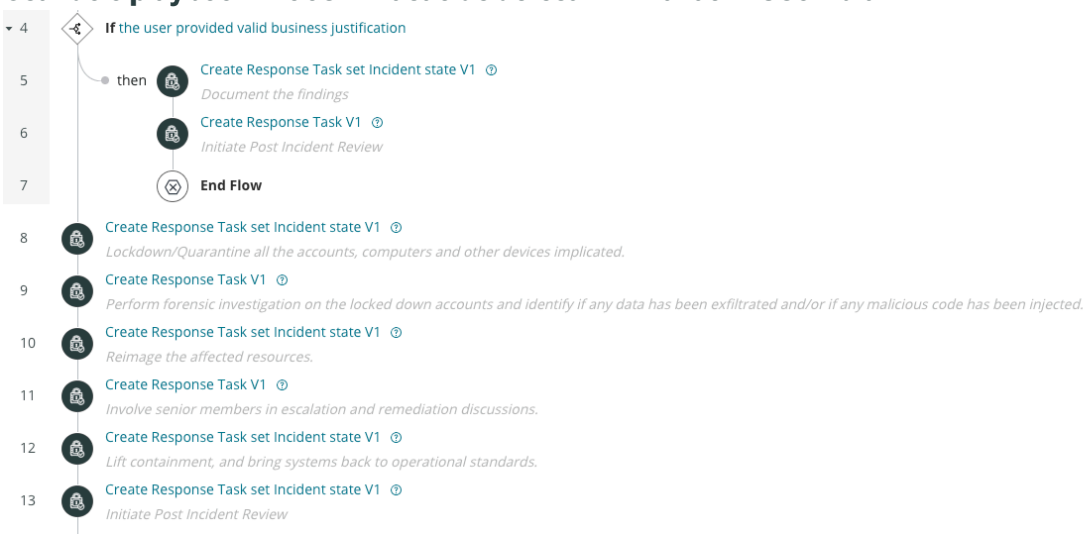
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na Ação 5, documente as descobertas até o momento.

b. Na Ação 6, inicie uma análise pós-incidente.
Na Ação 7, após a revisão pós-incidente, o fluxo termina.

5. Na Ação 8, se o usuário não forneceu uma justificativa comercial válida, execute as seguintes etapas:

Usando o playbook T1003 - Evasão de defesa - Mimakatz DCSombra



a. Na Ação 9, bloqueie ou coloque em quarentena todas as contas, computadores e outros dispositivos envolvidos.

b. Na Ação 10, execute uma investigação forense nas contas bloqueadas e identifique se algum dado foi exfiltrado ou algum código malicioso foi injetado.

c. Na Ação 11, crie novamente a imagem dos recursos afetados.

d. Na Ação 12, suspenda a contenção e traga os sistemas de volta aos padrões operacionais.

e. Na Ação 13, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook for T1003 - Despejo de credencial - Mimakatz DCSync

Este playbook fornece etapas de correção sistemática para investigar incidentes suspeitos de serem causados pelo Mimkatz DCSync. Este playbook é acionado quando uma das funções `Mimkatz (lsadump::dcsync)` é usada. A função é normalmente usada em controladores de domínio (DC) atacados.

O Mimkatz é uma ferramenta de invasão popular que permite aos usuários emitir comandos que ajudam a recuperar dados confidenciais do sistema atacado. Os dados confidenciais incluem senhas, seus hashes e outros.

Nota:
Este é um alerta de alta fidelidade, que é considerado como raramente acionado. Quando ele for acionado, você deve notificar um membro sênior da equipe ou o gerente imediatamente.

Configurar o playbook T1003 - Despejo de credencial - Mimakatz DCsync

Use as etapas a seguir para configurar o playbook T1003 - Despejo de credencial - Mimkatz DCsync.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

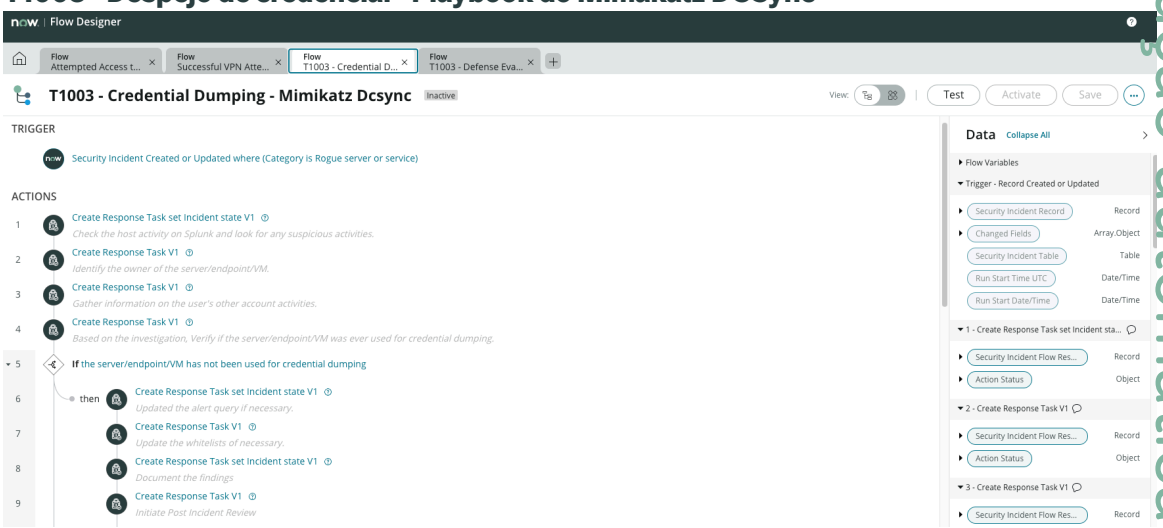
Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o **playbook T1003 - Despejo de credencial - Mimakatz DCsync**.
3. Crie uma cópia do fluxo do playbook T1003 - Despejo de credencial - Mimakatz DCsync e faça as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

   T1003 - Despejo de credencial - Playbook do Mimakatz DCSync

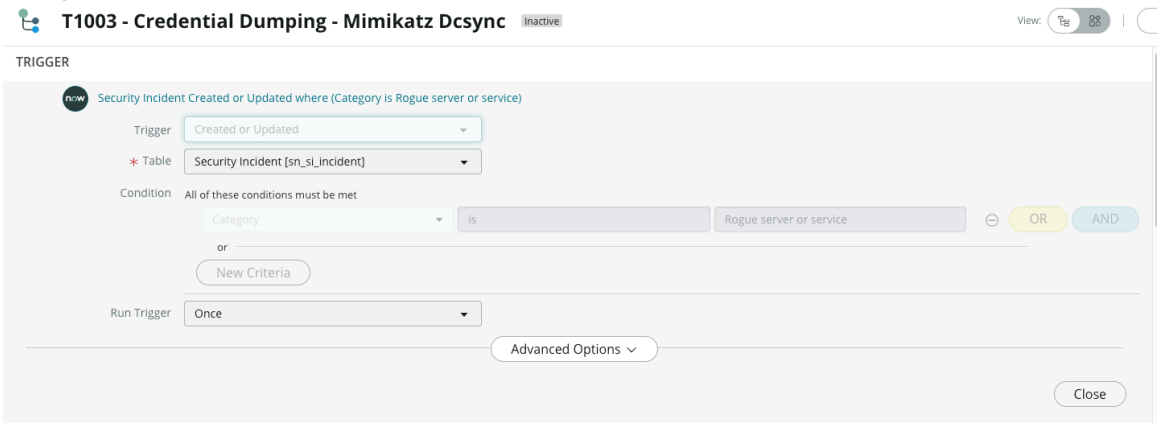
4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. **Condição do gatilho** para o playbook: este playbook é acionado e associado ao incidente de segurança quando a **Categoria** é **Servidor ou serviço invasor**.

T1003 - Despejo de credencial - Condição do gatilho do playbook Mimkatz DCSync



Use o playbook T1003 - Despejo de credencial - Mimakatz DCsync

Use este playbook para investigar incidentes suspeitos de serem causados pelo Mimkatz DCSync. As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook T1003 - Despejo de credencial - Mimkatz DCsync.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

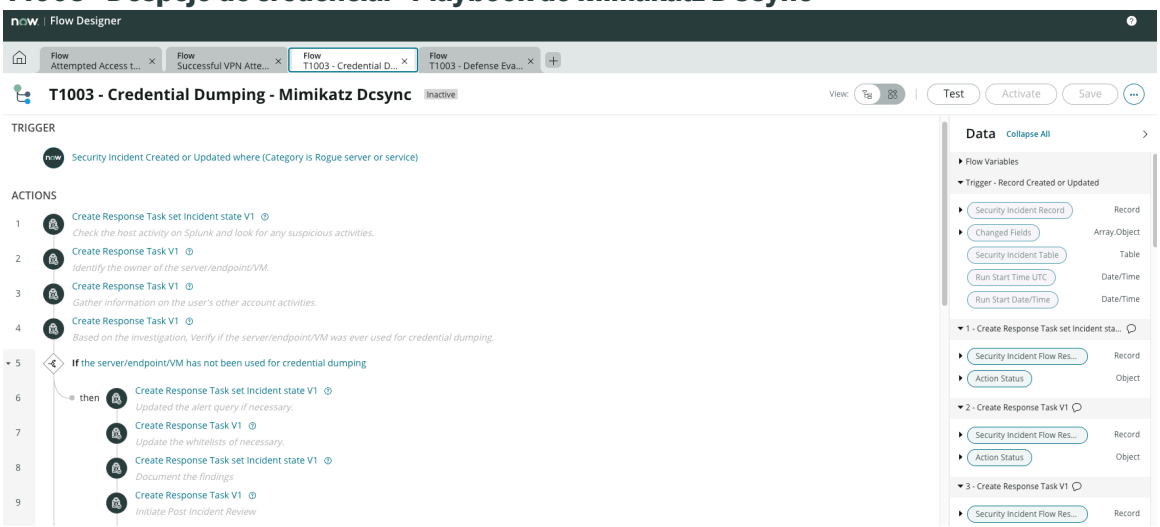
Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, verifique a atividade do host no Splunk e procure atividades suspeitas.
2. Na Ação 2, identifique o proprietário do servidor/endpoint/VM.
   Se o usuário estiver online, execute o CrowdStrike EDR para coletar um escopo melhor das atividades do sistema.
3. Na Ação 3, reúna informações sobre outras atividades da conta do usuário.
4. Na Ação 4, com base na investigação, verifique se o servidor/endpoint/VM já foi usado para despejo de credencial.
5. Na Ação 5, se o servidor/endpoint/VM não tiver sido usado para despejo de credencial, execute as seguintes ações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

T1003 - Despejo de credencial - Playbook do Mimakatz DCsync



a. Na Ação 6, atualize a consulta de alerta, se necessário.

b. Na Ação 7, atualize a lista de permissões, se necessário.

c. Na Ação 8, documente as descobertas até o momento.

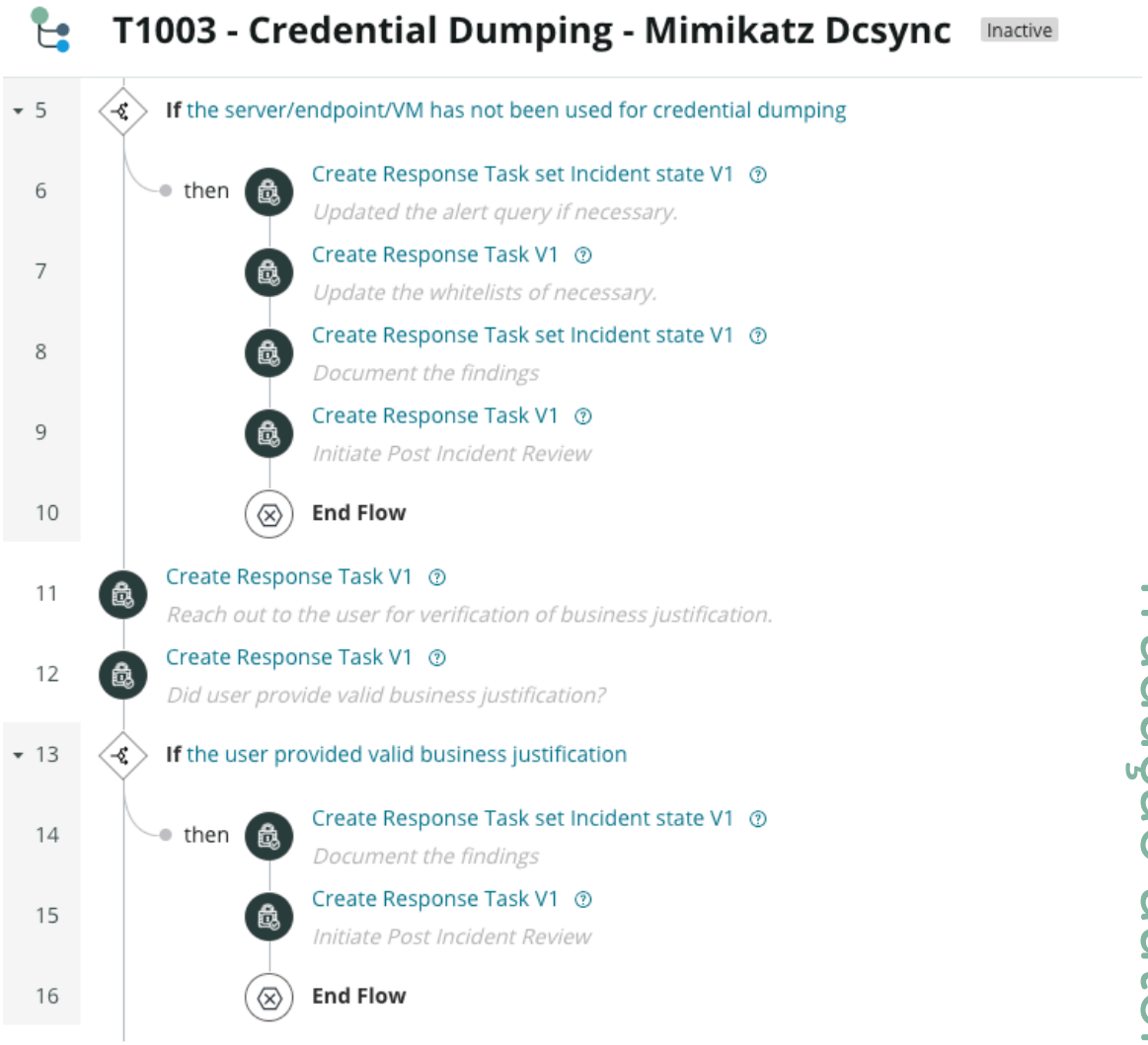
d. Na Ação 9, inicie uma revisão pós-incidente.
Na Ação 10, o fluxo termina.

6. Se o servidor/endpoint/VM foi usado para despejo de credencial, na Ação 11, entre em contato com o usuário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando o playbook T1003 - Despejo de credencial - Mimakatz DCsync



7. Na Ação 12, entre em contato com o usuário para validar a justificativa de negócios.
8. Na Ação 13, se o usuário forneceu uma justificativa comercial válida, execute as seguintes ações:
   a. Na Ação 14, documente as descobertas até o momento.
   b. Na Ação 15, inicie uma revisão pós-incidente.
      Na Ação 16, o fluxo termina.
9. Se o usuário não forneceu uma justificativa comercial válida, na Ação 17, coloque o sistema em quarentena.
10. Na Ação 18, remova todos os arquivos indesejados que possam ter sido criados ou excluídos pelas contas invasoras.
11. Na Ação 19, suspenda a contenção e traga os sistemas de volta aos padrões operacionais.
12. Na Ação 20, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook para falhas de login do usuário do Okta de vários IPs

Este playbook fornece etapas de correção sistemática para investigar incidentes de falhas de login do usuário no Okta.

Tradução automática

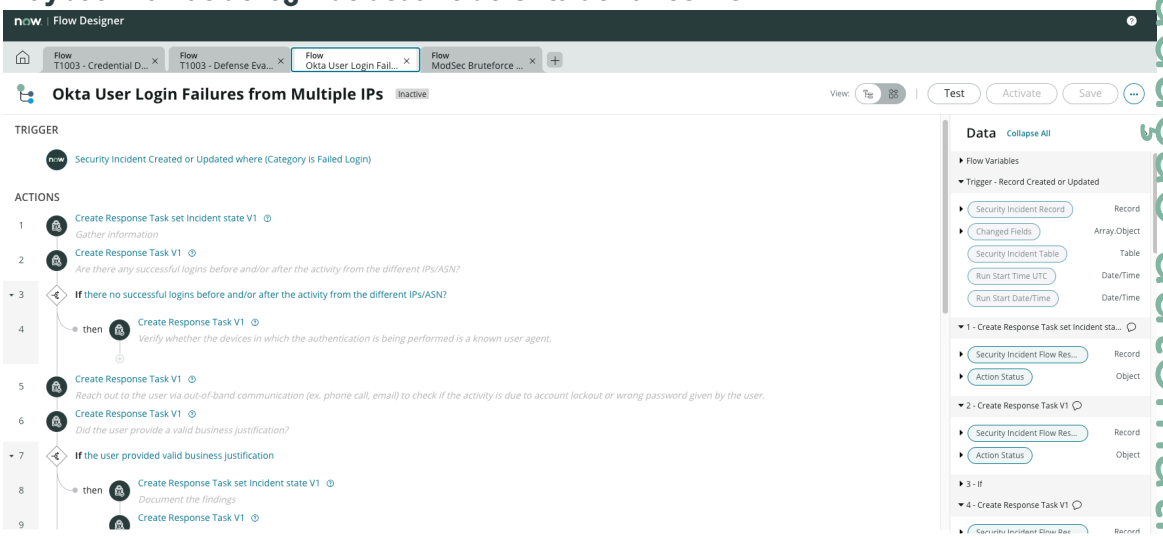
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O playbook Falhas de login do usuário do Okta de vários IPs fornece instruções sobre como analisar o alerta quando falhas de conta da ServiceNow são observadas no Okta de vários IPs que não são da ServiceNow. O alerta relacionado a este playbook verifica os logs do Okta. Ele aciona um alerta quando ocorre uma falha de login para IDs de usuário da ServiceNow de mais de três intervalos de IP que não sejam da ServiceNow em uma duração de 1 hora.

Introdução ao playbook Falhas de login do usuário do Okta de vários IPs

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Tudo** > **Flow Designer** e selecione o playbook **Falhas de login do usuário do Okta de vários IPs**.
3. (Opcional) Você pode criar uma cópia do fluxo do playbook Falhas de login do usuário do Okta de vários IPs e fazer as modificações necessárias. Para criar uma cópia do fluxo do playbook, clique no ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

Playbook Falhas de login do usuário do Okta de vários IPs



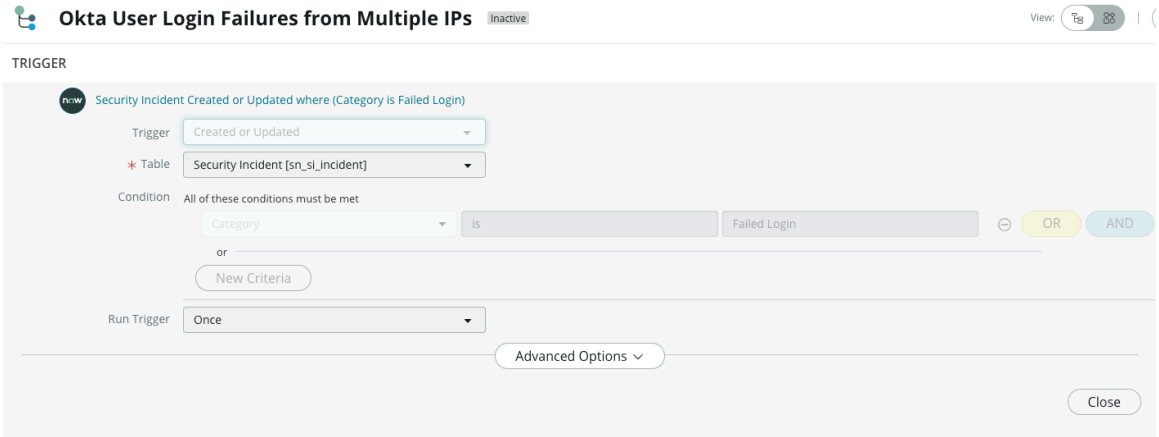
4. Ative os playbooks.
   - Ative o fluxo principal para usar o playbook disponível no sistema de base.
   - Ative os fluxos copiados depois de fazer as mudanças necessárias.

Condição do gatilho: este playbook é acionado e associado ao incidente de segurança quando a **Categoria** é **Falha no login**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Falhas de login do usuário do Okta de vários IPs Condição do gatilho do playbook



Configurar o playbook Falhas de login do usuário do Okta de vários IPs

Use as etapas a seguir para configurar o playbook Falhas de login do usuário do Okta de vários IPs.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Procedimento

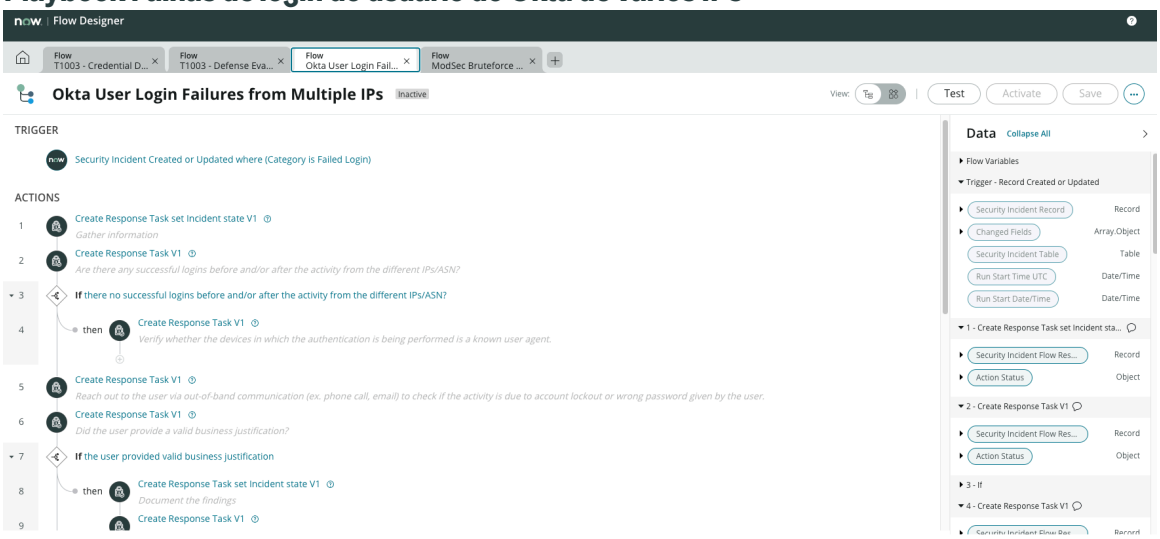
1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o playbook **Falhas de login do usuário do Okta de vários IPs**.
3. Crie uma cópia do fluxo do playbook Falhas de login do usuário do Okta de vários IPs e faça as modificações necessárias.

   Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

Tradução automática

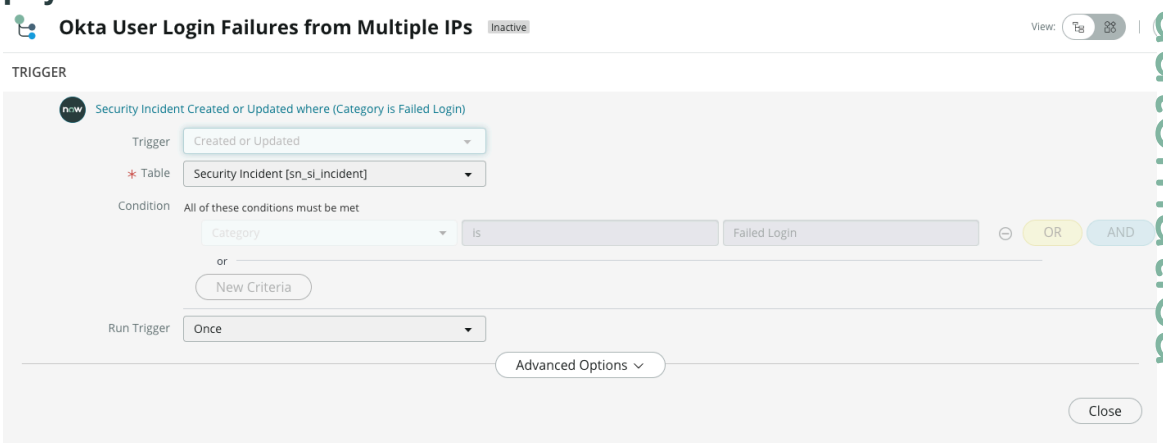
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Playbook Falhas de login do usuário do Okta de vários IPs



4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. **Condição do gatilho** para o playbook: este playbook é acionado e associado ao incidente de segurança quando a **Categoria** é **Falha no login**.

Falhas de login do usuário do Okta de vários IPs Condição do gatilho do playbook



Usar o playbook Falhas de login do usuário do Okta de vários IPs

Use este playbook para investigar incidentes de segurança para falhas de login do usuário no Okta. As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook Falhas de login do usuário do Okta de vários IPs.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

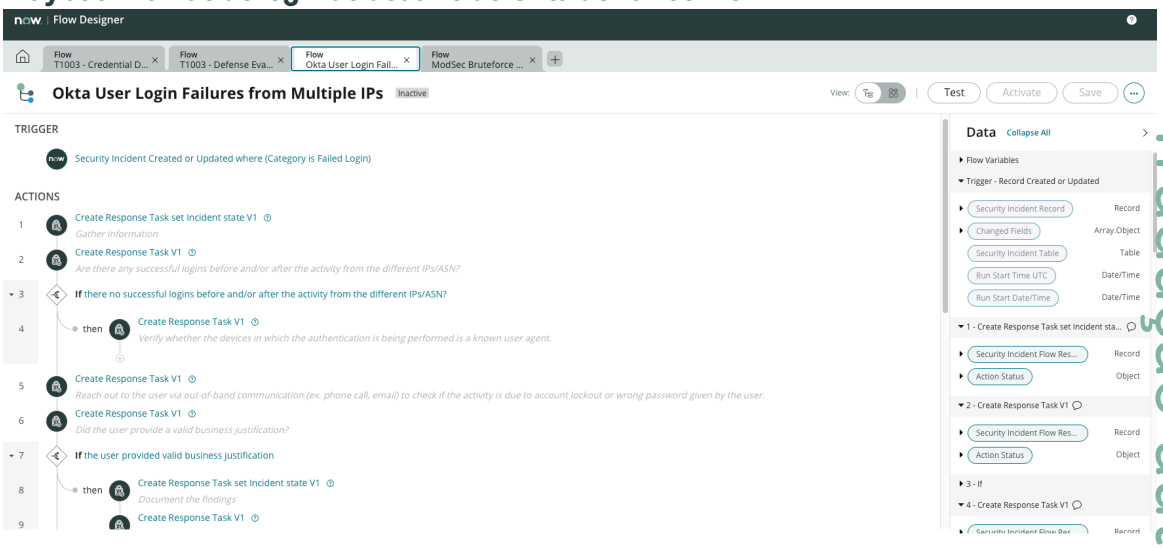
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, execute as seguintes tarefas:
   - Identifique a conta de usuário que está sendo direcionada.
   - Verifique a sub-rede IP e verifique se todas pertencem ao mesmo proprietário de ASN (Autonomous System Number, Número do sistema autônomo).
2. Na Ação 2, verifique se houve logins bem-sucedidos antes ou depois da atividade de diferentes IPs/ASNs.
3. Na Ação 3, se não houve logins bem-sucedidos antes ou depois da atividade dos diferentes IPs/ASNs, na Ação 4, verifique se os dispositivos nos quais a autenticação está sendo realizada são agentes de usuário conhecidos.
   Se os dispositivos forem autenticados por agentes de usuário conhecidos, o fluxo será encerrado.

Playbook Falhas de login do usuário do Okta de vários IPs



4. Na Ação 5, com base na investigação, entre em contato com o usuário por meio de comunicação fora de banda (por exemplo, chamada telefônica ou e-mail) para verificar se a atividade se deve a um bloqueio de conta ou a uma senha incorreta fornecida pelo usuário.
5. Na Ação 6, verifique se o usuário forneceu uma justificativa comercial válida.
6. Na Ação 7, se o usuário forneceu uma justificativa de negócios válida, execute as tarefas a seguir.

   a. Na Ação 8, crie uma tarefa de resposta para documentar as descobertas até o momento.

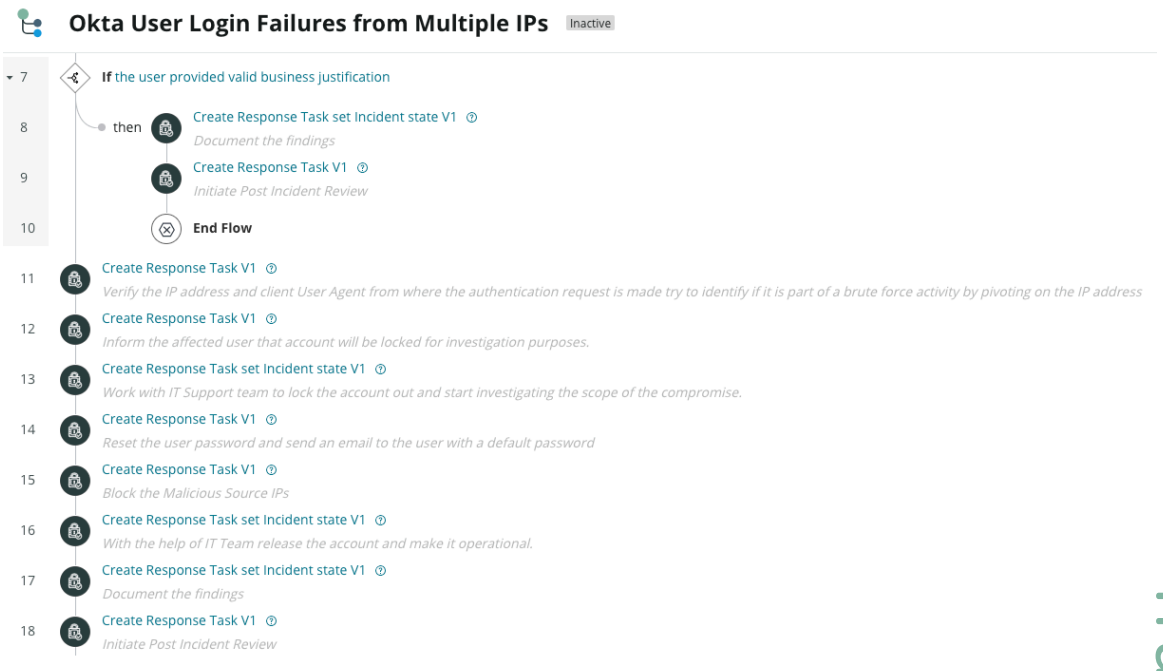
   b. Na Ação 9, crie uma resposta para iniciar uma revisão pós-incidente.
   Na Ação 10, o fluxo termina.

7. Na Ação 11, verifique o endereço IP e o agente do usuário do cliente de onde a solicitação de autenticação é feita e tente identificar se ela faz parte de uma atividade de força bruta girando no endereço IP.
8. Na Ação 12, informe ao usuário afetado que a conta será bloqueada para fins de investigação.
   Você pode usar o modelo de e-mail fornecido para informar o usuário afetado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando o playbook Falhas de login do usuário do Okta de vários IPs



9. Na Ação 13, trabalhe com a equipe de suporte de TI para bloquear a conta e começar a investigar o escopo do comprometimento.
10. Na Ação 14, redefina a senha do usuário e envie um e-mail para o usuário com a senha padrão.
11. Na ação 15, bloqueie os IPs de origem mal-intencionados.
12. Na Ação 16, obtenha ajuda da equipe de suporte de TI para liberar a conta e trazê-la de volta aos padrões operacionais.
13. Na Ação 17, documente as descobertas até o momento.
14. Na Ação 18, conclua a revisão pós-incidente antes de fechar a tarefa.

Playbook for ModSec Brute force by IP Burst

Este playbook fornece etapas de correção sistemática para investigar incidentes de tentativas de força bruta nas páginas de login de vários IPs detectados pelo ModSec. As condições do evento podem ser definidas na própria política do ModSec e gerarão um alerta no Splunk quando o evento for criado no ModSec.

Este playbook ajuda a detectar contagens de tráfego anormais na página de login. Neste exemplo, duas rajadas sucessivas de mais de 50 ocorrências/minuto devem ser de um IP para a página de login, o que indica uma tentativa de força bruta para fazer login.

Configurar força bruta do ModSec por playbook de rajada de IP

Use as etapas a seguir para configurar a força bruta do ModSec por playbook de rajada de IP.

Antes de Iniciar

Função necessária:

- sn_si.admin
- flow_designer

Certifique-se de ter instalado o Security Operations Spoke (*sn_sec_spoke*).

Tradução automática

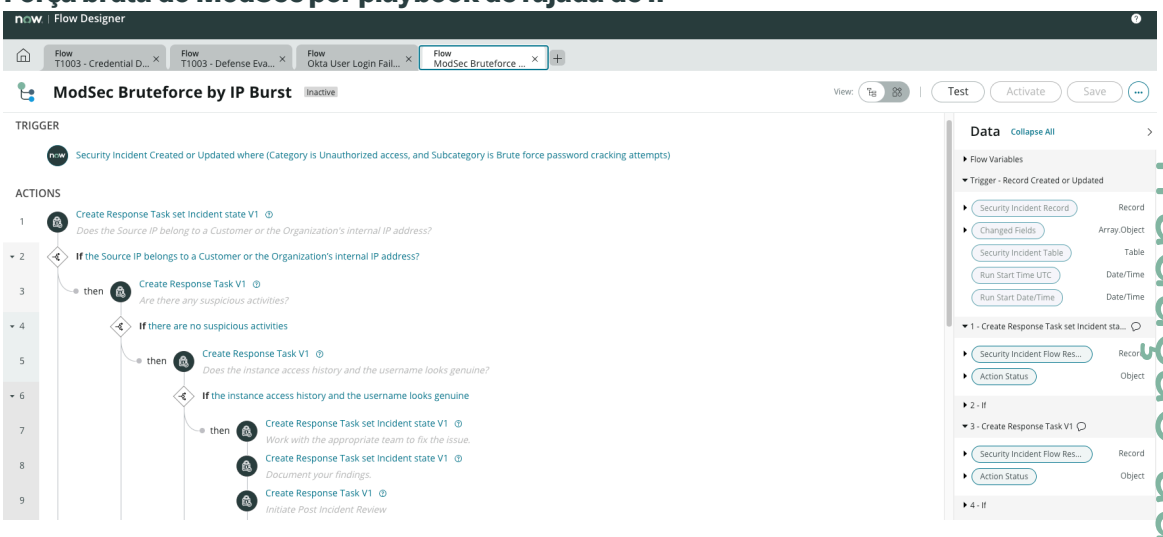
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login como um usuário com as funções sn_si.user e flow_designer.
2. Navegar até **Todos** > **Flow Designer** e selecione o **playbook ModSec Bruteforce by IP Burst**.
3. Crie uma cópia do fluxo do playbook de força bruta do ModSec por rajada de IP e faça as modificações necessárias.

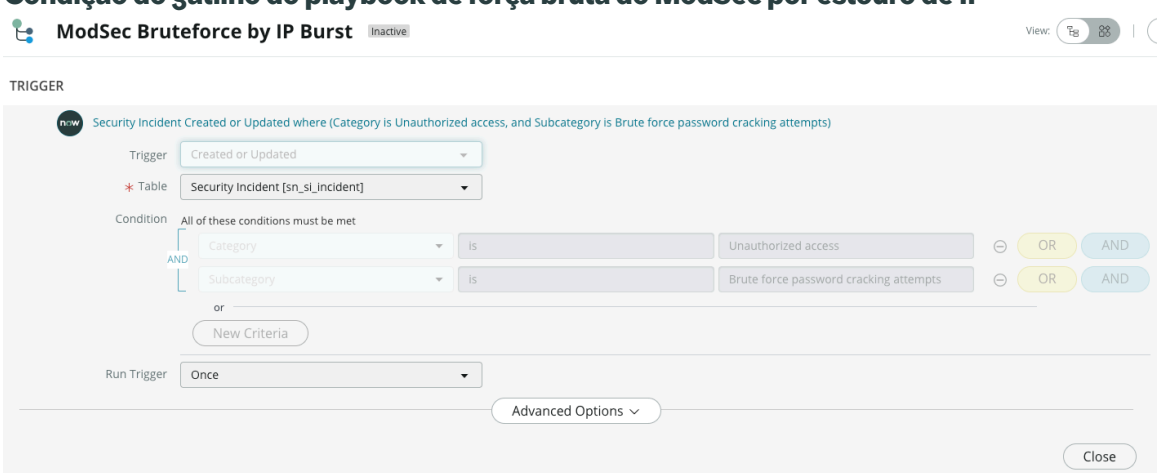
   Para criar uma cópia do fluxo do playbook, selecione o ícone de e selecione **Copiar fluxo**. Execute esta etapa somente se você planejar personalizar ou fazer mudanças específicas no fluxo.

Força bruta do ModSec por playbook de rajada de IP



4. Ative os playbooks.
   a. Ative o fluxo principal para usar o playbook disponível no sistema de base.
   b. Ative os fluxos copiados depois de fazer as mudanças necessárias.
5. **Condição do gatilho** para o playbook: este playbook é acionado e associado ao incidente de segurança quando as seguintes condições são atendidas:
   - A**categoria** é **Acesso não autorizado**.
   - **A subcategoria** é **Tentativas de quebra de senha de força bruta**.

Condição do gatilho do playbook de força bruta do ModSec por estouro de IP



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use o playbook de força bruta do ModSec por rajada de IP

Use este playbook para investigar incidentes de tentativas de força bruta nas páginas de login de vários IPs detectados pelo ModSec. As etapas a seguir fornecem instruções sobre as ações, tarefas e subfluxos que estão disponíveis no playbook de força bruta do ModSec por IP Burst.

Antes de Iniciar

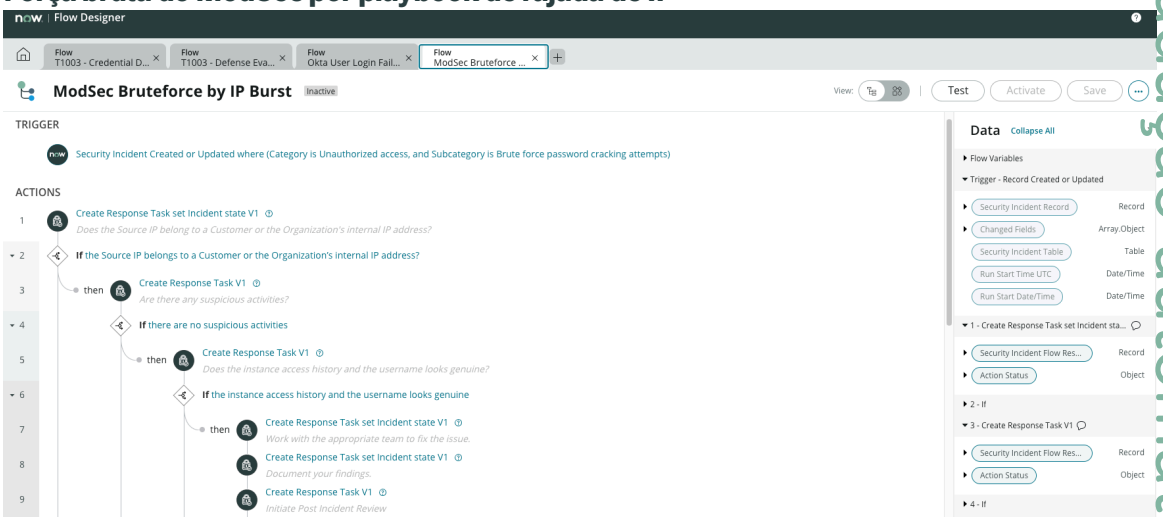
Função necessária:

- sn_si.admin
- flow_designer

Procedimento

1. Quando o playbook for acionado e começar a ser executado, na Ação 1, verifique se o IP de origem pertence a um cliente ou ao endereço IP interno da organização (Ação 1).
2. Na Ação 2, se o IP de origem pertencer a um cliente ou ao endereço IP interno da organização, execute as seguintes etapas:

Força bruta do ModSec por playbook de rajada de IP



   a. Na Ação 3, verifique se houve alguma atividade suspeita.

      - Verifique a atividade do IP de origem nos últimos dias. Se o IP tiver tráfego insignificante, isso indica um ataque real.
      - Verifique os nomes de usuário da aplicação. Por exemplo, verifique se os nomes de usuário estão organizados em ordem alfabética.
      - Procure nomes genéricos de conta envolvidos. Por exemplo, admin, sysadmin, root, administrador e outros nomes de conta de aplicação.

      Se não houver atividades suspeitas, o fluxo será encerrado.

   b. Na Ação 4, se houver alguma atividade suspeita, na Ação 5, verifique se o histórico de acesso à instância e o nome de usuário parecem verdadeiros.

      Verifique os logs *Appnode* em busca de alguma indicação de falha. Pode haver eventos de falha de SAML, SSO ou LDAP, o que pode ser devido a um problema operacional.

      Se o histórico de acesso à instância e o nome de usuário não parecerem verdadeiros, o fluxo será encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Na Ação 6, se o histórico de acesso à instância e o nome de usuário parecerem verdadeiros, execute as seguintes etapas:

i. Na Ação 7, coordene com a equipe apropriada para corrigir o problema.

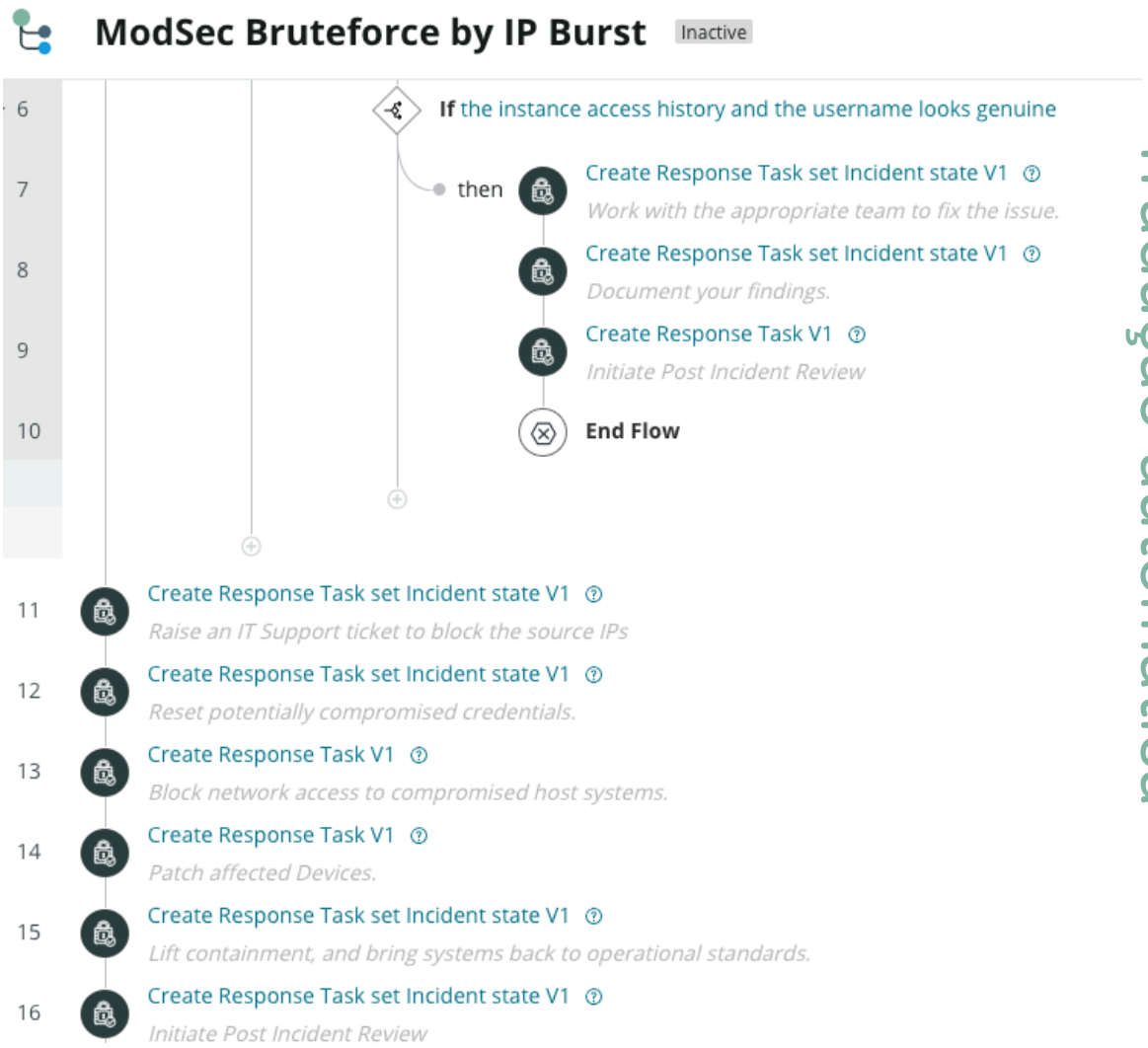
ii. Na Ação 8, documente as descobertas até o momento.

iii. Na Ação 9, conclua a revisão pós-incidente antes de fechar a tarefa.

Na Ação 10, o fluxo termina.

3. Se o IP de origem não pertencer a um cliente ou ao endereço IP interno da organização, na Ação 11, gere um tíquete de suporte de TI para bloquear os IPs de origem.

Usando o playbook de força bruta do ModSec por rajada de IP



4. Na Ação 12, redefina as credenciais potencialmente comprometidas.

5. Na Ação 13, bloqueie o acesso à rede para sistemas host comprometidos.

6. Na Ação 14, corrija os dispositivos afetados.

7. Na Ação 15, suspenda a contenção e traga os sistemas de volta aos padrões operacionais.

8. Na Ação 16, conclua a revisão pós-incidente antes de fechar a tarefa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ações do playbook do Security Incident Response

Esta seção descreve as ações fornecidas na biblioteca de ações do Flow Designer.

Nome da Ação	Descrição	Cenário de exemplo	
Adicionar um marcador de segurança ao incidente de segurança	Use esta ação para adicionar um marcador de segurança automaticamente usando a lógica do Flow Designer.	Se o fluxo detectar um IOC, o marcador **IOC detectado** poderá ser adicionado automaticamente usando esta ação. **Fluxo**:	• Entrada: incidente de segurança, marcador de segurança • Saída: não aplicável
Adicionar observáveis ao incidente de segurança	Use esta ação para adicionar observáveis a um incidente de segurança selecionado. • Por padrão, a lista de observáveis é separada pelo delimitador de vírgula (,), mas isso pode ser modificado. Você pode especificar outro caractere especial como delimitador. Ao adicionar observáveis, o tipo (URL, endereço IP, hash) é definido automaticamente. • Quando os observáveis são adicionados ao incidente de segurança, o tipo (URL, endereço IP, hash) é definido automaticamente. • Quando os observáveis estão sendo adicionados, a opção Filtrar observáveis da lista de permitidos identifica os observáveis da lista de permitidos e não os adiciona à lista relacionada de observáveis		• Entrada: ◦ incidente de segurança ◦ observáveis ◦ delimitador ◦ filtrar observáveis da lista de permitidos e publicar anotação de atividade • Saída: não aplicável

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Descrição	Cenário de exemplo	
	do incidente de segurança. Uma atividade do sistema automatizada (resposta) é adicionada para indicar que esses observáveis foram removidos.		
Obter usuários afetados (Listas relacionadas) de vários incidentes de segurança V1	Recupera todos os usuários afetados listados na lista relacionada Usuários afetados para os incidentes de segurança especificados.	Você pode ter incidentes de segurança primários com vários incidentes de segurança secundários. Use esta ação para acumular usuários afetados de todos os incidentes de segurança secundários para os incidentes de segurança primários correspondentes. Somente usuários afetados exclusivos são acumulados e todas as duplicatas são eliminadas.	• Entrada: incidentes de segurança • Saída: ◦ usuário afetado ◦ contagem
Obter usuários afetados de vários incidentes de segurança	Recupera o usuário afetado primário para o incidente de segurança especificado. Ele não inclui os usuários afetados da lista relacionada Usuários afetados.	• Ao investigar um incidente de segurança de phishing, envie um e-mail para os usuários primários afetados (que reportaram o incidente de phishing) para confirmar se algum dos usuários clicou nos links maliciosos no e-mail de phishing. • Atualize a severidade do incidente de segurança primário ou a pontuação de risco com base na contagem de usuários primários afetados.	• Entrada: incidentes de segurança • Saída: ◦ usuários afetados ◦ contagem

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Descrição	Cenário de exemplo	
Obter usuários afetados (lista relacionada) de um incidente de segurança	Recupera todos os usuários afetados listados na lista relacionada Usuários afetados para um incidente de segurança especificado.		• Entrada: incidentes de segurança • Saída: ◦ usuários afetados ◦ contagem
Adicionar usuários afetados ao incidente de segurança	Adiciona todos os usuários afetados a um incidente de segurança.	Suponha que você tenha um incidente de segurança primário com vários incidentes de segurança secundários. Você pode usar esta ação para acumular usuários afetados de todos os incidentes de segurança secundários para o incidente de segurança primário correspondente. Somente usuários afetados exclusivos são acumulados e todas as duplicatas são eliminadas.	• Entrada: ◦ incidente de segurança ◦ usuário • Saída: não aplicável
Obter itens de configuração dos usuários afetados	Recupera os itens de configuração (ICs) de todos os usuários afetados.	Em cenários de phishing ou malware, você pode usar esta ação para atualizar a lista relacionada de ICs (Itens de Configuração Afetados) e investigar os ICs. Você pode atualizar a severidade ou a pontuação de risco do incidente de segurança com base no número de ICs identificados.	• Entrada: usuários • Saída: ◦ itens de configuração ◦ contagem
Obter todos os incidentes de segurança secundários para um incidente de segurança	Recupera todos os incidentes de segurança secundários relacionados a um incidente de segurança primário específico.	Cenário de exemplo: use esta ação para: • Atualize o status dos incidentes de segurança secundários quando o status dos incidentes de segurança primários correspondentes for atualizado. • Atualize a severidade ou	• Entrada: ◦ incidente de segurança ◦ estado do incidente • Saída: ◦ incidente secundário de segurança ◦ contagem

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Descrição	Cenário de exemplo	
		a pontuação de risco do incidente de segurança automaticamente com base no número de incidentes de segurança secundários.	
Obter itens de configuração para os observáveis (tipo de endereço IP)	Recupera todos os itens de configuração (ICs) para observáveis do tipo endereço IP.	Um observável de endereço IP pode ser associado a um item de configuração. Por exemplo, o endereço IP de um servidor. Se você usar esta ação, poderá recuperar informações do servidor.	• Entrada: endereço IP do observável • Saída: ◦ itens de configuração ◦ contagem
É observável malicioso	Confirma a presença de um ou mais observáveis maliciosos em um conjunto de observáveis.	Depois que a pesquisa de ameaças tiver sido concluída e você tiver identificado a presença de observáveis mal-intencionados, poderá aumentar a severidade ou a pontuação de risco de um incidente de segurança.	• Entrada: incidente de segurança • Saída: malicioso (verdadeiro/falso)
Enviar e-mail para confirmar a interação do usuário	Envia e-mail em resposta a uma resposta do usuário.	Se um usuário tentar várias vezes fazer login em uma aplicação e falhar, isso resultará em um cenário de falha de login. Nesse caso, um e-mail é enviado ao usuário para confirmar se ele tentou fazer login ou não. Dependendo da resposta do usuário (Sim ou Não), diferentes ações podem ser realizadas. **Fluxo**: falha no login manual do playbook	
Filtrar observáveis da lista de permitidos	Use esta ação para permitir observáveis de lista de um determinado conjunto de observáveis.	Você pode identificar determinados observáveis que podem ser ignorados em um conjunto de observáveis. Esses observáveis não serão	• Entrada: incidente de segurança • Saída:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Descrição	Cenário de exemplo	
		levados em conta ao resolver o incidente de segurança.	◦ observáveis da lista permitidos ◦ contagem
Redefinir senha para usuários afetados	Use esta ação para redefinir a senha dos usuários afetados.	Se uma conta de usuário tiver sido invadida ou um usuário solicitar que uma senha seja redefinida, um e-mail será enviado ao usuário para redefinir a senha. **Fluxo**: falha no playbook manual de login.	
Obter grupo de usuários para usuário afetado	Recupera os detalhes do grupo de usuários afetados.	Em uma organização, se dois ou mais usuários relatarem e-mails de phishing, você poderá descobrir o grupo ao qual eles pertencem e identificar se mais usuários foram afetados	• Entrada: usuário • Saída: ◦ grupos de usuários ◦ contagem

Relatório do Security Incident Response

Os gerentes de segurança podem identificar áreas de preocupação usando interfaces gráficas de alto nível.

Acessar Gerenciador do Security Incident Response

Você pode acessar o painel do Security Incident Response Explorer para exibir a atividade do incidente de segurança para identificar instantaneamente as áreas de preocupação e resolver problemas rapidamente.

Antes de Iniciar
Funções necessárias:

- sn_si.admin (para gravar)
- sn_si_basic (para ler)

Procedimento

1. Navegar até **Tudo** > **Autoatendimento** > **Página inicial** ou navegue até **Autoatendimento** > **Painéis**.
2. Escolha o Explorador de incidentes de segurança na lista de relatórios.

Tradução automática

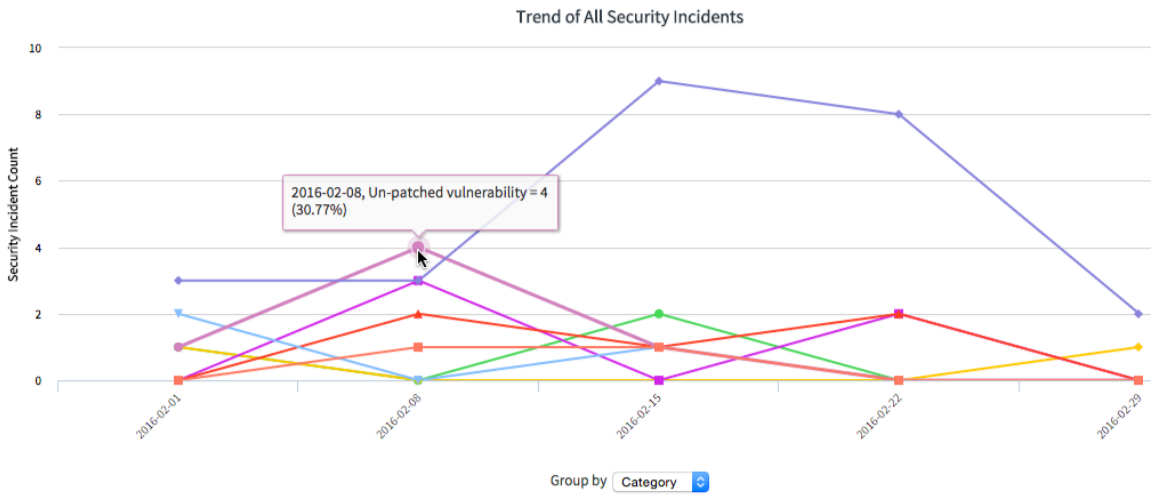
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral do Security Incident Response

A Security Incident Response Visão geral fornece uma visão executiva da atividade de incidente de segurança, fornecendo tendências e relatórios e detalhando dados específicos.

O módulo Visão geral exibe informações de incidente de segurança que são personalizadas para a função do usuário. Você pode apontar para qualquer parte de um gráfico (barra, pizza, ponto de dados, mapa térmico e assim por diante) para exibir dados gerais específicos dessa parte. Veja a imagem a seguir. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Tendência de todos os incidentes de segurança



Visão geral do gerenciador de Incidentes de segurança

Usuários com as funções Administrador de incidentes de segurança e Gerenciador de incidentes de segurança exibem a Visão geral do Gerenciador de incidentes de segurança. Ele contém os seguintes relatórios no sistema de base.

Relatórios de visão geral do gerenciador de incidentes de segurança

Nome	Visual	Descrição
Incidentes de segurança críticas da equipe	Pontuação única	O número de incidentes de segurança críticos atribuídos à equipe.
Incidentes de alta segurança da equipe	Pontuação única	O número de incidentes de alta segurança atribuídos à equipe.
ANS que expiram em 24 horas	Pontuação única	O número de SLAs que expiram nas próximas 24 horas.
Risco versus Severidade	Mapa térmico	A distribuição de incidentes de segurança atribuídos à equipe por risco e severidade.
Incidentes de segurança por classe de IC, últimos 3 meses	Gráfico de barras	A contagem de incidentes de segurança atribuídos à equipe por classe de item de configuração.
Tendência de todos os incidentes de segurança	Tendência	Representa graficamente a contagem do número de incidentes de segurança recebidos por categoria ou prioridade.
Incidentes de segurança de acesso não autorizado	Gráfico de barras	Exibe os tipos de categorias de incidentes de segurança recebidos ao longo do tempo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de visão geral do gerenciador de incidentes de segurança

Nome	Visual	Descrição
Tempo médio de contenção	Pontuação única	O tempo médio necessário para conter todos os incidentes de segurança.
Tempo médio de contenção crítica	Pontuação única	O tempo médio necessário para conter todos os incidentes de segurança críticos.
Tempo médio de identidade	Pontuação única	O tempo médio necessário para identificar todos os incidentes de segurança.

Visão Geral de Análise de Segurança

Usuários com a função de Analista de incidente de segurança exibem a Visão geral do analista de segurança. Ele contém os seguintes relatórios no sistema de base.

Relatórios de visão geral do analista de segurança

Nome	Visual	Descrição
Meu trabalho de prioridade crítica	Pontuação única	O número de incidentes de segurança críticos atribuídos a mim.
Meu trabalho de alta prioridade	Pontuação única	O número de incidentes de alta segurança atribuídos a mim.
Meus ANS que expiram em 24 horas	Pontuação única	O número de SLAs atribuídos a mim que expiram nas próximas 24 horas.
Incidentes de segurança atribuídos a mim	Gráfico de barras	Incidentes de segurança atribuídos a mim por estado ou categoria de incidente.
Trabalho atribuído a mim por tipo	Gráfico de barras	Tarefas de segurança (incidentes, tarefas ou solicitações) atribuídas a mim por tipo ou prioridade.
Incidentes de segurança, solicitações e tarefas atribuídos a mim	Lista	Uma lista de todos os incidentes de segurança, solicitações de segurança e tarefas atribuídas a mim.
Local do incidente de segurança	Mapa	Localização regional dos incidentes de segurança.
Contagem	Mapa	Número de incidentes de segurança por região.
Contagem mínima/máxima	Barra de Espectro de Cores	Os números mínimo e máximo de incidentes de segurança por região representados por uma barra de espetro de cores.
Porcentagem da contagem	Mapa	Percentual da contagem total de incidentes por região.

Security Incident CISO Overview with Security Incident Analytics ativado

Quando o plug-in Security Incident Analytics é ativado, os usuários com as funções de Incidente de segurança CISO e Administrador do sistema exibem a Visão geral do CISO de incidente de segurança. Os relatórios do CISO a seguir são fornecidos no sistema de base.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de visão geral do ICSO de incidente de segurança (com a Análise de incidente de segurança ativado)

Nome	Visual	Descrição
Novos Incidentes de segurança nesta semana	Pontuação única	O número de novos incidentes de segurança recebidos na semana atual.
Incidentes de segurança encerrados nesta semana	Pontuação única	O número de incidentes de segurança encerrados na semana atual.
Novos incidentes de segurança (em execução há 7 dias)	Pontuação única	O número de incidentes de segurança abertos nos últimos 7 dias.
Incidentes de segurança encerrados (em execução há 7 dias)	Pontuação única	O número de incidentes de segurança encerrados nos últimos 7 dias.
Novos incidentes de segurança diários versus incidentes de segurança encerrados	Tendência	Contagens de incidentes de segurança novos e encerrados ao longo do tempo por dia.
Novos incidentes de segurança semanais versus incidentes de segurança encerrados	Tendência	Incidentes de segurança novos e encerrados ao longo do tempo por semana.
Código de fechamento de incidentes de segurança	Tendência	Contagem total de códigos de fechamento ao longo do tempo.
Impacto de Incidente de segurança nos negócios	Mapa de Árvore	Serviços de negócios com incidentes de segurança com agrupamentos disponíveis por criticidade dos negócios.
Tempo Médio para Conter (Por Semana)	Tendência	O tempo médio de 7 dias necessário para conter um incidente de segurança ao longo do tempo.
Tempo Médio para Eliminar (Por Semana)	Tendência	O tempo médio de 7 dias necessário para erradicar um incidente de segurança ao longo do tempo.
Tempo médio para identidade (Semanalmente)	Tendência	O tempo médio de 7 dias necessário para identificar um incidente de segurança ao longo do tempo.
Local do incidente de segurança	Mapa	Localização regional dos incidentes de segurança.
Contagem	Mapa	Número de incidentes de segurança por região.
Contagem mínima/máxima	Barra de Espectro de Cores	Os números mínimo e máximo de incidentes de segurança por região representados por uma barra de espetro de cores.
Porcentagem da contagem	Mapa	Percentual da contagem total de incidentes por região.

Visão geral do ICSO de incidente de segurança sem análise de incidente de segurança ativada

Quando o plug-in Security Incident Analytics não está ativado, os usuários com as funções de CISO de incidente de segurança e Administrador do sistema exibem a Visão geral do relatório de CISO de incidente de segurança. Os relatórios do CISO a seguir são fornecidos no sistema de base.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de visão geral do ICSO de incidente de segurança (sem a Análise de incidente de segurança ativada)

Nome	Visual	Descrição
Novos Incidentes de segurança nesta semana	Pontuação única	O número de novos incidentes de segurança abertos na semana atual.
Incidentes de segurança encerrados nesta semana	Pontuação única	O número de incidentes de segurança encerrados na semana atual.
Novos incidentes de segurança (em execução há 7 dias)	Pontuação única	O número de incidentes de segurança abertos nos últimos 7 dias.
Incidentes de segurança encerrados (em execução há 7 dias)	Pontuação única	O número de incidentes de segurança encerrados nos últimos 7 dias.
Novos incidentes de segurança semanalmente	Tendência	Os novos incidentes de segurança foram abertos semanalmente.
Incidentes de segurança encerrados semanalmente	Tendência	Os incidentes de segurança encerrados semanalmente.
Códigos de fechamento de Incidentes de segurança	Tendência	Códigos de fechamento de incidente de segurança ao longo do tempo.
Serviços de negócios com incidentes de segurança - Impacto nos negócios	Mapa de Árvore	Serviços de negócios com incidentes de segurança com agrupamentos disponíveis por criticidade dos negócios.
Tempo médio de contenção	Pontuação única	O tempo médio necessário para conter todos os incidentes de segurança.
Tempo médio de contenção crítica	Pontuação única	O tempo médio necessário para conter todos os incidentes de segurança críticos.
Tempo médio de identidade	Pontuação única	O tempo médio necessário para identificar todos os incidentes de segurança.

Nota:
O sistema base Security Incident Response inclui Soluções de Performance Analytics para exibir painéis de práticas recomendadas pré-configurados. Os painéis apresentam métricas importantes para analisar seu processo de Security Incident Response, como novos incidentes de segurança ou a idade média dos incidentes de segurança em aberto. Para obter mais informações e instruções de instalação, consulte Security Incident Response Soluções Análise da plataforma.

Mapa de incidentes de segurança

O mapa de incidentes de segurança fornece dados por localização geográfica. O mapa-múndi é destacado em todas as áreas em que ocorre um incidente. Quando o plug-in Security Incident Analytics está ativado, você pode adicionar o mapa de incidente de segurança à visão geral Security Incident Response. Depois de adicionado, você pode configurar o mapa modificando os filtros do mapa.

Adicionar mapa à visão geral de Security Incident Response

Você pode adicionar o mapa à visão geral Security Incident Response para exibir dados de incidentes de segurança por localização geográfica. Um mapa permite que você faça uma busca detalhada nas informações do incidente de segurança por local.

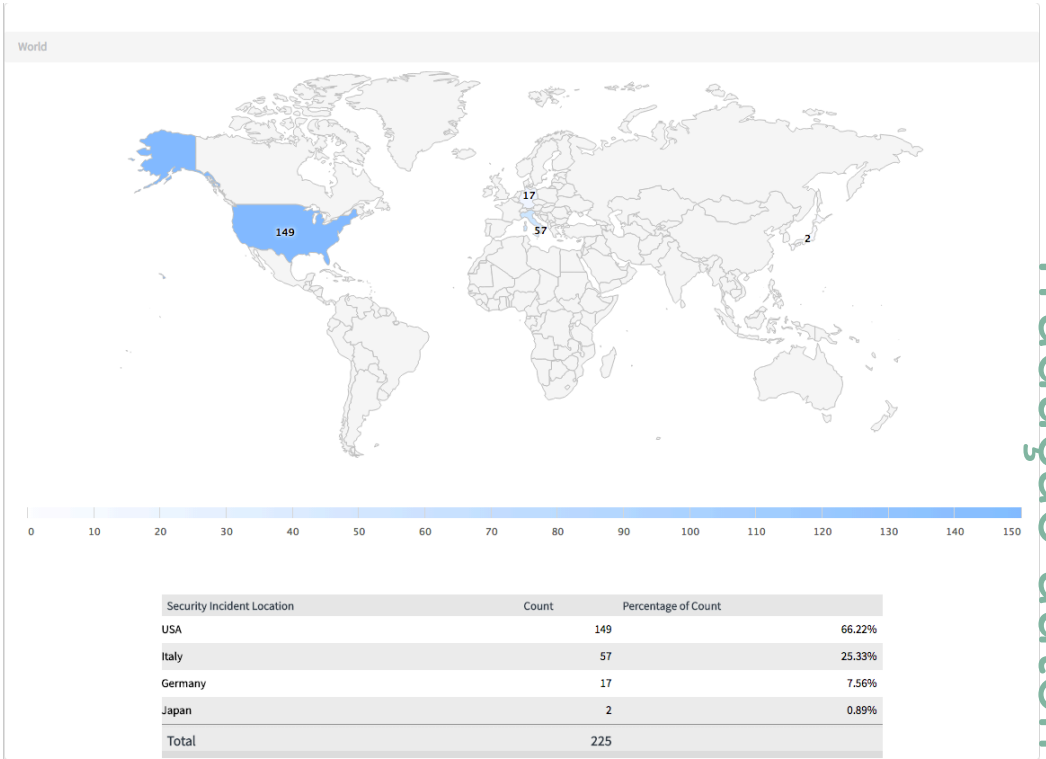
Antes de Iniciar
Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Visão geral**.
2. Clique em **Adicionar conteúdo** no canto superior esquerdo da página para abrir o controle de seleção de widget.
3. Na primeira caixa de seleção, clique em **Relatórios**.
4. Na segunda caixa de seleção, clique em **Incidente de segurança**.
5. Na terceira caixa de seleção, clique em **Mapa de incidente de segurança**.



Security Incident Location	Count	Percentage of Count
USA	149	66.22%
Italy	57	25.33%
Germany	17	7.56%
Japan	2	0.89%
Total	225	

6. Na parte inferior da tela, clique no local da tela que você deseja adicionar ao relatório.
7. Feche a caixa **Adicionar conteúdo**.

Modificar mapa de incidentes de segurança

Os administradores no domínio global podem modificar como o mapa de incidentes de segurança lida com incidentes de segurança usando filtros.

Antes de Iniciar

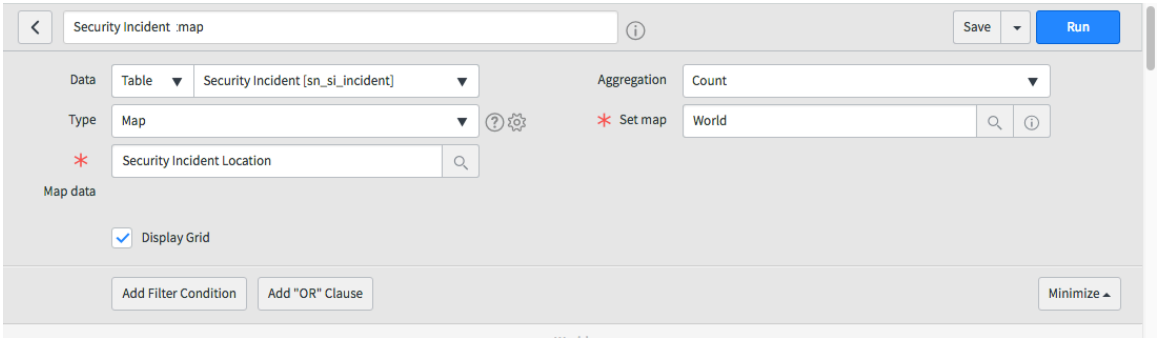
Função necessária: sn_si.admin

Procedimento

1. Navegar até **Relatórios** > **Administração** > **Todos**.
2. Pesquise **o mapa de Incidentes de segurança**.
3. Clique **em Editar relatório**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em **Adicionar condição do filtro** para adicionar ou editar filtros.
5. Clique em **Executar** para ver as mudanças aplicadas.
6. Clique em **Salvar**.

Mapas de árvore de incidentes de segurança

Quando o plug-in Security Incident Analytics está ativado, você pode adicionar o incidente de segurança - impacto no serviço e incidente de segurança - mapas de árvore em tempo real à visão geral de Security Incident Response. Depois que eles forem adicionados, você poderá configurar os mapas de árvore modificando as categorias e os indicadores do mapa de árvore.

Adicionar mapas de árvore à visão geral do Security Incident Response

Os mapas de árvore exibem dados hierárquicos (estruturados em árvore) como um conjunto de retângulos aninhados. Cada ramificação da árvore recebe um retângulo, que é lado a lado com retângulos menores que representam sub-ramificações. Os mapas de árvore permitem exibir informações de incidentes de segurança de forma dinâmica e envolvente.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Visão geral**.
2. Clique em **Adicionar conteúdo** no canto superior esquerdo da página para abrir o controle de seleção de widget.
3. Na primeira caixa de seleção, clique em Mapa de **árvore**.
4. Na segunda caixa de seleção, selecione o mapa de árvore que deseja inserir na seguinte lista:
   - Incidente de segurança - Impacto do serviço
   - Incidente de segurança - Tempo real
   - Incidente de segurança - Impacto nos negócios
   - Significância da vulnerabilidade

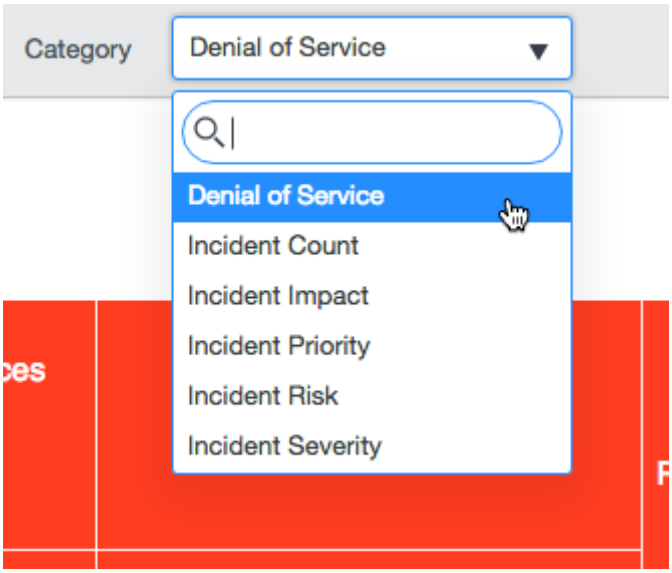
Nota:
O mapa de árvore do impacto nos negócios aparece na página inicial Security Incident Response por padrão. Os mapas de árvore de impacto do serviço e em tempo real exigem que o plug-in Análise de incidente de segurança esteja ativado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Na terceira caixa de seleção, selecione o nível de granularidade das informações que você deseja recuperar para o mapa de árvore selecionado.

Nota:
Para o mapa de árvore Incidente de segurança - Impacto do serviço, selecione **Incidente de segurança** na terceira caixa de seleção. Esta seleção fornece uma lista suspensa com várias categorias de dados.



6. Na parte inferior da tela, clique no local da tela que você deseja adicionar o medidor.
7. Feche a caixa **Adicionar conteúdo**.

Criar ou atualizar uma categoria de mapa de árvore

Você pode modificar as categorias predefinidas dos mapas de árvore de incidentes de segurança ou criar categorias conforme necessário.

Antes de Iniciar
Função necessária: sn_si.admin

Os mapas de árvore usam performance analytics como fonte de dados. O módulo Performance Analytics requer um plug-in separado.

Por Que e Quando Desempenhar Esta Tarefa
No sistema básico, as categorias de mapa de árvore, como Risco de incidente, Negação de serviço e Severidade do incidente, estão incluídas. Você pode modificar essas categorias ou definir mais categorias conforme necessário.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Administração**e abra a definição do mapa de árvore para o qual você deseja configurar as categorias:
   - **Definição de Relatório de Criticidade de Serviço**
   - **Definição em tempo real**
2. **Opcional:** Altere o nome da definição do mapa de árvore.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

No sistema de base, o nome padrão para a definição do mapa de árvore do impacto do serviço é **Incidente de segurança**. O nome padrão da definição do mapa de árvore em tempo real é **Incidente de segurança - Tempo real**.

3. A menos que você esteja usando um mapa de árvore personalizado, não altere o valor do **Grupo de Indicadores de PA**.
4. Para desativar a definição do mapa de árvore, desmarque a caixa de seleção **Ativo**.
   Se, por exemplo, você desativar a categoria de negação de serviço no painel de impacto do sistema, essa categoria de mapa de árvore não estará disponível.
5. Na lista relacionada **Categorias** de mapa de árvore, selecione uma categoria para modificar ou clique em **Novo** para criar uma nova categoria.
6. Preencha os campos.

Formulário Categoria de mapa de árvore

Campo	Descrição
Nome	O nome exibido para a categoria na lista **Categorias** acima do mapa de árvore.
Pedido	A ordem em que a categoria aparece na lista **Categorias** acima do mapa de árvore.
Mapa de Árvore	O nome do mapa de árvore que usa esta categoria.
Cor	A cor exibida para esta categoria no mapa de árvore.
Ativo	Selecione para ativar esta categoria.
Descrição	Uma descrição da categoria.
Visível para todas as funções	Selecione para tornar esta categoria visível para todos os usuários, independentemente de sua função.
Funções	Se você não marcou a caixa de seleção **Visível para todas as funções**, selecione as funções capazes de exibir esta categoria.

7. Clique em **Enviar** ou **Atualizar**.

Criar ou atualizar um indicador de mapa de árvore

Você pode modificar os indicadores predefinidos para uma categoria de mapa de árvore ou criar novos indicadores. Para cada indicador, você pode configurar sua fonte de dados e especificar como as listas de incidentes de segurança são abertas a partir de mapas de árvore que são exibidos com o indicador.

Antes de Iniciar

Função necessária: sn_si.admin

Os mapas de árvore usam performance analytics como fonte de dados. O módulo Performance Analytics requer um plug-in separado.

Procedimento

1. Abra a definição de mapa de árvore para a qual você deseja configurar os indicadores.
2. Na lista relacionada **Categorias** de mapa de árvore, selecione a categoria para a qual você deseja configurar os indicadores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na lista relacionada **Indicadores** de mapa de árvore, selecione um indicador para modificar ou clique em **Novo** para criar um novo indicador.
4. Preencha os campos.

Formulário Indicador de mapa de árvore

Campo	Descrição
Nome	O nome exibido para o indicador na lista **Indicadores** no painel de impacto do serviço.
Descrição resumida	Uma descrição que é exibida para o indicador na lista **Indicadores** acima do mapa de árvore.
Limite do resultado	O número máximo de resultados permitidos. O limite superior é 100.
Precisão do resultado	O número de dígitos a serem exibidos após o ponto decimal. Este campo é exibido somente para a definição de mapa de árvore em tempo real.
Ativo	Caixa de seleção para ativar este indicador.
Categoria	O nome da categoria inserido na tela anterior.
Direção	Indica se o bloco no mapa de árvore está minimizado ou maximizado. Este campo é exibido somente para a definição de mapa de árvore em tempo real.
Unidade	A unidade de medida a ser usada para a métrica. Este campo é exibido somente para a definição em tempo real.
Intervalo de atualização automática	Com que frequência atualizar o mapa de árvore.
Pedido	A ordem em que o indicador aparece na lista **Indicadores** acima do mapa de árvore.

5. Clique na guia **Configuração de fonte de dados** e configure uma das seguintes opções de fonte de dados para o indicador.

6. Clique na guia **Clique** de referência e especifique como as listas de incidentes de segurança são abertas no mapa de árvore.
   a. No campo **Clique no tipo de navegação de URL**, selecione se você deseja que a lista de incidentes de segurança seja aberta em uma nova janela, na mesma janela ou em uma caixa de diálogo.
   b. **Opcional:** No campo **Clique no script de URL**, modifique o script de exemplo, se necessário.
7. Clique em **Enviar** ou **Atualizar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionar gráficos de significância da vulnerabilidade a uma visão geral

Se o plug-in Vulnerability Response estiver ativado, você poderá adicionar gráficos de definição de significância de vulnerabilidade e outras visualizações à Visão geral.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegue até a página Visão geral à qual você deseja adicionar o medidor de significância da vulnerabilidade.
2. Clique em **Adicionar conteúdo** no canto superior esquerdo da página para abrir o controle de seleção de widget.
3. Nas três caixas de seleção, faça as seleções dependendo do medidor (mapa de árvore ou relatório de pontuação) que você deseja adicionar:
   - Para adicionar o mapa de árvore de significância da vulnerabilidade, faça estas seleções:
     - Mapa de Árvore
     - Significância da vulnerabilidade
     - Significância da vulnerabilidade
   - Para adicionar o relatório de pontuação de significância da vulnerabilidade, faça estas seleções:
     - Performance Analytics
     - Pontuação
     - Serviços com significância de vulnerabilidade
4. Clique no local na tela que você deseja adicionar o medidor.
5. Feche a caixa **Adicionar conteúdo**.

Gestão de incidentes graves de segurança

A aplicação ServiceNow® Gestão de incidentes graves de segurança rastreia o andamento de Incidente de segurança grave (MSI) desde a descoberta até a análise, propõe, promove e vincula incidentes de segurança e fechamento.

Gestão de incidentes graves de segurança

Explorar	Configurar	Integrar
Saiba mais sobre como analistas, administradores e gerentes usam o Gerenciamento de incidentes de segurança graves (MSIM)	Planejar e configurar sua implementação	Estenda as capacidades do MSIM integrando-as a outras aplicações Microsoft

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Administrar	Usar	Relatórios de Status
Tarefas de administração sobre como marcar registros de incidentes e configurar rótulos	Proponha, promova, vincule e rejeite registros de incidentes de segurança graves por meio da gestão de espaço	Monitorar tarefas relacionadas a incidentes e melhorar processos por meio de métricas, gráficos de tendências e relatórios
Capacidades adicionais		
Configurar informações para acumular registros		

Solicitar apps na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Solicitar um aplicativo Security Operations na Store

Se você é um novo cliente [Security Operations em Rome ou mais tarde, visite o ServiceNow Store site para exibir os aplicativos disponíveis e informações sobre como enviar solicitações para a loja.

Mais recursos

Visite o Gestão de incidentes graves de segurança fórum no ServiceNow Community.

Como explorar o Gerenciamento de incidentes de segurança graves

Explore Gestão de incidentes graves de segurança para entender como o aplicativo funciona em termos de acompanhamento de incidentes de segurança críticos de alta prioridade, que são identificados como uma ameaça para a organização.

Use esta seção para conhecer os principais recursos e várias funções envolvidas no trabalho com registros de incidentes de segurança graves. Esta seção também ajuda a entender como começar a usar a aplicação, os pré-requisitos e os plug-ins necessários para trabalhar com a aplicação.

Gestão de incidentes graves de segurança

Rastreie e gerencie várias atividades que normalmente fazem parte da resolução de um incidente de segurança grave por meio de Gestão de incidentes graves de segurança. Por meio de um espaço de trabalho intuitivo, os gerentes de incidentes e aqueles que trabalham em um incidente podem propor e promover incidentes a incidentes graves, rastrear atividades de incidentes de segurança graves e colaborar facilmente com colegas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

Os principais recursos de gerenciamento de incidentes de segurança funcionam em conjunto com os recursos de produto de resposta a incidentes de segurança existentes. Isso inclui a capacidade de um analista de segurança escalar um incidente de segurança padrão para um incidente de segurança grave, para que os novos recursos do produto estejam disponíveis para oferecer suporte ao processo de correção.

Depois de instalar em sua instância ServiceNow, um analista de incidente de segurança pode:

- Propor um incidente de segurança ao candidato a incidente de segurança grave para iniciar um processo de revisão sobre a necessidade de criar um incidente de segurança grave.
- Promova diretamente um incidente de segurança a um incidente de segurança grave sem a necessidade de um processo de revisão adicional.
- Rejeite um incidente de segurança que é proposto como um incidente de segurança grave (MSI).
- Vincule um incidente de segurança como um incidente secundário ao incidente de segurança grave (MSI) para que todos os incidentes de segurança possam ser trabalhados.

Principais recursos

O Gerenciamento de incidentes de segurança graves (MSIM) melhora o processo de correção de incidentes de segurança graves com os seguintes recursos:

- Espaço dedicado para gerenciar incidentes de segurança graves projetados para a função de usuário de gerenciador de incidentes de segurança graves.
- Organize tarefas de resposta em vários incidentes de segurança "secundários".
- Automatize a criação de pastas de colaboração e canais de comunicação de bate-papo após a criação de um incidente de segurança grave, bem como o arquivamento como parte do fechamento do incidente.
- Componente do explorador de arquivos para organizar e rastrear a coleção de artefatos (arquivos) relacionados ao incidente de segurança grave por meio de uma integração Microsoft SharePoint.
- Gerenciador de canal de bate-papo e componentes do fluxo de atividades para gerenciar as comunicações em vários grupos funcionais, de segurança e de TI por meio de uma integração Microsoft Teams.

Componentes do espaço

O produto Gestão de incidentes graves de segurança contém vários novos componentes de espaço e páginas de interface do usuário que oferecem a funcionalidade de recursos principais:

- Espaço dedicado para gerenciar incidentes de segurança graves projetados especificamente para a função de usuário Gerenciador de incidentes de segurança graves.
- Organize tarefas de resposta em vários incidentes de segurança secundários.
- Automatize a criação de pastas de colaboração e canais de comunicação de bate-papo após a criação de um incidente de segurança grave, bem como o arquivamento como parte do fechamento do incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Componente do explorador de arquivos para organizar e rastrear a coleção de artefatos (arquivos) relacionados ao incidente de segurança grave por meio de uma integração Microsoft SharePoint.
- Gerenciador de canal de bate-papo e componentes do fluxo de atividades para gerenciar as comunicações em vários grupos funcionais, de segurança e de TI por meio de uma integração Microsoft Teams.

Versões compatíveis do Gerenciamento de incidentes de segurança graves

Gestão de incidentes graves de segurança (MSIM) requer a versão Now Platform® Rome.

Este recurso é compatível com Microsoft Teams, que é um espaço de bate-papo no pacote Microsoft Office 365. Anteriormente Microsoft Teams, era uma instalação separada das aplicações Microsoft Office 365.

Now Platform Versões compatíveis

Este recurso é compatível com Rome e versões posteriores.

As aplicações Security Operations a seguir são os plug-ins Security Incident Response padrão que provavelmente serão instalados para a maioria dos usuários se eles já estiverem usando Security Incident Response (SIR). Se não estiver instalado, você deverá instalar e ativar a partir de ServiceNow Store. Instale e ative um aplicativo de cada vez na ordem mencionada para garantir uma instalação sem problemas:

1. Security Incident Response: com.snc.si_dep é o plug-in dependente. A instalação deste plug-in ativa os outros aplicativos do Security Operations.
2. Security Integration Framework
3. Security Support Common
4. Security Support Common Orchestration

Para começar com MSIM

Revise as informações a seguir antes de começar a trabalhar com Gestão de incidentes graves de segurança.

Função necessária: sn_msi.workspace_admin.

Para uma fácil instalação e configuração da aplicação Gestão de incidentes graves de segurança, talvez você precise verificar se os plug-ins a seguir estão ativados.

Importante:
Um conjunto de atualizações (KB1289784) está disponível no Guia de início rápido do Gerenciamento de incidentes de segurança graves para ajudar os usuários com uma configuração fácil. Você precisa importar o conjunto de atualizações depois de concluir a instalação da aplicação. Siga o procedimento detalhado no Guia de Início Rápido (Etapa 2) na seção Documentos de suporte na aplicação MSIM, que está na ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pré-requisito

Tarefa	Descrição
Antes de começar a usar a aplicação, certifique-se de ter os plug-ins dependentes necessários.	Como primeira etapa, instale: • ServiceNow IntegrationHub Installer (com.glide.hub.integrations) • ServiceNow® IntegrationHub Tempo de execução (com.glide.hub.integration.runtime). • ServiceNow® IntegrationHub Etapa de ação - REST (com.glide.hub.action_step.rest) • ServiceNow® IntegrationHub Modelo de ação - Fluxo de dados (com.glide.hub.action_type.datastream) • ServiceNow® IntegrationHub Flow Designer - Entradas dinâmicas (com.glide.hub.dynamic_inputs) **Nota:** Se você não tiver os privilégios necessários para qualquer um dos plug-ins ServiceNow® IntegrationHub listados, crie um tíquete de suporte para instalar esses aplicativos de pré-requisito.
Verifique se você tem o acesso necessário para instalar o Microsoft SharePoint Spoke e o Microsoft Teams Graph Spoke. **Nota:** As listadas acima são as principais aplicações dependentes para começar com Gestão de incidentes graves de segurança.	Antes de instalar o Microsoft SharePoint Spoke e o Microsoft Teams Graph Spoke, certifique-se de ter o acesso necessário às aplicações ServiceNow IntegrationHub. **Nota:** Microsoft SharePoint Spoke e Microsoft Teams Graph spoke são aplicações dependentes de aplicações ServiceNow® IntegrationHub.

Check-list para configuração de MSIM

Antes de usar a aplicação ServiceNow® Gestão de incidentes graves de segurança (MSIM), baixe a aplicação do ServiceNow® Store.

Acompanhe seu progresso com a instalação e a configuração na tabela a seguir.

Nota: As funções atribuídas à aplicação Gestão de incidentes graves de segurança estão listadas nas seções a seguir. Para obter mais informações, consulte Funções Gestão de incidentes graves de segurança.

Use a check-list a seguir para guiá-lo pelas etapas de ponta a ponta para instalar e configurar a aplicação Gestão de incidentes graves de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Verifique se a aplicação Gestão de incidentes graves de segurança está instalada e ativada em ServiceNow® Store.	Gestão de incidentes graves de segurança v1.1.1 está disponível em ServiceNow® Store. Siga estas instruções: download de uma aplicação do ServiceNow Store.
Verifique se as seguintes aplicações estão instaladas na ordem fornecida.	As aplicações a seguir serão instaladas por padrão após a instalação da aplicação Gestão de incidentes graves de segurança na versão atual da aplicação: • File Explorer Core para Security Operations v1.1.1 • Microsoft SharePoint File Explorer Conector para Security Operations v1.1.1 • File Explorer Componente para Security Operations v1.0.0 • Microsoft Teams Conector de bate-papo para Security Operations v1.0.0 • Bate-papo principal para Security Operations v1.0.0 • Incidente de segurança grave Resposta v1.1.1 • Cartão EVAM do Collab Chat para MSIM espaço v1.0.0 (esta aplicação é configurada somente para as visualizações de IU no plano de fundo da aplicação para Gestão de incidentes graves de segurança espaço) • Componente de IU do organizador de tarefas para o espaço Gestão de incidentes graves de segurança 1.0.0 • Security Incident Response v12.8.1
Verifique se as funções de usuário foram atribuídas a Incidente de segurança grave, conforme apropriado.	A seguir estão as funções envolvidas em todo o ciclo de vida do incidente do Incidente de segurança grave processo de correção: • Administrador do MSI [sn_msi.workspace_admin] • Gerente do MSI [sn_msi.workspace_manager] • Respondente do MSI [sn_msi.workspace_responder] Para obter informações mais detalhadas sobre cada função, consulte Funções Gestão de incidentes graves de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Verifique se você definiu com êxito a configuração Microsoft SharePoint v1.0.0.	Microsoft SharePoint gerencia sites, pastas, arquivos, grupos e usuários em Microsoft SharePoint. Adicione dados Microsoft SharePoint à sua instância ServiceNow®. Para fazer isso, você deve ter que configurar as conexões de Gráfico e REST. Para obter informações, consulte a documentação doMicrosoft SharePoint spoke v1.1.2 sobre como definir a configuração de conexões REST e do Graph. Estabeleça uma conexão Graph e REST para se conectar à sua instância [ServiceNow® de Microsoft SharePoint.
Verifique se você criou um site Microsoft SharePoint para criar uma biblioteca de documentos.	Crie um site Microsoft SharePoint, se necessário, ou você pode usar um site existente para criar nossa biblioteca de documentos.
Verifique se você criou uma biblioteca de documentos no site Microsoft SharePoint.	Crie uma biblioteca de documentos dedicada em um site Microsoft SharePoint novo ou existente.
Verifique se as permissões necessárias foram fornecidas aos usuários e atribuídas aos grupos de usuários necessários no Microsoft SharePoint.	Gerencie o acesso do site Microsoft SharePoint a diferentes usuários e grupos de usuários.
Verifique se você criou e configurou a unidade Microsoft SharePoint e as configurações necessárias.	Para verificar as configurações da unidade, configure o Microsoft SharePoint Conector do Explorador de Arquivos, Ações de Pasta e Arquivo e Modelos de Pasta: • Configurar Unidade do Repositório do Explorador de Arquivos: cria conexão da instância Microsoft SharePoint para ServiceNow®. • Definir configurações de ação de pasta e arquivo: configure e controle as ações individuais de pasta e arquivo exibidas no componente do explorador de arquivos. • Criar modelos de pasta: configure para criar pastas exclusivas para diferentes tipos de incidentes de segurança graves.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Verifique se você estabeleceu com sucesso uma conexão com a aplicação Conector de bate-papo do Microsoft Teams.	Para estabelecer a conexão da aplicação Conector de bate-papo do Microsoft Teams com a instância ServiceNow®, siga o procedimento explicado aqui: Estabelecer conexão de gráfico do MS Teams em Now Platform.
Verifique se você configurou o Microsoft Teams com a instância Now Platform® e criou conexões e configurações de credenciais.	Para verificar a configuração [Microsoft Teams com a instância ServiceNow®, siga o procedimento conforme explicado aqui: • Estabelecer conexão de gráfico do MS Teams em Now Platform • Criar um modelo de canal de bate-papo
Verifique se as definições de Administração de incidente de segurança grave - Configuração foram bem-sucedidas.	Como Administrador do MSI, você deve ser capaz de: • determinar se os analistas de segurança podem propor e promover o incidente e vincular outros incidentes de segurança. • habilite ou desabilite as notificações quando um incidente for proposto ou promovido. Capacidade de editar mensagens de modelo padrão. • configure marcadores de segurança que aparecem na interface do analista de segurança para diferenciar os incidentes que foram propostos como candidatos a incidentes de segurança graves ou promovidos a incidentes de segurança graves.
Verifique se as configurações de Administração de incidente de segurança grave - Notificações foram bem-sucedidas.	Como administrador do MSI, acione notificações por e-mail quando um incidente de segurança for proposto e enviado para todos os usuários e grupos que estão configurados para a lista de notificações. Para obter mais informações, consulte Definir preferências de notificação para MSIM.

Funções Gestão de incidentes graves de segurança

Atribua funções para garantir que os usuários possam executar todas as ações necessárias na aplicação MSIM.

Funções para Gestão de incidentes graves

Tipo de Função	Função	Descrição
Administrador do MSI	sn_msi.workspace_admin	Posso instalar e configurar Gestão de incidentes graves e definir as aplicações dependentes, como

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções para Gestão de incidentes graves

Tipo de Função	Função	Descrição
		File Explorer (FE), a configuração do Microsoft Teams e do canal de bate-papo, a configuração do espaço e a configuração da Administração do MSI: configurações e notificações. Como configurar: • Componente do Explorador de Arquivos (FE): ◦ Configure o repositório de arquivos. ◦ Configure as ações de arquivo e pasta, que são fornecidas no componente do File Explorer da guia Colaboração no espaço do Major Security Incident Management. ◦ Crie as pastas raiz e as subpastas e forneça acesso às subpastas. • Gestão de canal de bate-papo ◦ Ative e configure Microsoft Teams validando a conexão Microsoft Teams. ◦ Crie equipes de bate-papo e canais de bate-papo, além de adicionar usuários e atribuir usuários a vários grupos de usuários. • Administração do MSI: ◦ Configurações: configure as ações dos analistas de segurança, as notificações enviadas quando os incidentes são propostos e promovidos e exiba marcadores para os incidentes de segurança. ◦ Notificações: automatize o processo de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções para Gestão de incidentes graves

Tipo de Função	Função	Descrição
		notificação por e-mail e as notificações do usuário quando um incidente de segurança for proposto ou promovido como um incidente de segurança grave.
Gerenciador do MSI	sn_msi.workspace_manager	• Exiba o acesso à página de definições de configuração de gestão de incidentes de segurança graves. Restringido de modificar qualquer uma das definições de configuração. • Exiba e edite dados de registro de incidente nas guias **Detalhes**, **Colaboração**e **Organizador de tarefas** do espaço Gestão de incidentes graves. • Promova o incidente de segurança a um incidente de segurança grave. • Configure as ações de arquivos e pastas disponíveis no componente do Explorador de Arquivos na guia **Colaboração** do espaço Gestão de incidentes graves. • Vincular e desvincular registros adicionais de incidentes de segurança graves do espaço.
Respondente do MSI	sn_msi.workspace_responder	• Exibir e editar acesso (somente) a **Detalhes** e **Tarefas** guias do espaço Gestão de incidentes graves. • Vincular e desvincular registros adicionais de incidentes de segurança graves do espaço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrar Gestão de incidentes graves de segurança

Estenda os recursos de Gestão de incidentes graves de segurança e conecte-se com a instância Now Platform integrando-se às aplicações Microsoft.

Importante:
Um conjunto de atualizações (KB1289784) está disponível no Guia de início rápido do Gerenciamento de incidentes de segurança graves para ajudar os usuários com uma configuração fácil. Você precisa importar o conjunto de atualizações depois de concluir a instalação da aplicação. Siga o procedimento detalhado no Guia de Início Rápido (Etapa 2) na seção Documentos de suporte na aplicação MSIM, que está na ServiceNow Store.

Configurar Microsoft SharePoint Biblioteca de Documentos

Revise a configuração necessária que precisa ser feita no Microsoft SharePoint.

Antes de Iniciar

Verifique se o procedimento de configuração a seguir foi concluído.

Função necessária: administrador do sistema, sn_msi.workspace_admin

Procedimento

1. Crie uma nova biblioteca de documentos em um site Microsoft SharePoint novo ou existente e use esse mesmo site ao definir a configuração do repositório de arquivos Gestão de incidentes graves de segurança.
2. Registre uma aplicação com Microsoft para estabelecer uma conexão e se comunicar com Microsoft SharePoint usando a Microsoft SharePoint REST API.
   O registro da aplicação estabelece uma conexão entre a aplicação e a Microsoft. Para obter mais informações, consulte Configurar o acesso somente de aplicação ao SharePoint no portal docs.microsoft.com.

   Existem duas maneiras de registrar uma aplicação com Microsoft SharePoint:

   a. Conceder acesso via app somente do Azure AD

   b. Concedendo acesso usando Microsoft SharePoint Somente app

   Importante:
   Conceder acesso usando o app Microsoft SharePoint somente é uma abordagem legada, mas muito relevante e fácil de configurar.

   Use o ID do cliente e o segredo do cliente gerados na etapa acima ao configurar a conexão REST para o conector do explorador de arquivos Microsoft SharePoint.
3. Registre mais uma aplicação com Microsoft para se comunicar com Microsoft SharePoint usando as Microsoft Graph APIs.
   Para obter mais informações, consulte Registrar uma aplicação com a plataforma de identidade da Microsoft. **Registrar uma nova aplicação no Azure com a instância da Now Platform**

   a. Entre no portal do Azure usando sua conta Microsoft.

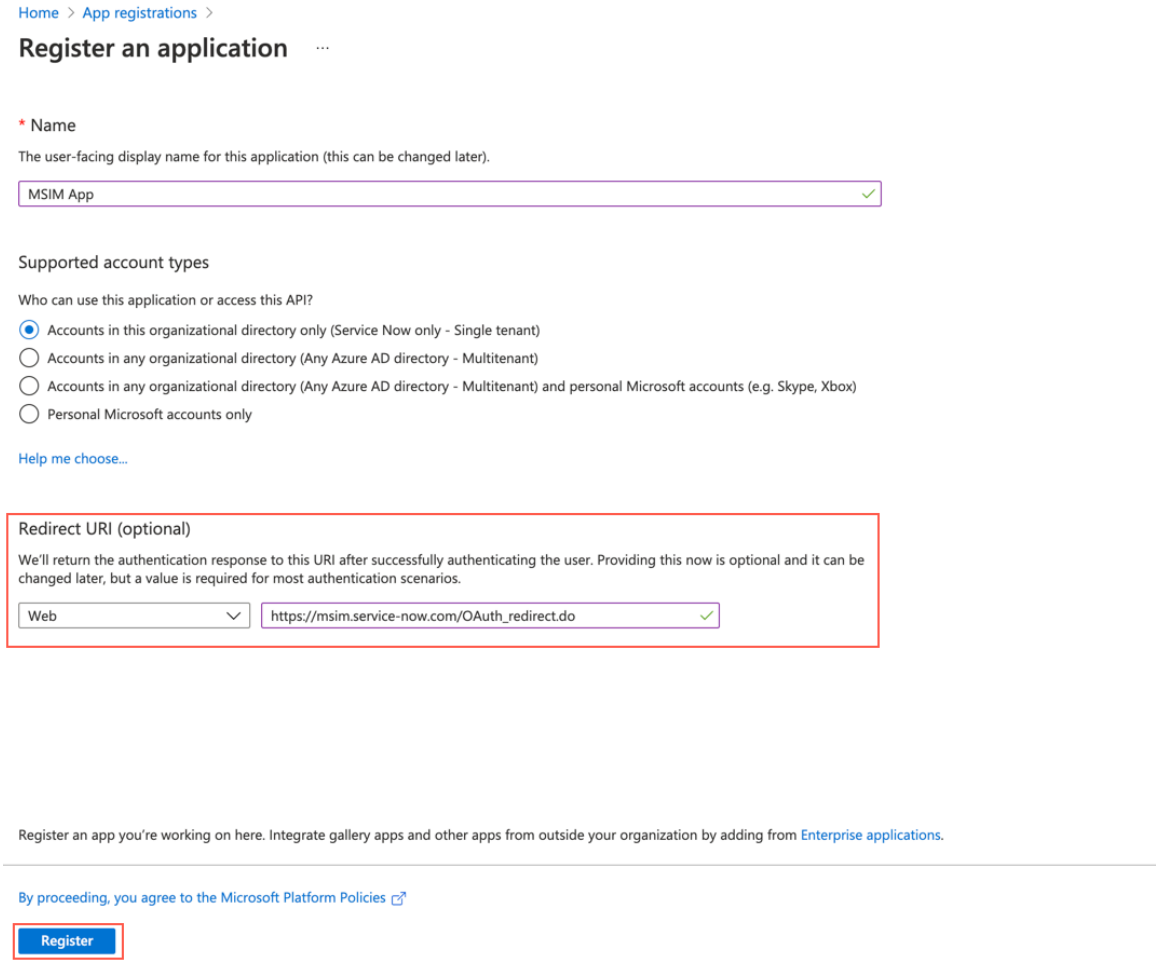
   b. Siga as instruções descritas no portal da Microsoft.

   c. Forneça Now Platform® URL de redirecionamento da instância no campo URL de redirecionamento permitido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, msim.service-now.com/OAuth_redirect.do



d. **Registrar** a aplicação.

e. Navegue até a seção **Certificados e segredos** e crie um novo segredo do cliente.

> **Nota:**
> Você também pode carregar um certificado de cliente e copiar e armazenar o valor de impressão digital gerado.

f. Copie e armazene o segredo do cliente gerado em algum lugar, pois ele é necessário ao configurar o registro da aplicação OAuth na instância ServiceNow®.

4. Em **Permissões de API**, adicione a permissão do Microsoft Graph:

a. Clique **em Adicionar uma permissão**.

b. Selecione **Microsoft Graph**.

c. Selecione **Permissões delegadas**.

d. Na lista **Sites**, selecione a permissão **Sites.ReadWrite.All**.

e. Na lista **Usuário**, selecione **Usuário**. Permissão de leitura.

f. Clique **em Adicionar permissões**.

5. Em **Permissões de API**, adicione a permissão do SharePoint:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Clique **em Adicionar uma permissão**.

b. Selecione **SharePoint**.

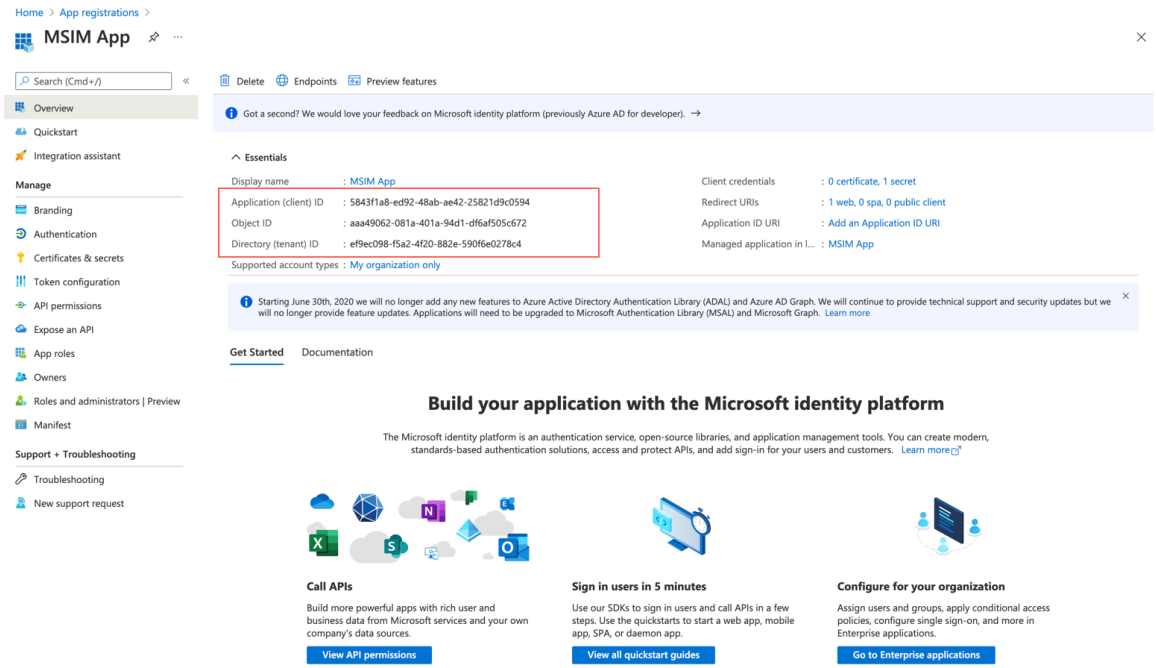
c. Selecione **Permissões da aplicação**.

d. Na lista **Sites**, selecione a permissão **Sites.FullControl.All**.

e. Clique **em Adicionar permissões**.

6. Depois de adicionar permissões, clique em **Conceder consentimento do administrador**.

7. Use os mesmos valores de ID de cliente e segredo do cliente gerados a partir deste registro de aplicação (que está disponível na seção Visão geral) ao configurar a Conexão do Graph para o conector do File Explorer Microsoft Teams.



Estabelecer Conexões de Gráfico e REST em Now Platform

Configure as conexões Graph e REST na instância Now Platform para se comunicar com Microsoft SharePoint.

Integre a instância [Now Platform e Microsoft SharePoint criando uma aplicação OAuth personalizada em Microsoft SharePoint para autenticar solicitações da Now Platform.

Configurar conexão REST para MS SharePoint

Configure a conexão REST na instância Now Platform para se comunicar com Microsoft SharePoint.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Configure um novo registro de locatário e selecione **MicrosoftSharepointOnline** como o registro de alias.
   Para obter mais informações, consulte Definir locatários do Microsoft SharePoint.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Para configurar o alias de conexão e credencial do **MicrosoftSharepointOnline**, .
3. Selecione o registro de locatário criado na etapa 2 acima como: **Conexão REST** ao preencher o formulário de **Configuração do repositório de arquivos**.

Configurar Graph Connection for MS SharePoint

Configure a conexão do Graph na instância Now Platform para se comunicar com Microsoft SharePoint.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Para configurar a conexão do gráfico e o alias de credencial usando o segredo do cliente, consulte .
   Siga as etapas abaixo para configurar a conexão do gráfico e o alias de credencial usando o certificado do cliente.

   Nota:
   Por padrão, o Provedor JWT, a Chave JWT e o Certificado, que está configurado na conexão REST anterior, serão usados aqui neste procedimento. Para obter mais informações, consulte Configurar conexão REST para MS SharePoint.

   a. Navegar até **Todos** > **Conexões e Credenciais** > **Aliases de conexões e credenciais**.

   b. Abra o registro, **MicrosoftSharePointGraph**.

   c. Clique no link relacionado **Criar nova conexão e credencial**.

   d. No formulário, preencha estes detalhes.

Campo	Descrição
Nome da entidade OAuth	Nome para identificar o registro da aplicação OAuth.
ID do cliente OAuth	ID de cliente
Segredo do cliente OAuth	Você pode inserir qualquer valor. **Nota:** Isso não é importante, pois você usará a autenticação baseada em certificado.
URL de autorização do OAuth	URL de autorização neste formato: `https://login.microsoftonline.com/`<tenant-id> `/oauth2/v2.0/authorize?response_mode=query`
URL do token Oauth	URL do token neste formato: `https://login.microsoftonline.com/`<tenant-id> `/oauth2/v2.0/token`
URL de revogação do token	URL de revogação de token neste formato: `https://login.microsoftonline.com/`<tenant-id> `/oauth2/v2.0/token` .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
URL de redirecionamento do OAuth	ServiceNow URL de redirecionamento neste formato: https://empipaas.service-now.com/oauth_redirect.do

Nota:
Você pode alterar os valores padrão de acordo com seus requisitos.

e. Clique em **Criar e obter token do OAuth**.
Uma mensagem de erro será exibida solicitando 401- não autorizado.

f. Recarregue o formulário e abra o registro na lista relacionada **Conexões**.

g. Insira o valor de **impressão digital** codificado em Base64 no atributo **Valor** de impressão digital codificado na seção **Atributos**.

Nota:
O valor de **impressão digital** é um valor hexadecimal. Você pode usar uma ferramenta de conversão de Hexadecimal para Base64 (Hex para Base64) para codificar o valor de **Impressão digital** para um valor Base64.

h. Navegar até **Sistema Oauth** > **Registro de aplicações**.

i. Abra o registro que tem o mesmo nome de **Nome da entidade OAuth**, que é a etapa d neste mesmo procedimento.

j. Modifique o script da API do OAuth para: **OAuthUtilJWTFESPGraph**

k. Navegar até **Conexões e Credenciais** > **Credenciais**.

l. Abra o registro: **Credencial do Microsoft SharePoint Graph**.

m. Clique em **Obter token OAuth** na seção Links relacionados.

2. Atualize o escopo da entidade OAuth.

a. Navegar até **Sistema Oauth** > **Registro de aplicações**.

b. Abra o registro da aplicação OAuth gerado na Etapa 1.

c. Selecione a lista relacionada **Escopos de entidade OAuth**.

d. Substitua o campo **Escopo do OAuth** pelo seguinte valor **offline_access** :

```
https://graph.microsoft.com/Sites.ReadWrite.All
```

Nota:
Você pode ignorar a etapa 2 e passar para a próxima etapa se estiver adicionando um certificado de cliente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Configure um novo registro de locatário e selecione o registro de alias conforme criado na Etapa 1. Para obter mais informações, consulte Definir locatários do Microsoft SharePoint.
4. Selecione o registro de locatário criado na etapa 3 como: **Conexão do Graph** ao preencher o formulário de Configuração do repositório de arquivos.

Estabelecer conexão de gráfico do MS Teams em Now Platform

Integre a instância Microsoft TeamsNow Platform e a conta [] estabelecendo uma conexão Microsoft Teams Graph.

Antes de Iniciar

Se desejar, você pode usar a mesma aplicação que criou para o SharePoint para estabelecer a conexão do Microsoft Teams Graph.

Função necessária: administrador, administrador do Azure

Registrar uma nova aplicação no Azure para conexão do gráfico do Microsoft Teams

Procedimento

1. Entre no portal do Azure usando sua conta Microsoft.
2. Navegar até **Serviços do Azure** > **Registro da aplicação** > **Novo registro**.
3. Insira o nome da aplicação.
   Por exemplo, Microsoft Teams Graph.
4. Selecione a respectiva opção de **tipos de conta compatível** que for aplicável à sua organização.
   Por exemplo, selecione a opção **Contas somente neste diretório organizacional (somente Service Now - locatário único)**.

   Nota:
   Para obter informações sobre os tipos de conta compatíveis, consulte Registrar uma aplicação com a plataforma Microsoft Identity .
5. Selecione o tipo de **Web** na lista suspensa em Redirecionar URL.
6. Insira Now Platform URL de redirecionamento de instância no campo URL de redirecionamento permitido.
   Por exemplo, https://<<InstanceName> >.service-now.com/oauth_redirect.do
7. Clique **em Registrar** para registrar sua nova aplicação e certifique-se de que a página seja exibida com a seção **Visão geral**.

Uso de certificados para autenticação

Solicite um token de acesso com uma credencial de certificado.

Antes de Iniciar

1. Você pode usar um certificado autoassinado ou um certificado emitido pela CA. Você pode criar um certificado autoassinado executando o script do PowerShell conforme descrito emConfiguração de uma aplicação do Azure AD para acesso somente à aplicação . O script gera dois arquivos: arquivo .PFX e arquivo .CER.

   Nota:
   Certifique-se de estar ciente da senha usada para criptografar a chave privada para gerar o arquivo .PFX e o arquivo .CER.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Use o arquivo .PFX para criar um arquivo Java Key Store (JKS).

Nota:
Certifique-se de estar ciente da senha usada para gerar o arquivo JKS a partir do arquivo .PFX.

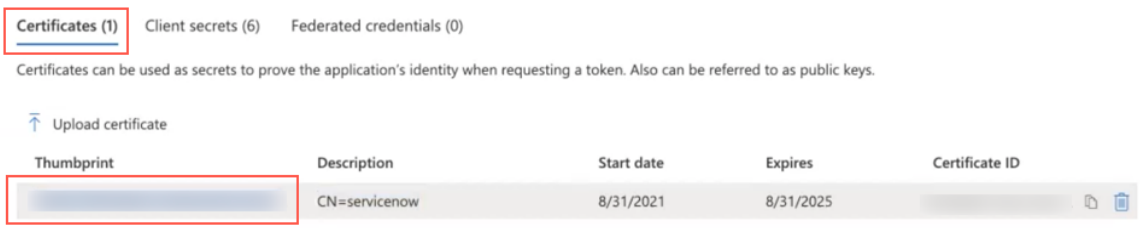
Função necessária: administrador

Procedimento

1. Navegue até **Registros do aplicativo** no portal do Azure AD.
2. Clique em **Certificados e segredos** na seção **Gerenciar**.
3. Na guia **Certificados**, clique em **Carregar certificado**.
4. No formulário, preencha estes valores.

Campo	Descrição
Carregue um certificado (chave pública) com um dos seguintes tipos de arquivo: .cer, .pem, .crt	Arquivo .CER que você gerou usando o script do PowerShell.
Descrição	Descrição do certificado.

5. Clique em **Adicionar**.
   O certificado é carregado e seus detalhes são exibidos na guia **Certificados**.
6. Copie o valor de **impressão digital** do certificado carregado.
   O valor de **impressão digital** é um valor hexadecimal.



7. Codifique o valor de **impressão digital** para um valor Base64 e registre o valor para uso posterior.

Nota:
Você pode usar uma ferramenta de conversão de hexadecimal para Base64 (Hex para Base64) para codificar o valor de **impressão digital** para um valor Base64.

Anexar um certificado Java Key Store para MS Teams

Habilite a autenticação de token de Concessão do Portador JWT anexando um certificado Java Key Store (JKS) válido.

Antes de Iniciar

Faça login na sua instância da ServiceNow para executar o procedimento a seguir.

- Certificado de armazenamento de chaves Java válido
- Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Definição do Sistema** > **Certificados**.
2. Abra o registro **Certificado do conector do Microsoft Teams**.
   Certifique-se de usar somente **o certificado do conector do Microsoft Teams** de registro padrão.
3. Insira a senha associada ao arquivo JKS em Senha do **armazenamento de chaves**.
4. Clique no ícone de anexos (ícone de) e anexe o certificado JKS que você gerou.
   Para obter mais informações, consulte .
5. Clique **em Validar armazenamentos/certificados**.
6. Clique em **Atualizar**.

Configurar a chave de assinatura JWT para MS Teams

Crie uma chave de assinatura JSON Web Token (JWT) para atribuir ao seu certificado Java Key Store.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **OAuth de Sistema** > **Chaves de JWT**.
2. Abra o registro **JWT do Conector do Microsoft Teams**.
3. Insira a senha usada para criptografar a chave privada para gerar o arquivo .PFX e o arquivo .CER em **Senha da chave de assinatura**.
4. Clique em **Atualizar**.

Configurar o provedor JWT para MS Teams

Adicione um provedor JSON Web Token (JWT) à sua instância da ServiceNow.

Antes de Iniciar

- Copie e registre o valor do ID da **aplicação (cliente) e do IDdo diretório (locatário)** da aplicação que você registrou no portal do Azure.

- Função necessária: administrador

Procedimento

1. Navegar até **OAuth de Sistema** > **Provedores JWT**.
2. Abra o registro do **Provedor JWT do conector do MS Teams**.
3. Insira valores para **iss**, **sub**e **aud** na lista relacionada Declarações padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Valor
aud	URL do Microsoft Online neste formato: https://login.microsoftonline.com/<tenant-id> /oauth2/token . Substituir<tenant-id> com o valor do ID do diretório (locatário) da sua aplicação registrado no portal do Azure.
iss	**ID da aplicação (cliente)** da aplicação que você registrou no portal do Azure.
sub	**ID da aplicação (cliente)** da aplicação que você registrou no portal do Azure.

4. Clique em **Atualizar**.

Estabelecer uma conexão usando certificados

Estabeleça uma conexão entre a aplicação de gráfico Microsoft Teams recém-criada usando certificados.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Conexões e Credenciais** > **Aliases de conexões e credenciais**.
2. Abra **o Microsoft Teams Spoke**.
3. Modifique o valor do campo **Modelo de configuração: MSIM Microsoft Teams ConnectorAuthorization Code Template** e salve o formulário.

   Nota:
   Este modelo contém a permissão de API delegada necessária para a integração do MSTeams.

4. Na seção Links relacionados, clique em Criar **nova conexão e credencial**.
5. Clique **em Criar e obter token Oauth**.
   Uma mensagem de erro será exibida solicitando 401- não autorizado.
6. Recarregue o formulário e abra o registro na lista relacionada Conexões.
7. Insira o valor de **Impressão digital** codificada em Base64 no atributo **Impressão digital do certificado codificado** na seção **Atributos**.

   Nota:
   O valor de impressão digital é um valor hexadecimal. Você pode usar uma ferramenta de conversão de Hexadecimal para Base64 (Hex para Base64) para codificar o valor de Impressão digital para um valor Base64.

8. Navegar até **OAuth de Sistema** > **Registro de aplicações**
9. Abra o registro **do código de autorização do conector MSIM do Microsoft Teams**.
10. Modifique o Script da API do OAuth: **OAuthUtilJWTMSTeamsConnector**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

11. Navegar até **Conexões e Credenciais** > **Credenciais**.
12. Abra o registro **Credencial do conector MSIM do Microsoft Teams**.
13. Em Links relacionados, clique em **Obter token OAuth**.
    Em caso de sucesso, as seguintes permissões de API são adicionadas à aplicação Azure.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

Usando o valor do segredo do cliente

Use o valor de segredo do cliente para configurar o registro da aplicação Graph.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegue até **Registros do aplicativo** no portal do Azure AD.
2. Clique em **Certificados e segredos** na seção **Gerenciar**.
3. Clique **em Novo segredo do cliente**.
4. Copie e anote o segredo do cliente criado no campo **Valor**.

Estabelecer uma conexão usando o segredo do cliente

Estabeleça uma conexão entre a aplicação de gráfico Microsoft Teams recém-criada com a instância Now Platform.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Conexões e Credenciais** > **Aliases de conexões e credenciais**.
2. Abra **o Microsoft Teams Spoke**.
3. Modifique o valor do campo **Modelo de configuração: MSIM Microsoft Teams ConnectorAuthorization Code Template** e salve o formulário.

Nota:
Este modelo contém a permissão de API delegada necessária para a integração do MSTeams.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Na seção Links relacionados, clique em Criar **nova conexão e credencial**.

5. Clique **em Criar e obter token Oauth**.
   Em caso de sucesso, as seguintes permissões de API são adicionadas à aplicação Azure.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

Ativar o conector de bate-papo do MS Teams para o usuário do MS Teams Graph Spoke

Se você for um usuário existente, siga o procedimento nesta seção para ativar o conector de bate-papo do Microsoft Teams.

Antes de Iniciar

Função necessária: administrador

Procedimento

Se você já é usuário do Microsoft Teams Graph Spoke, siga as etapas abaixo:

- Navegue até a aplicação registrada no portal do Azure que é usado pelo Microsoft Teams Graph Spoke.
- Navegue até a seção **Permissões de API** para configurar as permissões de API necessárias.
- Clique **em Adicionar uma permissão**.
- Selecione **Microsoft Graph**.
- Para usar a aplicação Conector do Microsoft Teams, você precisa adicionar mais duas permissões delegadas à sua aplicação no portal do Azure: "ChannelMember.ReadWrite.All" e "TeamMember.ReadWrite.All".
- Depois de adicionar as permissões necessárias acima, clique em **Conceder consentimento do administrador**.

Configure o MS Teams na instância da Now Platform para um usuário existente:

- Navegue até **Conexão e Aliases de credencial**.
- Selecione o registro do **Microsoft Teams Spoke**, conforme mostrado na imagem abaixo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Selecione o registro de credencial associado ao Microsoft Teams Spoke.
- Clique **em Obter token OAuth**. Uma mensagem de confirmação exibe que o token de atualização do OAuth está disponível.

Como usuário existente, você concluiu a integração da aplicação do conector de bate-papo do Microsoft Teams com a Graph API do Microsoft Teams.

Gestão de incidentes graves de segurança Integração de chamada em conferência

Com a integração de chamadas em conferência Gestão de incidentes graves de segurança, você pode colaborar com seus clientes e colegas de trabalho para resolver problemas do cliente usando as opções de compartilhamento de vídeo e tela em Microsoft Teams, Cisco Webexou Zoom da aplicação MSIM.

A integração de chamada em conferência Gestão de incidentes graves de segurança permite que você integre o canal de comunicação de conferência com o canal de comunicação Notify, gerenciando e iniciando uma reunião Microsoft Teams, Cisco Webexou Zoom diretamente da aplicação Gestão de incidentes graves de segurança.

Como gerente do MSI, você pode usar a integração da Chamada em conferência do MSIM para iniciar Microsoft Teams, Cisco Webex ou Zoom reuniões. Integre a Gestão de incidentes graves de segurança Chamada em conferência com os provedores de serviços de terceiros como um canal de comunicação para se reunir com as partes interessadas para resolver os principais incidentes de segurança.

Principais recursos

A integração de Chamada em conferência de gestão Incidente de segurança grave fornece os seguintes recursos principais:

- Os gerentes do MSI podem iniciar uma chamada em conferência Microsoft Teams, Cisco Webexou Zoom diretamente do incidente de segurança grave.
- Convidar participantes adicionais para a chamada.
- Exibir gravações de chamadas e detalhes do bate-papo.
- Envia convites para os participantes por e-mail e Microsoft Teams bate-papo.

Como iniciar uma chamada em conferência

Inicie uma chamada em conferência a partir de uma tarefa ou de uma segurança importante convidando um ou mais usuários para ingressar em uma chamada em conferência. A chamada em conferência será iniciada somente quando pelo menos dois participantes ingressarem.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Verifique se você fez o seguinte na instância ServiceNow® :

- Instalado e ativado o plug-in Notify (com.snc.notify).
- Instalou o app Notify Componentes de IU para espaços configuráveis.
- Instalou e ativou o plug-in Visual Task Board (com.devsnc.snb_vtb).

Para obter mais informações, consulte Solicitação de IntegrationHub .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

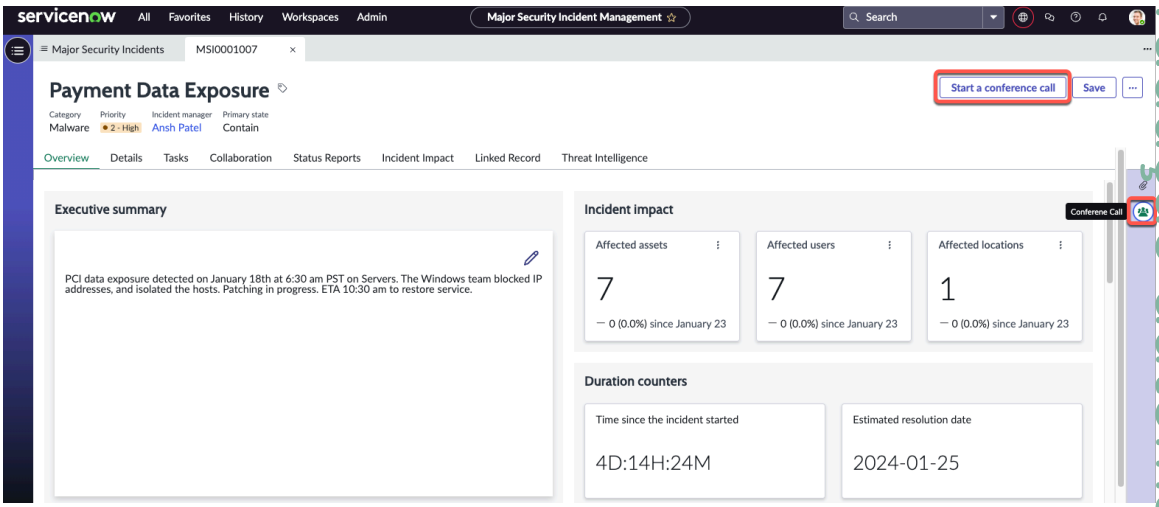
Os participantes da chamada podem incluir o seguinte:

- Usuários que receberam responsabilidades específicas.
- Contatos ad hoc ou sob demanda
- Outros contatos de terceiros

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione um incidente de segurança grave.
3. Selecione a ação **Iniciar uma chamada em conferência**.
4. Você também pode iniciar uma chamada em conferência selecionando o ícone de em conferência no menu de contexto direito e selecionando o ícone +.
   O pop-up Iniciar chamada em conferência é exibido.

Chamada em conferência do MSIM



5. No campo Ponte de conferência, escolha uma **ponte de conferência da** qual você deseja se conectar. Por exemplo, Microsoft Team, Zoom ou Cisco Webex.
6. No campo Título, forneça um título que descreva o motivo da chamada em conferência.
7. No campo Adicionar participantes, selecione os participantes da chamada em conferência.
   Você pode usar a opção de pesquisa para localizar e adicionar os participantes necessários ou selecionar os participantes na lista **Recomendações**, que fornece recomendações de participantes para adicionar à chamada em conferência.

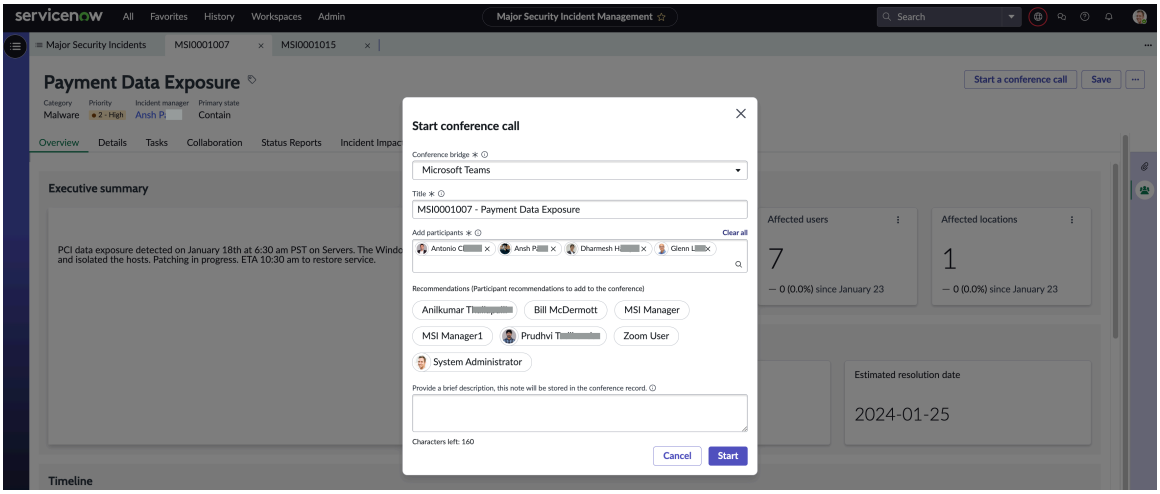
   O usuário (host) que inicia a chamada em conferência é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão na lista **Recomendações**.

Nota:
Verifique se os participantes selecionados têm um endereço de e-mail válido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como iniciar uma chamada em conferência



8. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.
   A descrição fornecida será adicionada ao registro da conferência.
9. Depois que a lista de participantes for finalizada, selecione **Iniciar**.
   A chamada em conferência começa na ponte de conferência selecionada. Todos os participantes são notificados por e-mail e também por meio da respectiva ponte de conferência que foi selecionada.
10. Selecione a opção **Clique aqui** sobre o incidente de segurança grave para ingressar na chamada em conferência.
    Os participantes podem usar o link da notificação por e-mail ou a notificação da ponte de conferência selecionada para ingressar na chamada.
11. Abra o incidente de segurança grave associado para exibir os detalhes da chamada em conferência.
    Quando o participante final sair da conferência, a chamada em conferência será encerrada ou selecione **Encerrar chamada** para encerrar a chamada em conferência.

Como adicionar participantes a uma chamada em conferência

Adicione participantes a uma chamada em conferência usando a opção de pesquisa no pop-up **Iniciar chamada em conferência** para localizar e adicionar os participantes necessários. Você também pode adicionar participantes selecionando-os na lista Recomendações, que fornece recomendações de participantes para adicionar à chamada em conferência.

Antes de Iniciar
Função necessária: sn_msi.workspace_manager

Por Que e Quando Desempenhar Esta Tarefa
O usuário (host) que inicia a chamada em conferência é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão na lista Recomendações.

Os participantes da chamada podem incluir o seguinte:

- Usuários que receberam responsabilidades específicas.
- Contatos ad hoc ou sob demanda
- Outros contatos de terceiros

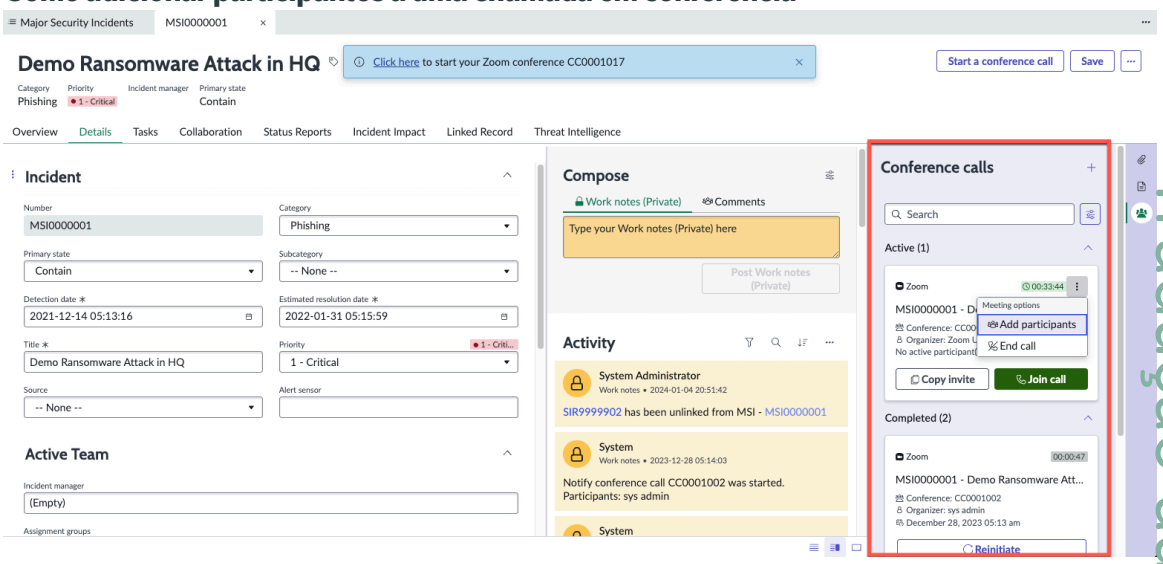
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione o incidente de segurança grave que você está tentando resolver na chamada em conferência.
3. Selecione o ícone no menu de contexto direito para exibir os detalhes das chamadas em conferência. Isso inclui detalhes como nome da ponte de conferência, nome do organizador, data, hora, duração da chamada, participantes ativos e inativos.
4. Selecione ao lado da chamada em conferência ativa e selecione a opção **Adicionar participantes**.

Como adicionar participantes a uma chamada em conferência



5. Você pode usar a opção de pesquisa para localizar e adicionar os participantes necessários ou selecionar os participantes na lista **Recomendações**, que fornece recomendações de participantes para adicionar à chamada em conferência.
6. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.
   Todos os participantes são notificados por e-mail e também por meio da respectiva ponte de conferência que foi selecionada. Os participantes podem usar o link da notificação por e-mail ou a notificação da ponte de conferência selecionada para ingressar na chamada.
7. Como alternativa, você pode adicionar participantes selecionando a opção **Copiar convite** na seção Chamadas em conferência no menu de contexto à direita e compartilhar com os participantes necessários.

Ativar mudo dos participantes de uma chamada em conferência

Como gerente do MSI ou host de chamada em conferência, você tem a opção de silenciar um participante específico ou todos os participantes da chamada em conferência.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Antes de iniciar este procedimento, verifique se há uma chamada em conferência ativa com um ou mais participantes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione o incidente de segurança grave que você está tentando resolver na chamada em conferência.
3. Selecione o ícone no menu de contexto direito para exibir os detalhes das chamadas em conferência.
4. Selecione **Ingressar na chamada** na ponte de conferência ativa.
5. Depois de ingressar na chamada em conferência, selecione um participante que você deseja silenciar e selecione **Mudo** na ponte de conferência.
6. Para silenciar todos os participantes da chamada em conferência, selecione **Participantes** nos controles da reunião e selecione **Silenciar tudo**.

Exibir detalhes da chamada em conferência

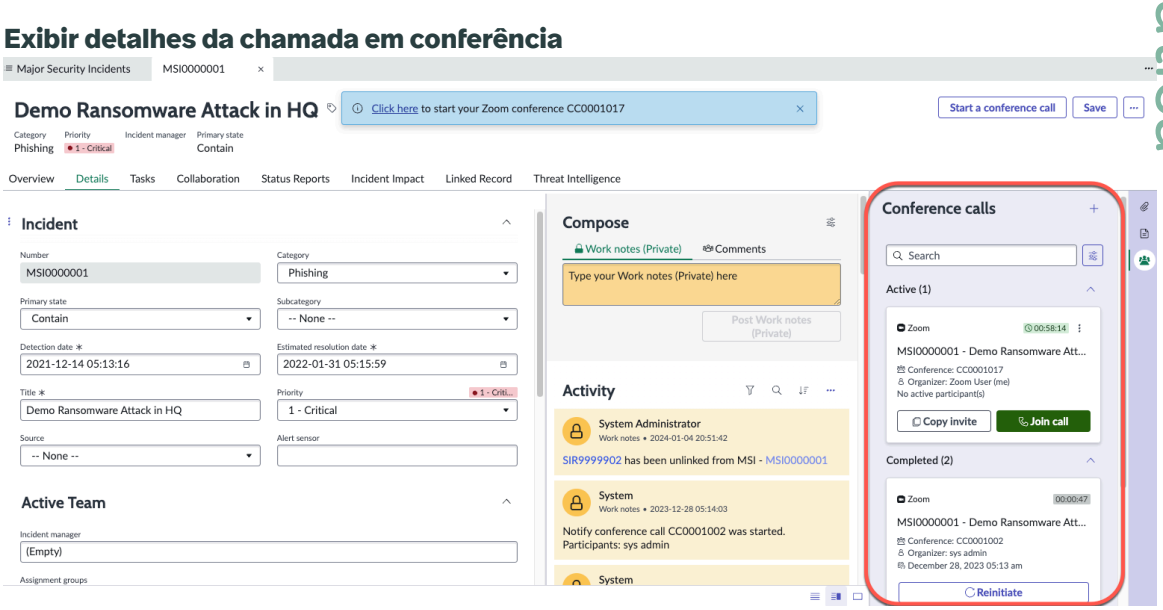
As chamadas em conferência são listadas como atividades do sistema na seção Atividade do incidente de segurança grave e também listadas na lista relacionada de Chamadas em conferência. Você pode exibir detalhes como nome da ponte de conferência, nome do organizador, data, hora, duração da chamada, participantes ativos e inativos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione o incidente de segurança grave que você está tentando resolver na chamada em conferência.
3. Selecione o ícone no menu de contexto direito para exibir os detalhes das chamadas em conferência. Isso inclui detalhes como nome da ponte de conferência, nome do organizador, data, hora, duração da chamada, participantes ativos e inativos.



4. Você pode usar a opção de pesquisa para procurar uma chamada em conferência específica. Pode haver várias chamadas para o mesmo incidente de segurança grave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Para adicionar participantes a uma chamada em conferência, selecione ⋮ ao lado da chamada em conferência ativa e selecione a opção **Adicionar participantes**.
6. Você também pode adicionar participantes usando a opção **Copiar convite** e compartilhando o link com os participantes necessários.
7. Para ingressar em uma chamada em conferência, navegue até a seção Ativa e selecione a opção **Ingressar na chamada** em conferência necessária.
8. Para encerrar uma chamada em conferência, selecione ⋮ ao lado da chamada em conferência ativa e selecione a opção **Encerrar chamada**.
9. Para reiniciar uma chamada em conferência, navegue até a seção Concluído e selecione a opção **Reiniciar** da chamada em conferência necessária.

Integrar chamadas em conferência do MSIM com Microsoft Teams

A integração da Chamada em conferência Microsoft Teams permite que você gerencie e inicie uma chamada em conferência Microsoft Teams diretamente de um incidente de segurança grave.

Principais recursos

- Inicie e encerre Microsoft Teams chamadas em conferência diretamente dos incidentes de segurança graves ou de uma tarefa do workbench de segurança principal.
- Gerencie uma chamada em conferência Microsoft Teams adicionando ou removendo participantes.

Pré-requisitos

Verifique se você instalou os seguintes plug-ins IntegrationHub em sua instância ServiceNow.

- Notify plug-in (com.snc.notify)
- Microsoft Teams Plug-in do spoke de comunicação (sn_msteams_com_spk).
- Plug-in Azure Active Directory User Mapping (sn_now_azure).
- Notify Componentes de IU para espaços configuráveis

Para obter mais informações, consulte Solicitação de IntegrationHub .

Configuração

- Para configurar a integração da Chamada em conferência do MSIM Microsoft Teams usando o app pré-configurado, consulte Integrate Notify connector pre-published app with Microsoft Teams .
- Para configurar a integração da Chamada em conferência do MSIM Microsoft Teams usando o aplicativo autoconfigurado, consulte Integrating Notify connector self-configured app with Microsoft Teams .

Usar a integração de chamada em conferência do MSIM Microsoft Teams

As etapas a seguir fornecem um passo a passo de como você pode gerenciar e iniciar uma chamada em conferência Microsoft Teams diretamente de um incidente de segurança grave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

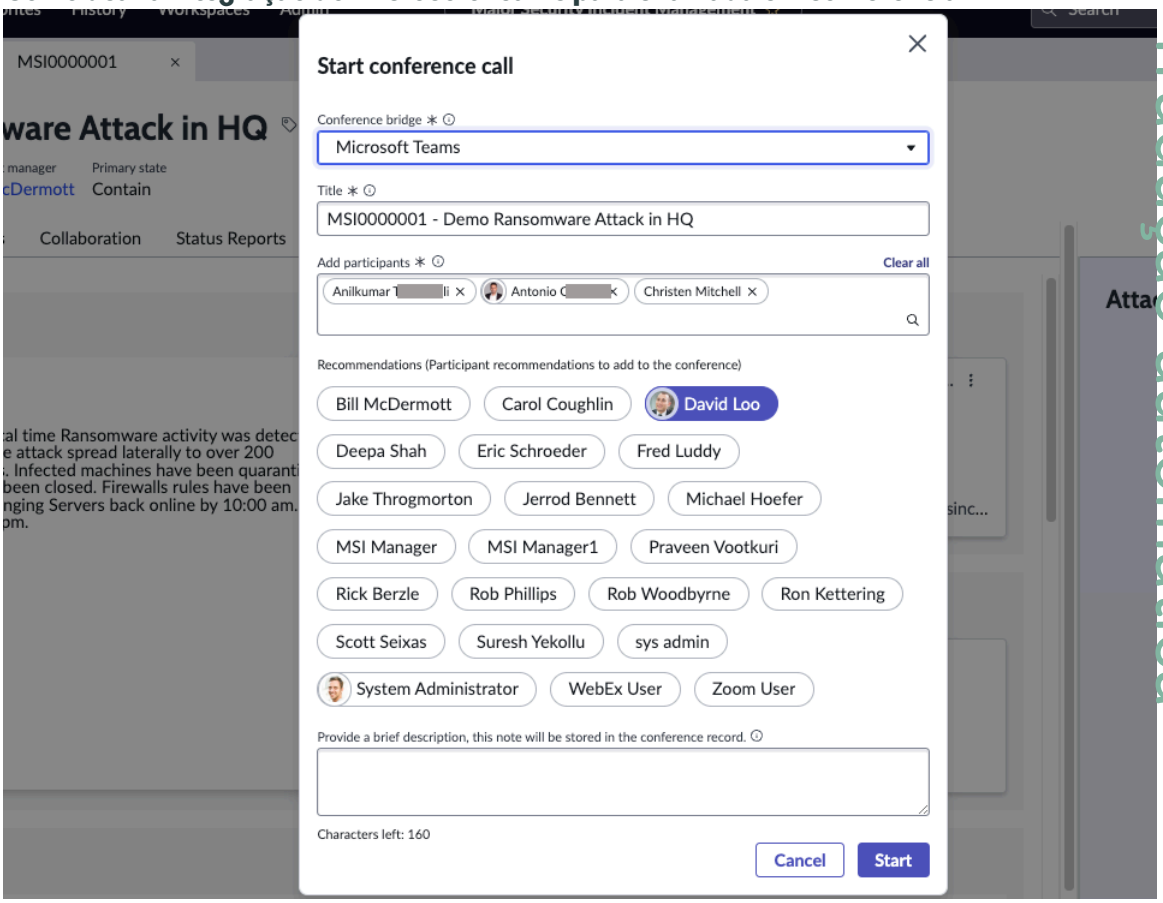
Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione um incidente de segurança grave.
3. Selecione a ação **Iniciar uma chamada em conferência**.
4. Você também pode iniciar uma chamada em conferência selecionando o ícone de em conferência no menu de contexto direito e selecionando o ícone +.
   O pop-up Iniciar chamada em conferência é exibido.
5. Escolha **o Microsoft Teams** como a ponte de conferência da qual você deseja se conectar.
6. No campo Título, forneça um título que descreva o motivo da chamada em conferência do Microsoft Teams.

Como usar a integração do Microsoft Teams para chamada em conferência



7. No campo Adicionar participantes, selecione os participantes da chamada em conferência do Microsoft Teams.
   Você pode usar a opção de pesquisa para encontrar e adicionar os participantes necessários ou selecionar os participantes na lista **Recomendações**, que fornece recomendações de participantes para adicionar à chamada em conferência do Microsoft Teams.

   O usuário (host) que inicia a chamada em conferência do Microsoft Teams é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão na lista **Recomendações**.

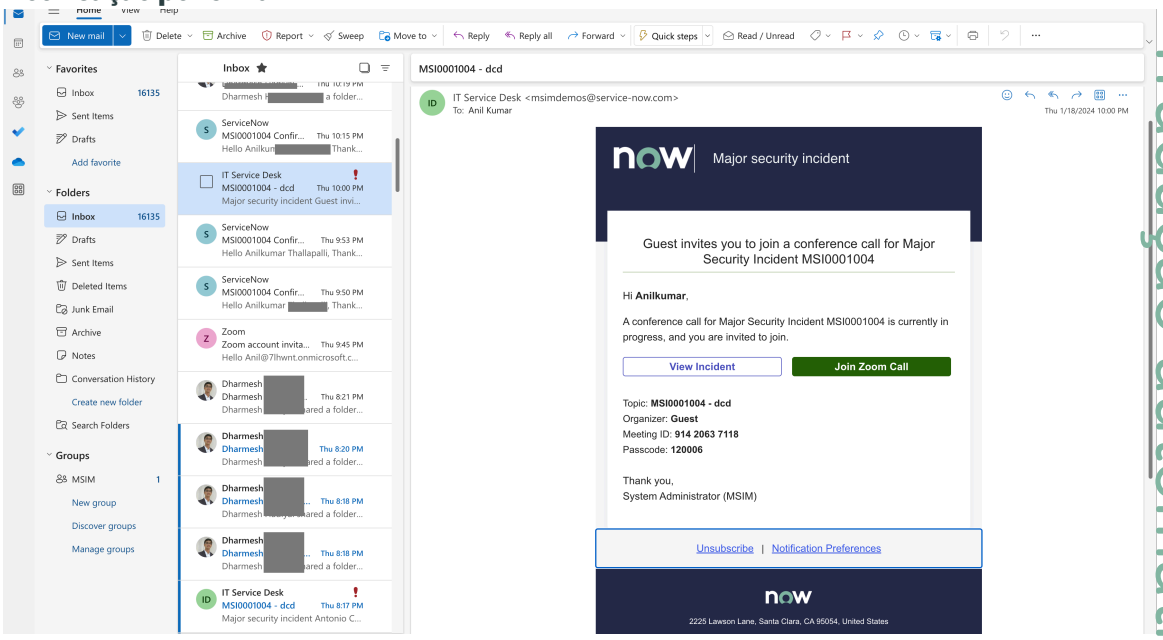
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Verifique se os participantes selecionados têm um endereço de e-mail válido.

8. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.
   A descrição fornecida será adicionada ao registro da conferência.
9. Depois que a lista de participantes for finalizada, selecione **Iniciar**.
   A chamada em conferência começa no aplicativo Microsoft Teams. Todos os participantes são notificados por e-mail do aplicativo MSIM e a outra notificação é enviada por meio de um bot no aplicativo Microsoft Teams.
10. Selecione a opção **Clique aqui** sobre o incidente de segurança grave para ingressar na chamada em conferência no aplicativo Microsoft Teams.
    Os participantes podem usar o link da notificação por e-mail do MSIM ou a notificação do aplicativo Microsoft Teams para ingressar na chamada.

Notificação por e-mail



11. Abra o incidente de segurança grave associado no espaço do MSIM para exibir os detalhes da chamada em conferência.

    Quando o participante final sai da chamada, a chamada em conferência termina ou selecione **Encerrar chamada** na seção Chamada em conferência para encerrar a chamada em conferência.

Integrar chamadas em conferência do MSIM com Zoom

A integração da Chamada em conferência Zoom permite que você gerencie e inicie uma chamada em conferência Zoom diretamente de um incidente de segurança grave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Principais recursos

- Inicie e termine Zoom reuniões diretamente de qualquer registro de tarefa, como um incidente de segurança grave ou uma mudança ou até mesmo do workbench de incidente grave.
- Gerencie Zoom reuniões adicionando ou removendo participantes.
- Rastreie e relate os detalhes da reunião, como a duração da reunião e os participantes, para análise posterior.

Pré-requisitos

Verifique se você instalou os seguintes plug-ins IntegrationHub em sua instância ServiceNow.

- Notify plug-in (com.snc.notify)
- Zoom Spoke (sn_zoom_spoke)
- Notify Zoom (sn_notify_zoom)
- Notify Componentes de IU para espaços configuráveis

Para obter mais informações, consulte Solicitação de IntegrationHub .

Configuração

Para configurar a integração da Chamada em conferência do MSIM Zoom usando o canal de comunicação Notify, consulte Configure Notify Zoom connector in Notify .

Usar a integração de chamada em conferência do MSIM Zoom

As etapas a seguir fornecem um passo a passo de como você pode gerenciar e iniciar uma chamada em conferência Zoom diretamente de um incidente de segurança grave.

Antes de Iniciar
Função necessária: sn_msi.workspace_manager

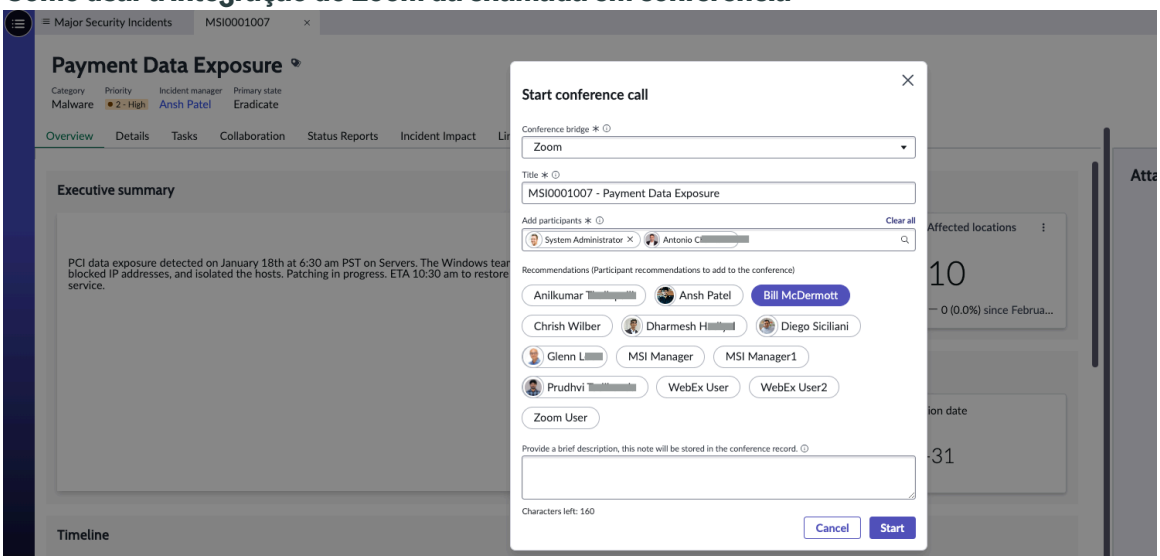
Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione um incidente de segurança grave.
3. Clique na ação **Iniciar uma chamada em conferência**.
4. Você também pode iniciar uma chamada em conferência clicando no ícone de em conferência no menu de contexto direito e selecionando o ícone +.
   O pop-up Iniciar chamada em conferência é exibido.
5. Escolha o **Zoom** como a ponte de conferência da qual você deseja se conectar.
6. No campo Título, forneça um título que descreva o motivo da chamada em conferência do Zoom.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como usar a integração do Zoom da chamada em conferência



7. No campo Adicionar participantes, selecione os participantes da chamada em conferência do Zoom.
   Você pode usar a opção de pesquisa para encontrar e adicionar os participantes necessários ou selecionar os participantes na lista **Recomendações**, que fornece recomendações de participantes para adicionar à chamada em conferência do Zoom.

   O usuário (host) que inicia a chamada em conferência do Zoom é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão na lista **Recomendações**.

   Nota:
   Verifique se os participantes selecionados têm um endereço de e-mail válido.

8. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.
   A descrição fornecida será adicionada ao registro da conferência.

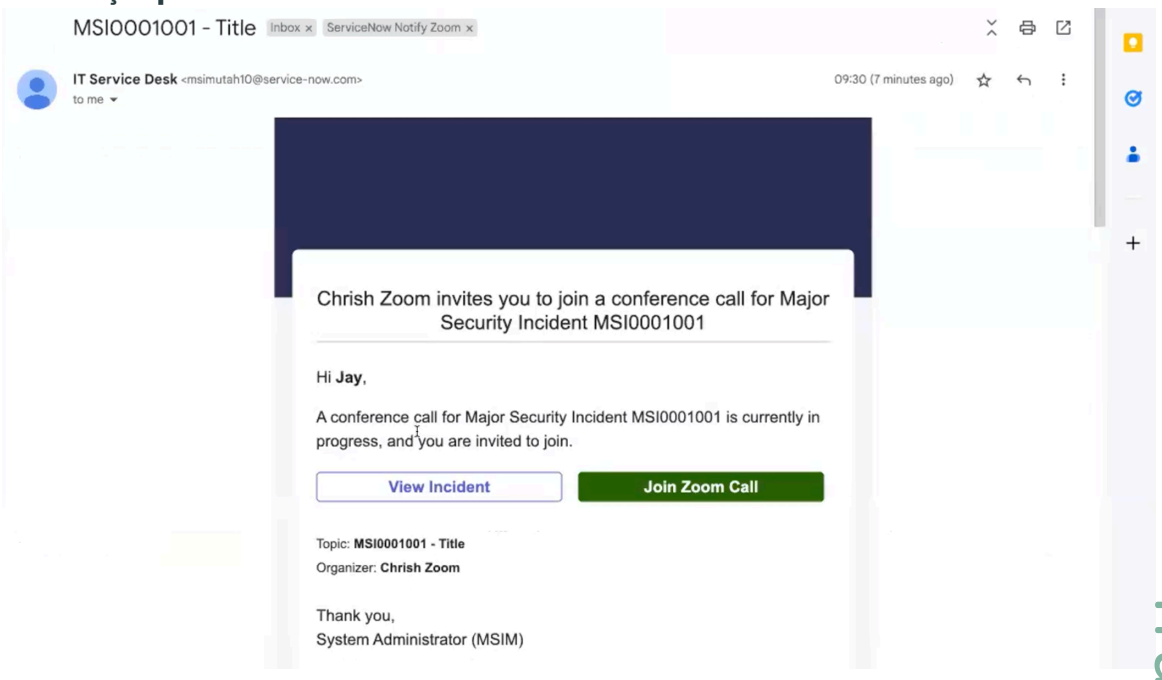
9. Depois que a lista de participantes for finalizada, clique em **Iniciar**.
   A chamada em conferência começa no aplicativo Zoom. Todos os participantes são notificados por meio de dois e-mails, um e-mail é enviado aos participantes do aplicativo MSIM e o outro e-mail é enviado da ponte de conferência do Zoom.

10. Selecione a opção **Clique aqui** sobre o incidente de segurança grave para ingressar na chamada em conferência no aplicativo Zoom.
    Os participantes podem usar o link da notificação por e-mail do MSIM ou a notificação do aplicativo Zoom para ingressar na chamada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Notificação por e-mail



11. Abra o incidente de segurança grave associado no espaço do MSIM para exibir os detalhes da chamada em conferência.

    Quando o participante final sai da chamada, a chamada em conferência termina ou selecione **Encerrar chamada** na seção Chamada em conferência para encerrar a chamada em conferência.

    Se a chamada em conferência foi gravada, a gravação estará disponível na seção Chamada em conferência do incidente de segurança grave associado após algum tempo.

Integrar chamadas em conferência do MSIM com Cisco Webex

A integração da Chamada em conferência do MSIM Cisco Webex permite que você gerencie e inicie uma chamada em conferência Cisco Webex diretamente de um incidente de segurança grave.

Principais recursos

- Inicie e termine Cisco Webex reuniões diretamente dos incidentes de segurança graves.
- Gerencie uma Cisco Webex reunião adicionando ou removendo participantes.

Pré-requisitos

Verifique se você instalou os seguintes plug-ins IntegrationHub em sua instância ServiceNow.

- Notify plug-in (com.snc.notify)
- Notify Cisco Webex Conector (sn_notify_webex)
- Cisco Webex Spoke do Teams (sn_cisco_teams_spk)
- Notify Componentes de IU para espaços configuráveis

Para obter mais informações, consulte Solicitação de IntegrationHub .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração

Para configurar a integração da Chamada em conferência do MSIM Cisco Webex usando o canal de comunicação Notify, consulte Configure Notify Cisco Webex Connector .

Usar a integração de chamadas em conferência Cisco Webex

As etapas a seguir fornecem um passo a passo de como você pode gerenciar e iniciar uma chamada em conferência Cisco Webex diretamente de um incidente de segurança grave.

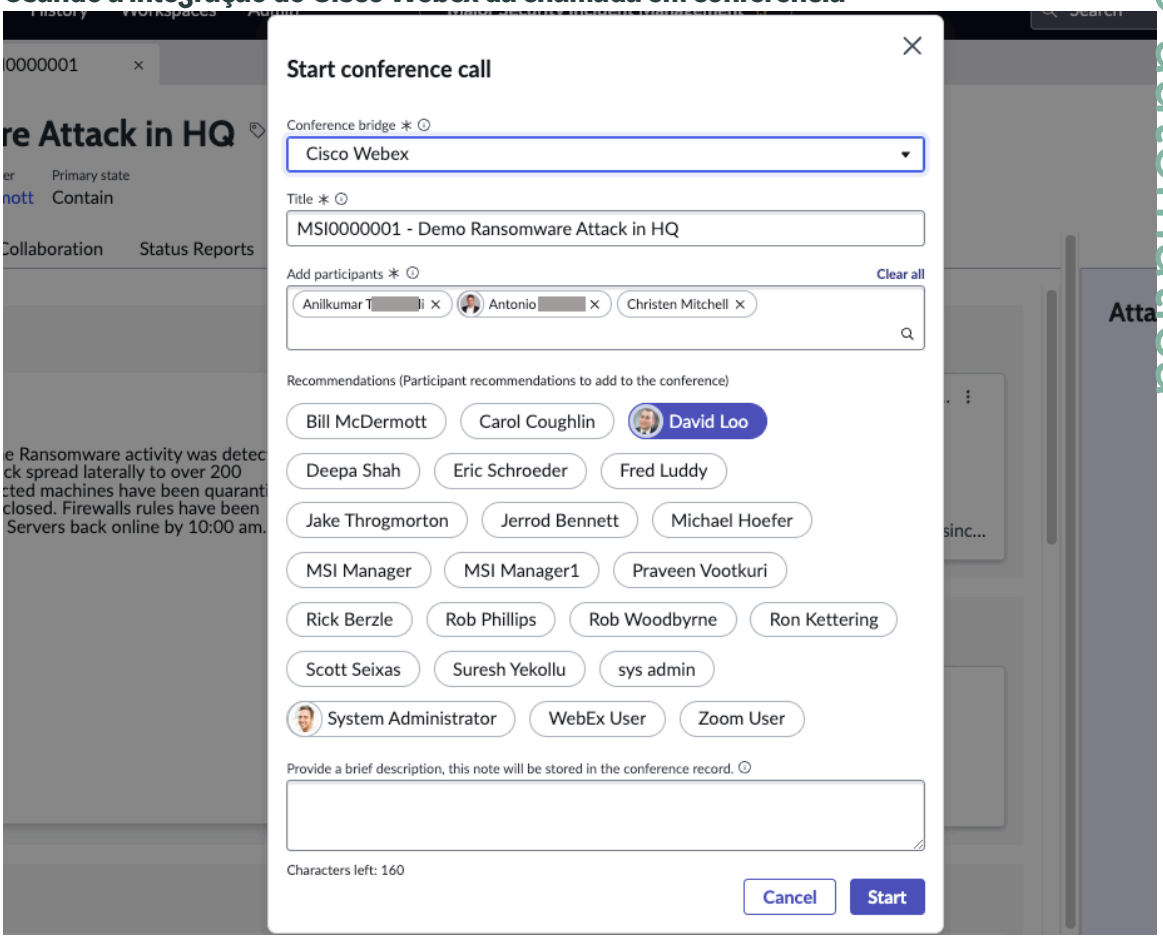
Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança**.
2. Na lista Incidente de segurança grave, selecione um incidente de segurança grave.
3. Selecione a ação **Iniciar uma chamada em conferência**.
4. Você também pode iniciar uma chamada em conferência selecionando o ícone de em conferência no menu de contexto direito e selecionando o ícone +.
   O pop-up Iniciar chamada em conferência é exibido.
5. Escolha o **Cisco Webex** como a ponte de conferência da qual você deseja se conectar.
6. No campo Título, forneça um título que descreva o motivo da chamada em conferência do Cisco Webex.

Usando a integração do Cisco Webex da chamada em conferência



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. No campo Adicionar participantes, selecione os participantes da chamada em conferência do Cisco Webex. Você pode usar a opção de pesquisa para encontrar e adicionar os participantes necessários ou selecionar os participantes na lista **Recomendações**, que fornece recomendações de participantes para adicionar à chamada em conferência do Cisco Webex.

   O usuário (host) que inicia a chamada em conferência do Cisco Webex é adicionado automaticamente à lista de participantes selecionados. Todos os usuários associados ao incidente de segurança grave estão disponíveis por padrão na lista **Recomendações**.

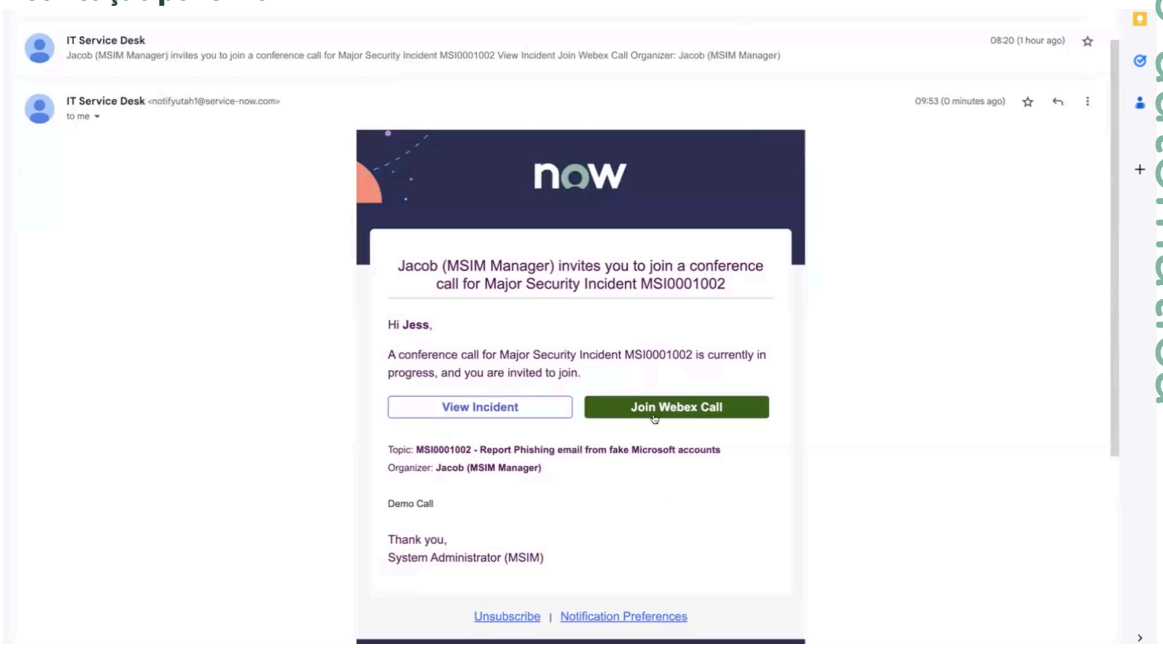
   Nota:
   Verifique se os participantes selecionados têm um endereço de e-mail válido.

8. Depois de selecionar os participantes, forneça uma breve descrição do motivo para iniciar a chamada em conferência no campo Descrição.
   A descrição fornecida será adicionada ao registro da conferência.

9. Depois que a lista de participantes for finalizada, selecione **Iniciar**.
   A chamada em conferência começa no aplicativo Cisco Webex. Todos os participantes são notificados por meio de dois e-mails, um e-mail é enviado aos participantes do aplicativo MSIM e o outro e-mail é enviado da ponte de conferência Cisco Webex.

10. Selecione a opção **Clique aqui** na parte superior do incidente de segurança grave para ingressar na chamada em conferência no aplicativo Cisco Webex.
    Os participantes podem usar o link da notificação por e-mail do MSIM ou a notificação do aplicativo Cisco Webex para ingressar na chamada.

Notificação por e-mail



11. Abra o incidente de segurança grave associado no espaço do MSIM para exibir os detalhes da chamada em conferência.

    Quando o participante final sai da chamada, a chamada em conferência termina ou selecione **Encerrar chamada** na seção Chamada em conferência para encerrar a chamada em conferência.

    Se a chamada em conferência foi gravada, a gravação estará disponível na seção Chamada em conferência do incidente de segurança grave associado após algum tempo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração do Gestão de incidentes graves de segurança

Instale e configure a aplicação Gestão de incidentes graves de segurança.

Use esta seção para saber como definir as configurações necessárias para trabalhar com registros Incidente de segurança grave integrando-se a outras aplicações externas Microsoft para estabelecer conexões com a instância ServiceNow.

Configurar componente do File Explorer

O componente do espaço do explorador de arquivos organiza e rastreia a coleção de artefatos (arquivos) relacionados a um incidente de segurança grave. Ele foi projetado para oferecer suporte à integração com qualquer provedor de hospedagem de arquivos de terceiros, como Microsoft SharePoint no espaço Gestão de incidentes graves de segurança.

- File Explorer Componente: fornece uma interface gráfica do usuário para exibir o sistema de arquivos e permite que os usuários executem operações de arquivo.
- File Explorer Núcleo: fornece uma camada de abstração que permite que o componente do Explorador de arquivos exiba o sistema de arquivos e execute várias operações de arquivo sem saber nada sobre o conector subjacente usado para se comunicar com repositórios externos.
- File Explorer Microsoft SharePoint Aplicação de conector: fornece os módulos de implementação necessários para rastrear e buscar metadados de arquivos/pastas de uma biblioteca de documentos Microsoft SharePoint e executar operações de arquivo.

O componente File Explorer Core fornece uma infraestrutura de base necessária para que as diferentes aplicações do conector de compartilhamento de arquivos definam suas propriedades de conexão.

Você deve instalar e configurar a unidade do repositório de arquivos e o provedor do repositório de arquivos adicionando as propriedades da conexão para extrair os metadados dos arquivos de um local do provedor de hospedagem de arquivos.

Para esta versão atual do File Explorer, essas instruções incluem a configuração e a assinatura de um arquivo de recuperação metadados como Microsoft SharePoint atualizações de arquivo e pasta, operações de arquivo e registro em log da atividade do arquivo. Uma biblioteca de documentos Microsoft SharePoint designada e a configuração da unidade relacionada serão necessárias para criar pastas individuais específicas para um incidente de segurança grave.

File Explorer também permite aplicações de conector como Microsoft SharePoint. Você pode usar este exemplo para configurar suas implementações de operação de arquivo, como **Baixar** ou **Renomear** as ações de pasta e arquivo serão habilitadas no componente do espaço do explorador de arquivos. Essas ações são habilitadas e executadas usando os subfluxos do Flow Designer integrado. Para obter mais informações, consulte Configurações de ação de pasta e arquivo.

File Explorer configuração inclui a seguinte configuração:

- Configurar Unidade do Repositório do Explorador de Arquivos
- Definir configurações de ação de pasta e arquivo
- Criar modelos de pasta

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Introdução ao Explorador de Arquivos

Revise as informações a seguir antes de começar a trabalhar com o componente File Explorer.

Revise as informações a seguir antes de começar a estabelecer a conexão com Microsoft SharePoint, criar ações de pasta e arquivo e criar modelos de pasta para o componente do explorador de arquivos.

Pré-requisitos

Nome	Descrição
Microsoft SharePoint spoke, versão 2.0.2 para ServiceNow® IntegrationHub.	Use o ID do plug-in **sn_sp_spoke** para pesquisar e instalar o Microsoft SharePoint spoke. A instalação deste plug-in fornece fluxos e ações para automatizar a colaboração, a gestão de documentos e os direitos de acesso do usuário em Microsoft SharePoint.
Componente do File Explorer v1.1.0	Use o ID do plug-in **sn_file_explorer** para pesquisar e instalar o componente do explorador de arquivos v1.1.0 A instalação deste plug-in fornece uma interface gráfica do usuário para navegar pelo sistema de arquivos, que está disponível no núcleo do explorador de arquivos.
File Explorer Core para Security Operations v1.1.1	Use o ID do plug-in **sn_fe** para pesquisar e instalar o File Explorer Core. A instalação deste plug-in fornece infraestrutura de base para integração com qualquer provedor de hospedagem de arquivos de terceiros.
Microsoft SharePoint Conector do File Explorer para Security Operations v1.1.1	Use o ID do plug-in **sn_fe_sharepoint** para pesquisar e instalar o Microsoft SharePoint File Explorer Connector. A instalação deste plug-in gerenciará os Microsoft SharePoint arquivos/pastas usando o Explorador de arquivos.

Configurar Unidade do Repositório do Explorador de Arquivos

O conector Microsoft SharePoint fornece vários recursos a serem implementados nos recursos do Explorador de arquivos Microsoft SharePoint, gerenciando e rastreando os metadados do arquivo.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Tudo** > **Incidente de segurança grave** > **Gerenciador de Arquivos** > **Configuração do repositório de arquivos**.
2. Preencha os seguintes campos conforme descrito na tabela a seguir:

Nome do campo	Descrição do Campo
Nome	Nome do registro do repositório de arquivos que identifica o uso. Por exemplo, MSIM.
Provedor	Nome do provedor que é o provedor do repositório de hospedagem do arquivo de terceiros. Por exemplo,Microsoft SharePoint.
Propriedades	
Caminho de URL de site	Insira uma URL Microsoft SharePoint com um caminho de site específico. Forneça somente o caminho relativo para o site, e um URL de site completo pode não ser necessário. Por exemplo, Sites/MSIM.
Nome da Biblioteca de Documentos	Crie uma biblioteca de documentos no site Microsoft SharePoint e forneça o mesmo nome de biblioteca de documentos aqui. Esta seria a mesma biblioteca de documentos que você criou na configuração da Microsoft SharePoint Connector Drive.
Conexão do Graph	Selecione o registro de locatário do Explorador de arquivos do Graph. Para obter mais informações sobre a configuração de conexão do locatário, consulte Microsoft SharePoint spoke.
Conexão REST	Selecione o registro do locatário REST do Explorador de Arquivos. Para obter mais informações sobre a configuração de conexão do locatário, consulte Microsoft SharePoint spoke.

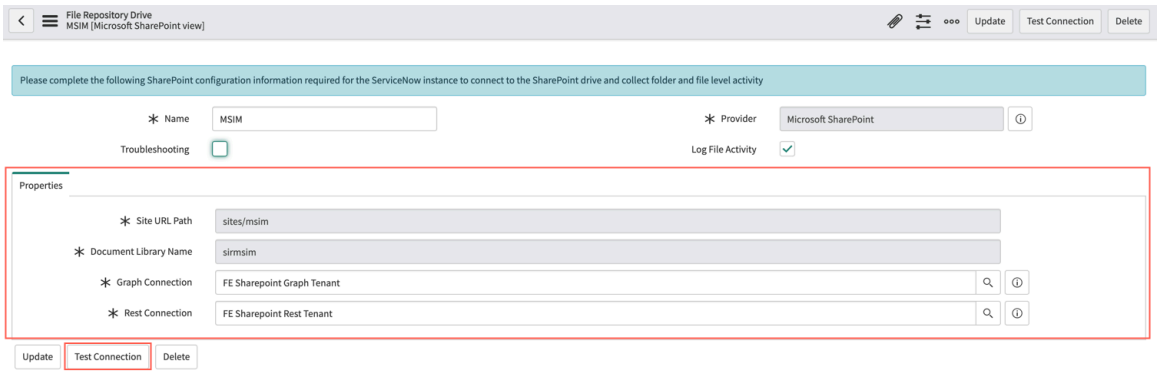
3. Selecione **Salvar**.
4. Clicar **Testar conexão** Guia para testar a conexão e validar as propriedades de configuração da unidade do repositório de arquivos.

> **Nota:**
> Antes de **ativar** o repositório de arquivos, certifique-se de que a biblioteca de documentos correspondente em Microsoft SharePoint não tenha dados de pasta ou arquivo.

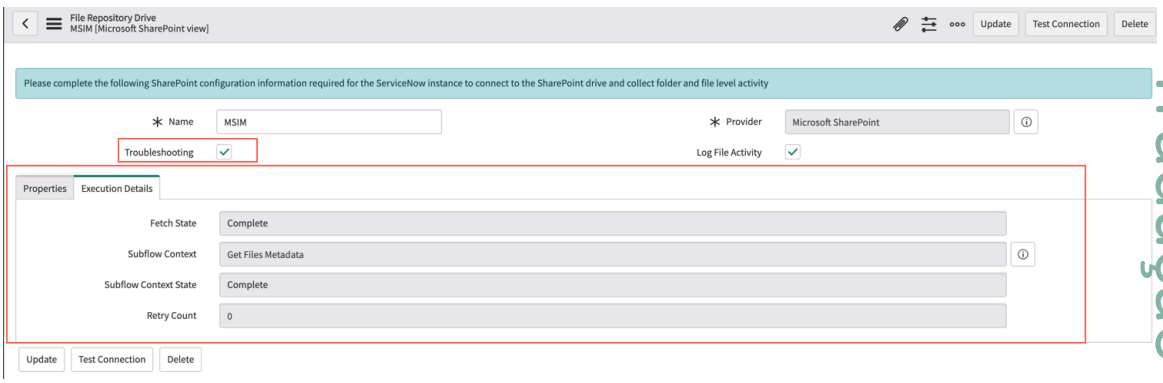
5. Clique em **Ativar** para ativar o repositório de arquivos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Marque a caixa de seleção **Solução** de problemas para verificar os **Detalhes de execução** do repositório de arquivos e verifique o **Buscar estado** está concluído e certifique-se de que Microsoft SharePoint Assinaturas de unidade foram criadas e o estado está concluído.



Nota:
Usando o botão **Testar conexão**, o Administrador do MSI ou o Gerenciador do MSI só podem validar a configuração do repositório de arquivos.

Definir configurações de ação de pasta e arquivo

Configura as ações de pasta e arquivo que você gostaria de habilitar no componente do Explorador de Arquivos no espaço do Major Security Incident Management, usando a página de configuração Configurações de ação de pasta e arquivo. Como administrador do MSI, você pode controlar as ações individuais de pasta e arquivo exibidas no componente do explorador de arquivos.

Antes de Iniciar

A seguir estão as capacidades de operações de arquivo implementadas no componente do explorador de arquivos usando o ServiceNow® Flow Designer:

Capacidades de operações de arquivo

Operação de arquivo	Descrição
Abrir em Microsoft SharePoint	Abre uma nova guia do navegador para exibir Microsoft SharePoint exibição de arquivo da biblioteca de documentos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Capacidades de operações de arquivo

Operação de arquivo	Descrição
Criar pasta	Capacidade de criar pastas ad hoc adicionais após a criação do incidente de segurança grave.
Renomear pasta	Capacidade de renomear as pastas criadas.
Mover arquivo	Permite mover arquivos entre pastas no componente do explorador de arquivos do espaço, resultando na movimentação de arquivos em Microsoft SharePoint
Localizar arquivo	Mostra o local da pasta ao usar o **Recentes** exibição do Explorador de Arquivos.
Exclusão de arquivo	Exclua o arquivo.
Excluir pasta	Exclua a pasta.
Baixar arquivo	Baixa o arquivo na guia do navegador do Espaço do MSIM existente para exibição rápida.
Renomear arquivo	Renomeia o arquivo.

Nota:

1. Todas as ações listadas estão habilitadas por padrão. Você precisará editar o **Configurações de ação de arquivo** se você não quiser que determinadas ações sejam exibidas. No momento, todas as configurações são globais para todos os usuários, o que significa que não há capacidade de habilitar ações para um subconjunto dos usuários que têm uma função específica.
2. **Revogar acesso do usuário** e **Adicionar permissão** ações são ações relacionadas ao sistema. É recomendável não modificar essas ações de arquivo.

O exemplo a seguir procedimento descreve um dos recursos de operações de arquivoies para desabilitar qualquer pasta específica e ação de arquivo durante a configuração do repositório do explorador de arquivos. Este procedimento é aplicável a todas as outras ações que podem precisar ser editadas:

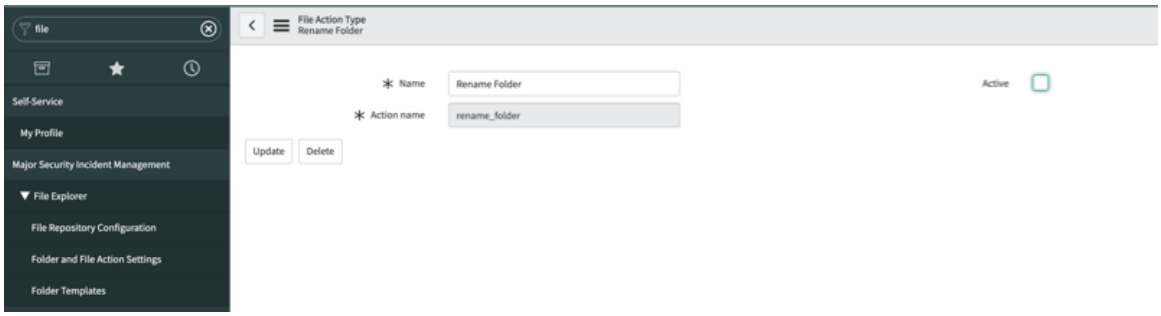
Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Gerenciador de Arquivos** > **Configurações de ação de pasta e arquivo**.
2. Selecione o registro desejado para habilitar ou desabilitar a ação de pasta ou arquivo, respectivamente.
3. Desmarcar o **Ativo** caixa de seleção para desabilitar a ação de pasta e arquivo.

Tradução automática

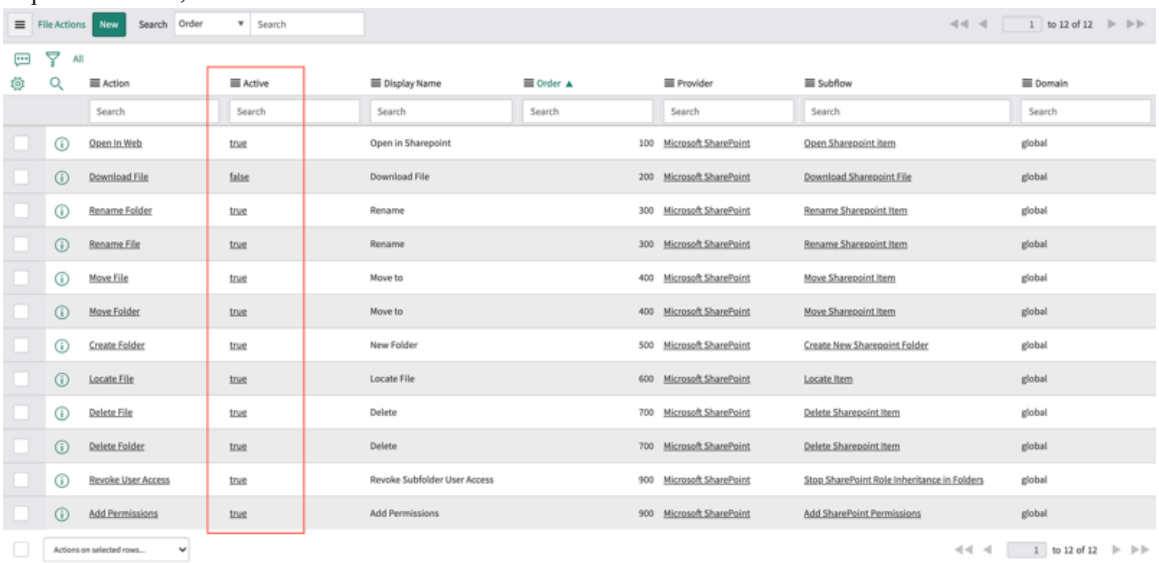
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



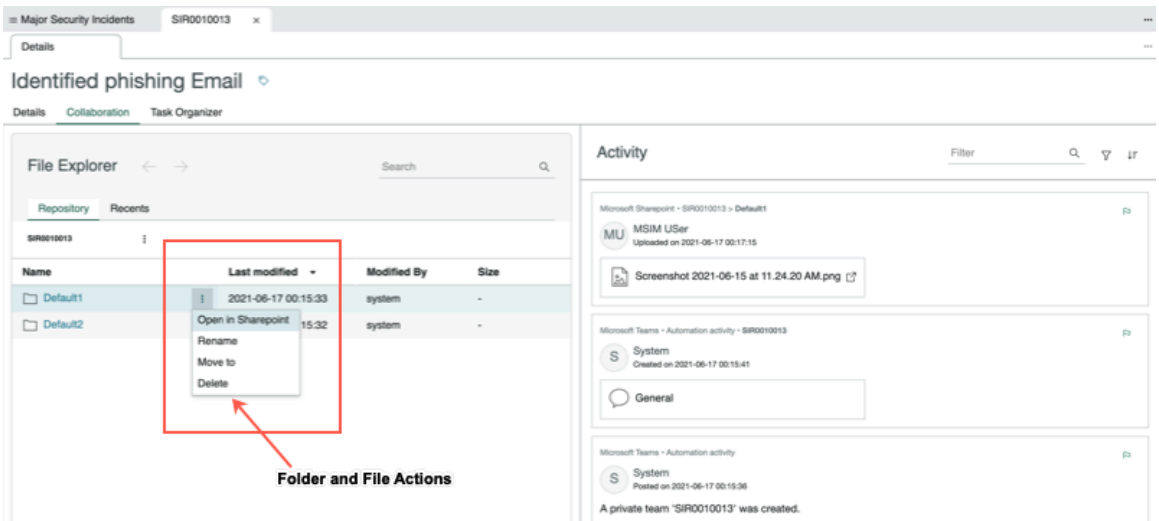
4. **Atualize** o registro da unidade.

Nota:

Você também pode executar a ação de arquivo diretamente da lista de operações de arquivo exibidas, escolhendo o **Ativo** valores de coluna como Verdadeiro ou Falso.



Se a ação de arquivo realizada estiver desabilitada, a ação não será exibida no **Colaborações** guia do **Gestão de incidentes graves de segurança** espaço.



Criar modelos de pasta

Use modelos de pasta para criar automaticamente pastas exclusivas para diferentes tipos de incidentes de segurança graves. Os modelos de pasta no componente do File Explorer

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

são usados para criar uma estrutura de pastas base para o incidente de segurança no Microsoft SharePoint.

Antes de Iniciar

Como administrador do MSI, você define a estrutura de pastas inicial necessária para permitir a colaboração em diferentes grupos de respondentes do incidente e atribui privilégios de acesso apropriados em um nível de subpasta. Várias configurações podem ser criadas para diferentes tipos Incidente de segurança grave usando um construtor de condição para valores de campo Incidente de segurança grave específicos, o que inclui permitir o acesso a diferentes usuários e grupos de usuários em cada nível de subpasta.

Nota:
Esses modelos de pasta são usados por todos os incidentes de segurança graves que atendem às condições especificadas no construtor de condição. É recomendável que você considere o uso de variáveis de campo de incidente, como o número do incidente ou a categoria, para criar nomes de pasta raiz exclusivos que distinguem um conjunto de subpastas com nomes de pasta comuns para um incidente de segurança grave de pastas semelhantes com esses nomes que fazem parte de um incidente de segurança grave diferente.

A configuração de modelos de pasta definida é aplicada ao incidente de segurança grave somente quando a condição é correspondida.

Nota:
Uma configuração de sistema de base (sem subpastas) é aplicada a todos os incidentes de segurança. Você pode editar esta configuração padrão para incluir subpastas específicas ou criar uma nova configuração com base em um conjunto especificado de valores de campo de incidente de segurança grave. Por exemplo, categoria = atividade de código malicioso.

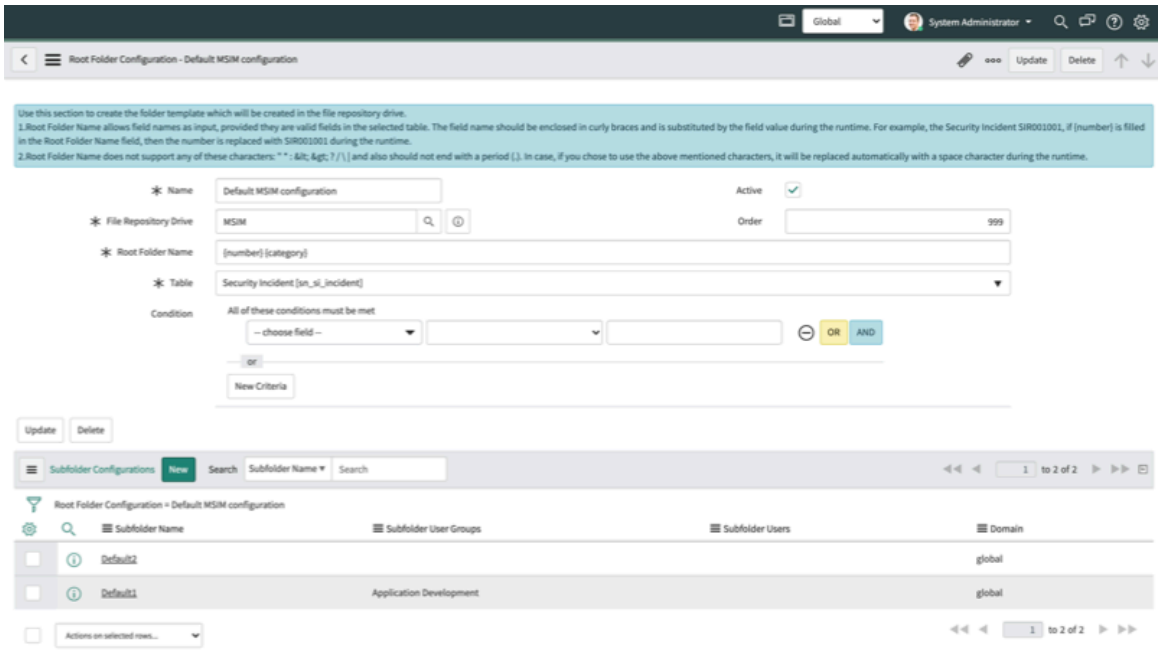
Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Tudo** > **Gestão de incidentes graves de segurança** > **Gerenciador de Arquivos** > **Modelos de pasta**.
2. Clicar **Novo** para configuração de pasta raiz.
3. No formulário, preencha os campos.
4. Definir o incidente de segurança **Condição** valores.

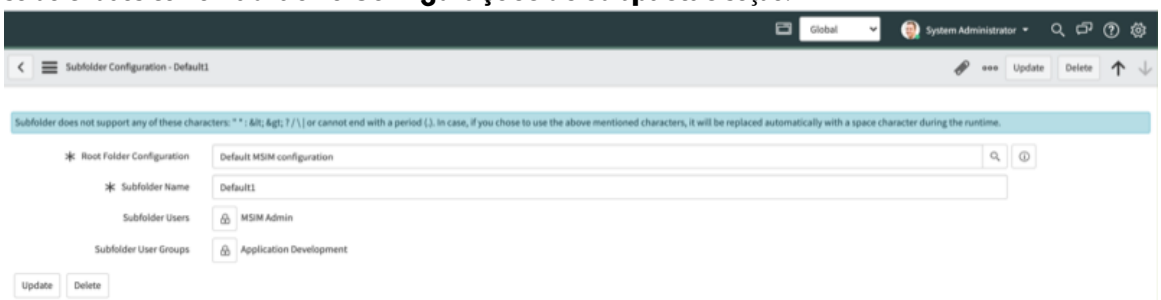
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. **Atualizar** o registro.
   As subpastas são criadas com os valores definidos.

6. Clique na **subpasta**desejada.
   Se você não criar uma subpasta com um nome apropriado, os nomes das subpastas serão criados como **Padrão** no **Configurações de subpastas** seção.



A mesma estrutura de pastas será criada automaticamente em Microsoft SharePoint usando os mesmos privilégios de acesso configurados em **Modelos de pasta** página.

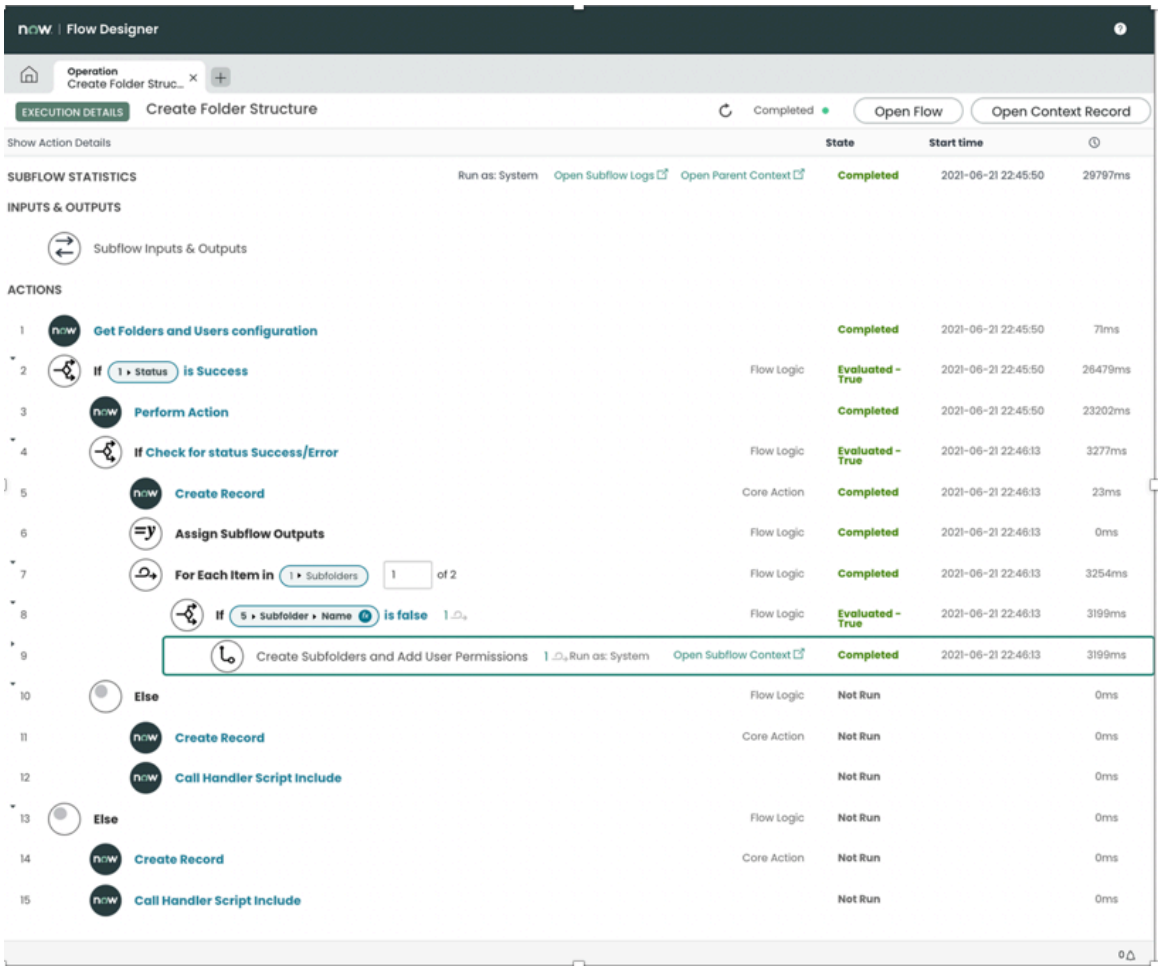
Nota:

- **O nome da pasta raiz** permite nomes de variáveis de campo como entrada, desde que sejam campos válidos na tabela selecionada. O nome do campo deve ser colocado entre chaves e é substituído pelo valor do campo durante o tempo de execução do fluxo. Por exemplo, o incidente de segurança SIR001001, se a variável {number} estiver configurada no campo **Nome da pasta raiz**, o número será substituído por SIR001001 durante o tempo de execução.
- **Nome da pasta raiz** não é compatível com nenhum destes caracteres: " * : < > ? / \ | e também não deve terminar com um ponto final (.). Se você usar os caracteres mencionados acima, eles serão substituídos automaticamente por um caractere de espaço durante o tempo de execução.
- Se a **pastaraiz** e o nome da subpasta excederem o limite definido (256 caracteres), o nome da pasta será truncado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seguir está a execução do tempo de execução do subfluxo Criar estrutura de pastas:



File Explorer Fluxo de atividades no espaço

Use a seção do Explorador de arquivos do espaço Gestão de incidentes graves de segurança para exibir as pastas e os arquivos, a sequência em que foram criados na Microsoft SharePoint biblioteca de documentos.

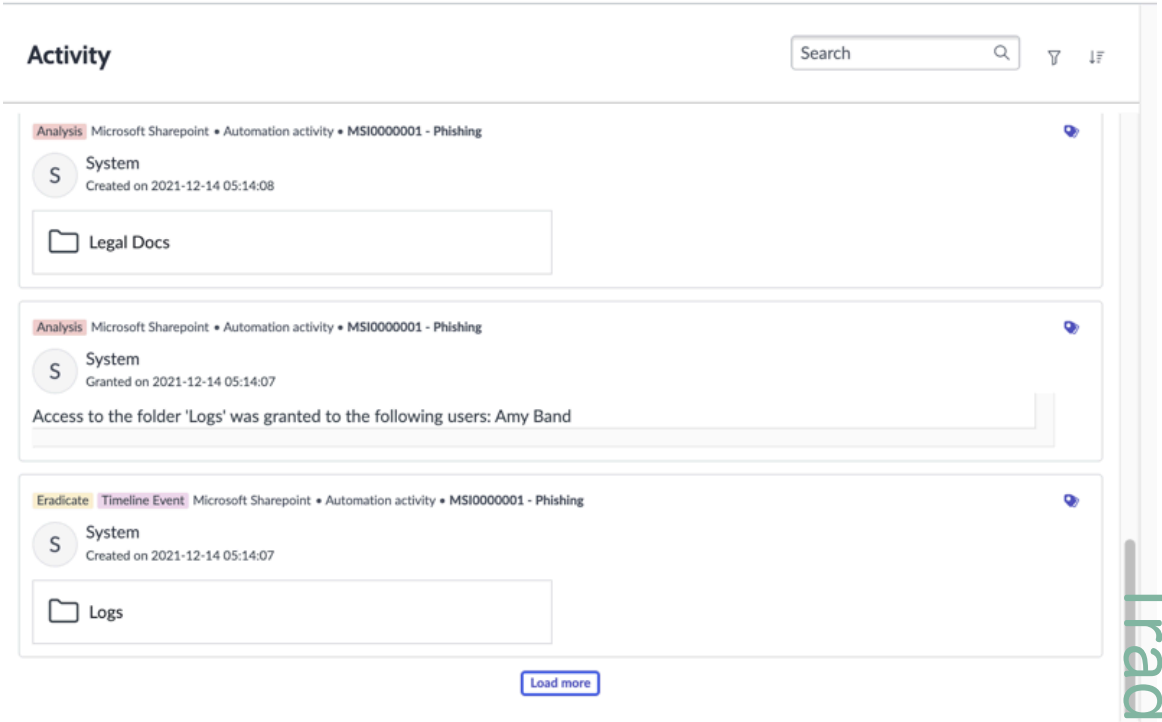
O fluxo de atividades lista todas as publicações de atividade de automação sempre que houver qualquer atividade de pasta e arquivo ou logs que ocorram durante a resolução Incidente de segurança grave. A estrutura do fluxo de atividades está alinhada no mesmo formato da biblioteca Microsoft SharePoint, que mostra as pastas que foram criadas e quais usuários ou grupos de usuários foram atribuídos a essas pastas.

O fluxo de atividades permite que os gerentes do espaço e outros usuários ou grupos de usuários se comuniquem e colaborem de forma eficaz, listem as atividades que foram realizadas em Microsoft SharePoint pastas e arquivos, monitorem o status do incidente, publiquem as anotações ou adicionem comentários adicionais que eles tem no registro do incidente. Os gerentes

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

do espaço podem selecionar e trabalhar com base na última atividade



atualizada.

Solução de problemas File Explorer

A seção de solução de problemas pode ajudar a resolver alguns dos problemas técnicos que você pode encontrar ao configurar o componente File Explorer.

Consulte a seção a seguir sobre os trabalhos programados, as propriedades do sistema e os subfluxos do Flow Designer File Explorer em detalhes.

Trabalhos programados para File Explorer

Trabalhos programados são trabalhos automatizados executados para processar as notificações de Microsoft SharePoint, ingerir os metadados dos arquivos na instância ServiceNow e renovar as assinaturas do repositório de arquivos em uma programação recorrente.

Trabalhos programados são trabalhos automatizados que são executados em segundo plano para:

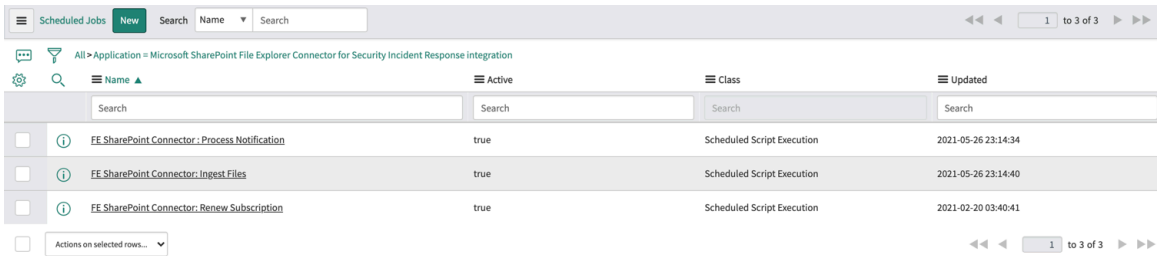
- processar as notificações do Microsoft Microsoft SharePoint.
- ingerir os metadados dos arquivos na instância Now Platform.
- renove a assinatura com Microsoft SharePoint biblioteca de documentos para receber notificações.

Trabalho	Descrição
Microsoft SharePoint File Explorer Conector: processar notificação	É executado a cada 30 segundos e é responsável pela leitura das notificações que indica qualquer mudança na biblioteca de documentos assinada e marca o estado das unidades (sn_fe_file_repo_drive) como pendente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho	Descrição
Microsoft SharePoint File Explorer Conector: ingerir arquivos	É executado a cada 30 segundos e é o principal responsável pelo processamento das unidades (sn_fe_file_repo_drive) que estão no estado pendente e extrai as mudanças do arquivo delta da biblioteca de documentos Microsoft SharePoint configurada desde a última extração.
Microsoft SharePoint File Explorer: renovar assinatura	É executado a cada 10 minutos e é responsável pela renovação da assinatura da biblioteca de documentos Microsoft SharePoint um dia antes da data de vencimento. Normalmente, essas assinaturas expiram em 30 dias.



Propriedades do sistema do Explorador de Arquivos disponíveis

A seguir estão as propriedades do sistema do conector do explorador de arquivos Microsoft SharePoint disponíveis.

Propriedades do sistema

Nome da Propriedade	Descrição
sn_fe_sharepoint.max_retry_count	Controla a frequência de tentativas que a aplicação do conector Microsoft SharePoint tentou extrair a unidade com falha ou renovar a assinatura com falha. O valor de frequência padrão é definido como 50.
sn_fe_sharepoint.retry_after_seconds	Intervalo de tempo entre cada tentativa de extrair a unidade com falha ou renovar a assinatura. O valor padrão é definido como 900 s ou 15 minutos.
sn_fe_sharepoint.max_subscription_expiration_time	Período máximo de expiração da assinatura em número de dias para Microsoft SharePoint. O período de expiração padrão é definido como 30 dias.

File Explorer Subfluxos do Flow Designer

A seguir estão os subfluxos do Flow Designer que são instalados com o conector Microsoft SharePoint File Explorer.

Subfluxos

Nome	Descrição
Adicionar Microsoft SharePoint Permissões	Concede permissão de edição para uma pasta específica a usuários específicos.
Criar assinatura do Drive	Assina com uma biblioteca de documentos Microsoft SharePoint configurada para receber notificações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Subfluxos

Nome	Descrição
	sobre quaisquer atualizações que ocorram na biblioteca de documentos.
Criar nova pasta Microsoft SharePoint	Cria uma nova pasta Microsoft SharePoint em uma determinada pasta primária.
Excluir Microsoft SharePoint Item	Exclui Microsoft SharePoint arquivos e pastas.
Baixar arquivo Microsoft SharePoint	Retorna a URL de download de Microsoft SharePoint arquivos
Obter metadados de arquivos	Assina e extrai as mudanças da Microsoft SharePoint biblioteca de documentos.
Mover item Microsoft SharePoint	Move os arquivos/pastas Microsoft SharePoint para a pasta de destino
Abrir Microsoft SharePoint Item	Retorna o URL da Web de Microsoft SharePoint arquivo/pasta a ser aberto em um navegador.
Renovar assinatura do Drive	Renova a assinatura com Microsoft SharePoint biblioteca de documentos.
Criar Estrutura de Pastas	Segue as configurações do modelo de pasta e cria a estrutura de pastas na Microsoft SharePoint biblioteca de documentos.

Configurar Microsoft Teams.

Integre e colabore facilmente com Microsoft Teams para resolver Incidente de segurança grave para exibir e filtrar atividades de bate-papo de colaboração.

Configurar e assinar um ambiente de bate-papo Microsoft Teams, recuperar conversas de bate-papo de dentro de canais especificados e arquivar a Equipe e os canais associados estão incluídos como parte do processo de fechamento do incidente. Um ambiente Microsoft Teams designado e a configuração de API Microsoft Teams Graph relacionada são necessários para criar canais individuais que são específicos para um Incidente de segurança grave.

Para configurar o Microsoft Teams, ative o Teams como o provedor de bate-papo. Você pode criar canais de bate-papo para as várias partes interessadas e grupos que se comunicam sobre atividades e rastrear conversas de bate-papo para resolver o Incidente de segurança grave. A configuração do Microsoft Teams e do Microsoft Graph API inclui:

- Estabelecer conexão de gráfico do MS Teams em Now Platform
- Ativar o MS Teams como um provedor de bate-papo
- Criar um modelo de canal de bate-papo
- Exibir atividade de mensagem de bate-papo

Para começar com Microsoft Teams

Revise as informações a seguir antes de começar a trabalhar com Microsoft Teams como uma aplicação de conector.

Certifique-se de que os plug-ins a seguir estejam instalados antes de começar a estabelecer, ativar e validar Microsoft Teams as conexões de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Plug-ins necessários

Nome	Descrição
Integração de bate-papo com o Security Incident Management	Use o ID do plug-in **sn_chat_collab_core** para pesquisar e instalar o Microsoft Teams Bate-papo. A instalação deste plug-in permite rastrear a atividade de bate-papo para aplicações de terceiros, como o Microsoft Teams (ou Slack e outras aplicações de bate-papo de terceiros).
Conector de bate-papo do Microsoft Teams para Gestão de incidentes de segurança	Use o ID do plug-in **sn_ms_teams_connector** para pesquisar e instalar o Microsoft Teams Chat Connector for Major Security Incident Management. A instalação deste plug-in permite rastrear as atividades de bate-papo usando o componente de colaboração específico para Microsoft Teams.
Microsoft Teams Spoke do gráfico	A instalação deste plug-in estabelece uma conexão de spoke do Graph com Microsoft Teams. Para obter mais informações, consulte Spoke do Microsoft Teams Graph

Ativar o MS Teams como um provedor de bate-papo

Ative Microsoft Teams validando a conexão Microsoft Teams.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Depois que a conexão é ativada e validada, uma mensagem informativa é exibida informando que a conexão do provedor foi validada com sucesso. Você pode modificar a configuração do canal adicionando e removendo usuários e, possivelmente, adicionando mais canais ou renomeando os canais existentes.

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Configuração do provedor de bate-papo**.
2. Selecione **o registro do Microsoft Teams**.
3. Clique **em Validar conexão**.
   Uma mensagem de confirmação exibe que a conexão do provedor foi validada com sucesso.
4. Marque a caixa de seleção **Ativa** para ativar o registro do provedor.
   Uma mensagem de confirmação exibe que a conexão do provedor foi validada com sucesso.
5. **Salve** o formulário depois de ativar a configuração do provedor de bate-papo.
   Com esta conexão entre o Microsoft Teams e a instância Now Platform, a instância foi estabelecida com sucesso.

Criar um modelo de canal de bate-papo

Configure equipes de bate-papo e modelos de canal para criar equipes de bate-papo e canais para colaborar, rastrear as conversas de bate-papo e adicionar usuários e grupos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de usuários a esses canais de bate-papo. Esses modelos de canal são criados no Microsoft Teams quando um incidente de segurança grave é promovido.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

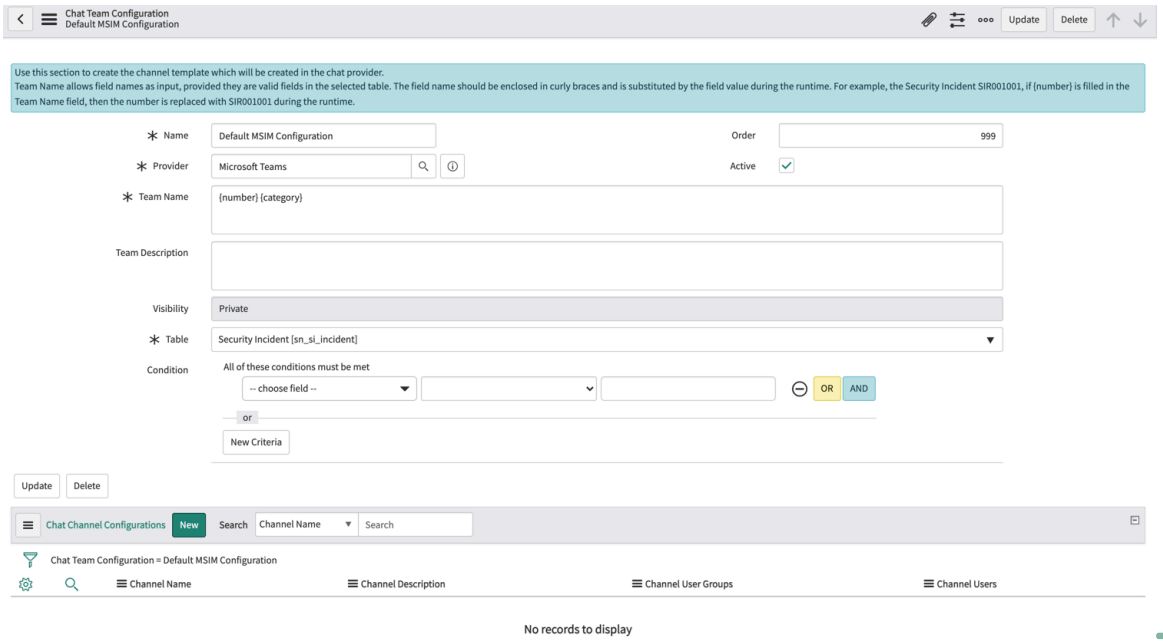
1. Navegar até **Gestão de incidentes graves de segurança** > **Canal de bate-papo** > **Modelos de canal**.
2. No formulário Configuração do canal de bate-papo, clique em **Novo** no cabeçalho do formulário.
3. No formulário, preencha os campos.

Formulário Configuração da equipe de bate-papo

Campo	Descrição
Nome	Nome da pasta.
Provedor	Microsoft Teams.
Nome da Equipe	Nome da equipe, por exemplo, no formato {number}-{category}. **Nota:** O nome da equipe fornecido aqui será usado em todos os registros de incidentes de segurança graves. Para garantir que o nome real do Microsoft Teams seja exibido na aplicação MS Teams e tenha um valor de nome exclusivo para diferentes incidentes de segurança graves, é recomendável usar um valor de campo de incidente exclusivo, como o número do incidente - {number}. Conforme mostrado no exemplo de captura de tela, o {number} seguido por um separador '-' e a variável de campo {category} forneceria um número exclusivo e uma descrição do incidente de segurança grave para o qual o Microsoft Teams foi criado, por exemplo {number} - {categoria}.
Descrição da equipe	Descrição opcional da equipe.
Tabela	Incidente de segurança grave (sn_msi_incident).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em **Enviar**.
5. Navegue até a seção Configuração do canal de bate-papo.
6. Clicar **Novo** para criar uma nova configuração de canal de bate-papo.
7. Insira o **Configuração da equipe de bate-papo** e **Nome do canal**.

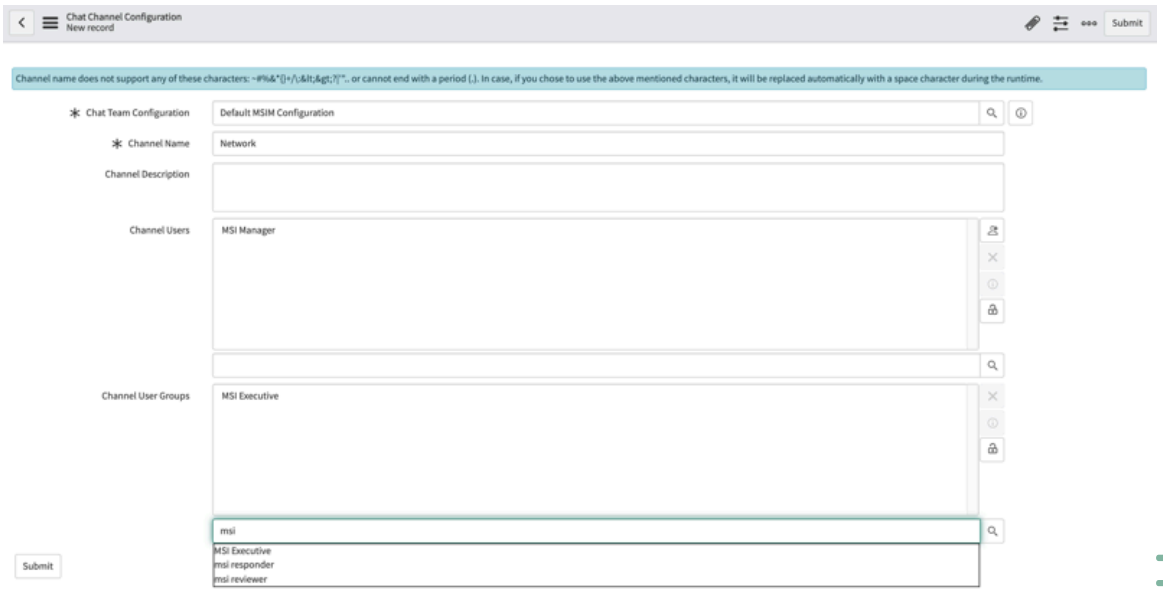
   Nota:
   O novo canal que você criou aqui também será o nome do seu canal no Microsoft Teams. Você pode pesquisar o mesmo canal e adicionar suas conversas.

8. Adicionar o **Usuários do canal** e **Grupos de usuários do canal** na lista de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Enviar o novo registro de configuração do canal de bate-papo.



Resultado

O canal de bate-papo agora foi criado e os usuários são atribuídos a esses grupos de canal de bate-papo. Você pode exibir as atividades de bate-papo de colaboração em Microsoft Teams e no fluxo de atividades de colaboração do espaço do MSIM com a estrutura de hierarquia do canal de bate-papo organizado conforme definido na configuração do provedor do canal de bate-papo.

Exibir atividade de mensagem de bate-papo

A atividade de mensagem de bate-papo é registrada e exibida na guia Colaboração do espaço do Major Security Incident Management.

A atividade de mensagem de bate-papo inclui todas as conversas de bate-papo ocorridas entre os participantes, diferentes grupos de usuários.

Solução de problemas do conector de bate-papo do MS Teams para MSIM

Consulte a seção de solução de problemas do conector de bate-papo do Microsoft Teams nos trabalhos programados, nas propriedades do sistema e nos subfluxos do designer de fluxo do Microsoft Teams.

Em qualquer caso, verifique os trabalhos programados do processo do conector de bate-papo se as mensagens do bate-papo de colaboração não forem publicadas no Microsoft Teams e no fluxo de atividades de colaboração externo do espaço do MSIM.

Trabalhos programados para Microsoft Teams

Trabalhos programados são trabalhos automatizados que são executados para processar as notificações do Microsoft Teams conector de bate-papo e renovar as assinaturas do Microsoft Teams em uma programação recorrente.

Função necessária: administrador

- **Conector de bate-papo do MS Teams: notificação de processo**

  Para cada evento de mensagem de bate-papo, será recebida uma notificação que terá o ID do recurso e a notificação armazenados em uma tabela. Um trabalho programado é executado a cada 30 segundos para selecionar notificações não processadas e consultar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a API do Microsoft Teams para obter o conteúdo real da mensagem, que é armazenado em uma tabela diferente.

- **Conector de bate-papo do MS Teams: renovar assinaturas**

  Para cada canal da equipe, são criadas assinaturas para ser notificado dos eventos criados, atualizados e excluídos. Esta assinatura está ativa por apenas 60 minutos. As assinaturas são renovadas a cada 25 minutos por meio do trabalho de programação do Conector do Microsoft Teams: Notificação de Renovação.

Microsoft Teams Fluxo funcional do conector de bate-papo

Exiba esta seção para entender os Microsoft Teams subfluxos do Flow Designer relacionados usados para administrar a criação de canais de bate-papo e o acesso do usuário do incidente de segurança grave.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

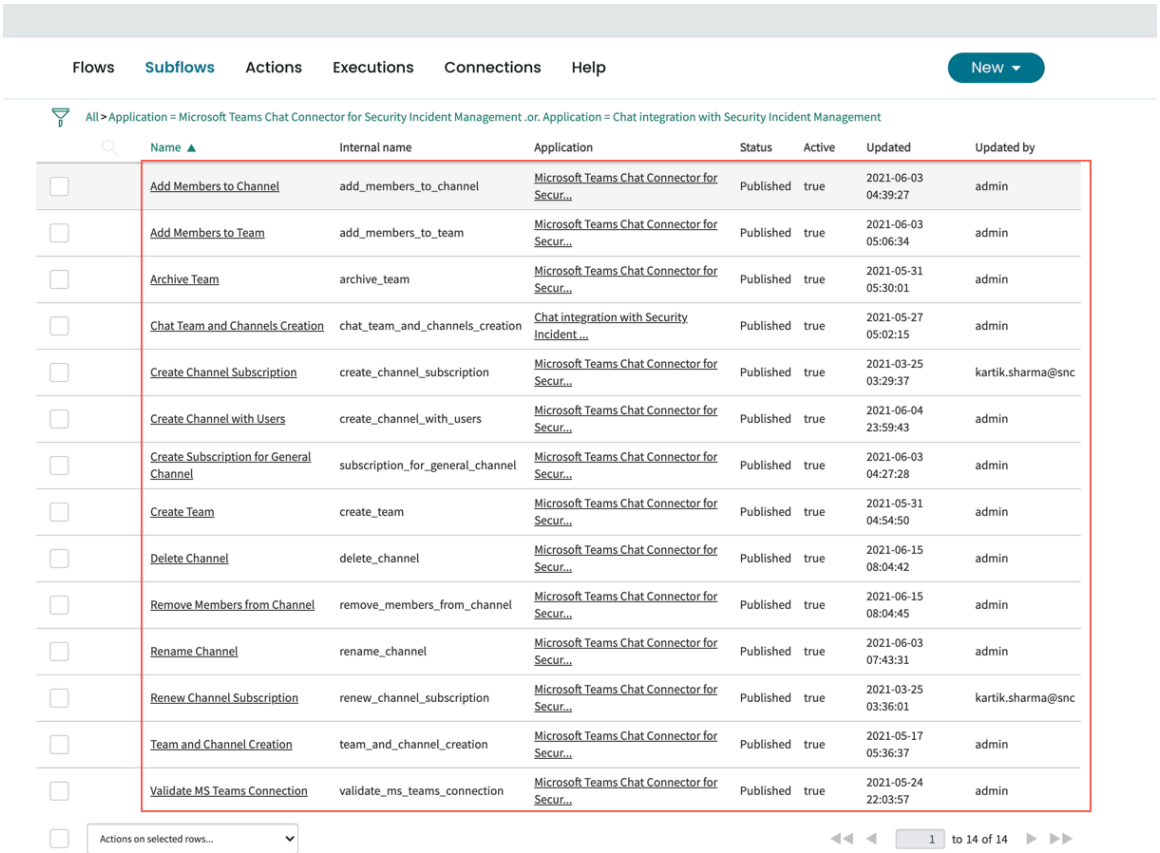
Procedimento

1. Navegar até **Todos** > **Flow Designer**.
2. Adicionar membros ao canal
3. Adicionar membros à equipe
4. Arquivar equipe
5. Criação de equipe e canais de bate-papo
6. Criar assinatura de canal
7. Criar canal com usuários
8. Criar assinatura para canal geral
9. Criar Equipe
10. Excluir canal
11. Remover membros do canal
12. Renomear canal
13. Renovar assinatura de canal
14. Criação de equipe e canal

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

15. Validar conexão do MS Teams



Administração do Gestão de incidentes graves de segurança

Planeje e configure a sua implementação do Gestão de incidentes graves de segurança.

Você pode configurar os seguintes aspectos da administração de Gestão de incidentes graves de segurança :

Habilitar proposta, promoção e vinculação de incidentes de segurança graves

Permita que os usuários decidam propor ou promover incidentes como incidentes de segurança graves. Rastreie facilmente todos os incidentes relacionados a um incidente de segurança grave, permitindo que os incidentes de segurança sejam vinculados ao incidente primário ou secundário.

Antes de Iniciar
Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configurações**.
2. Permita que os usuários proponham um incidente de segurança a um incidente de segurança grave, marcando a caixa de seleção **Propor** incidente de segurança grave na seção Ações do espaço de SIR/VR.
3. Permita que os usuários promovam um incidente de segurança a um incidente de segurança grave, marcando a caixa de seleção **Promover a** incidente de segurança grave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Habilite a vinculação de um incidente de segurança a um incidente de segurança grave para que eles possam ser rastreados juntos, marcando a caixa de seleção **Vincular ao** incidente de segurança grave.
5. Selecione **Atualizar**.

Marcar incidentes de segurança como incidentes de segurança graves

Marque ou rotule os incidentes de segurança ou registros vulneráveis para um incidente de segurança grave quando o incidente for proposto ou promovido. Se um incidente de segurança for proposto, o registro do incidente será referido como candidato a incidente de segurança grave. Quando uma segurança é promovida, o registro do incidente é referido como Incidente de segurança grave com o estado Aceito.

Antes de Iniciar
Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configurações**.
2. Habilite a caixa de seleção **Exibir rótulos** para rotular o candidato a incidente proposto como incidente de segurança grave, selecionando o campo de pesquisa **Nome do rótulo - Propor como candidato** e selecione Candidato a incidente de segurança grave na seção **Rótulos do espaço de SIR/VR**.
3. Habilite a caixa de seleção **Exibir rótulos** para rotular o candidato a incidente promovido como incidente de segurança grave, selecionando o campo de pesquisa **Nome do rótulo - Promoção a** incidente de segurança grave e selecione Incidente de segurança grave na seção **Rótulos do espaço de SIR/VR**.
4. Selecione **Atualizar**.

Configurar rótulos para incidentes de segurança graves

Configure rótulos na gestão de incidentes de segurança graves para criar rótulos personalizados e filtrar as atividades e tarefas de colaboração externas no fluxo de atividades. Os diferentes tipos de rótulos implementados são rótulos de estado e rótulos de linha do tempo.

Antes de Iniciar
Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configurações**.
2. Habilite a caixa de seleção **Exibir rótulos** para habilitar a rotulagem de diferentes estados de incidente, como Análise, Conter, Erradicar, Recuperar, Revisar, Evento da linha do tempo na seção **Rótulos do espaço do MSIM (Exibir em atividades e tarefas de colaboração)**.
3. Selecione **Atualizar**.

Configurar rótulos para incidentes de segurança graves

Configure diferentes tipos de rótulos para filtrar melhor e também indicar os estados do incidente. Os rótulos de incidentes de segurança graves fornecem a flexibilidade para rotular as atividades e tarefas de colaboração dos registros de incidentes.

Antes de Iniciar
Função necessária: sn_msi.workspace_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode selecionar ou desmarcar os rótulos usando o ícone de rótulos que está disponível na seção Fluxo de atividades da seção Colaboração e organizador de tarefas do espaço do MSIM.

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Rótulos do ISG**.
2. Clique em **Novo** para criar um novo rótulo.
3. Preencha o formulário com **Nome dorótulo e Cor do rótulo**.
4. Clique **em Criar rótulo**.
5. OOTB. A seguir estão os rótulos configurados para cada estado de incidente e você não pode modificar o nome ou a cor do rótulo:
   - Análise
   - Contém
   - Erradicar
   - Revisão
   - Recuperar
   - Evento da linha do tempo

Nota:
Você pode modificar os rótulos personalizados e suas propriedades.

Definir preferências de notificação para MSIM

Automatize o processo de notificação por e-mail e notifique os usuários quando um incidente de segurança for proposto ou promovido a um candidato a incidente de segurança grave.

Função necessária: sn_msi.workspace_admin.

As notificações são acionadas somente quando um incidente de segurança é proposto e enviado a todos os usuários e grupos que estão configurados para a lista de notificações. Por padrão, a notificação por e-mail é recebida pelo usuário que propôs o incidente de segurança como um candidato a incidente de segurança grave.

Notificação: incidente de segurança proposto (SI) como incidente de segurança grave (MSI)

Quem receberá:

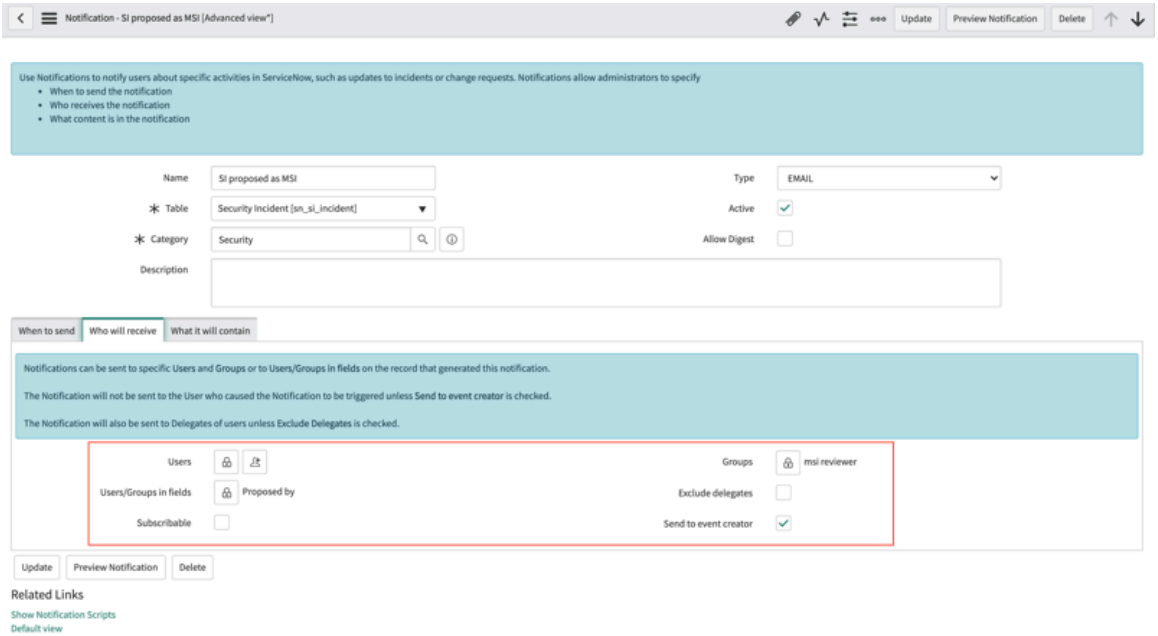
- Por padrão, **Revisores do ISG** O nome do grupo foi criado e qualquer usuário adicionado a este grupo terá o privilégio de ser um **Gerenciador do MSIM** e os usuários desse grupo receberão os e-mails de notificação.
- Qualquer usuário específico que seja adicionado ao **Usuários** A lista também receberá os e-mails de notificação.

O que conterá:

Se você quiser modificar o conteúdo do e-mail, como o corpo do e-mail que inclui o Assunto ou a Mensagem HTML, você deve ter o acesso à função de Administrador do Sistema ou ser atribuído como Administrador do Sistema e não Administrador do MSI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Notificação: incidente de segurança promovido (SI) como incidente de segurança grave (MSI)

Esta notificação é acionada quando um incidente de segurança é promovido e quando o Explorador de arquivos e a estrutura de base Microsoft Teams são criados. Por padrão, esta notificação é recebida pelo usuário que promoveu o incidente de segurança a um incidente de segurança grave.

Quem receberá

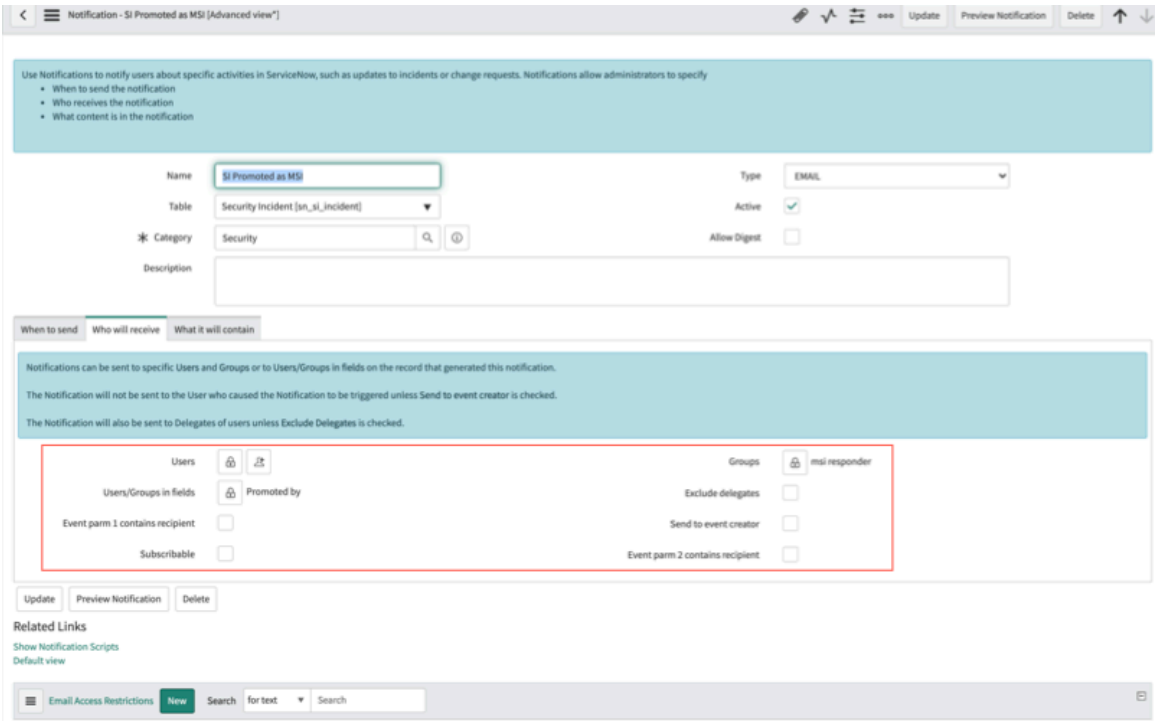
- Por padrão, um **Grupo** por nome **Respondente do MSI** foi criado e qualquer usuário adicionado a este grupo terá o privilégio de ter **Respondente do MSIM** A função e todos os usuários desse grupo receberão o e-mail de notificação.
- Qualquer usuário específico que seja adicionado ao **Usuários** A lista também receberá os e-mails de notificação.

O que isso conterá

Se você quiser modificar o conteúdo do e-mail, como o corpo do e-mail, que inclui o Assunto ou o HTML da mensagem, você deve ter o acesso à função de Administrador do sistema ou ser atribuído como Administrador do sistema e não como Administrador do MSI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Configurar atividades de fechamento do ISG

Estabeleça ações que ocorrerão automaticamente quando um incidente de segurança grave for encerrado. Aumente a segurança arquivando e removendo automaticamente o acesso a pastas que contêm informações de resolução.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configurações**.
2. Arquive as comunicações de bate-papo relacionadas à resolução do incidente marcando a caixa de seleção **Arquivar canais de colaboração** na seção Ações de fechamento automatizadas.
3. Remova pastas que contêm material relacionado à resolução do incidente marcando a caixa de seleção **Remover pastas de colaboração**.
4. Selecione **Atualizar**.

Gestão de incidentes graves de segurança espaço

Gestão de incidentes graves de segurança fornece um espaço dedicado para gerenciar incidentes de segurança graves projetados especificamente para o gerente Incidente de segurança grave.

Colabore facilmente em atividades que ajudam a resolver os principais incidentes de segurança compartilhando e exibindo arquivos e pastas, exibindo e atualizando tarefas de incidente e se comunicando com aqueles que trabalham no incidente por meio de canais de bate-papo dedicados.

O Gerenciamento de incidentes de segurança graves (MSIM) fornece um mecanismo para rastrear e resolver incidentes de segurança graves. O MSIM funciona em conjunto com os recursos de produto de resposta a incidentes e vulnerabilidades de segurança existentes

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e melhora o processo de correção de incidentes de segurança graves com os seguintes recursos:

- Espaço dedicado para gerenciar incidentes de segurança graves projetados especificamente para a função de usuário de gerenciador de incidentes de segurança graves.
- Organize as principais tarefas de resposta a incidentes de segurança, incluindo tarefas rastreadas em incidentes de segurança vinculados e grupos de vulnerabilidades.
- Automatize a criação de pastas de colaboração e canais de comunicação de bate-papo depois que um incidente de segurança grave for criado, bem como o arquivamento como parte do fechamento do incidente.
- Componente do explorador de arquivos para organizar e rastrear a coleção de artefatos (arquivos) relacionados ao incidente de segurança grave por meio de uma integração Microsoft SharePoint.
- Gerenciador de canal de bate-papo e componentes do fluxo de atividades para gerenciar as comunicações em vários grupos funcionais, de segurança e de TI por meio de uma integração Microsoft Teams.
- Relatório resumido do impacto do incidente de segurança grave e métricas de progresso, incluindo acúmulo de ativos afetados, usuários, locais e recursos da equipe, bem como linha do tempo de marcos de incidentes significativos.

Use o espaço do MSIM para rastrear e resolver incidentes de segurança graves:

1. Exiba os gráficos de tendências e o andamento do incidente de segurança grave.
2. Rastreie e organize a atividade de arquivos do Microsoft SharePoint por meio do espaço do MSIM.
3. Rastreie e organize a atividade de bate-papo do Microsoft Teams por meio do espaço do MSIM.
4. Exiba e atualize os detalhes do incidente por meio do espaço do MSIM.
5. Filtrar atividades de colaboração no Fluxo de atividades do espaço do MSIM.

Como usar Gestão de incidentes graves de segurança

Os gerentes podem usar o espaço Gestão de incidentes graves de segurança para exibir os registros de incidentes propostos, promovidos, vinculados e rejeitados e rastrear suas atividades relacionadas.

Propor, promover e vincular registros de incidentes

Proponha ou promova incidentes de segurança como incidentes de segurança graves quando os incidentes forem identificados como ameaça crítica para a organização.

Depois que o Gerenciamento de incidentes de segurança graves estiver instalado na sua instância ServiceNow, você poderá lidar com a transição de incidentes de segurança para incidentes graves da seguinte forma:

- Propor um incidente de segurança ao candidato a incidente de segurança grave para iniciar um processo de revisão.
- Promova diretamente um incidente de segurança a um incidente de segurança grave sem um processo de revisão.
- Rejeitar um incidente de segurança proposto como um incidente de segurança grave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você também pode vincular um incidente de segurança como um incidente secundário ao incidente de segurança grave para que todos os incidentes de segurança relacionados possam ser rastreados juntos.

Propor como Incidente de segurança grave

Propor um incidente de segurança para um incidente de segurança grave.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança na categoria relacionada que você deseja propor como incidente de segurança grave.
3. Selecione o ícone Ações adicionais e selecione **Propor incidente de segurança grave**.
4. Na caixa de diálogo Propor incidente de segurança grave, preencha os campos.
   a. **Data de detecção**: data em que o incidente de segurança grave foi criado ou proposto pela primeira vez
   b. **Justificativa**: forneça a justificativa para propor o incidente.
   c. **Impacto potencial**: indique o impacto do incidente.
5. Selecione **Propor**.

Resultado

O incidente é proposto e as seguintes ações ocorrem:

- No registro de incidente de segurança, uma mensagem de faixa de verificação é exibida e o marcador de incidente de segurança grave definido é exibido.
- O registro aparece na lista relacionada Incidente de segurança grave no registro do incidente, com o estado listado como Proposto e na lista de Candidatos ao espaço do MSIM.
- A seção Atividade no Espaço do MSIM mostra que o incidente de segurança foi proposto para ser promovido como um incidente de segurança grave.
- Uma mensagem é enviada para aqueles na lista de notificação definida que contém um link para o registro do incidente e a guia Detalhes do incidente.

Promover a um Incidente de segurança grave

Promova um incidente de segurança a um incidente de segurança grave ou rejeite propostas promovidas por meio do espaço Gestão de incidentes graves de segurança (MSIM).

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Espaço do MSIM**.
2. Na lista Incidentes de segurança graves, selecione **Candidatos**.
3. No formulário Incidentes de segurança, selecione o incidente proposto para promoção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. **Opcional:** Revise os detalhes do incidente de segurança na seção Detalhes ou exiba os detalhes estendidos no registro do incidente em uma guia separada clicando em **Exibir mais detalhes**.
5. Promova o incidente de segurança ou rejeite a proposta de promoção.
   - Para promover o incidente, clique em **Promover a incidente de segurança grave**.
   - Para rejeitar a proposta de promoção, clique em **Rejeitar como incidente de segurança grave**.
6. Selecione **Salvar**.

Resultado

- Se você rejeitou a proposta de promoção, o incidente não será promovido e a entrada do incidente será movida para a guia Rejeitado.
- Se você promoveu o incidente, a entrada do incidente será movida para a guia Abrir e o registro de segurança exibirá um marcador indicando que é um incidente de segurança grave.
- A decisão é listada na seção Atividade do espaço do MSIM.

Depois que um incidente é promovido, a configuração padrão é aplicada.

- Uma estrutura de pastas é criada com base na configuração do modelo de pasta.
- Os canais de bate-papo são criados com base na configuração dos canais.
- Uma mensagem de e-mail é enviada aos usuários designados. A notificação padrão contém um link para o incidente de segurança grave e os detalhes do incidente. Os usuários designados agora também têm acesso aos recursos de colaboração, portanto, a notificação também inclui o nome do Microsoft Team e um link para pastas do Microsoft SharePoint relacionadas ao incidente.

Link para Incidente de segurança grave

Vincule incidentes de segurança a um incidente de segurança grave.

Antes de Iniciar

Função necessária: sn_msi.workspace_admin

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança na categoria relacionada que você deseja vincular ao incidente de segurança grave.
3. Selecione o ícone **Ações adicionais** e selecione **Vincular ao incidente de segurança grave**.
4. Selecione o incidente de segurança grave ao qual você deseja vincular.
   a. Na caixa de diálogo, selecione o ícone Pesquisar usando a lista.
   b. Selecione o incidente de segurança grave ao qual você deseja vincular.
   c. Selecione **OK**.
5. Selecione **Propor**.

Resultado

A proposta é enviada e ocorrem as seguintes ações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- No registro de incidente de segurança, uma mensagem de faixa de verificação é exibida e o marcador de Incidente de segurança grave definido aparece ao lado do campo **Selecionar marcador de segurança**.

- Na guia **Detalhes** do incidente de segurança grave em Gestão de incidentes graves de segurança, a lista suspensa do número de registro inclui ambos os incidentes.

- O registro aparece na lista relacionada de Incidente de segurança grave do registro do incidente, com o estado listado como Proposto.

- Uma mensagem é enviada para aqueles na lista de notificação definida que contém um link para o registro do incidente e a guia Detalhes do incidente.

- A seção **Atividade** no Espaço do MSIM mostra que o incidente de segurança foi adicionado como um incidente de segurança secundário ao incidente de segurança grave com um link.

Uso da exibição de lista do MSI no espaço do MSIM

Com a exibição de lista no espaço do MSIM, você pode exibir os incidentes de segurança graves propostos, promovidos e rejeitados.

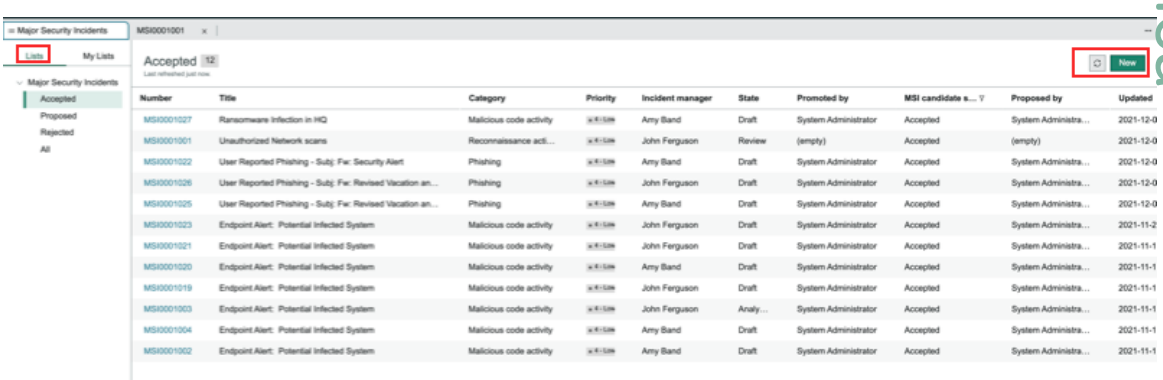
Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Você também pode criar novos incidentes usando o botão **Novo** disponível no canto superior direito do espaço.

Procedimento

1. Navegar até **Security Incident Response grave** > **Espaço do MSIM**.
2. Clique no ícone de listas para exibir a exibição Listas.



3. Clique em **Minhas listas** para criar sua própria lista de incidentes de segurança graves.
4. Consulte a tabela a seguir para saber o que você pode fazer na exibição de lista:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
Minhas listas	Crie novas listas de registros MSI e exiba as listas que você criou.
Definir filtros para uma coluna em uma lista	Selecione uma coluna e expanda o menu de pontos verticais para exibir opções que filtram ainda mais os dados na coluna.
Filtrar itens ou corresponder itens de uma linha em uma coluna	Selecione uma célula em uma coluna e refine os dados exibidos escolhendo um: ○ Mostrar correspondência: exibe somente os itens que correspondem ao item selecionado na coluna. ○ Filtrar — Filtra os itens da coluna que correspondem ao item selecionado na respectiva coluna.
Atualizar lista	Atualize as listas e exiba as listas completas que foram atualizadas.
Nova	Crie um novo registro MSI.

Exibir Incidente de segurança grave gráficos de tendências

Fornecer relatórios de resumo atualizados do impacto e do andamento do incidente de segurança grave é um aspecto importante do gerenciamento de um incidente de segurança grave usando o novo espaço.

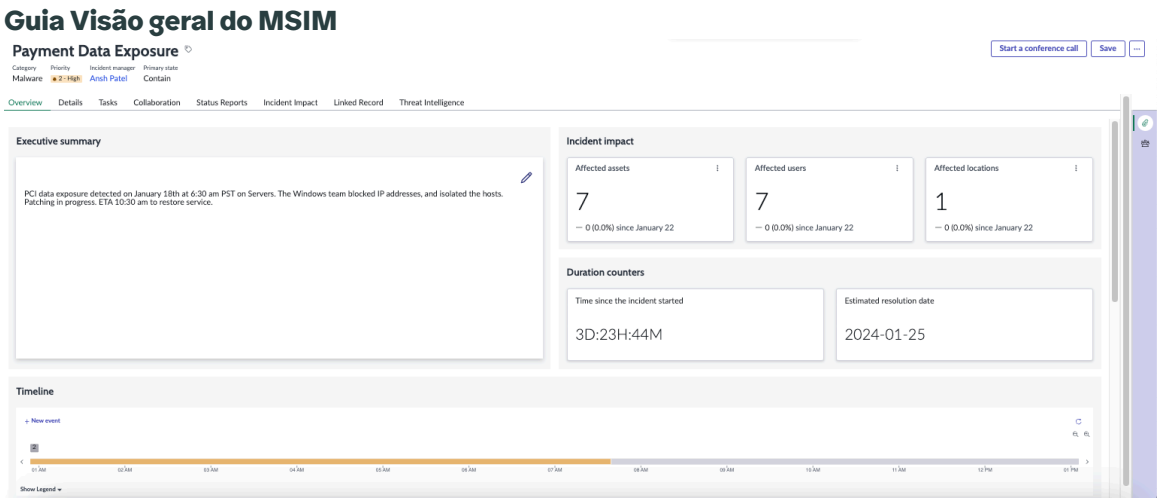
A guia **Visão geral** fornece as métricas relevantes para gerenciar o escopo e o andamento do incidente, incluindo o acúmulo de ativos afetados, usuários, locais e recursos da equipe, bem como a linha do tempo de marcos de incidentes significativos.

A linha do tempo fornece uma exibição horizontal dos principais eventos e marcos que ocorreram como parte da resolução do incidente de segurança grave específico. O componente da linha do tempo é exibido na parte superior de todas as guias do espaço do Gerenciamento de incidentes de segurança graves, com a capacidade de recolher e expandir para exibição conforme necessário. Os dados de eventos representados serão atualizados e atualizados sempre que eventos de marco designados ou marcos forem adicionados ou atualizados.

Cada evento ou marco é indicado com uma opção de tipo de evento de linha do tempo diferente para identificar o número e o tipo de eventos ou marcos. Por exemplo, atualizações de registro do NOW, tarefas e atividades de colaboração. Além disso, o período de intervalo de tempo para os diferentes estados de incidente de segurança grave é rastreado automaticamente e exibido usando intervalos codificados por cores exibidos junto com a duração de cada estado de incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você pode habilitar ou desabilitar a exibição de determinados tipos de evento para indicadores de linha do tempo e intervalos de linha do tempo usando os botões de alternância de filtro.

Consulte a tabela a seguir abaixo para obter recursos adicionais disponíveis com o componente da linha do tempo.

Recursos adicionais do componente da linha do tempo

Tarefa	Descrição
Novo evento	Cria novos eventos personalizados e associa esses eventos ao registro do MSI. Isso ajuda a criar eventos para datas passadas e futuras que podem não ser capturadas por meio de uma tarefa rotulada, mudança de estado de registro ou atividade de colaboração rotulada, que são exibidas por padrão na linha do tempo.
Redefinir	Redefine qualquer ampliação/redução ou filtros que tenham sido aplicados à linha do tempo para que a exibição padrão seja fornecida.
Indicadores da linha do tempo	Lista os vários tipos de eventos, como mudanças de campo do Now Record, tarefas rotuladas, atividades de colaboração rotuladas e outro (personalizado), junto com os ícones e o número total de eventos que ocorreram em relação a cada indicador de tipo de evento. O indicador deslizante permite habilitar ou desabilitar todos os eventos para um tipo de evento específico.
Mostrar legenda	Selecione para exibir a legenda suspensa com diferentes tipos de indicadores de linha do tempo.
Barra de andamento da linha do tempo	Exibe o andamento geral do incidente por meio de eventos de linha do tempo designados ou marcos que ocorreram nos diferentes intervalos de linha do tempo exibidos.
Intervalos de linha do tempo	Exibe vários tipos de estado de incidentes e duração conforme o incidente progride ao longo do ciclo de vida completo do incidente de segurança grave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

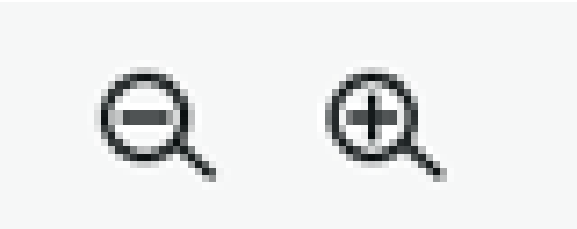
Recursos adicionais do componente da linha do tempo

Tarefa	Descrição
	Habilite ou desabilite um evento específico com base no estado do incidente.

Para criar um novo evento, siga estas etapas:

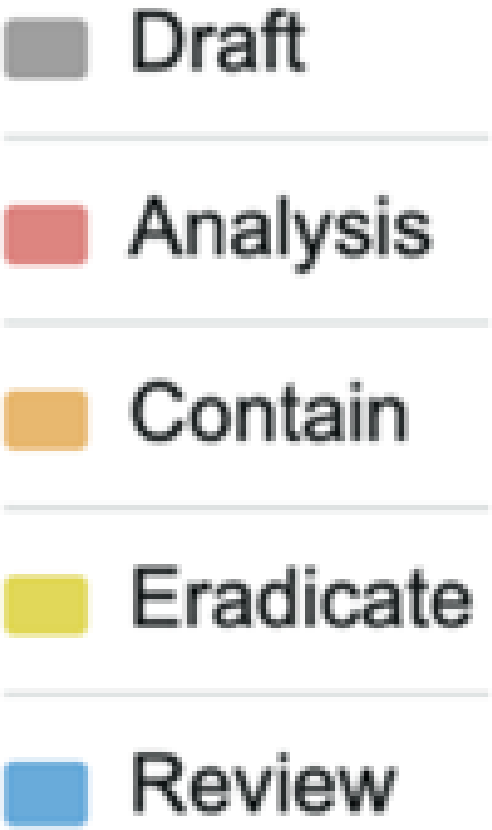
1. Na seção Linha do tempo da guia Visão geral, selecione **Novo evento**.
2. No pop-up Adicionar um novo evento da linha do tempo, forneça o **Título**do **evento, o Carimbo**de data/hora do **evento e o Corpo do evento**.
3. Selecionar **Criar**.

A tabela a seguir descreve os ícones usados no componente da linha do tempo.

Ação	Descrição
	Aumente ou diminua o zoom na barra de andamento da linha do tempo, incluindo a exibição de eventos individuais quando os números forem exibidos para representar vários eventos próximos.
	Os eventos de chave do Now Record, que são criados automaticamente durante uma nova criação de registro do MSI ou mudança de estado de promoção, mudança de data de detecção, data de resolução estimada e outras mudanças de valor de campo de registro de chave.
	O evento de tarefa detalha quando uma tarefa foi rotulada com o rótulo ou marcador da linha do tempo na seção da guia Organizador de tarefas do espaço.
	Os outros eventos ou marcos personalizados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação	Descrição
	O evento de colaboração detalha quando há bate-papos específicos ou atividades de colaboração que foram rotuladas com o rótulo ou marcador da linha do tempo na seção da guia Colaboração do espaço.
	A duração da linha do tempo para os diferentes estados de incidente do registro do ISG.

Exibir Incidente de segurança grave métricas de impacto

Exiba as métricas de andamento do impacto do incidente de segurança grave visualizadas como gráficos de barras e tabelas.

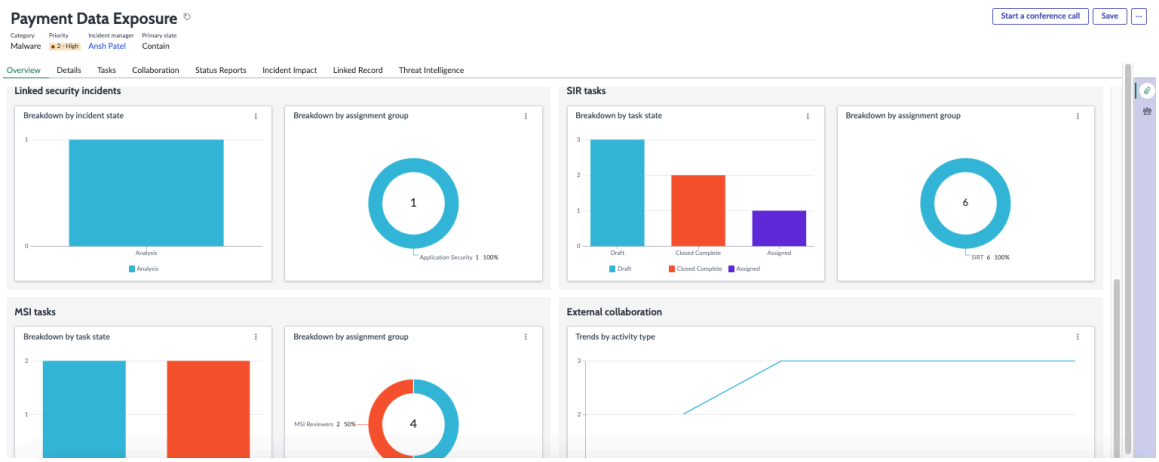
Além da linha do tempo do incidente e das visualizações do gráfico de tendências de andamento, o **Visão geral** A guia fornece métricas de impacto relevantes para gerenciar o escopo de mudança do incidente, incluindo acúmulo de ativos afetados, usuários, locais e recursos da equipe.

As contagens exibidas nos componentes de visualização são baseadas em tarefas ativas em incidentes vinculados do Security Incident Response (SIR). Conforme as tarefas são abertas e encerradas, essas contagens mudam em termos de natureza e volume da atividade restante planejada para o incidente de segurança grave para representar as tendências mostradas nos componentes de visualização do gráfico de tendências.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral do MSIM



Consulte a tabela a seguir para obter as ações de IU que você pode executar em **Visão geral** seção:

Seções de IU de visão geral

Título	Descrição
Impacto do incidente	Esses componentes exibem os recursos afetados com base em um acúmulo de todas as tarefas ativas e incidentes vinculados com ativos identificados, usuários, locais e membros da equipe atribuídos. Os recursos afetados são: • Ativos afetados • Usuários afetados • Locais afetados • Indicadores • Observáveis Clicar nos valores numéricos permite que você faça uma busca detalhada e navegue até os ativos afetados, usuários e detalhes do local e exibe as tarefas relacionadas na guia **Impacto do incidente** do espaço. Com base no link do tipo de impacto do incidente selecionado, os detalhes do incidente relacionado, como tipo de tarefa e sua descrição, grupo de atribuição e estado do incidente são exibidos no **Impacto do incidente** Guia do espaço do MSIM.
Hora	Exibe o período em número total de dias a partir do momento em que o incidente de segurança grave está ativo. O tempo é calculado com base no **Data de detecção** inserido em **Detalhes** Guia do espaço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seções de IU de visão geral

Título	Descrição
	A data de detecção geralmente é capturada inicialmente quando o incidente de segurança grave foi criado ou proposto pela primeira vez. Sempre que esta data for modificada, a hora será calculada automaticamente, atualizada e exibida no formato dias: horas: minutos, por exemplo, 20D: 13H: 58M. **Data de resolução estimada**: a data em que a data de resolução do incidente é estimada para resolver. Essa data geralmente é capturada inicialmente quando o incidente de segurança grave foi criado ou promovido pela primeira vez. A data é atualizada e atualizada com base na data estimada fornecida no **Detalhes** Guia do espaço. Se a data estimada não for fornecida na seção Detalhes, esta seção exibirá "hífen" sem qualquer valor de data.
Equipe ativa	Exibe as diferentes equipes de resposta e os membros de cada equipe que estão trabalhando ativamente no incidente de segurança grave e nas tarefas relacionadas. **Equipe ativa** tendência: exibe o gráfico de tendências de cada equipe e dos membros da equipe que estão trabalhando ativamente no incidente de segurança grave e nas tarefas relacionadas em intervalos regulares. **Nota:** Exibir os grupos ativos atribuídos do **Detalhes** Guia do espaço.
Incidentes de SIR vinculados	**Por estado do incidente**: exibe a distribuição de incidentes de segurança vinculados com base em um estado de incidente, como Análise, Conter, Erradicar, Recuperar ou Revisar. **Tendências por estado do incidente**: indica ainda a exibição de tendência de como o número de incidentes vinculados está progredindo com base no estado do incidente. Selecionar cada link de estado de incidente permite que você navegue e exiba os detalhes do incidente de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seções de IU de visão geral

Título	Descrição
	vinculado diretamente no **Incidente de segurança/IV vinculado** Guia do espaço. Esta seção é atualizada e atualizada automaticamente sempre que ocorrem mudanças nos incidentes subjacentes.
Tarefas de resposta	Exibe os totais de tarefas ativas que estão vinculadas ao registro do MSI por meio de incidentes de SIR. • **Por estado da tarefa**: exibe as tarefas de resposta do incidente com base no estado do incidente, como Rascunho, Atribuído, Trabalho em andamento, Encerrado concluído. Este gráfico de distribuição permite um detalhamento de distribuição adicional por grupos de atribuição. Selecionar cada estado de tarefa permite que você exiba uma lista filtrada por estado de tarefa de incidente no **Tarefas** Guia do espaço. A exibição filtrada permite que você exiba e atualize os detalhes da tarefa individual. • **Tarefas em andamento por rótulo do estado do incidente**: exibe tarefas e grupos ativos com base no rótulo de estado do incidente que deve ser aplicado nos componentes do organizador de tarefas. Esses rótulos padrão têm valores como Análise, Conter, Erradicar, Recuperar ou Revisar para indicar a natureza da tarefa envolvida. • **Atrasado**: exibe as tarefas de resposta do incidente de segurança, que estão ativas e excederam a data de vencimento. Você pode exibir os detalhes de todas as tarefas atrasadas selecionando a contagem total de Atrasados e navegando automaticamente para a guia Tarefas. • **Tendências por estado da tarefa**: exibe a tendência de andamento do trabalho em andamento e das tarefas de resposta encerradas ao longo da duração do incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seções de IU de visão geral

Título	Descrição
	Nota: O gráfico de tendências recupera os dados mais recentes com base no trabalho programado. Você pode configurar ou modificar o intervalo de tempo de recuperação de dados conforme necessário.
Tarefas do MSI	Exibe as tarefas ativas no total, que foram criadas diretamente no registro do MSI (e não são tarefas de resposta vinculadas): **Por estado da tarefa:** Exiba as tarefas criadas pelo incidente de segurança grave, as tarefas atribuídas e suas informações relacionadas. Selecionar cada estado de tarefa permite que você exiba uma lista filtrada por estado de tarefa de incidente no **Tarefas** Guia do espaço. A exibição filtrada permitirá exibir e atualizar os detalhes da tarefa individual.
Colaboração externa	Exibe as atividades de colaboração no total para todas as atividades de colaboração rotuladas do fluxo de atividades de colaboração: • **Por rótulo de estado do incidente:**Exiba os dados de atividades de colaboração de incidentes que são coordenados com arquivos e pastas Microsoft Teams e Microsoft SharePoint e são rotulados usando rótulos de estado de incidente, como Análise, Conter, Erradicar ou Recuperar na guia **Colaboração** do espaço. • **Tendências por tipo de atividade**: exibe o gráfico de tendências para o número de Microsoft Teams e Microsoft SharePoint atividades de arquivos e pastas ao longo da duração do incidente.

Atualizar Incidente de segurança grave detalhes

Exiba e atualize detalhes específicos relacionados ao incidente de segurança grave, como Detalhes do registro do incidente, Participantes ativos da equipe e o log de atividades correspondente.

Todos os detalhes relacionados ao incidente de segurança grave são exibidos com várias seções de formulário na guia **Detalhes** do espaço. Exibe os detalhes, como Detalhes do registro do incidente, Participantes da equipe ativa e o log de atividades correspondente. Você também pode exibir os incidentes de SIR vinculados, os detalhes do registro de grupo de vulnerabilidade e uma capacidade de transmitir uma publicação de atividade para todos os registros de incidentes vinculados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A guia Detalhes contém principalmente:

1. Campos de formulário de incidente de segurança grave e seções de IU relacionadas a incidentes.
2. Fluxo de atividades

A tabela a seguir fornece os detalhes dos campos do formulário de incidente de segurança grave:

Seções de formulário de Incidente de segurança grave

Campo	Descrição
Incidente	
Número	Número do incidente de segurança grave.
Estado principal	O estado primário do incidente de segurança grave.
Data de detecção	A data em que o incidente de segurança grave foi criado ou proposto pela primeira vez. Sempre que você modifica a Data de detecção na guia Detalhes, a data e a hora do MSI são automaticamente calculadas, atualizadas e exibidas na **Hora** > **Tempo desde o início do incidente** seção na seção **Visão geral** do espaço.
Título	Título de incidente de segurança grave.
Origem	Origem do incidente de segurança grave.
Categoria	Categoria do incidente de segurança grave.
Subcategoria	Tipo de subcategoria do incidente de segurança grave.
Data de resolução estimada	A data em que a data de resolução do incidente é estimada para resolver. A data estimada é a data em que o incidente de segurança grave foi criado ou promovido pela primeira vez.
Prioridade	Indica a prioridade do incidente de segurança grave.
Equipe ativa	
Gestão de incidentes	Nome do gerente de incidentes.
Grupos Designados	Indica as diferentes equipes de resposta e os membros de cada equipe que estão trabalhando ativamente no incidente de segurança grave.
Candidato	
Estado do candidato a ISG	Indica o estado do candidato a incidente de segurança grave, como proposto ou promovido. Se o incidente for promovido, o estado será exibido como Aceito.
Promovido por	Usuário que promoveu o incidente de segurança grave.
Promovido	Data em que o incidente de segurança grave foi promovido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seções de formulário de Incidente de segurança grave

Campo	Descrição
Justificativa	Justificativa do incidente de segurança grave.
Impacto potencial	Indica o possível impacto e a severidade do incidente de segurança grave.
Restrição	
Impor restrição	Selecione esta opção para impor restrições a determinados incidentes de segurança graves. Você pode impor restrições para limitar o acesso de exibição ou modificação somente a determinados usuários ou grupos. Para obter mais informações, consulte Restringir o acesso a determinados incidentes de segurança graves
Membros permitidos	Lista de usuários que podem acessar o incidente de segurança grave.
Grupos permitidos	Lista de grupos que podem acessar o incidente de segurança grave.
Outras ações	
Anexo	Quaisquer anexos relacionados ao incidente de segurança grave. Selecionar **Selecione** a opção para adicionar anexos ao incidente.
Chamada em conferência	Use chamadas em conferência com os provedores de serviços de terceiros como um canal de comunicação para se reunir com as partes interessadas para resolver os principais incidentes de segurança. Para obter mais informações, consulte Gestão de incidentes graves de segurança Integração de chamada em conferência

Atividade:

Use a seção Atividade para adicionar anotações de trabalho e comentários, publique sua atividade em particular e adicione comentários adicionais conforme necessário usando a seção Compor. Salve a atividade depois de publicar suas anotações de trabalho e comentários para exibir a atividade ou as anotações de trabalho adicionadas na seção Atividade.

Nota:
Clique no link **Mostrar mais** detalhes para exibir os detalhes de um registro de incidente de segurança específico, que está associado a esse incidente de segurança grave.

Você define suas preferências para exibir as atividades relacionadas, como:

1. **Filtros**: selecione o ícone **Conjuntos** de filtros para definir filtros.

   Defina filtros para exibir as conversas de atividade, como atividades adicionadas às anotações de trabalho, e-mail, linha do tempo e comentários adicionais.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. **Sinalizado**: clique no ícone Sinalizado para **sinalizar** as atividades.

   Sinalize todas as conversas de atividade importantes para você revisitar rapidamente quando necessário.

Restringir o acesso a determinados incidentes de segurança graves

Gerencie quem pode exibir ou modificar os incidentes de segurança graves que contêm informações confidenciais. Você pode impor restrições de incidentes de segurança graves para determinar quem tem acesso para exibir ou modificar determinados registros de incidentes de segurança graves e listas relacionadas e limitar o acesso de leitura ou gravação somente a determinados usuários ou grupos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Por Que e Quando Desempenhar Esta Tarefa

As restrições de incidente de segurança grave permitem que você oculte incidentes de segurança graves críticos de serem acessados ou modificados por todos os usuários ou grupos em uma organização específica. Essas restrições permitem que você forneça uma maneira mais granular de controlar os incidentes de segurança graves que um usuário ou grupo pode exibir ou modificar. Você pode impor uma restrição de incidente de segurança grave marcando a caixa de seleção **Impor restrição** e selecionando os usuários ou grupos com permissão para exibir ou modificar o incidente de segurança grave específico.

Depois de impor a restrição de incidentes de segurança graves ou listas relacionadas a determinados usuários ou grupos, todos os usuários ou grupos restantes em sua organização não poderão exibir ou modificar esses incidentes de segurança graves ou listas relacionadas.

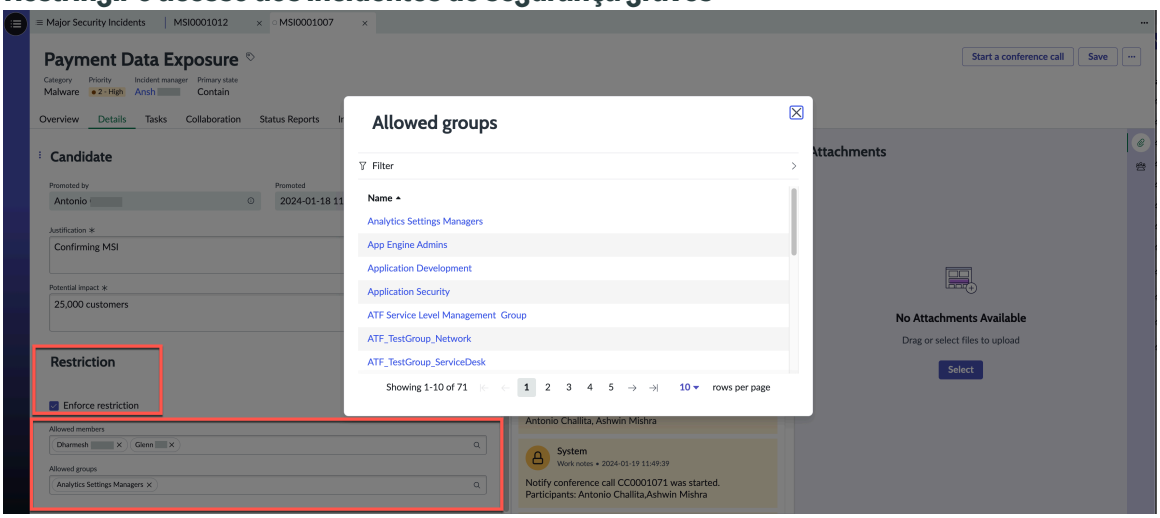
Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Detalhes**.
5. Role para baixo e selecione a seção **Restrição**.
6. Marque a caixa de seleção **Impor restrição** para habilitar a restrição do incidente de segurança grave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Restringir o acesso aos incidentes de segurança graves



7. No campo Membros permitidos, selecione os usuários que podem exibir ou modificar o incidente de segurança grave usando a opção Pesquisar.
8. No campo Grupos permitidos, selecione os grupos que podem exibir ou modificar o incidente de segurança grave usando a opção Pesquisar.

> **Nota:**
> Depois que a caixa de seleção **Impor restrição** estiver habilitada para o incidente de segurança grave, somente o sn_msi.workspace_manager e os membros ou grupos permitidos terão acesso para exibir ou modificar o incidente de segurança grave.

9. Selecione **Salvar**.

Vincular registros adicionais a Incidente de segurança grave

No espaço de trabalho, use a funcionalidade de vinculação de registros para vincular quaisquer registros de incidentes de segurança relacionados e seus incidentes de segurança secundários, Tarefas de correção do Vulnerability Response e Casos de segurança da Inteligência contra ameaças a um registro Incidente de segurança grave (MSI).

Antes de Iniciar

Função necessária: sn_msi.workspace_manager e sn_msi.workspace_responder

Procedimento

1. Navegar até **Security Incident Response grave** > **Espaço do MSIM**.
2. Navegue até a exibição **Listas**, que é exibida no painel esquerdo do espaço.
3. Clique em **Aceito** para selecionar os registros de incidentes de segurança graves promovidos.
4. Selecione o registro de incidente que precisa ser vinculado e que não está no estado Encerrado na lista de registros promovidos.
5. Clique na guia **Registros vinculados**.
   Uma lista suspensa é fornecida para selecionar outras tabelas de registro vinculadas.
   A seção Registros vinculados exibe os registros vinculados e os registros relacionados que foram vinculados ao incidente de segurança grave.
6. Selecione a exibição de tabela desejada, como Incidentes de segurança, Tarefas de correção (itens vulneráveis) ou Caso de segurança na lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Com base na exibição da tabela de registros do tipo de seleção, os registros vinculados que estão vinculados aos registros de incidentes de segurança graves são exibidos.

7. Vincule um registro que não esteja vinculado a nenhum registro do MSI e esteja no estado **Aberto** selecionando o registro e clicando em **Vincular registro** no canto superior direito da página.

   Nota:
   Você não pode vincular um registro de incidente a um registro do MSI se ele estiver no estado **Encerrado**.

8. Selecione o registro a ser vinculado e clique em **Vincular**.
   Uma mensagem de confirmação exibe que o registro foi vinculado com sucesso e que o acúmulo de registros relacionados será processado em segundo plano.

   Nota:
   Depois que um registro é vinculado, a exibição de lista é atualizada automaticamente e lista a lista atualizada de registros de incidentes.

Tópicos relacionados

Desvincular registros de Incidente de segurança grave

Desvincular registros de Incidente de segurança grave

Usando o espaço do Gerenciamento de incidentes de segurança graves, desvincule os registros de incidentes de segurança graves da seção Registros vinculados.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager e sn_msi.workspace_responder

Nota:
Você só pode desvincular um único registro de cada vez. Depois de desvincular um registro, as informações acumuladas relacionadas serão removidas das seções Impacto do incidente e Inteligência contra ameaças no espaço de trabalho, e a ação não poderá ser desfeita.

Para obter mais informações sobre registros de acúmulo, consulte Estrutura de Rollup para MSIM.

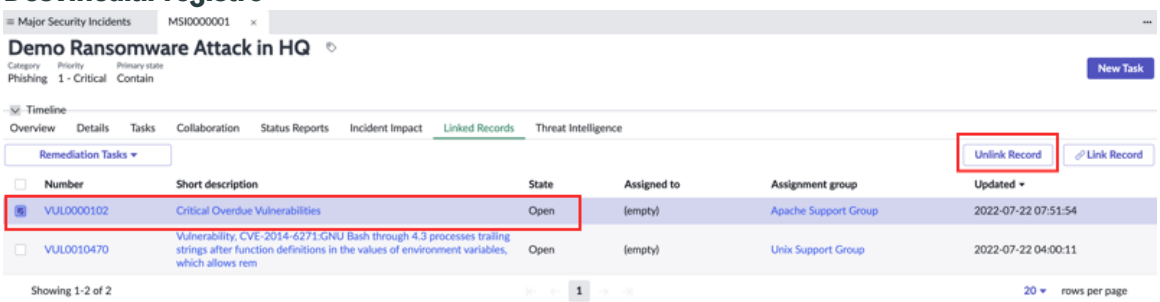
Procedimento

1. Navegar até **Security Incident Response grave** > **Espaço do MSIM**.
2. Navegue até a exibição **Listas**, que é exibida no painel esquerdo do espaço.
3. Clique em **Aceito** para selecionar os registros de incidentes de segurança graves promovidos.
4. Clique na guia **Registros vinculados**.
   Esta seção exibe os registros vinculados e seus registros relacionados, que estão vinculados ao incidente de segurança grave.
5. Selecione a exibição de tabela desejada, como Incidentes de segurança, Tarefas de correção (itens vulneráveis) ou Caso de segurança.
6. Selecione o registro a ser desvinculado da exibição de lista de registros.
7. Clique **em Desvincular registro**.

Tradução automática

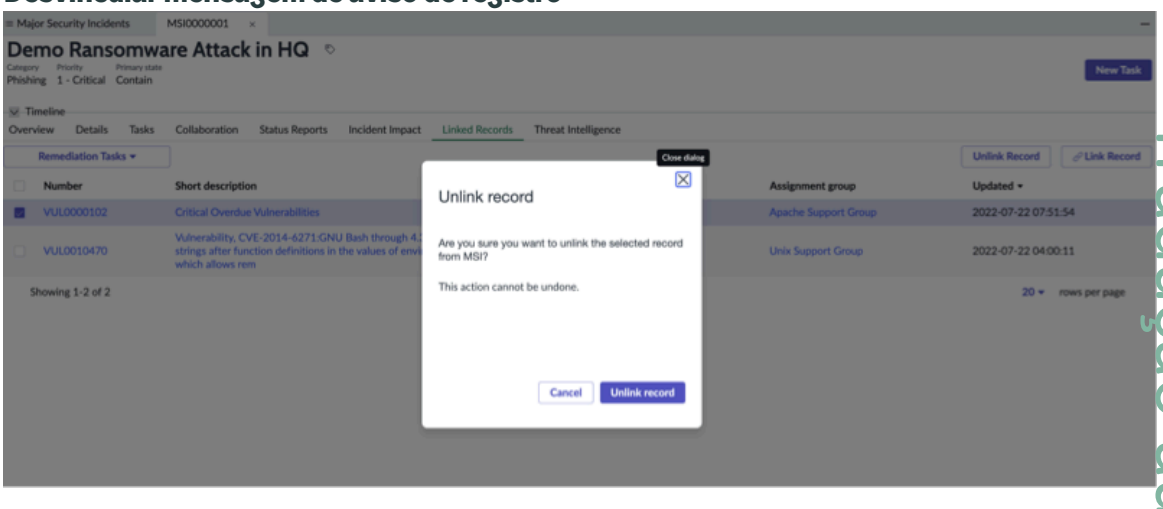
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Desvincular registro



8. Uma mensagem de aviso será exibida perguntando se você deseja desvincular o registro selecionado do MSI.

Desvincular mensagem de aviso de registro



9. Clique **em Desvincular registro**.
   O registro é desvinculado e, uma vez desvinculado, as mudanças não podem ser revertidas. A exibição de lista de registros vinculados será atualizada após a desvinculação.

Tópicos relacionados

Configurar registros vinculados no Gestão de incidentes graves de segurança

Configurar registros de acúmulo no Gestão de incidentes graves de segurança

Gerenciar tarefas em um Incidente de segurança grave

A guia Tarefa permite rastrear e gerenciar todas as tarefas associadas a um incidente de segurança grave no espaço do MSIM. Você pode exibir as várias tarefas usando o Visual Task Board padrão (exibição Kanban) ou a exibição de lista.

O sn_msi.workspace_manager pode fazer o seguinte na guia Tarefas:

- Criar uma tarefa
- Modificar tarefas
- Exibir e atribuir tarefas a si mesmo ou a outras pessoas
- Excluir tarefas

Tradução automática

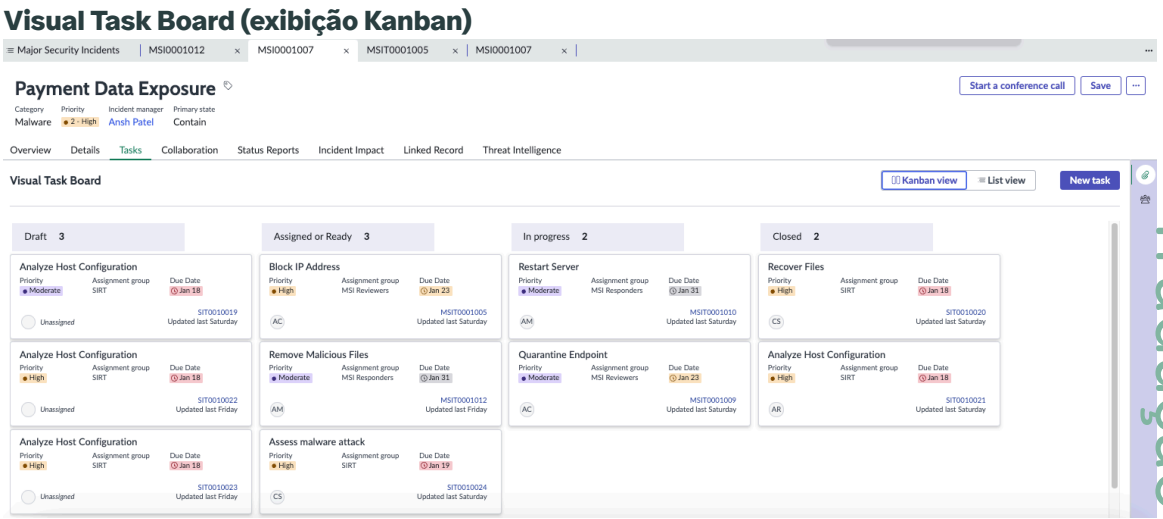
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Certifique-se de ter instalado o aplicativo **MSIM VTB Task Card: 1.0.1v** separadamente depois de instalar o aplicativo MSIM.

A guia Tarefas exibe os detalhes de todas as tarefas associadas a um incidente de segurança grave. A guia Tarefa oferece suporte a duas exibições:

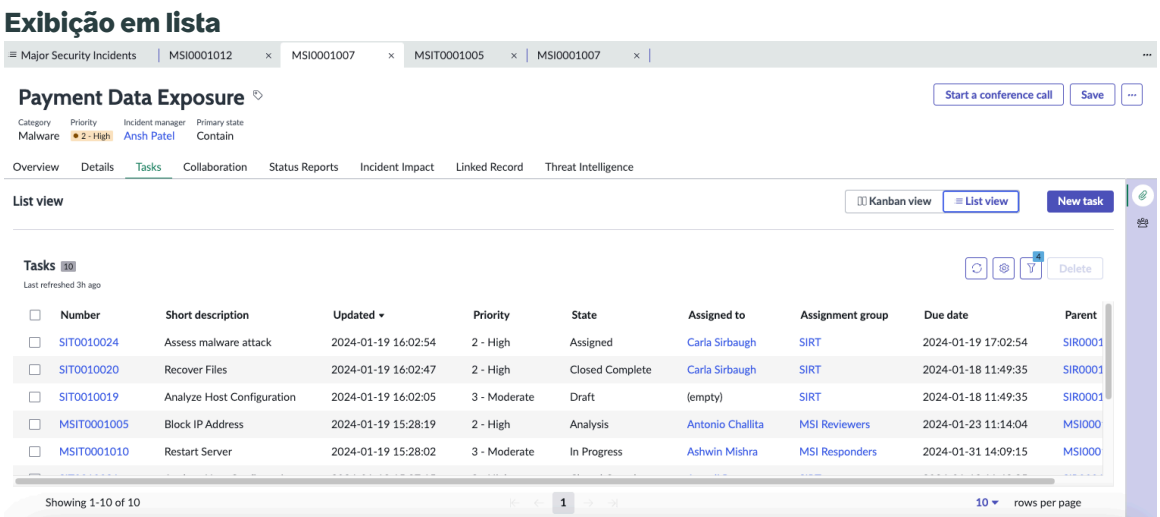
- **Visual Task Board (exibição Kanban)**:

  Exiba e atualize vários registros de tarefa, que aparecem como cartões no Visual Task Board que podem ser movidos entre as raias com base no status das tarefas no incidente de segurança grave.



- **Exibição de lista**:

  Exiba e atualize vários registros de tarefa usando o na forma de listas. Usando essas categorias de lista e filtros, você pode encontrar e rastrear rapidamente as tarefas nas quais precisa trabalhar em um incidente de segurança grave.



As atividades rotuladas são resumidas e exibidas na seção Visão geral do incidente de segurança grave. Um gráfico de tendência está disponível na seção Visão geral para exibir o estado consolidado das atividades da tarefa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gerenciar tarefas usando o Visual Task Board

Rastreie e gerencie todas as tarefas associadas a um incidente de segurança grave usando o Visual Task Board (exibição Kanban).

Você pode usar o Visual Task Board para mover os cartões passo a passo entre raias como Rascunho, Atribuído ou Pronto, Em andamento e Encerrado, dependendo do status das tarefas. Um fluxo de atividades no quadro exibe a atividade recente para rastrear facilmente as mudanças de tarefa. Você pode adicionar cartões de tarefa de qualquer tabela que estenda Tarefa para rastrear rapidamente as atualizações e editar os incidentes de segurança graves diretamente do quadro.

Criar uma tarefa usando o Visual Task Board

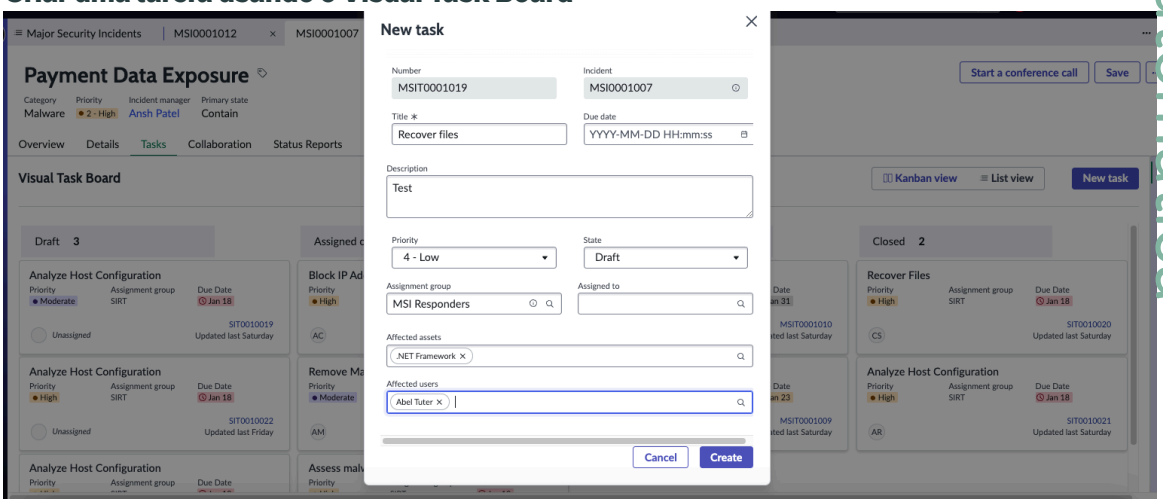
Função necessária: sn_msi.workspace_manager.

Nota:
Certifique-se de ter instalado o aplicativo **MSIM VTB Task Card: 1.0.1v** separadamente depois de instalar o aplicativo MSIM.

Os gerentes do MSI podem criar uma tarefa no Visual Task Board usando as seguintes etapas:

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Tarefas**.

Criar uma tarefa usando o Visual Task Board



5. Selecione **a exibição Kanban**e escolha **Nova tarefa**.
6. No formulário, preencha os campos.

Campo	Descrição
Número	Um número exclusivo que é gerado automaticamente para a tarefa selecionada. Este campo não é editável.
Incidente	Número do incidente de segurança grave. Este campo não é editável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Título	Forneça um nome para a tarefa.
Prazo	Selecione uma data e hora de vencimento para a tarefa ser concluída. Selecione uma data usando a opção **Calendário** e especifique a hora na seção **Selecionar hora**.
Descrição	Forneça uma descrição exclusiva para a tarefa.
Prioridade	Selecione a prioridade da tarefa para determinar quando a tarefa será realizada. A prioridade pode ser um dos seguintes valores: ○ **Nenhum(a)** ○ **1-Crítico** ○ **2 - Alta** ○ **3 - Moderada** ○ **4 - Baixa** ○ **5- Planejamento**
Estado	Selecione o estado atual da tarefa. O estado pode ser um dos seguintes: ○ **Rascunho** ○ **Análise** ○ **Em andamento** ○ **Encerrado** O estado padrão é **Rascunho**.
Grupo de atribuição	Selecione um grupo de atribuição do usuário para atribuir a tarefa usando a opção de pesquisa.
Atribuído a	Selecione o usuário para atribuir a tarefa usando a opção de pesquisa.
Ativos afetados	Selecione os ativos afetados pela tarefa usando a opção de pesquisa.
Usuários afetados	Selecione os usuários afetados pela tarefa usando a opção de pesquisa.

Tradução automática

7. Selecione **Criar** para criar a tarefa.

Exibir e modificar uma tarefa usando o Visual Task Board

Função necessária: sn_msi.workspace_manager.

Nota:
Certifique-se de ter instalado o aplicativo **MSIM VTB Task Card: 1.0.1v** separadamente depois de instalar o aplicativo MSIM.

Os gerentes do MSI podem exibir os detalhes de uma tarefa e as informações da atividade dos respondentes do MSI e modificar uma tarefa no Visual Task Board usando as seguintes etapas:

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Tarefas** e escolha a **exibição Kanban**.
5. Escolha o cartão de tarefa desejado em uma das raias para exibir os detalhes da tarefa.

   O cartão de tarefa pode estar em uma das raias: Rascunho, Atribuído ou Pronto, Em andamento ou Encerrado.
6. Na seção Informações da tarefa, você pode modificar os seguintes detalhes:

Campo	Descrição
Número	Um número exclusivo que é gerado automaticamente para a tarefa selecionada. Este campo não é editável.
Incidente	Número do incidente de segurança grave. Este campo não é editável.
Título	Forneça um nome para a tarefa.
Prazo	Selecione uma data e hora de vencimento para a tarefa ser concluída. Selecione uma data usando a opção **Calendário** e especifique a hora na seção **Selecionar hora**.
Descrição	Forneça uma descrição exclusiva para a tarefa.
Prioridade	Selecione a prioridade da tarefa para determinar quando a tarefa será realizada. A prioridade pode ser um dos seguintes valores: ○ **Nenhum(a)** ○ **1-Crítico** ○ **2 - Alta** ○ **3 - Moderada** ○ **4 - Baixa** ○ **5- Planejamento**
Estado	Selecione o estado atual da tarefa. O estado pode ser um dos seguintes: ○ **Rascunho** ○ **Análise** ○ **Em andamento** ○ **Encerrado** O estado padrão é **Rascunho**.
Grupo de atribuição	Selecione um grupo de atribuição do usuário para atribuir a tarefa usando a opção de pesquisa.
Atribuído a	Selecione o usuário para atribuir a tarefa usando a opção de pesquisa.

Tradução automática

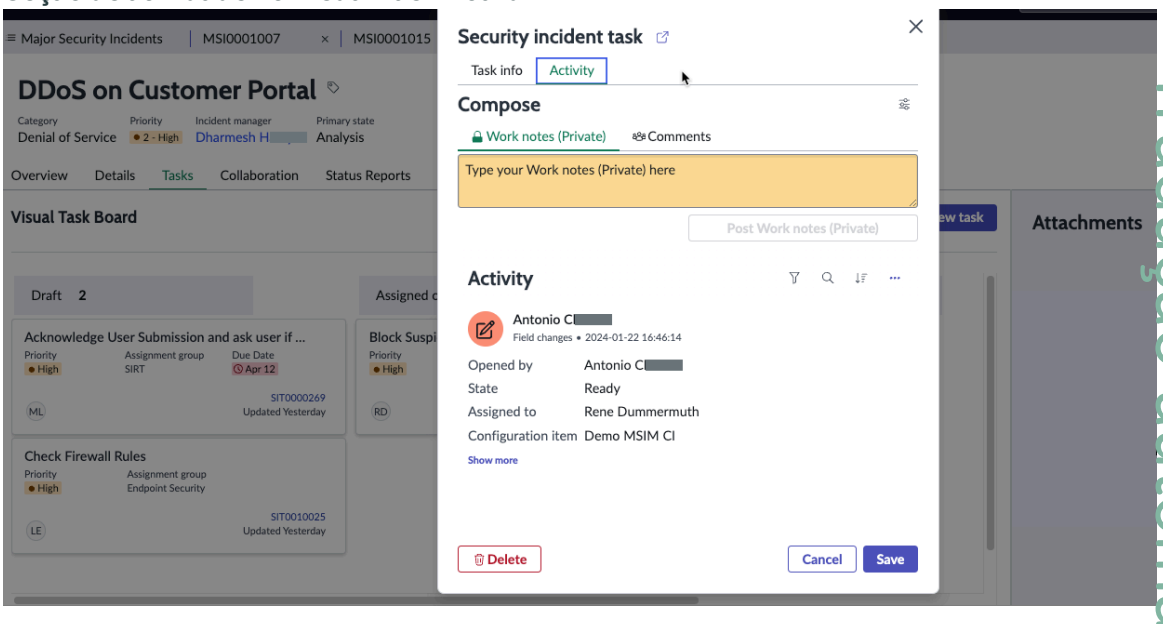
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativos afetados	Selecione os ativos afetados pela tarefa usando a opção de pesquisa.
Usuários afetados	Selecione os usuários afetados pela tarefa usando a opção de pesquisa.

7. Selecione a seção **Atividade** para exibir os detalhes da atividade dos Respondentes MSI.

   Use a seção Atividade para adicionar anotações de trabalho e comentários, publique sua atividade em particular e adicione comentários adicionais conforme necessário usando a seção Compor. Salve a atividade depois de publicar suas anotações de trabalho e comentários para exibir a atividade ou as anotações de trabalho adicionadas na seção Atividade.

Seção de atividade no Visual Task Board



Nota:
Selecione o link **Mostrar mais** detalhes para exibir os detalhes de um registro de incidente de segurança específico, que está associado a esse incidente de segurança grave.

8. Selecione **Salvar** para atualizar as informações da tarefa.

   As informações da tarefa são atualizadas instantaneamente.

Excluir uma tarefa usando o Visual Task Board

Função necessária: sn_msi.workspace_manager.

Nota:
Certifique-se de ter instalado o aplicativo **MSIM VTB Task Card: 1.0.1v** separadamente depois de instalar o aplicativo MSIM.

O Gerenciador do MSI pode excluir uma tarefa no Visual Task Board usando as seguintes etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Tarefas** e escolha a **exibição Kanban**
5. Escolha o cartão de tarefa que você deseja excluir.
6. No pop-up de tarefa de incidente de segurança grave, selecione a opção **Excluir**.

   O pop-up Excluir tarefa aparece solicitando que você confirme a exclusão da tarefa.
7. Selecione **Excluir**.

Gerenciar tarefas usando a exibição de lista

Rastreie e gerencie todas as tarefas associadas a um incidente de segurança grave usando a exibição de lista.

A exibição de lista mostra os detalhes de todas as tarefas associadas ao incidente de segurança grave, como número da tarefa, prioridade, estado atual, atribuído a, grupo atribuído. Usando essas categorias de lista e filtros, você pode encontrar e rastrear rapidamente as tarefas necessárias nas quais precisa trabalhar em um incidente de segurança grave.

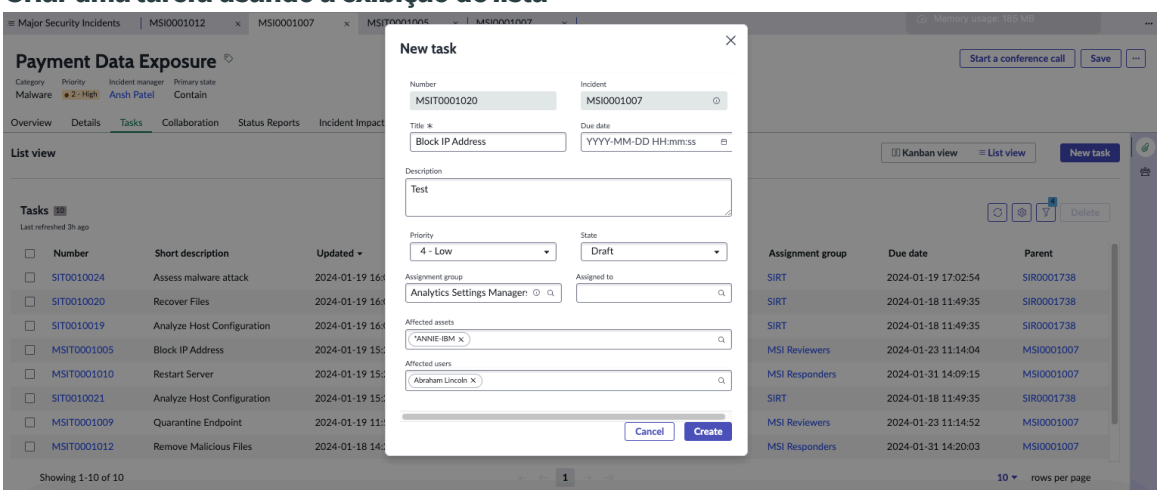
Criar uma tarefa usando a exibição de lista

Função necessária: sn_msi.workspace_manager.

Os gerentes do MSI podem criar uma tarefa na exibição de lista usando as seguintes etapas:

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Tarefas**.

Criar uma tarefa usando a exibição de lista



5. Selecione **Exibição de lista**e escolha **Nova tarefa**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. No formulário, preencha os campos.

Campo	Descrição
Número	Um número exclusivo que é gerado automaticamente para a tarefa selecionada. Este campo não é editável.
Incidente	Número do incidente de segurança grave. Este campo não é editável.
Título	Forneça um nome para a tarefa.
Prazo	Selecione uma data e hora de vencimento para a tarefa ser concluída. Selecione uma data usando a opção **Calendário** e especifique a hora na seção **Selecionar hora**.
Descrição	Forneça uma descrição exclusiva para a tarefa.
Prioridade	Selecione a prioridade da tarefa para determinar quando a tarefa será realizada. A prioridade pode ser um dos seguintes valores: ○ **Nenhum(a)** ○ **1-Crítico** ○ **2 - Alta** ○ **3 - Moderada** ○ **4 - Baixa** ○ **5- Planejamento**
Estado	Selecione o estado atual da tarefa. O estado pode ser um dos seguintes: ○ **Rascunho** ○ **Análise** ○ **Em andamento** ○ **Encerrado** O estado padrão é **Rascunho**.
Grupo de atribuição	Selecione um grupo de atribuição do usuário para atribuir a tarefa usando a opção de pesquisa.
Atribuído a	Selecione o usuário para atribuir a tarefa usando a opção de pesquisa.
Ativos afetados	Selecione os ativos afetados pela tarefa usando a opção de pesquisa.
Usuários afetados	Selecione os usuários afetados pela tarefa usando a opção de pesquisa.

7. Selecione **Criar** para criar a tarefa.

Exibir e modificar uma tarefa usando a exibição de lista

Função necessária: sn_msi.workspace_manager.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os gerentes do MSI podem exibir os detalhes de uma tarefa e as informações da atividade dos respondentes do MSI e modificar uma tarefa na exibição de lista usando as etapas a seguir

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Tarefas** e escolha **Exibição de lista**.
5. Escolha a Tarefa desejada na exibição de lista para exibir os detalhes da tarefa.
6. Na seção Informações da tarefa, você pode modificar os seguintes detalhes:

Campo	Descrição
Número	Um número exclusivo que é gerado automaticamente para a tarefa selecionada. Este campo não é editável.
Incidente	Número do incidente de segurança grave. Este campo não é editável.
Título	Forneça um nome para a tarefa.
Prazo	Selecione uma data e hora de vencimento para a tarefa ser concluída. Selecione uma data usando a opção **Calendário** e especifique a hora na seção **Selecionar hora**.
Descrição	Forneça uma descrição exclusiva para a tarefa.
Prioridade	Selecione a prioridade da tarefa para determinar quando a tarefa será realizada. A prioridade pode ser um dos seguintes valores: ○ **Nenhum(a)** ○ **1-Crítico** ○ **2 - Alta** ○ **3 - Moderada** ○ **4 - Baixa** ○ **5- Planejamento**
Estado	Selecione o estado atual da tarefa. O estado pode ser um dos seguintes: ○ **Rascunho** ○ **Análise** ○ **Em andamento** ○ **Encerrado** O estado padrão é **Rascunho**.
Grupo de atribuição	Selecione um grupo de atribuição do usuário para atribuir a tarefa usando a opção de pesquisa.
Atribuído a	Selecione o usuário para atribuir a tarefa usando a opção de pesquisa.

Tradução automática

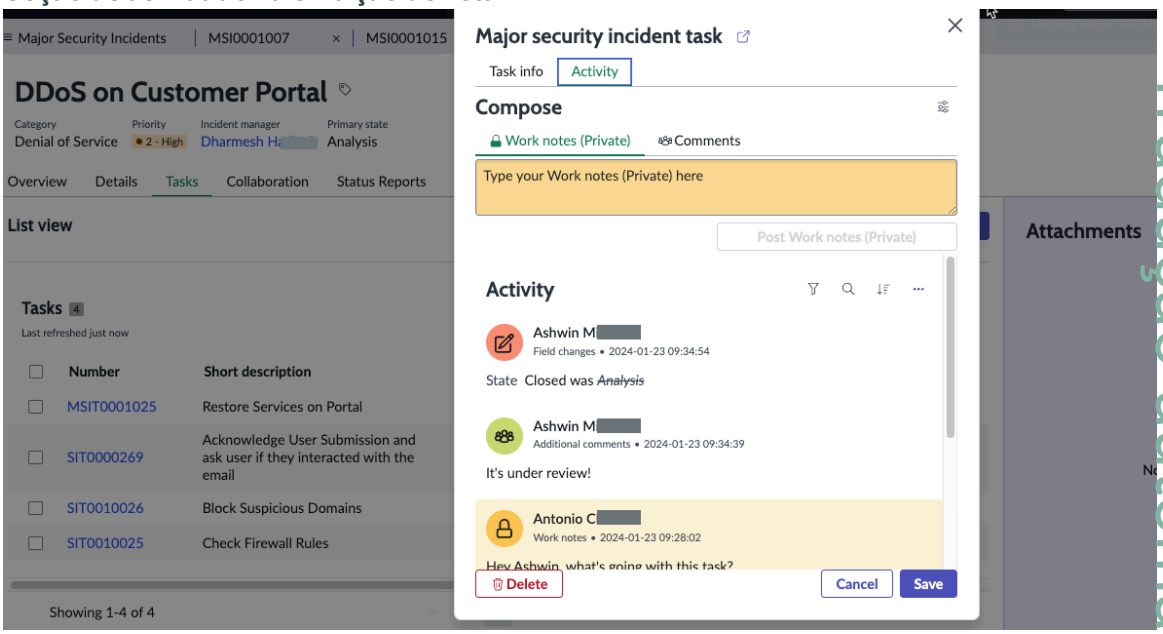
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativos afetados	Selecione os ativos afetados pela tarefa usando a opção de pesquisa.
Usuários afetados	Selecione os usuários afetados pela tarefa usando a opção de pesquisa.

7. Selecione a seção **Atividade** para exibir os detalhes da atividade dos Respondentes MSI.

   Use a seção Atividade para adicionar anotações de trabalho e comentários, publique sua atividade em particular e adicione comentários adicionais conforme necessário usando a seção Compor. Salve a atividade depois de publicar suas anotações de trabalho e comentários para exibir a atividade ou as anotações de trabalho adicionadas na seção Atividade.

Seção de atividade na exibição de lista



Nota:
Selecione o link **Mostrar mais** detalhes para exibir os detalhes de um registro de incidente de segurança específico, que está associado a esse incidente de segurança grave.

8. Selecione **Salvar** para atualizar as informações da tarefa.

   As informações da tarefa são atualizadas instantaneamente.

9. Você também pode executar as seguintes ações na exibição de lista:
   a. Selecione o ícone **Atualizar** para atualizar a lista de tarefas na exibição de lista.
   b. Selecione o ícone **Configurações** e use a opção **Editar colunas** para modificar a lista de colunas que aparecem na exibição de lista. Use a opção **Redefinir larguras** para redefinir as larguras das colunas.

Excluir uma tarefa usando a exibição de lista

Função necessária: sn_msi.workspace_manager.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O Gerenciador do MSI pode excluir uma tarefa na exibição de lista usando as seguintes etapas:

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Escolha o registro de incidente de segurança grave necessário.
4. Selecione a guia **Tarefas**.
5. Selecione **Exibição de lista**.
6. Escolha uma tarefa que você deseja excluir da lista.
7. No pop-up de tarefa de incidente de segurança grave, selecione a opção **Excluir**.

   O pop-up Excluir tarefa aparece solicitando que você confirme a exclusão da tarefa.
8. Selecione **Excluir**.

Rastrear atividade de colaboração por meio do espaço MSIM

Rastreie as atividades de bate-papo e arquivo relacionadas à resolução de incidentes de segurança graves por meio do espaço do MSIM.

As atividades são coordenadas usando o bate-papo Microsoft SharePointMicrosoft Teams e arquivos e pastas [] e, em seguida, publicadas de volta no Incidente de segurança grave por meio de integrações.

Depois que o Microsoft Teams e o Microsoft SharePoint estiverem integrados ao Gestão de incidentes graves de segurança, você poderá usar o espaço MSIM para rastrear a colaboração entre usuários de resposta do incidente e outros grupos que estão contribuindo para a resolução de um incidente de segurança grave. Todas as atualizações de pastas e arquivos de colaboração em Microsoft SharePoint são sincronizadas com o MSIM Espaço File Explorer e também refletidas nos componentes do Fluxo de atividades.

Quando um incidente de segurança é promovido como incidente de segurança grave:

1. Uma estrutura de pastas será criada em Microsoft SharePoint com base na configuração do modelo de pasta. A mesma estrutura de pastas será refletida no componente File Explorer do espaço.
2. Uma equipe com vários canais é criada na aplicação Microsoft Teams e o mesmo será refletido no componente Gestão de bate-papo do espaço.

Função necessária: sn_msi.workspace_manager.

Interagir com arquivos e pastas

O Explorador de arquivos exibe o sistema de arquivos para que você possa exibir e interagir com arquivos e pastas relacionados à resolução do incidente.

Exibe o arquivo e as pastas que são capturados no Microsoft SharePoint para um incidente de segurança específico. Essas pastas serão criadas automaticamente no Microsoft SharePoint para esse incidente de segurança grave. Você pode usar essas pastas criadas padrão para carregar arquivos de suporte, se necessário. Você pode renomear, mover ou excluir esses arquivos e pastas conforme necessário.

Além disso, sempre que você carregar um arquivo em qualquer uma das pastas, a atividade correspondente a essas pastas será automaticamente associada às pastas do Explorador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de Arquivos na guia Colaboração e a atividade será registrada e exibida na seção Atividade da Gestão de incidentes de segurança graves Espaço.

Nota:
Na guia **Colaboração**, o registro do incidente é anexado ao arquivo primário no sharepoint com um número de incidente exclusivo e uma categoria de incidente.

1. **Exibição de repositório**: lista os arquivos e as pastas listados no Microsoft SharePoint para esse incidente de segurança específico. Para cada arquivo ou pasta, a exibição do repositório exibe o Nome, Modificado por, Última modificação e o Tamanho será exibido.

Exibição do repositório

Campo	Descrição
Abrir no SharePoint	Selecione esta opção disponível ao lado do seu incidente de segurança grave. Clique no link para selecionar e exibir a estrutura de pastas no Microsoft SharePoint.
Nova Pasta	Selecione esta opção para criar uma nova pasta conforme necessário. Depois de criar uma nova pasta, a mesma nova pasta será criada e associada ao seu Microsoft SharePoint, por padrão.

2. **Recentes**: exibe todos os logs de atividades recentes. Esses logs incluem as atividades do SharePoint e do Explorador de arquivos. As atividades recentes geralmente são seus arquivos de suporte, que incluem a pasta primária.

   A seguir está o procedimento para **localizar o arquivo de log:**

   a. Selecione o respectivo arquivo para exibir os detalhes.

   b. Clique **em Localizar arquivo**.

   Nota:
   A navegação e os detalhes do arquivo primário e das pastas primárias são exibidos na seção de exibição da lista **Recentes**. Você pode abrir o mesmo arquivo no seu SharePoint. Sempre que você carrega os arquivos de log relacionados ou qualquer atividade, todos esses arquivos e atividades são exibidos no SharePoint e no Explorador de arquivos.

Gerenciar comunicações de canais de bate-papo

O gerenciador de canal de bate-papo exibe o Microsoft Teams com vários canais criados na aplicação Microsoft Teams com base em um modelo de configuração.

Esses canais configurados serão refletidos no componente de Gestão de bate-papo junto com os usuários e grupos de usuários atribuídos a eles. Você também pode criar novos canais. De acordo com a configuração dos modelos de canal, a equipe e os canais são criados no Microsoft Teams.

Criar novos canais de bate-papo

1. Navegar até **Gerenciador de canal de bate-papo** > **Criar novo canal** na guia Colaboração.
2. Adicione um novo **Nome de Canal**, **Descrição**e selecione os **Membros** do canal.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique em **Criar**.

> **Nota:**
> Um novo registro de canal é criado na seção Canais do MS Teams da aplicação MS Teams e o mesmo registro será refletido no MSIM.

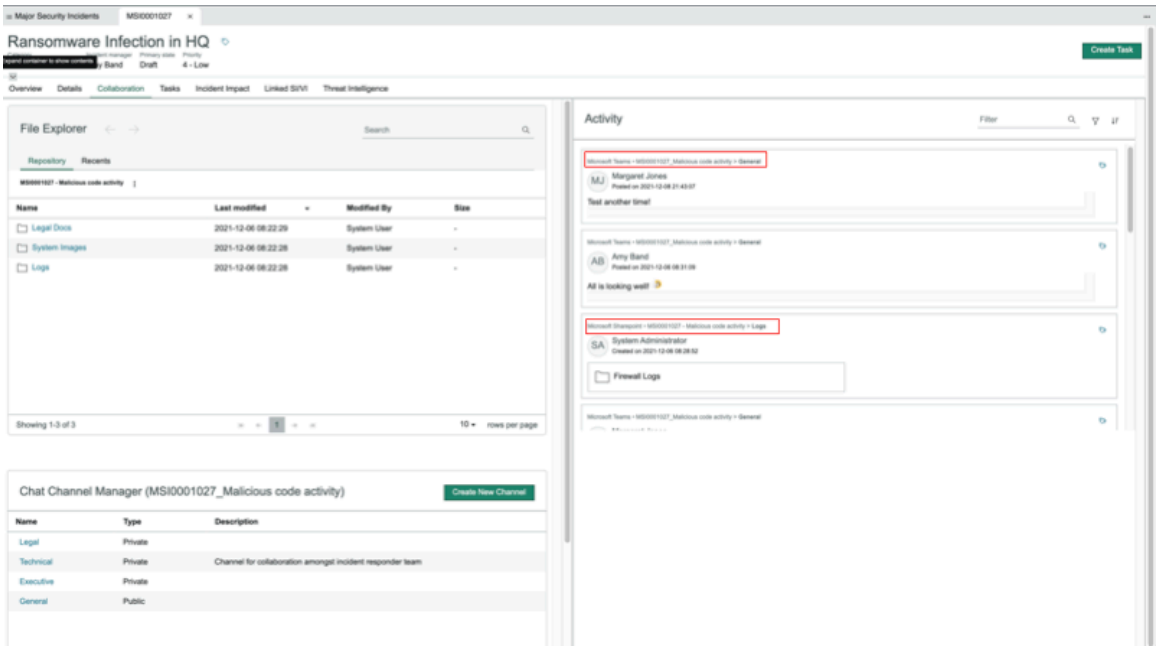
Gerenciar conversas de fluxo de atividades

Exibe todas as atividades, logs e status que foram realizados em Microsoft SharePoint, explorador de arquivos e Microsoft Teams.

Se você quiser exibir qualquer atividade específica ou pesquisar os detalhes da atividade de colaboração que interagiram entre vários arquivos e pastas e também no Microsoft Teams, use o recurso de filtro exibido na parte superior direita da seção Fluxo de atividades e localize o desejado detalhes da atividade.

Pastas e conversas de bate-papo compartilhadas com o Gerenciamento de incidentes de segurança graves são refletidas como trilhas com a estrutura:

nome da aplicação do conector<incident number – category ><folder name>).

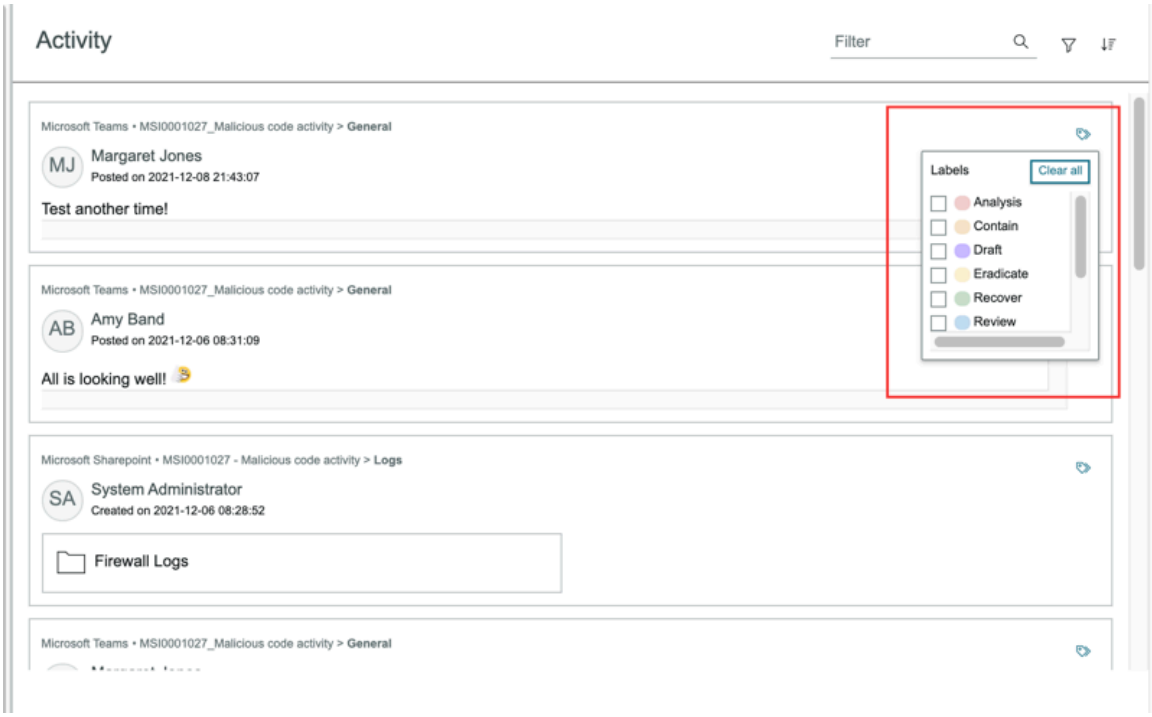


Rotular as atividades:

1. Clique no ícone **Rótulo**.
2. Marque a caixa de seleção do respectivo rótulo de atividade de incidente, conforme mostrado na captura de tela abaixo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. As atividades rotuladas são codificadas por cores e representadas como gráfico de tendência de andamento na seção **Colaboração externa** do espaço.

Criar e distribuir MSIM Relatórios de status

Como gerente de Incidente de segurança grave, você pode criar e distribuir os diferentes relatórios de status para diferentes partes interessadas em vários intervalos com base no modelo de relatório configurado ou em um relatório de status anterior ao longo da resolução do incidente de segurança grave.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Você pode visualizar os elementos de dados do relatório de resumo configurados anteriormente, adicionar texto ou resumo adicional, remover componentes de relatório individuais conforme necessário e verificar a precisão e a completude do relatório antes de distribuí-lo para diferentes partes interessadas.

Crie os relatórios de status selecionando o modelo de relatório desejado que foi configurado inicialmente na página Configuração de modelos de relatório do MSI.

Procedimento

1. Navegar até **Espaços** > **Gestão de incidentes graves de segurança** > **Incidentes de segurança graves**.
2. Selecione a exibição **Listas**.
3. Selecione o respectivo registro MSI promovido.
4. Selecione a guia **Relatórios de status**.
   A guia Relatórios de status contém três tipos diferentes de subseções, como abaixo.

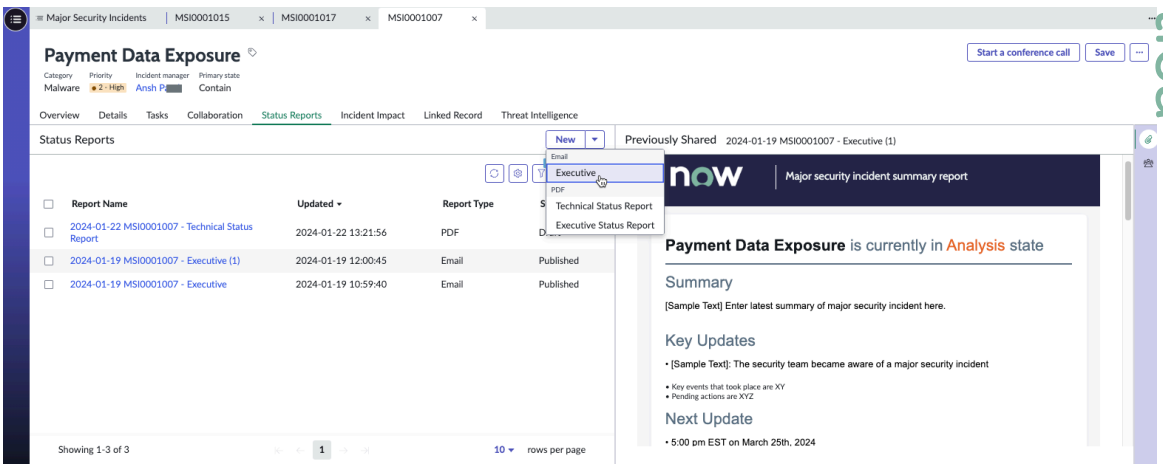
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome de relatório	Nome do modelo de relatório de status. **Nota:** A exibição Relatórios de status lista os modelos de relatório predefinidos existentes que estão disponíveis como parte do sistema de base para a persona em questão. Por exemplo, relatórios de status executivo por e-mail (compatível com dispositivos móveis), relatórios de status técnico e relatórios de status executivo como PDFs.
Atualizado	A data em que o modelo de relatório foi atualizado pela última vez.
Tipo de relatório	Tipo de relatório de status. O relatório de status pode ser um dos seguintes tipos: ○ PDF ○ E-mail
Estado	Estado dos relatórios de status. Os relatórios de status podem estar em um dos seguintes estados: ○ Rascunho ○ Em fila ○ Publicado

5. Selecione o tipo de relatório de status que você deseja exibir ou selecione **Novo** para criar um relatório de status.

Guia Relatórios de status do MSIM



6. Escolha um dos seguintes tipos de relatório de status na lista.
   - Relatórios de status do e-mail**executivo** que são compatíveis com dispositivos móveis.
   - PDF**do relatório de status técnico**
   - PDF**do relatório de status executivo**

Tradução automática

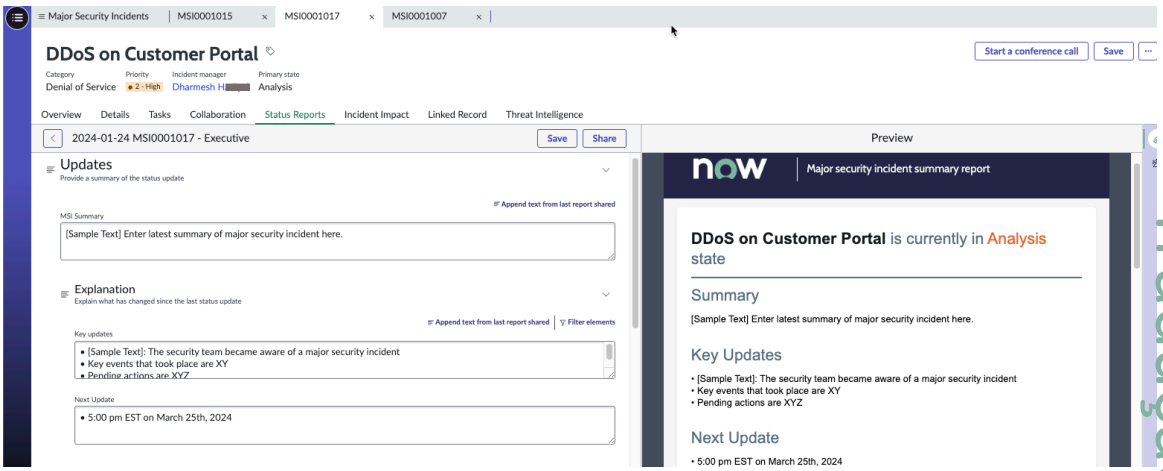
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Quando você seleciona qualquer modelo de relatório desejado, a visualização do relatório selecionado é gerada imediatamente no painel direito. Você pode exibir o relatório de status selecionado do MSI.

7. No modelo de relatório de status do e-mail executivo, preencha as seções com os detalhes do relatório de status.

Nota:
As opções que você selecionou na seção Relatórios de status são as mesmas opções renderizadas no relatório de visualização.

Modelo de relatório de status

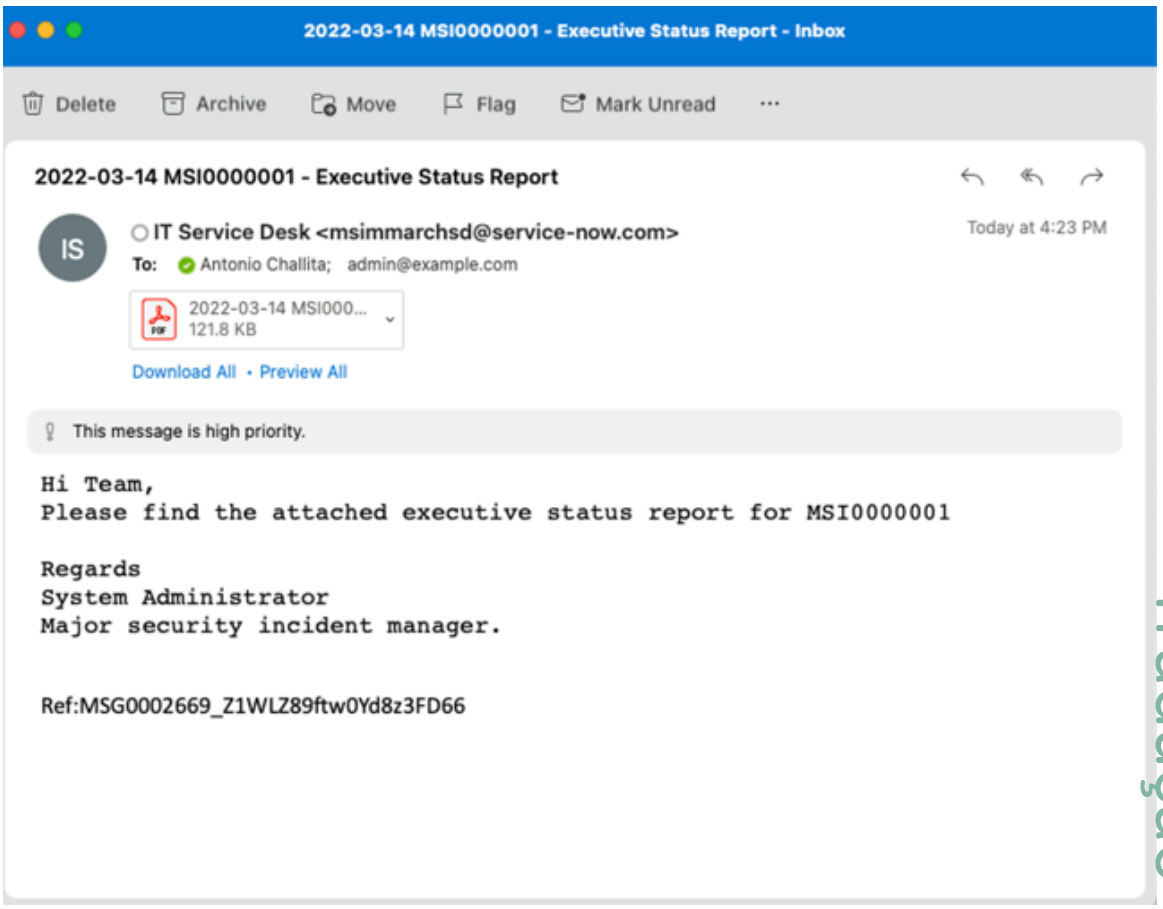


8. Selecione **Salvar** para armazenar as atualizações feitas no relatório de status.
9. Selecione **Compartilhar** para compartilhar o relatório com as várias partes interessadas.
   A caixa de diálogo Compartilhar relatório é exibida.
10. Preencha os campos **Destinatário**, **Assunto**e **Corpo** conforme necessário.
11. Selecione **Relatório de e-mail**.
    Um e-mail com o relatório de status em PDF anexado é enviado com sucesso ao destinatário em questão para verificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatório de status - e-mail



12. Você também pode executar as seguintes ações na guia Relatórios de status:
    a. Use a ação **Atualizar** na exibição Relatórios de status para atualizar a lista de relatórios de status.
    b. Use a ação **Listar ações** na exibição Relatórios de status para editar colunas ou redefinir as larguras da lista de relatórios de status.
    c. Use a ação **Filtrar** na exibição Relatórios de status para filtrar os relatórios de status com base em determinadas condições.

Tópicos relacionados

Configurar Incidente de segurança grave relatórios de status

Gerenciando MSIM relatórios de status

Os Relatórios de status fornecem gráficos de tendências pré-configurados com visualizações de dados acionáveis para melhorar os processos de operações de segurança, medir e analisar a linha do tempo de resolução, a contagem de atrasos e o status de cada tarefa atribuída.

Configurar Incidente de segurança grave relatórios de status

Configure relatórios de incidentes de segurança graves para configurar e baixar os relatórios de acordo com suas necessidades de negócios durante todo o ciclo de vida do processo de correção de registro de incidente de segurança grave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode criar os modelos de relatório com um formato e layout específicos e personalizar esses relatórios de acordo com seus requisitos específicos usando o recurso Relatórios de status do espaço Gestão de incidentes graves de segurança.

Um usuário com a função sn_msi.workspace_manager pode criar e configurar os modelos de relatório que descrevem o tipo de informações do relatório que podem ser usadas para gerar todos os relatórios de status, que podem ser compartilhados com usuários específicos, como partes interessadas executivas, departamentos jurídicos e mapear esses modelos para os registros de incidentes de segurança graves.

Para personalizar seus relatórios de status do ISG, primeiro configure os modelos de relatório usando **Modelos**de relatório. Com a ajuda de Modelos de relatório, você pode criar os tipos de modelo de relatório, definir os componentes do relatório para esses modelos de relatório, adicionar informações adicionais, criar dados visualizados para rastrear as métricas de escopo e andamento, adicionar dados da lista relacionada e gerar os relatórios de status.

A seguir, descrevemos os campos padrão fornecidos em todos os tipos de modelo de relatório. Você pode configurar e formatar o modelo de relatório com base em seus requisitos usando seções, subseções e seus elementos:

Componentes do relatório de status

Tipo de componente	Descrição
Título do relatório	Título do tipo de relatório. Por exemplo, o formato padrão do tipo de relatório é: {Número do MSI} - {Relatório de parte interessada executiva} descrito como MSI0001001: Relatório de parte interessada executiva.
Nome	Exibe o nome do usuário que gerou o relatório usando a seção Relatórios de status do espaço do Gerenciamento de incidentes de segurança graves.
Resumo	Exibe um breve resumo do relatório.
Data	Exibe a data em que o relatório é compartilhado com o destinatário em questão.
Andamento	Exibe o escopo e as métricas de andamento, como incidentes de SIR vinculados, tarefas de resposta, tarefas suplementares, colaboração externa, componentes da linha do tempo e eventos recentes da linha do tempo.
Desafios	Esta seção exibe uma breve descrição dos desafios envolvidos em todo o processo de correção de incidente de segurança grave.
Próximas etapas	Esta seção exibe uma breve descrição das próximas etapas envolvidas na resolução do incidente de segurança grave. Por exemplo, a subseção da equipe ativa no relatório de parte interessada executiva fornece as informações com a próxima etapa na atribuição da equipe que está envolvida na análise posterior do registro de incidente de segurança grave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Componentes do relatório de status

Tipo de componente	Descrição
Outras personalizações	O modelo de relatório também fornece a capacidade de carregar o logotipo e personalizar os cabeçalhos e rodapés no relatório.

A seguir estão os tipos de categorias de relatório que podem ser configuradas e exibidas:

- E-mail**executivo**
- PDF**do relatório de status técnico**
- PDF**do relatório de status executivo**

Os relatórios acima estão configurados e disponíveis para o usuário selecionar, exibir e gerar o relatório no espaço do Gerenciamento de incidentes de segurança graves.

Relatórios de status executivo otimizados para dispositivos móveis - E-mail

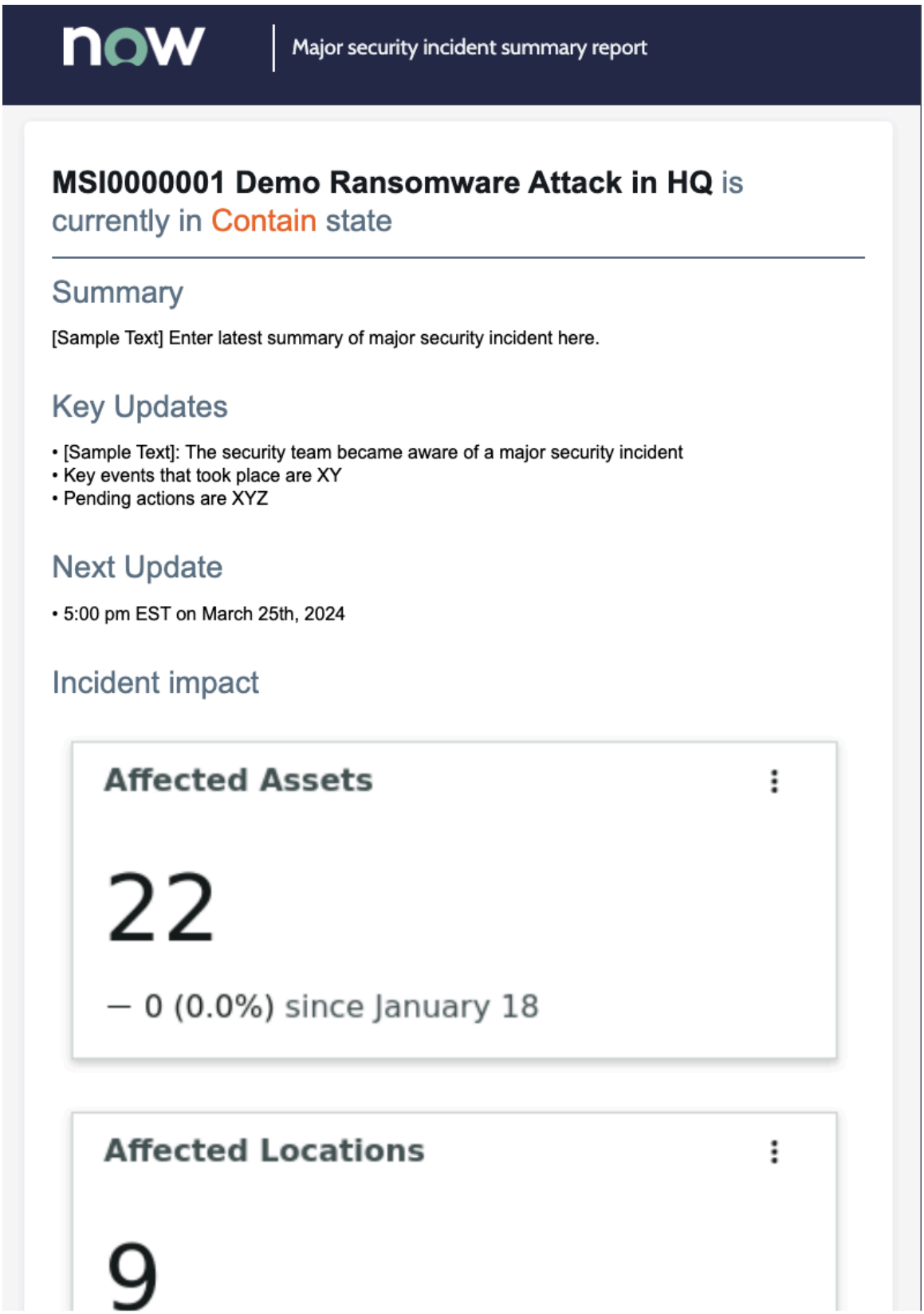
Os Relatórios de status executivo - E-mail são relatórios de status otimizados para dispositivos móveis que são gerados em formato de e-mail. A seção de relatório inclui um resumo do relatório, a coluna de duração do ISG, o escopo/impacto do incidente, as métricas de equipe ativas, as métricas de andamento e os componentes da linha do tempo, como os eventos recentes da linha do tempo para esse registro de incidente de segurança grave específico.

Personalize e configure os seguintes recursos de modelo de relatório para adicionar informações adicionais ao relatório. Um exemplo de relatório de status de e-mail executivo é mostrado abaixo para sua referência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

E-mail do relatório de status executivo



Tradução automática

Relatórios Executivos de Status - PDF

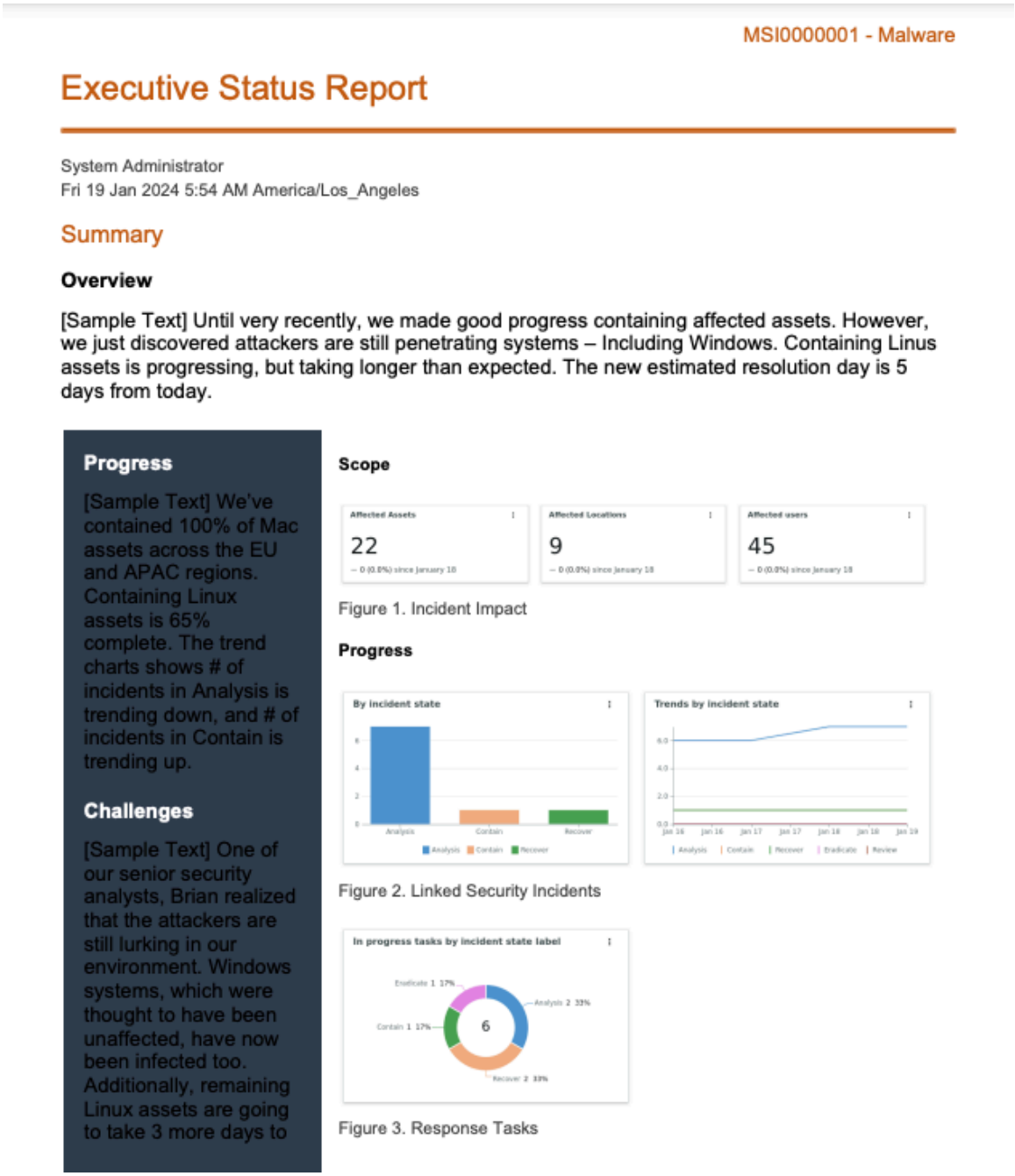
Os Relatórios de status executivo - PDF são relatórios de status gerados no formato PDF. A seção de relatório inclui um resumo do relatório, a coluna de duração do ISG, o escopo/impacto do incidente, as métricas de equipe ativas, as métricas de andamento e os

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

componentes da linha do tempo, como os eventos recentes da linha do tempo para esse registro de incidente de segurança grave específico.

Personalize e configure os seguintes recursos de modelo de relatório para adicionar informações adicionais ao relatório. Um exemplo de relatório executivo é mostrado abaixo para sua referência.

PDF do relatório de status executivo



MSI0000001 - Malware

Executive Status Report

System Administrator
Fri 19 Jan 2024 5:54 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22
Affected Locations 9
Affected users 45

Figure 1. Incident Impact

Progress

By incident state
Trends by incident state

Figure 2. Linked Security Incidents

In progress tasks by incident state label
6

Figure 3. Response Tasks

Relatórios de status técnico - PDF

Os Relatórios de status técnico - PDF são relatórios de status gerados no formato PDF. A seção de relatório inclui um resumo do relatório, coluna de duração do ISG, escopo/impacto do incidente, métricas de equipe ativas, métricas de andamento e componentes da linha do tempo, como os eventos recentes da linha do tempo para esse registro de incidente de segurança grave específico, atualizações de tarefa rotuladas e atividades rotuladas, com base no grupo de atribuição e no rótulo do marcador selecionado desde quando o

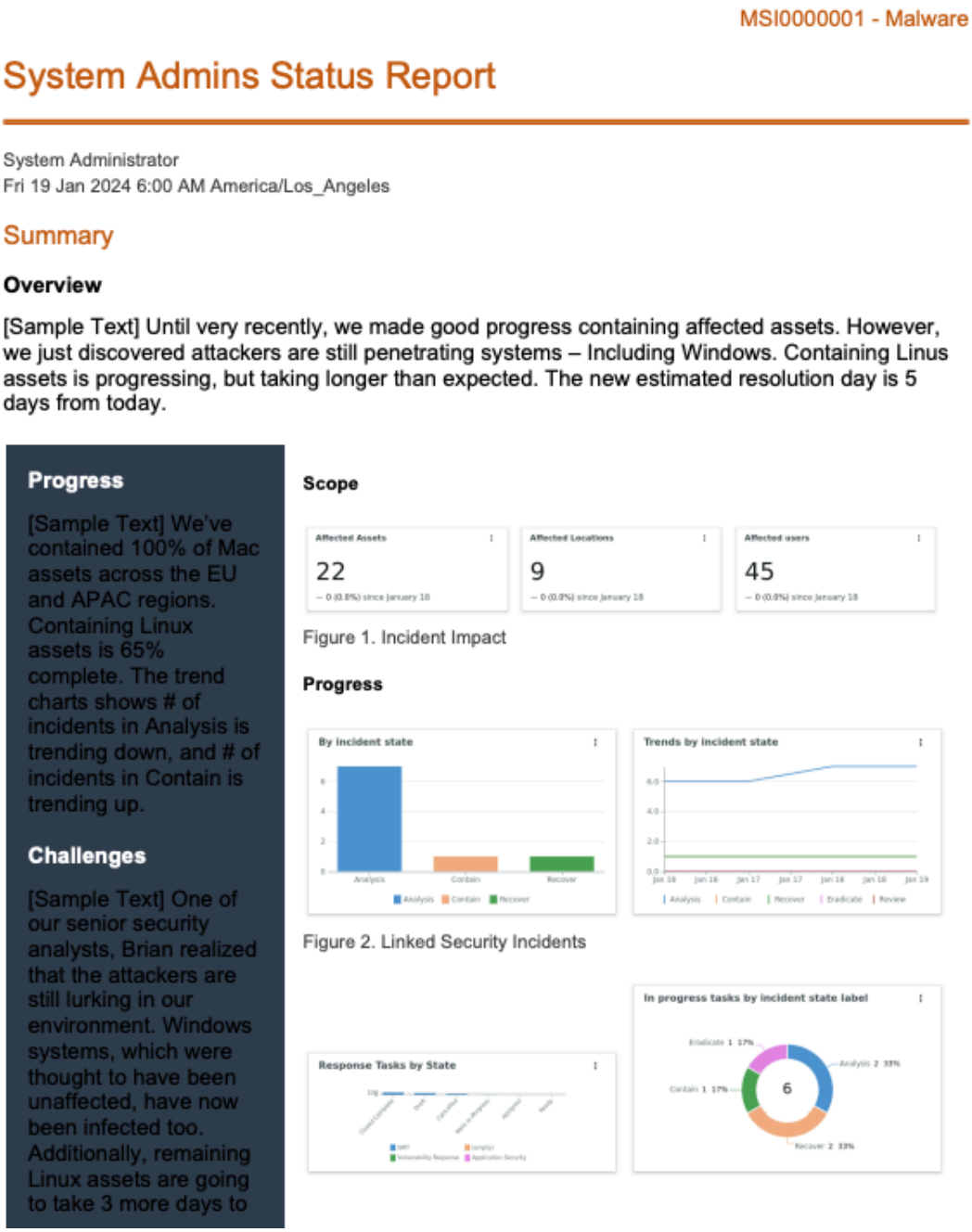
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

último relatório de status foi gerado e informações adicionais, como impacto do incidente e incidentes vinculados.

Personalize e configure o modelo de relatório para adicionar informações adicionais ao relatório. Um exemplo de relatório técnico que mostra as informações adicionais, como o impacto do incidente, é ilustrado abaixo para sua referência, e a parte restante das informações do relatório é semelhante aos relatórios executivos.

Relatório de status técnico - PDF


MSI0000001 - Malware

System Admins Status Report

System Administrator
Fri 19 Jan 2024 6:00 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22
Affected Locations 9
Affected users 45

Figure 1. Incident Impact

Progress

By incident state
Trends by incident state

Figure 2. Linked Security Incidents

Response Tasks by State
In progress tasks by incident state label

As seções do modelo de relatório contêm várias subseções, que descrevem como você pode criar as subseções do relatório e seus elementos, como:

1. Identidade visual: Adicionar identidade visual aos seus modelos de relatório
2. Scripts de modelo: Usar scripts de modelo em seus modelos de relatório

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Usar visualizações em modelos de relatório
4. Usar listas de relatórios em modelos de relatório

Criar um modelo de relatório

Crie vários modelos de relatório, que podem ser aplicados aos incidentes de segurança graves e gerem um relatório de status. Você pode adicionar campos de formulário padrão e personalizados do Major Security Incident Response ao modelo de relatório que seja referência com pontos. Além disso, você pode formatar e configurar o relatório com base em seus requisitos usando seções, subseções e seus elementos.

Antes de Iniciar

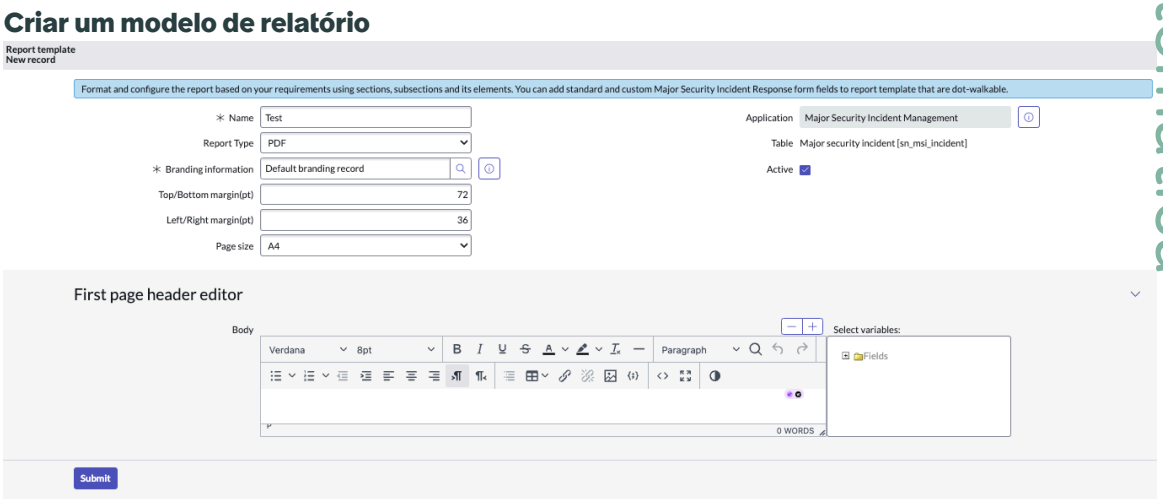
Função necessária: sn_msi.workspace_manager

Por Que e Quando Desempenhar Esta Tarefa

Você pode definir componentes de relatório para seus modelos de relatório e fornecer informações adicionais. Crie dados visualizados para rastrear o escopo e as métricas de andamento, adicione dados da lista relacionada, visualize e gere ou compartilhe os relatórios de status.

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Selecione **Novo** para criar um modelo de relatório.
4. No formulário de Modelo de relatório, preencha os campos.



5. **Envie** o novo registro de modelo de relatório.
   Um novo modelo de relatório é criado na página Modelos de relatórios.

Tópicos relacionados

Criar e distribuir MSIM Relatórios de status

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionar identidade visual aos seus modelos de relatório

Adicione a identidade visual aos seus relatórios. Você pode adicionar imagem de cabeçalho e rodapé, texto de cabeçalho e rodapé. Você pode incluir essas informações de identidade visual em qualquer um dos tipos de modelo de relatório que deseja criar, exceto os dois relatórios predefinidos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Por Que e Quando Desempenhar Esta Tarefa

As principais considerações ao adicionar a identidade visual aos seus modelos de relatório são as seguintes:

- Carregue a imagem do cabeçalho e do rodapé e alinhe a posição da imagem.
- O limite máximo de tamanho para a imagem do cabeçalho e rodapé é de 5 MB. Se o tamanho exceder o limite especificado, uma mensagem de erro, "O formato da imagem não pode ser reconhecido", será exibida no incidente de segurança grave.
- Ajuste a altura da imagem do cabeçalho e do rodapé.
- O tamanho do texto do rodapé está limitado a 100 caracteres.

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
2. Detalhar para **Modelo de relatório** > **Identidade visual**.
3. Selecione **Configurar**.
4. Selecione **Novo** para adicionar uma identidade visual ao seu modelo de relatório.
5. No formulário de modelo de Identidade visual, preencha os campos.
6. Selecione **Enviar**.
   Um novo modelo de identidade visual é criado na página Modelos de identidade visual.

Usar visualizações em modelos de relatório

Use widgets de relatório para definir e incluir elementos do UIB (User Interface Builder), como visualizações de dados, nos relatórios de status do MSIM.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Detalhar para **Modelo de relatório** > **Visualizações**.
3. Selecione **Configurar**.
   A seguir estão as visualizações predefinidas do UIB como parte do sistema de base, que você pode usar para configurar e modificar seus relatórios de status.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Criar um elemento de tipo de visualização

Usar listas de relatórios em modelos de relatório

Use listas de relatórios para definir e incluir os artefatos da lista relacionada para gerar listas no PDF com base nos registros de lista do MSI configurados.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Detalhar para **Modelo de relatório** > **Listas**.
3. Selecione **Configurar**.
   A seção Listas de relatórios de status do MSI descreve como cada lista relacionada específica é afetada desde que o incidente é criado. A seguir estão as Listas de Relatórios do MSI predefinidas como parte do sistema de base, que você pode usar para configurar e modificar seus relatórios de status.

Tópicos relacionados

Criar um elemento de tipo de lista

Usar scripts de modelo em seus modelos de relatório

Crie um script para incluir os dados de listas relacionadas, operações de data e quaisquer outros dados que não sejam diretamente orientados por pontos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar este script de modelo predefinido em seus modelos de relatório para incluir todos os dados relacionados depois que os modelos de relatório forem configurados e personalizados.

Construa um script de modelo para exibir os dados da lista relacionada no modelo de relatório. Se você quiser utilizar e preencher qualquer script de modelo, deverá adicionar o marcador de script de modelo de marcador como: `${template_script:script name}`.

Exemplo: `${template_script:msi_collab_cards}`

Nota:
Você não pode excluir os scripts de modelo predefinidos. Uma mensagem de erro será exibida se um usuário com função de administrador tentar excluir um registro de script de modelo se ele estiver mapeado com qualquer modelo de relatório.

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Detalhar para **Modelo de relatório** > **Scripts do Modelo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione **Configurar**.
   A seguir estão os scripts de modelo predefinidos como parte do sistema de base, que você pode usar para configurar e modificar seus relatórios de status.

> **Nota:**
> Você também pode criar seu próprio script de modelo para incluir os dados de listas relacionadas, operações de data e quaisquer outros dados que não sejam diretamente orientados por pontos, além dos scripts de modelo listados.

Visualizar o modelo de relatório

Use a funcionalidade Visualização para visualizar seu modelo de relatório de tempo de design para gerar e compartilhar o relatório com outras partes interessadas durante o tempo de execução no espaço Gestão de incidentes graves de segurança.

Antes de Iniciar
Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Selecione o modelo de relatório desejado.
4. Selecione o tipo de relatório como E- **mail** ou **PDF** com base em seus requisitos.
5. Selecione a ação **Salvar e visualizar relatório**.

   A caixa de diálogo Visualizar relatório é exibida.
6. Selecione um incidente de segurança grave usando a opção Pesquisar para visualizar um relatório com o modelo selecionado.
7. Selecione **Visualizar relatório**.
   O relatório gera uma visualização de acordo com a configuração do modelo selecionado. Se você selecionou o tipo de relatório como E- **mail**, a visualização estará no formato de modelo de e-mail. Os relatórios de status em formato de e-mail são compatíveis com dispositivos móveis.

Criar um modelo de seção de relatório

Um relatório pode ser dividido em várias seções. Use a seção Relatório para dividir o relatório em várias seções e reorganizá-las em ordem.

Antes de Iniciar
Função necessária: sn_msi.workspace_manager

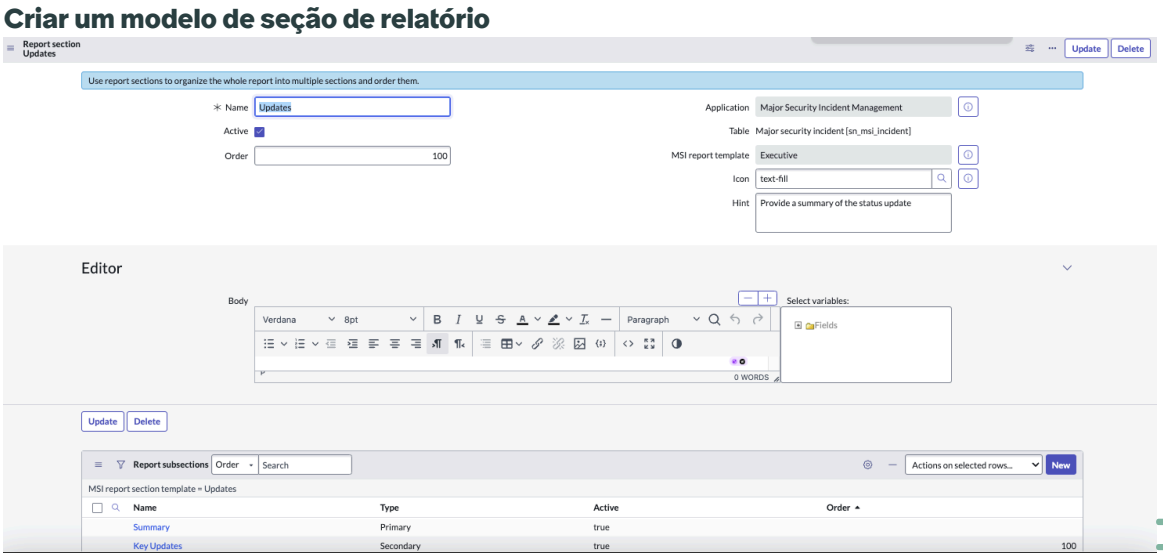
Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Abra um modelo de relatório existente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Navegar até **Seções de relatório** > **Novo**.
   A página da nova seção de relatório é exibida.



5. No formulário de Modelo de seção de relatório, preencha os campos.

6. Salve e **envie** a nova seção de modelo de relatório.

Criar um modelo de subseção de relatório

Use a subseção do relatório para organizar ainda mais a seção em várias subseções e configurar seu alinhamento e posição usando os tipos disponíveis, como painel lateral de texto, primário e secundário.

Antes de Iniciar

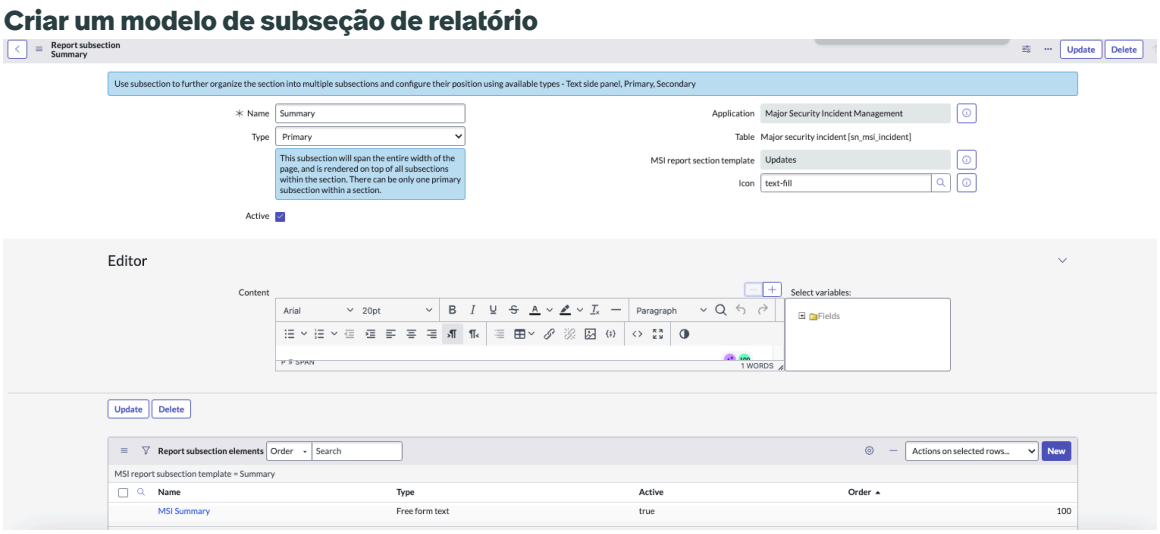
Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Abra um modelo de relatório existente e navegue até a respectiva lista de Seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Navegar até **Subseções de relatório** > **Novo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. No formulário de subseção Relatório, preencha os campos.

7. Salve e **envie** a nova seção de modelo de relatório.

Criar modelo de elemento de subseção de relatório

Use elementos de subseção para organizar ainda mais uma subseção em vários elementos. Os elementos de subseção ajudam a definir visualizações, listas e texto de forma livre de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Antes de Iniciar

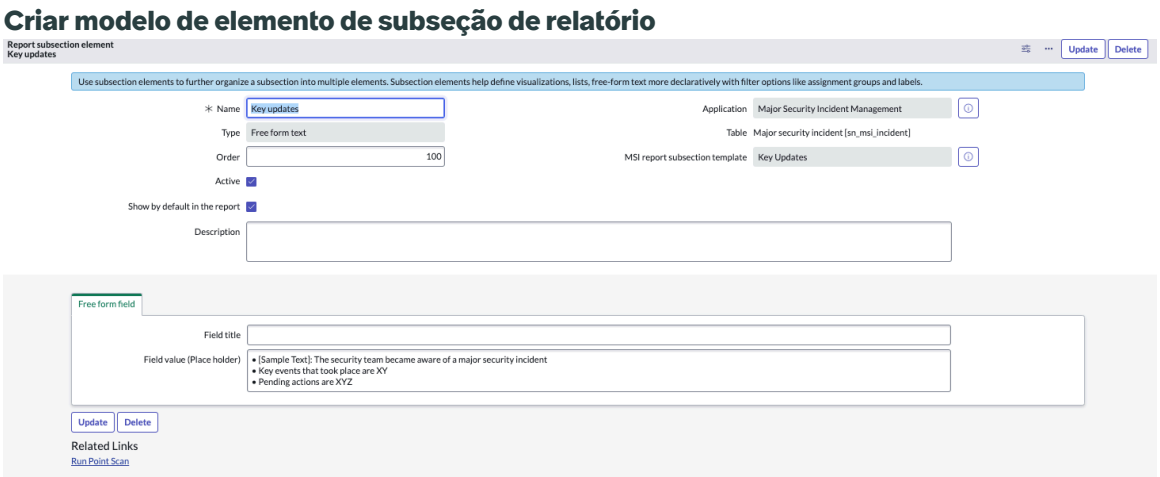
Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Abra um modelo de relatório existente e navegue até a respectiva lista de Seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. No formulário Elementos de subseção do relatório, preencha os campos.

8. Salve e **atualize** a nova seção de modelo de relatório.

Criar um elemento de tipo de forma livre

Crie um tipo de elemento de forma livre para definir o texto de forma livre de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Abra um modelo de relatório existente e navegue até a respectiva lista de Seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo**.
7. Preencha o formulário de elementos de subseção de relatório com os detalhes necessários, conforme explicado em Criar modelo de elemento de subseção de relatório.
8. Navegue até o campo Tipo de elemento de subseção de relatório e selecione a opção **de campo de formulário livre**.
   Isso exibe a seção **Campo de formulário livre**.
9. Na guia Formulário livre, preencha os campos.

Criar um elemento de tipo de visualização

Crie um tipo de elemento de visualização para definir os elementos de visualização de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

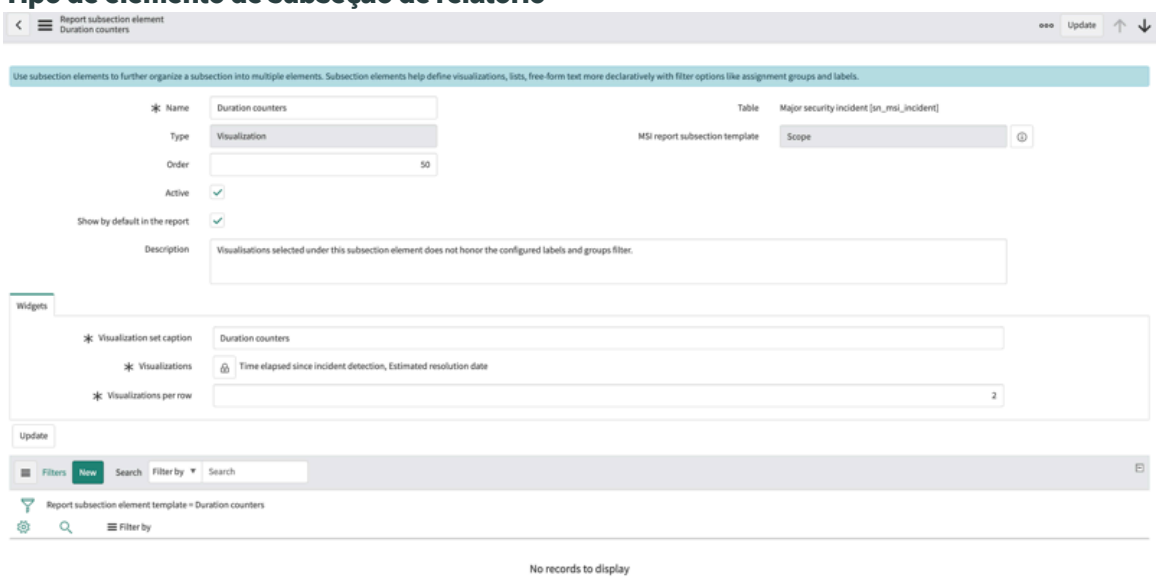
Função necessária: sn_msi.workspace_manager

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Abra um modelo de relatório existente e navegue até a respectiva lista de Seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo**.
7. Preencha o formulário de elementos de subseção de relatório com os detalhes necessários, conforme explicado em Criar modelo de elemento de subseção de relatório.
8. Navegue até o campo Tipo de elemento de subseção de relatório e selecione a opção **Visualização**.
   Isso exibe a seção **Visualização**.
9. No formulário Visualização, preencha os campos.
10. Selecione **Enviar**.

Example: Tipo de elemento de subseção de modelo de relatório para um relatório de status técnico

Tipo de elemento de subseção de relatório



Criar um elemento de tipo de lista

Crie um elemento de tipo de lista, que define os elementos da lista relacionada de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Abra um modelo de relatório existente e navegue até a respectiva lista de Seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo**.
7. Preencha o formulário de elementos de subseção de relatório com os detalhes necessários, conforme explicado em Criar modelo de elemento de subseção de relatório.
8. Navegue até o campo Tipo de elemento de subseção de relatório e selecione a opção **Lista**.
   Isso exibe a seção **Listas**.
9. No formulário Lista, preencha os campos.

Criar um elemento de tipo personalizado

Crie um elemento de tipo de lista, que define os elementos da lista relacionada de forma mais declarativa com opções de filtro, como grupos de atribuição e rótulos.

Antes de Iniciar

Função necessária: sn_msi.workspace_manager

Procedimento

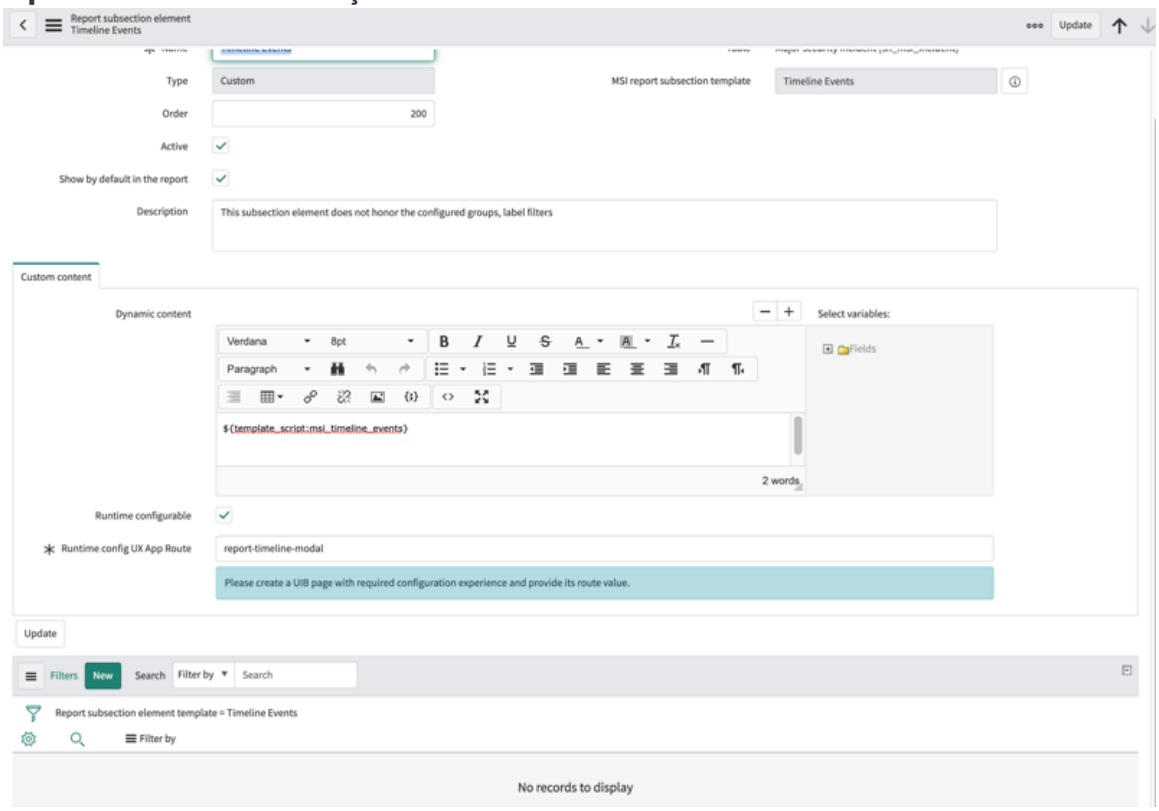
1. Navegar até **Gestão de incidentes graves de segurança** > **Administração do MSI** > **Configuração do relatório de status**.
   A página Configuração do relatório de status do MSI é exibida.
2. Na seção Modelo de relatório, selecione **Configurar**.
3. Abra um modelo de relatório existente e navegue até a respectiva lista de Seções de relatório.
4. Na lista Seções de relatório, abra um modelo de seção de relatório existente.
5. Na lista Modelo de seção de relatório, abra um modelo de subseção de relatório existente.
6. Navegar até **Elementos de subseção de relatório** > **Novo**.
7. Preencha o formulário de elementos de subseção de relatório com os detalhes necessários, conforme explicado em Criar modelo de elemento de subseção de relatório.
8. Navegue até o campo Tipo de elemento de subseção de relatório e selecione a opção **Personalizado**.
   Isso exibe a seção **Conteúdo personalizado**.
9. No formulário Conteúdo personalizado, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example: A seguir está um exemplo do tipo de elemento de subseção de modelo de relatório para um relatório de status técnico

Tipo de elemento de subseção de relatório



Adicionar propriedades do sistema

Adicione propriedades do sistema para controlar o comportamento da aplicação MSIM. A seguir estão as propriedades do sistema padrão que são introduzidas como parte dos Gestão de incidentes graves de segurança relatórios de status.

Propriedades do sistema

Nome da Propriedade	Descrição
sn_msi.import_img	Use esta propriedade para controlar a exportação de imagens. O valor padrão é definido como ATIVADO.
sn_msi.export_img_log	Use esta propriedade para habilitar o login no console do navegador. O valor padrão é definido como DESLIGADO.
sn_msi.export_img_parallel_threshold	Use esta propriedade para controlar o número máximo de solicitações paralelas para gerar as imagens das configurações do widget de relatório. O valor padrão é definido como 14.
sn_msi.img_export_log	Use esta propriedade para habilitar os logs do console no navegador.
sn_msi.img_export_poll_interval	Use esta propriedade para controlar o intervalo de tempo entre as pesquisas que verifica se a imagem foi gerada ou não. O tempo de intervalo de pesquisa padrão é definido como 3000 milissegundos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades do sistema

Nome da Propriedade	Descrição
sn_msi.export_poll_request_timeout	Use esta propriedade para controlar o tempo máximo que o sistema pode pesquisar para obter a imagem exportada. O valor padrão é 120000 milissegundos.
sn_msi.msi_report_uib_element_js_path	Use esta propriedade para controlar o caminho genérico para capturar a imagem da parte da página UIB.
sn_msi.report_default_style_objects	Use esta propriedade para mudar o CSS dos PDFs gerados, como tamanho da fonte, cor da fonte ou valor do campo. Por exemplo, se sn_msi.workspace_manager preferir mudar a cor da fonte do painel esquerdo do relatório de status de PDF gerado, o gerente do espaço poderá modificar a cor da fonte da propriedade do sistema e renderizar o PDF na exibição desejada.

Estrutura de Rollup para MSIM

Estende a capacidade de vincular os registros de origem do espaço Gestão de incidentes graves de segurança.

Visão geral

A Estrutura de Acúmulo torna o fluxo de acúmulo configurável e extensível. Use este modelo de estrutura para configurar as informações, que podem ser acumuladas para um incidente de segurança grave.

Anteriormente, o sn_msi.workspace_manager era capaz de vincular os incidentes de segurança e os itens vulneráveis que foram propostos ou promovidos como MSI. Depois de vincular o incidente de segurança ou o item vulnerável, as informações foram acumuladas para um incidente de segurança grave. O tipo de informação necessário para ser acumulado foi codificado nos scripts.

Você pode usar o modelo de estrutura para configurar o fluxo de acúmulo, que oferece suporte aos seguintes recursos e também soluciona os problemas existentes no aplicativo:

O modelo de estrutura de acúmulo permite que o sn_msi.workspace_manager com os seguintes benefícios:

- Adicione ou remova as capacidades de vinculação, proposta ou promoção de registro MSI em qualquer tabela, o que estende a tabela de tarefas.
- Controle o tipo de informação a ser acumulado para MSI ao executar ações como vincular/propor/promover nos registros de incidentes.
- Suporte à vinculação, proposta ou promoção de incidentes de segurança, tarefas de correção e casos de segurança prontos para uso (OOTB) no ambiente clássico e no espaço Gestão de incidentes graves de segurança.

A estrutura de acúmulo exibe as configurações conforme explicado na tabela a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações da Estrutura de Acúmulo

Nome	Descrição
Configuração de registro vinculada	Armazena as informações das tabelas de tarefas que podem ser usadas para vincular/promover/propor a Incidente de segurança grave.
Acumular configuração de registro	Captura as informações que podem ser acumuladas da tabela de tarefas quando as ações vincular/promover/propor são executadas.
Configuração de layout de lista	Controla os rótulos e o layout da lista de várias tabelas, conforme mostrado nas Gestão de incidentes graves de segurança guias do espaço, como Impacto do incidente, Registros vinculados e Inteligência contra ameaças.

Configurar registros vinculados no Gestão de incidentes graves de segurança

Use a configuração de registros vinculados para armazenar as informações das tabelas de tarefas que podem ser usadas para vincular/promover/propor a Incidente de segurança grave.

Função necessária: admin e sn_msi.workspace_admin.

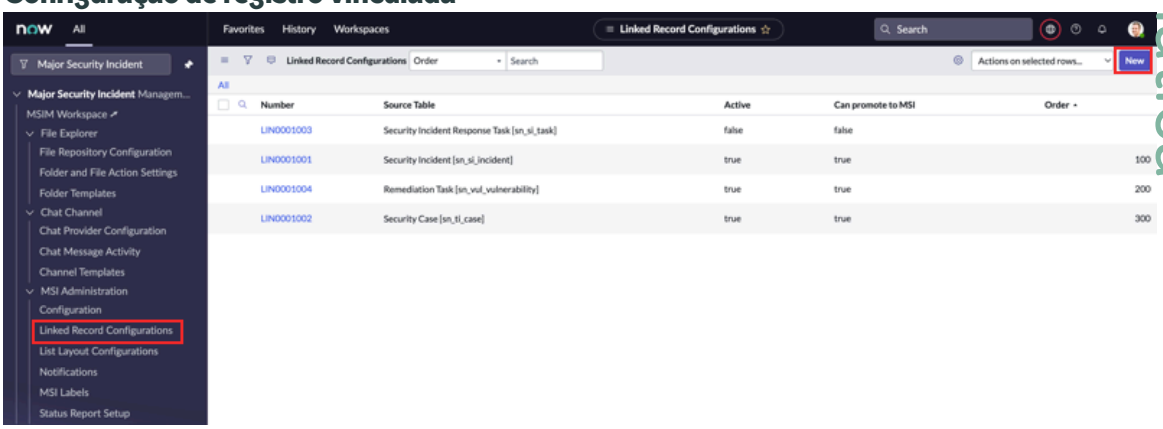
Nota:
O administrador pode criar o registro e o administrador do espaço MSIM pode atualizar o registro.

Procedimento

1. Navegar até **Gestão de incidentes graves de segurança** > **Configurações de registro vinculadas**.

   A página Configuração de registro vinculado é exibida.

   Configuração de registro vinculada

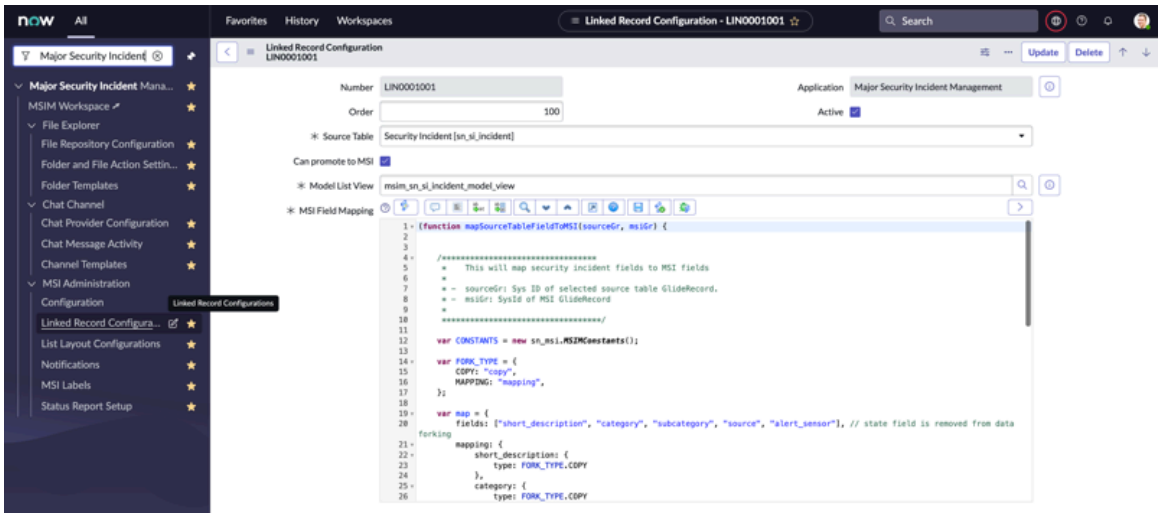


2. Na página Configuração de registro vinculado, clique em **Novo**

Nota:
Certifique-se de que a aplicação esteja no escopo Gestão de incidentes graves de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. No formulário de configuração de registro, preencha os campos.

Descrições do campo de registros vinculados

Campo	Descrição
Tabela de Origem	Indica a tabela de tarefas que deve ser vinculada e acumulada para Incidente de segurança grave.
Ordem	Permite que você controle a ordem da tabela de origem atual no menu suspenso do espaço do MSIM. Abaixo está um exemplo da **ordem**. Consulte a imagem 1 abaixo, que é fornecida após esta tabela.
Exibição de lista de modelos	Selecione uma exibição que pode controlar o layout da lista que é mostrado na Lista modal de registro vinculado.
Pode promover a MSI	Marque esta caixa de seleção para confirmar se o registro é primário. Abaixo está um exemplo da seleção da opção **Pode promover a MSI**. Consulte a imagem 2 a seguir, fornecida após esta tabela. Se esta caixa de seleção estiver marcada e o valor for verdadeiro, então: ○ você pode propor e promover diretamente um registro de origem para Incidente de segurança grave usando as ações de ambiente clássicas com configurações adicionais. ○ você pode vincular registros de origem a incidentes de segurança graves do ambiente clássico e do espaço MSIM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Gestão de incidentes graves de segurança A página de registro vinculado do espaço exibe os registros da tabela de origem vinculados. **Nota:** Se um registro puder ser proposto/promovido diretamente como Incidente de segurança grave, esse registro será um registro primário. Por exemplo, na configuração da tabela de tarefas do Security Response, o valor de **Pode promover para MSI** é falso, pois você não pode promover diretamente a tarefa do Security Response para Incidente de segurança grave. Portanto, ele não aparece na lista suspensa da guia de registro vinculado do espaço MSIM.
MSI Mapeamento de campo	Grave um script para mapear os campos de registro de origem para um incidente de segurança grave recém-criado quando o registro das tabelas de origem estiver no processo de ser proposto ou promovido. Este script é executado somente quando o valor **Pode promover a MSI** é verdadeiro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Imagem 1: ordem de exibição da lista de registros vinculados

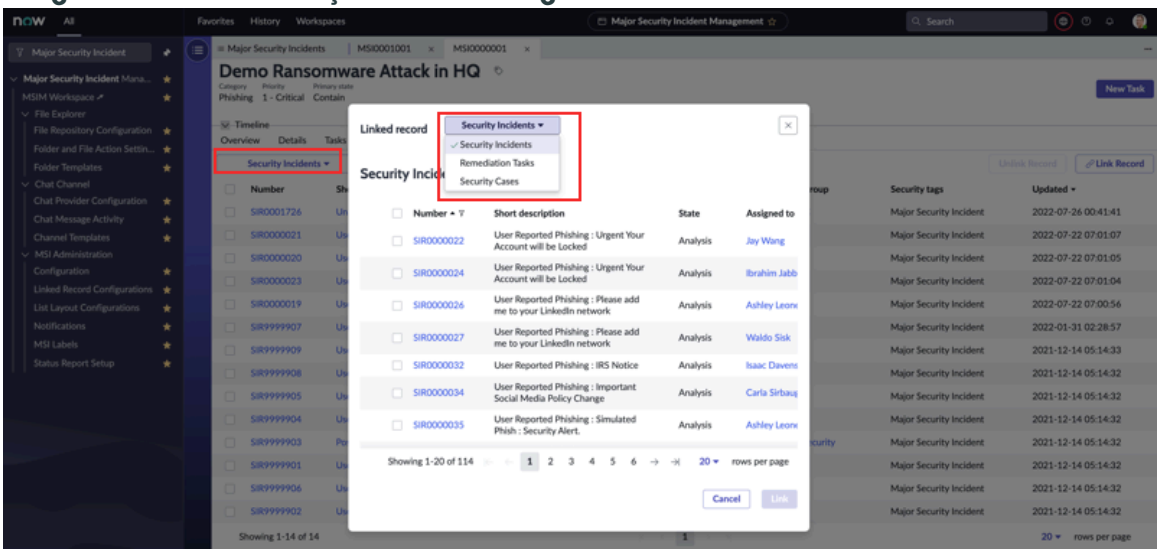
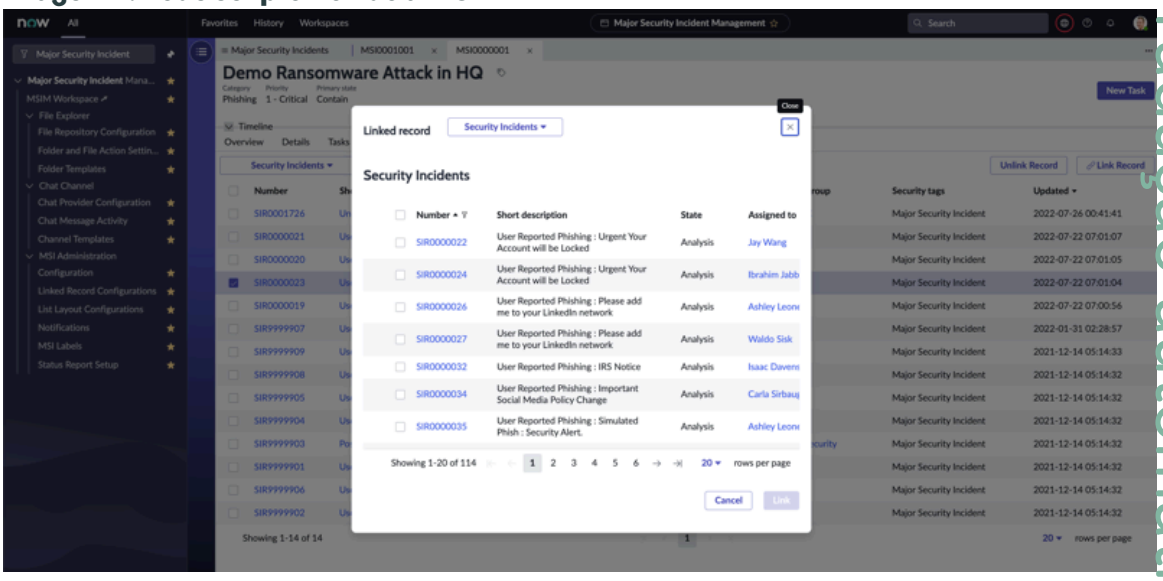


Imagem 2: Pode ser promovido a MSI



Tradução automática

Configurar registros de acúmulo no Gestão de incidentes graves de segurança

Configure os registros de acúmulo em Gestão de incidentes graves de segurança para controlar as informações, que serão acumuladas quando o registro de origem for vinculado/proposto/promovido como incidentes de segurança graves.

Função necessária: admin e sn_msi.workspace_admin.

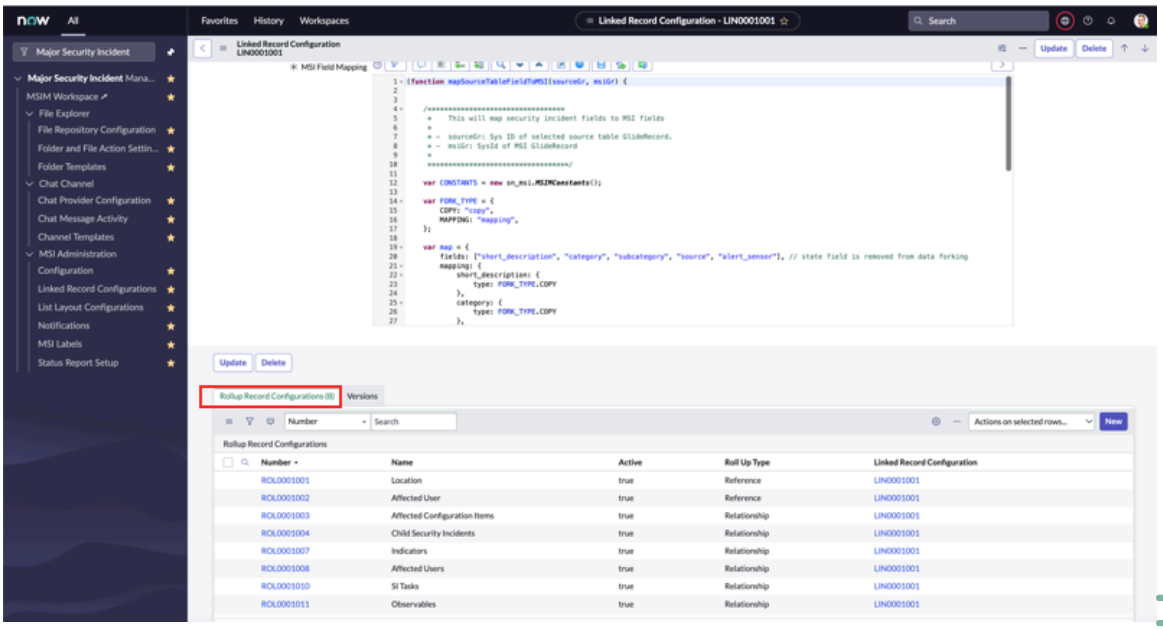
Nota:
O administrador do sistema pode criar o registro e o administrador do espaço do MSI pode atualizá-lo.

Procedimento

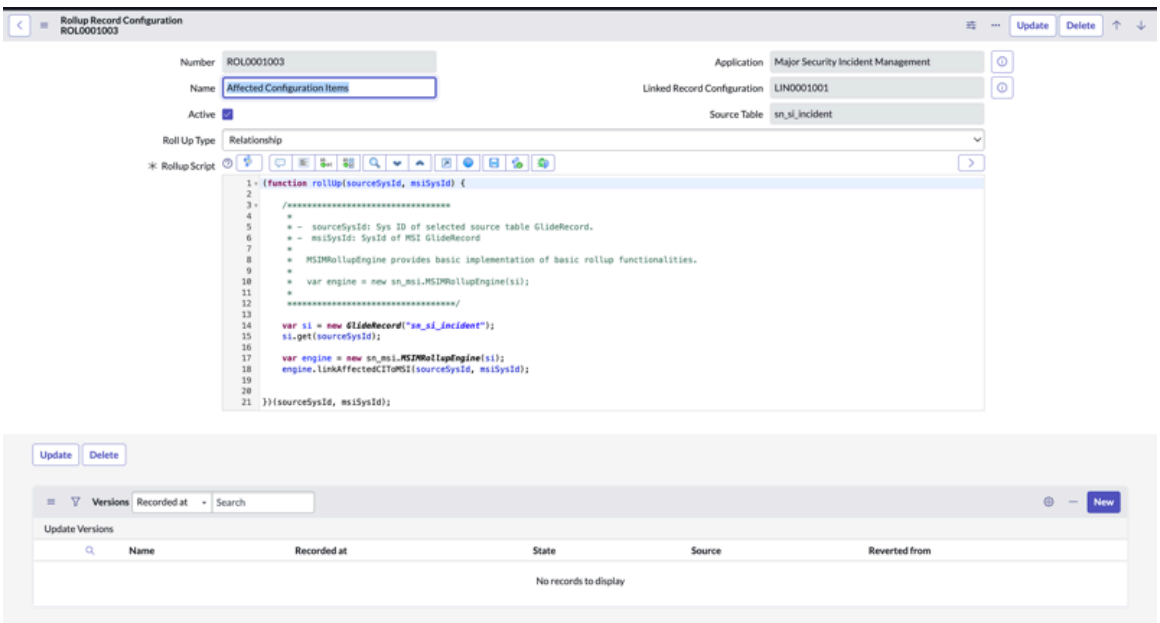
1. Navegar até **Security Incident Response grave** > **Configuração de registros vinculados**. A página Configurações de registro vinculado é exibida.
2. Selecione ou crie um novo registro vinculado e navegue até a seção **Configuração de registro** de acúmulo na mesma página.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Seção Configuração de registro de acúmulo



3. Clique em **Nova**.



4. Na página de configuração, preencha os detalhes.

Acumular configuração de registro

Nome do Campo	Descrição do campo
Nome	Indica o nome do registro de acúmulo.
Ativo	Marque esta caixa de seleção para implementar a configuração atual quando ocorrer o acúmulo do registro de origem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do Campo	Descrição do campo
Configuração de registro vinculada	Indica um número exclusivo, que se refere à configuração de registros vinculados primários e somente leitura.
Tabela de Origem	O nome da tabela de origem usada na configuração do registro vinculado, que é somente leitura.
Tipo de Rollup	Descreve o tipo de informação que deve ser acumulada. ○ **Relacionamento**: selecione esta opção se os dados precisarem estar presentes como uma lista relacionada. ○ **Referência**: selecione esta opção se os dados estiverem presentes como um campo de referência no formulário da tabela de origem.
Script de Acúmulo	Se o tipo de rollup for: **Relacionamento**, o campo **Script de Rollup** será habilitado, o que permite escrever um script e pode ser usado para acumular informações. Aqui, o script receberá as entradas que contêm informações do registro de origem e do incidente de segurança grave. O script deve ser capaz de encontrar as informações das tabelas de relacionamento e acumular para a tabela Registro vinculado (sn_msi_m2m_child).
Campo de origem	Se o tipo de acúmulo for: **Referência**, o **Campo de origem** estará disponível. Isso permite que você selecione o campo de referência Tabela de origem que contém as informações que precisam ser acumuladas.
Campo de destino	Se o tipo de acúmulo for: **Referência**, o **Campo de destino** estará disponível. Isso permite que você faça referência ao campo da tabela Registro vinculado (sn_msi_m2m_child) e armazenará os dados que estão presentes no campo de origem selecionado e no registro da tabela de origem.

Gravando script para acúmulo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

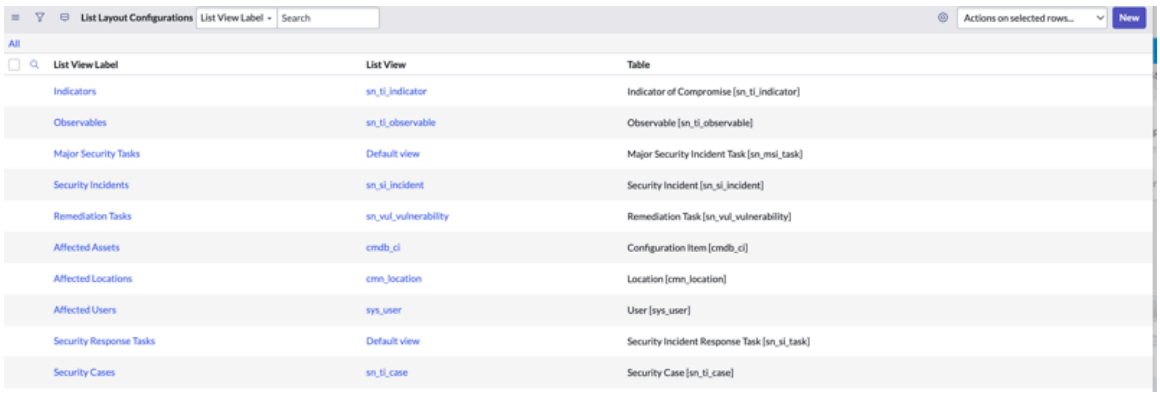
Nome	Descrição
Entradas	• sourceSysId: ID do sistema do registro da tabela de origem que está sendo vinculado/proposto/promovido. • msiSysId: ID do sistema do incidente de segurança grave ao qual o registro de origem está sendo vinculado/proposto/promovido.
Saída	Nenhum valor de retorno de saída.
Responsabilidade	O script deve acumular informações na tabela Registro vinculado (sn_msi_m2m_child). • Use sourceSysID para consultar dados de tabelas de relacionamento ServiceNow. • Depois que os dados forem obtidos, acumule os dados em um registro vinculado (sn_msi_m2m_child) usando o utilitário MSIRollupEngine para acumular dados.

Configurar layout de lista no Gestão de incidentes graves de segurança

Configure o layout de lista para personalizar o layout e os rótulos usados no espaço Gestão de incidentes graves de segurança, como as guias Impacto do incidente, Registros vinculados e Inteligência contra ameaças.

Função necessária: admin e sn_msi.workspace_admin.

Nota:
O administrador do sistema pode criar o registro e o administrador do espaço do MSI pode atualizá-lo.



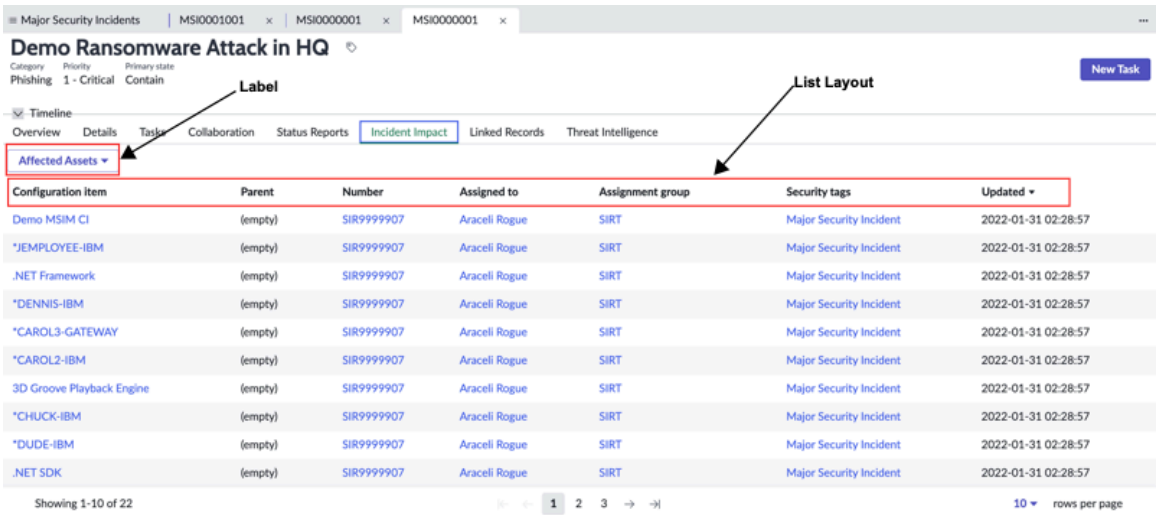
As configurações de layout de lista já foram enviadas para tabelas conhecidas existentes mostradas no espaço Gestão de incidentes graves de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Se você quiser renderizar a exibição personalizada das tabelas existentes, poderá atualizar o respectivo registro de tabela na configuração do layout de lista com a exibição de lista personalizada.
- Para novas tabelas de tarefas, você pode criar uma nova configuração de Layout de lista para renderizar a exibição de lista personalizada e os rótulos. Para obter um procedimento mais detalhado, consulte em como Etapa 4. Criar uma exibição para uma nova guia de registro vinculado para um caso de segurança



Exemplo de implementação de caso de uso de acúmulo para um caso de segurança

As etapas a seguir explicam um exemplo de caso de uso sobre como adicionar suporte para vincular/propor/promover a incidente de segurança grave para uma tabela de caso de segurança.

- Etapa 1. Criar configuração de registro vinculado para um caso de segurança
- Etapa 2. Criar uma exibição da janela modal de um caso de segurança
- Etapa 3. Criar ações de IU para a tabela de origem de um caso de segurança
- Etapa 4. Criar uma exibição para uma nova guia de registro vinculado para um caso de segurança
- Etapa 5. Adicionar listas de controle de acesso (ACLs) para usuários do espaço Gestão de incidentes graves de segurança
- Etapa 6. Criar regras de negócios para um caso de segurança
- Etapa 7. Criar configurações de registro de acúmulo

Etapa 1. Criar configuração de registro vinculado para um caso de segurança

Crie uma configuração de registro vinculado para um caso de segurança.

Antes de Iniciar

Função necessária: admin e sn_msi.workspace_admin

Nota:

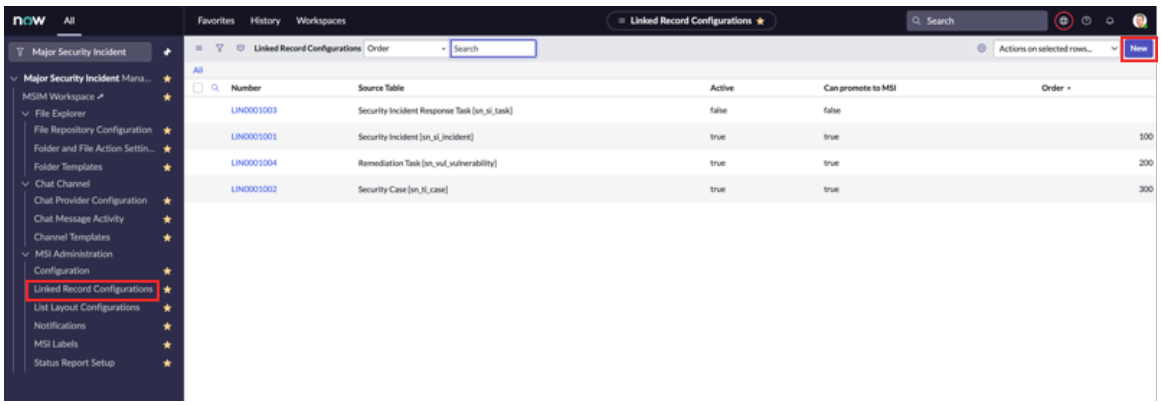
O administrador do sistema pode criar o registro e o administrador do espaço do MSI pode atualizá-lo.

Tradução automática

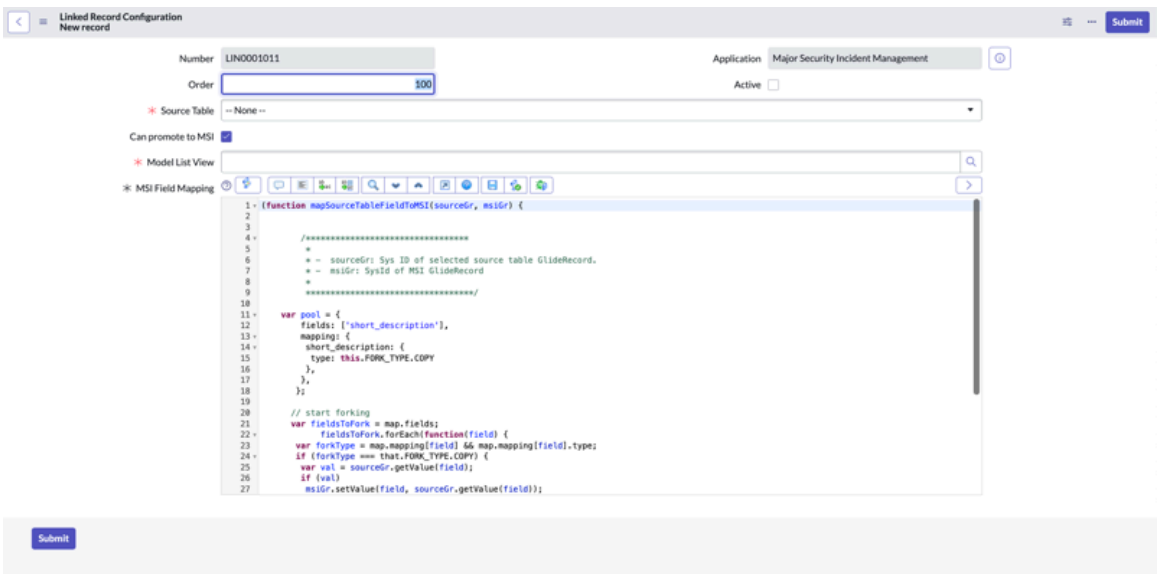
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Pesquise a configuração de registro vinculado na navegação à esquerda.
2. Clique em **Nova**.



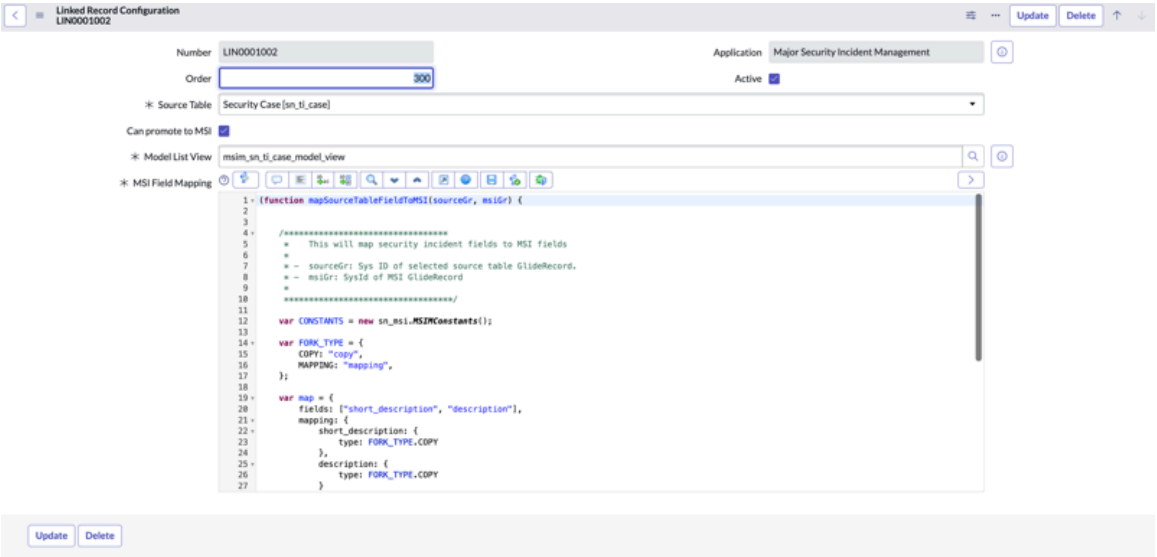
3. Preencha o formulário com as colunas necessárias e escreva um script de mapeamento de campo.



4. Agora você criou uma configuração de registro vinculado para o caso de segurança adicionando os valores conforme descrito na tabela a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nome	Descrição
Tabela de Origem	Caso de segurança (sn_ti_case). Aqui, neste exemplo, vincule/promova/proponha um caso de segurança como MSI.
Ordem	Valor de entrada: 300 **Nota:** A ordem inferior tem precedência sobre as ordens superiores. Como um caso de segurança tem uma ordem superior ao incidente de segurança e à tarefa de correção, ele aparecerá na última sequência.
Pode promover para MSI	Verdadeiro, marque esta caixa de seleção para promover o caso de segurança para MSI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	Nota: ◦ Vincule e desvincule registros de caso de segurança de incidentes de segurança graves no espaço Gestão de incidentes graves de segurança. Além disso, a funcionalidade de desvincular registro está visível somente para os registros vinculados. ▪ Isso habilitará o link, a promoção e a proposta de Caso de segurança para Incidente de segurança grave usando ações de ambiente clássicas, mas essas ações de IU não estarão disponíveis pronta para uso. Cada ação de IU precisa ser criada manualmente. Para obter mais informações, consulte Etapa 3. Criar ações de IU para a tabela de origem de um caso de segurança. ▪ A ação de IU Vincular/Promover/Propor está disponível para Incidente de segurança, Tarefa de correção e Caso de segurança prontos para uso. ◦ A página de registro vinculada do espaço do MSIM mostrará os registros de caso de segurança vinculados. Consulte a imagem abaixo 1 para exibir as opções disponíveis depois de marcar esta caixa de seleção.
Exibição de lista modal	msim_sn_ti_case_model_view **Nota:** Esta exibição contém campos e a ordem de campos mostrados na exibição de lista no modal de registro de link no espaço do MSIM. Para obter mais informações, consulte Etapa 2. Criar uma exibição da janela modal de um caso de segurança Consulte a imagem abaixo 2 para exibir na página **Registros vinculados**.
Script de mapeamento de campo	Este script descreve os campos do registro das tabelas de origem que serão mapeados para o incidente de segurança grave recém-criado quando o

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	registro das tabelas de origem estiver sendo proposto ou promovido. que receberá entradas: ○ sourceGr: objeto de registro do glide do caso de segurança ○ msiGr: objeto de registro do glide de incidente de segurança grave O script lerá a descrição resumida do caso de segurança e a copiará como título para o incidente de segurança grave.

Imagem 1: Pode ser promovido a MSI

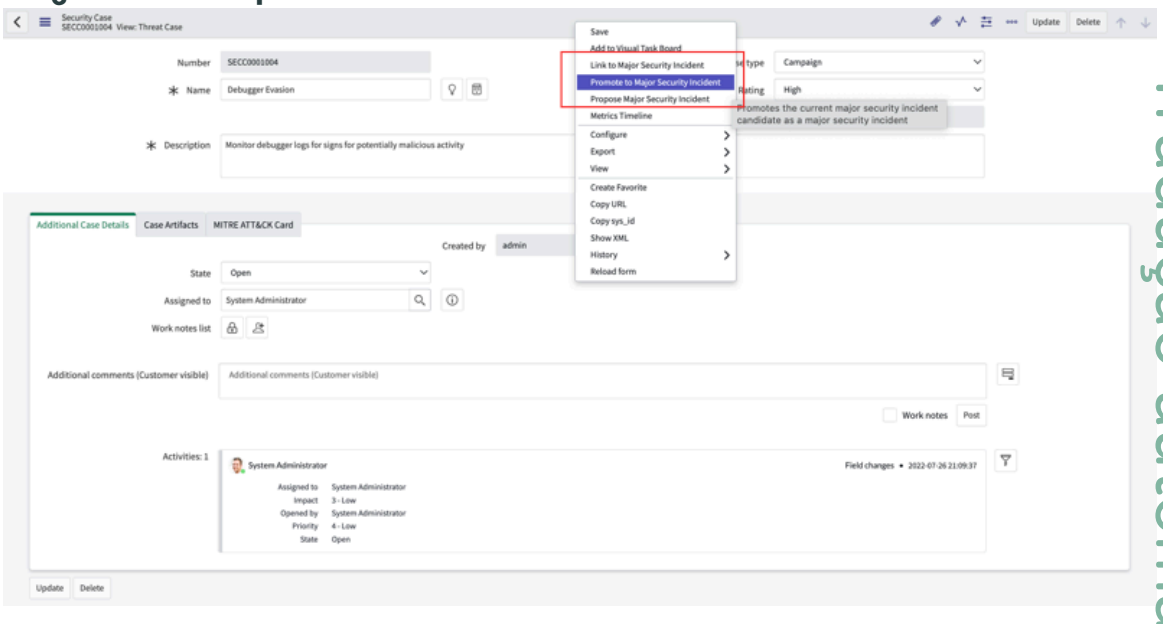
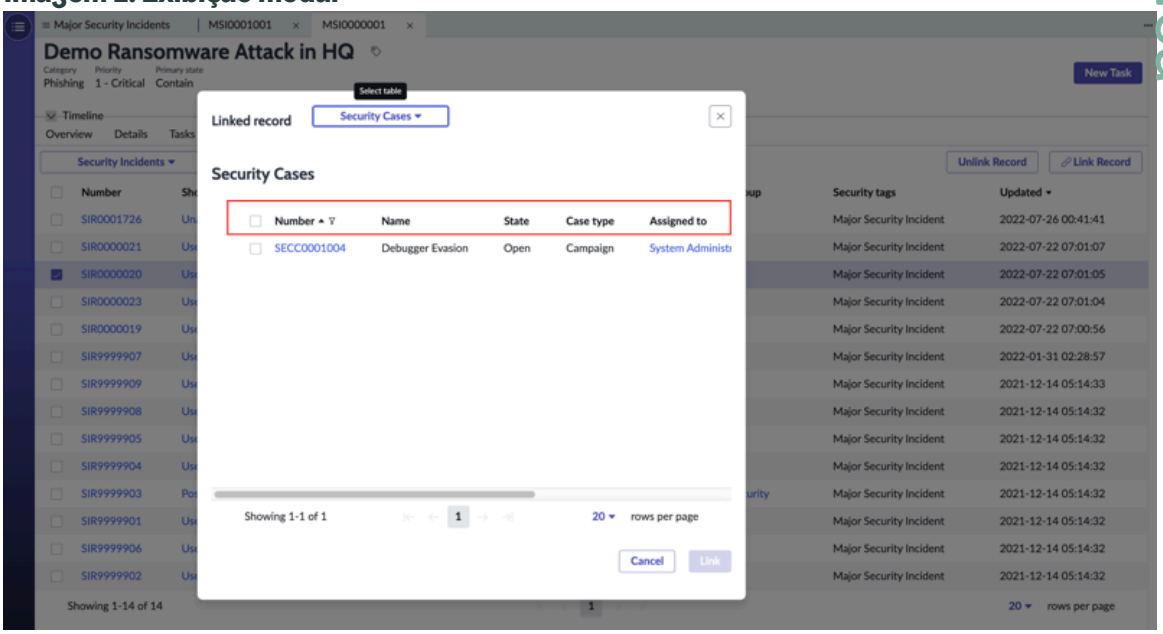


Imagem 2. Exibição modal



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Etapa 2. Criar uma exibição da janela modal de um caso de segurança

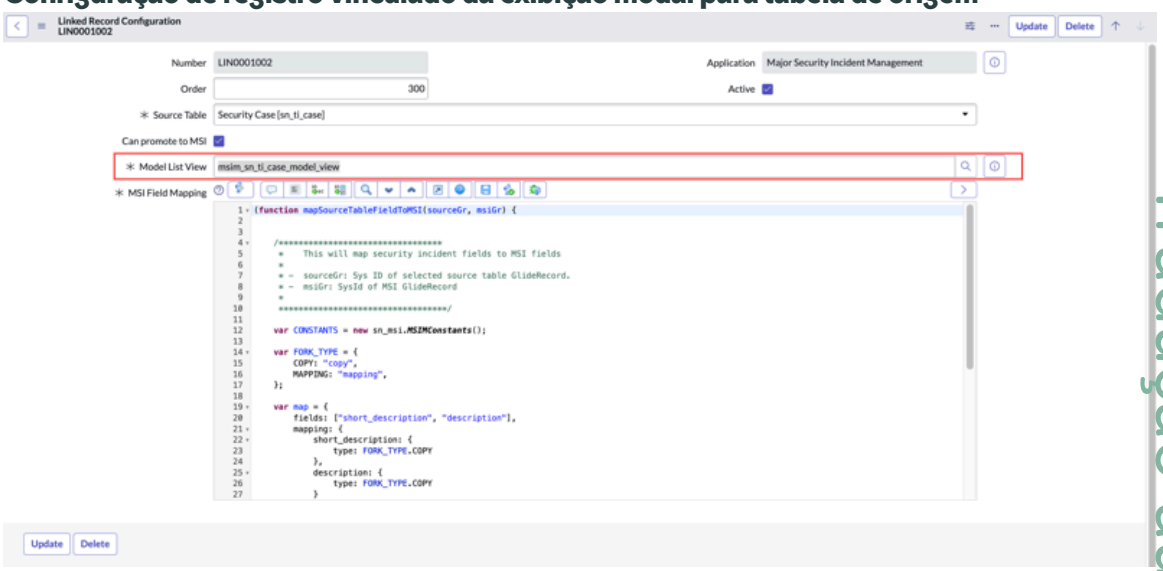
Crie uma exibição para a janela modal de um caso de segurança.

Antes de Iniciar

Consideração principal:

- Por padrão, a lista modal de registro vinculada mostrará somente o layout da lista **padrão**. Se você quiser personalizar o layout da lista, poderá fazê-lo usando a **Exibição Personalizada** na Tabela de Origem.
- Se você quiser renderizar a exibição personalizada, a exibição personalizada também deverá ser selecionada na Configuração de registro vinculado da tabela de origem.

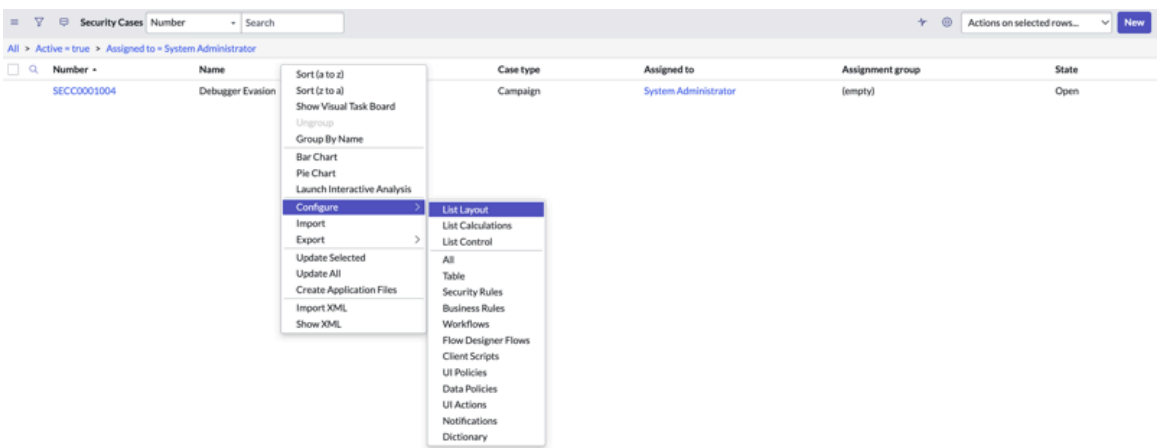
Configuração de registro vinculado da exibição modal para tabela de origem



Função necessária: administrador

Procedimento

1. Vá para a tabela de origem e clique em **Configurar** > **Layout de lista**.



2. Ir para **Exibição em lista** > **Nome de exibição**.
3. Clique em **Novo** na lista suspensa Nome da exibição e crie uma nova exibição, por exemplo, msim_sn_ti_case_modal_view.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione a exibição recém-criada.
   Depois de selecionado, você pode escolher os campos obrigatórios na lista Disponível.
5. Clique em **Salvar**.
6. Navegar até **Menu** > **Exibições** para verificar se a exibição foi renderizada corretamente.

Etapa 3. Criar ações de IU para a tabela de origem de um caso de segurança

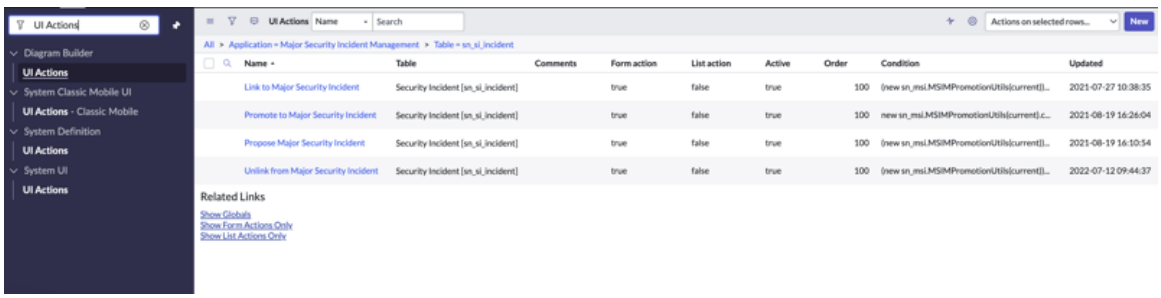
Crie ações de IU para a tabela de origem de um caso de segurança.

Antes de Iniciar

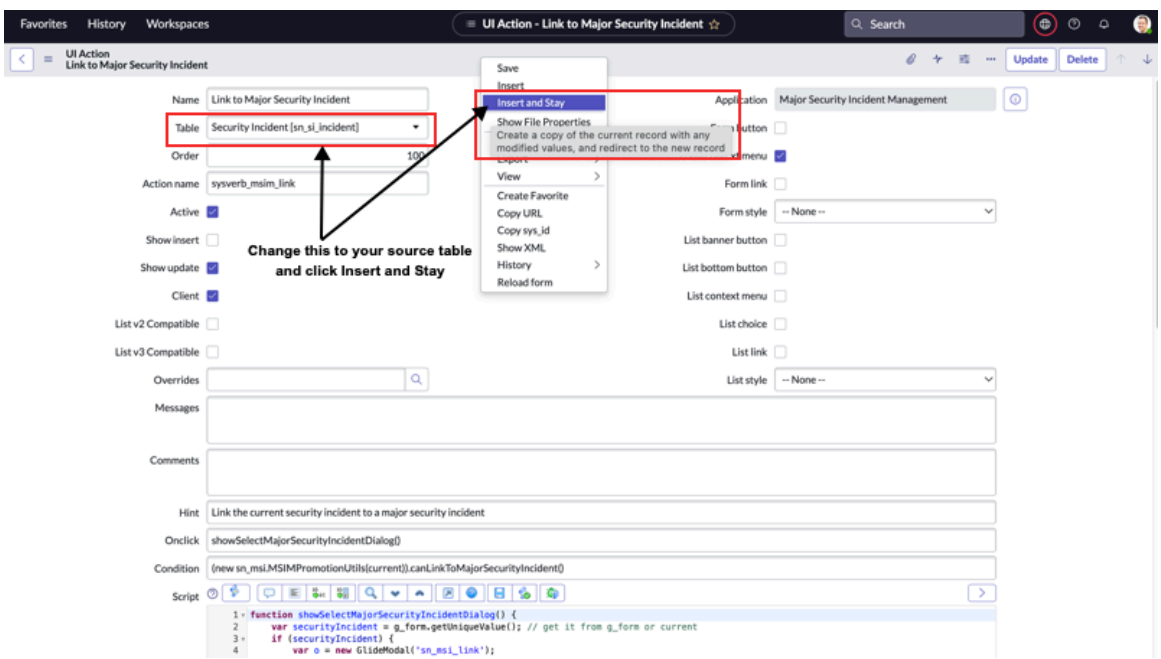
Função necessária: administrador

Procedimento

1. Navegar até **Definição do Sistema** > **Ações de IU**.
2. Execute a opção Filtrar para filtrar a lista por **Aplicação**: Gerenciamento de incidentes de segurança graves e **Tabela**: sn_si_incident.



3. Selecione cada ação de IU uma a uma e salve os detalhes da tabela de origem.



4. Repita as mesmas etapas acima para as seguintes ações de IU:
   - Link para o incidente de segurança grave
   - Incidente de segurança grave proposto

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Desvincular de um incidente de segurança grave
- Promover a incidente de segurança grave

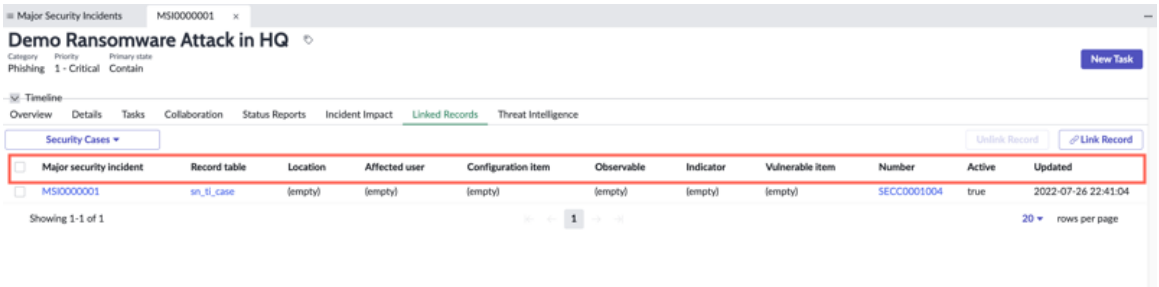
Etapa 4. Criar uma exibição para uma nova guia de registro vinculado para um caso de segurança

Personalize o layout de lista para uma tabela de caso de segurança quando ela for exibida na página Vincular registros com o espaço Gestão de incidentes graves de segurança.

Antes de Iniciar

Pré-requisitos:

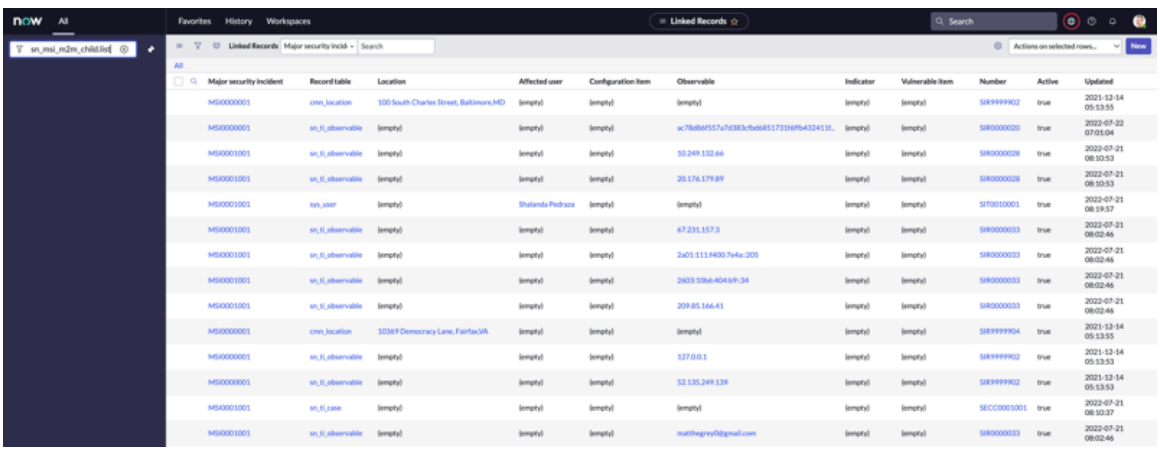
- Escolha a coluna que deve estar visível quando uma lista for renderizada para uma tabela de Caso de Segurança.
- Escolha a ordem dos campos a serem exibidos na lista suspensa.



Função necessária: administrador

Procedimento

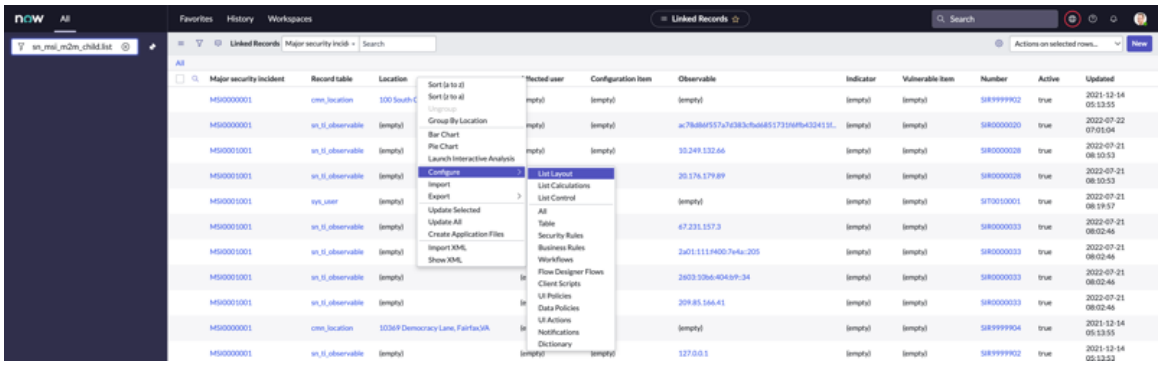
1. Pesquise **sn_msi_m2m_child.list** usando a navegação à esquerda.
   A tabela Registros vinculados é exibida.



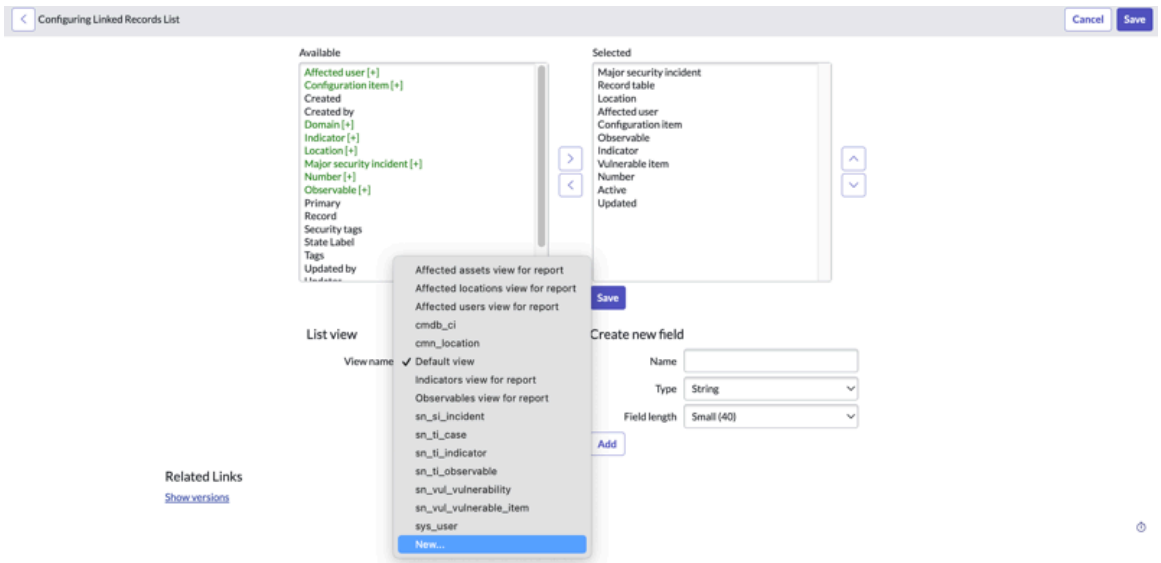
2. Clique com o botão direito do mouse no cabeçalho e selecione **Configurar** > **Layout de lista**.
   A página Configurando a lista de registros vinculados é exibida.

Tradução automática

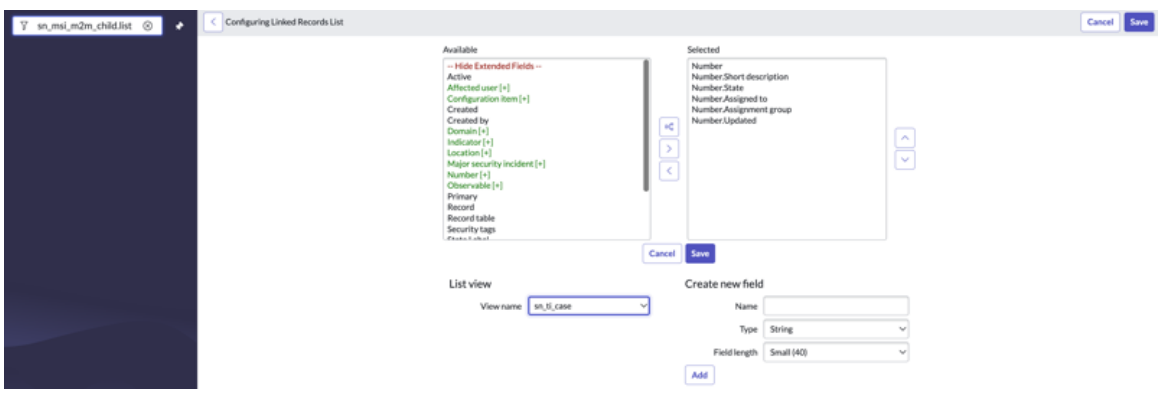
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Ir para **Exibição de lista** > **Nome de exibição**.
4. Selecione **Novo** na lista suspensa Exibir nome.



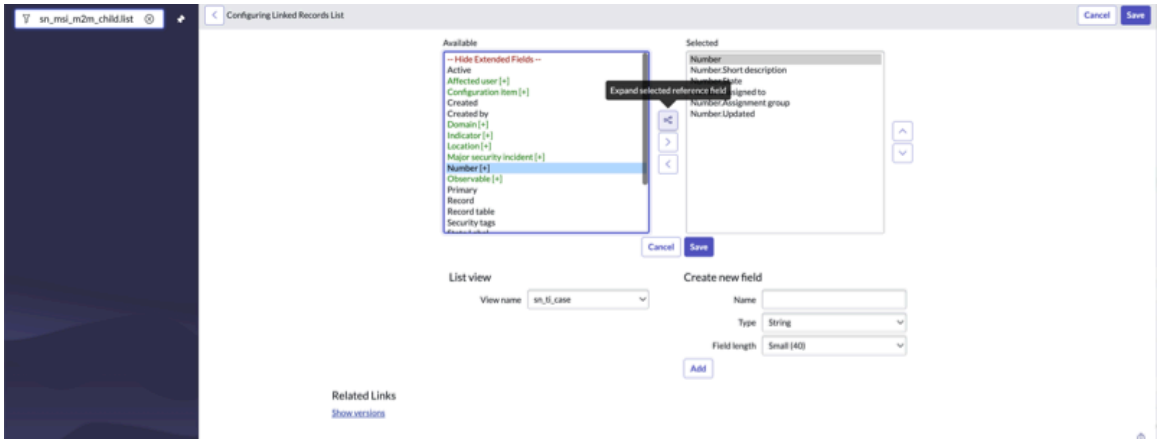
5. Selecione as colunas que serão renderizadas na exibição de lista do espaço.
   O registro do caso de segurança é armazenado na coluna **Número**. Para renderizar informações de um caso de segurança, você deve fazer a referência com pontos na coluna **Número**.



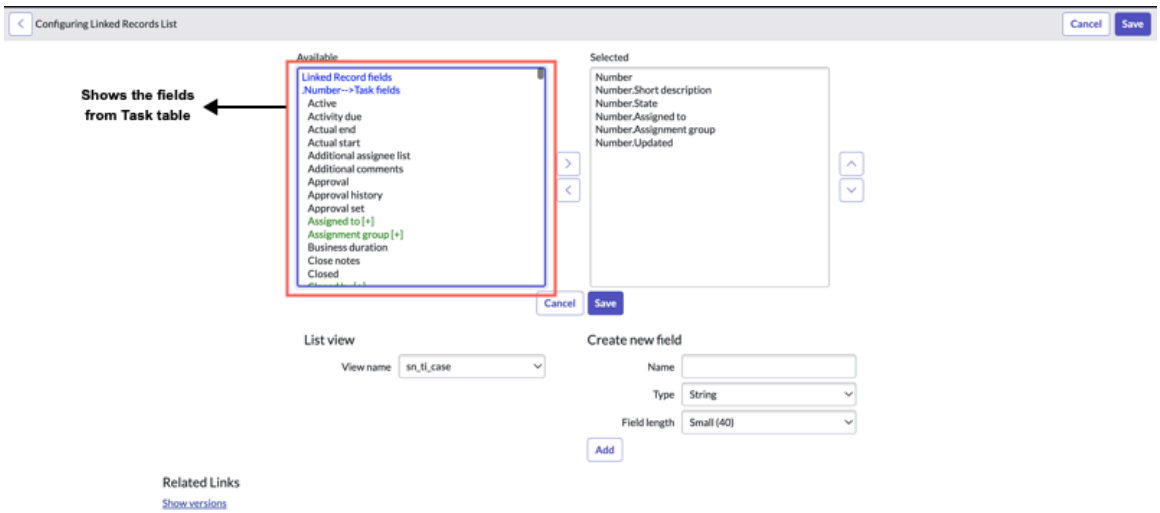
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Para fazer referência com pontos, primeiro selecione a coluna **Número** na lista Disponível e clique em **Expandir campo de referência selecionado**.



b. Expanda as colunas de **Número** para selecionar e mova-as para a lista Selecionado.



c. Clique em **Salvar** para salvar e criar uma exibição.

6. A próxima etapa é renderizar a exibição criada no espaço Gestão de incidentes graves de segurança. Você precisa criar uma **Configuração de layout de lista**.

a. Pesquise a **Configuração de layout de lista** usando a navegação à esquerda.

b. Clicar **Administração do MSI** > **Listar configurações de layout**.

c. Clique em **Novo** para criar uma nova configuração.

d. Selecione a tabela de origem na coluna Tabela e selecione a exibição recém-criada no campo Exibição de lista.

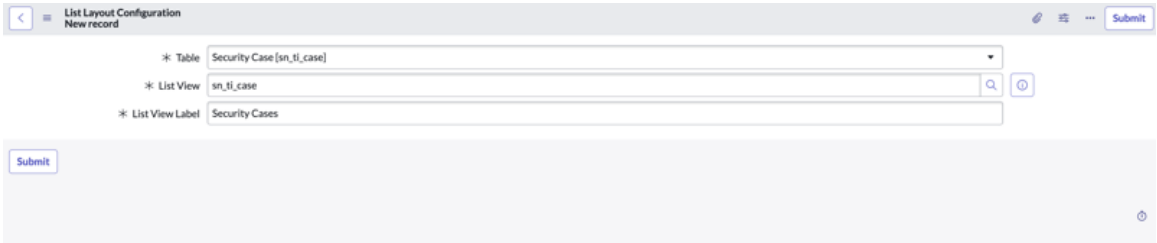
e. O rótulo **Exibição de lista** permite que você controle os rótulos quando a mesma tabela de origem é renderizada no espaço Gestão de incidentes graves de segurança.

f. Salve o registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Depois que o registro for salvo, navegue até o espaço Gestão de incidentes graves de segurança para exibir a exibição de lista renderizada e o rótulo no espaço.



Etapa 5. Adicionar listas de controle de acesso (ACLs) para usuários do espaço Gestão de incidentes graves de segurança

Adicione ACLs (Access Control Lists, listas de controle de acesso) para usuários do espaço Gestão de incidentes graves de segurança.

Antes de Iniciar

Função necessária: administrador

Nota:
As permissões necessárias para vincular e desvincular recursos são controladas pela função sn_msi.linkedsivi_read.

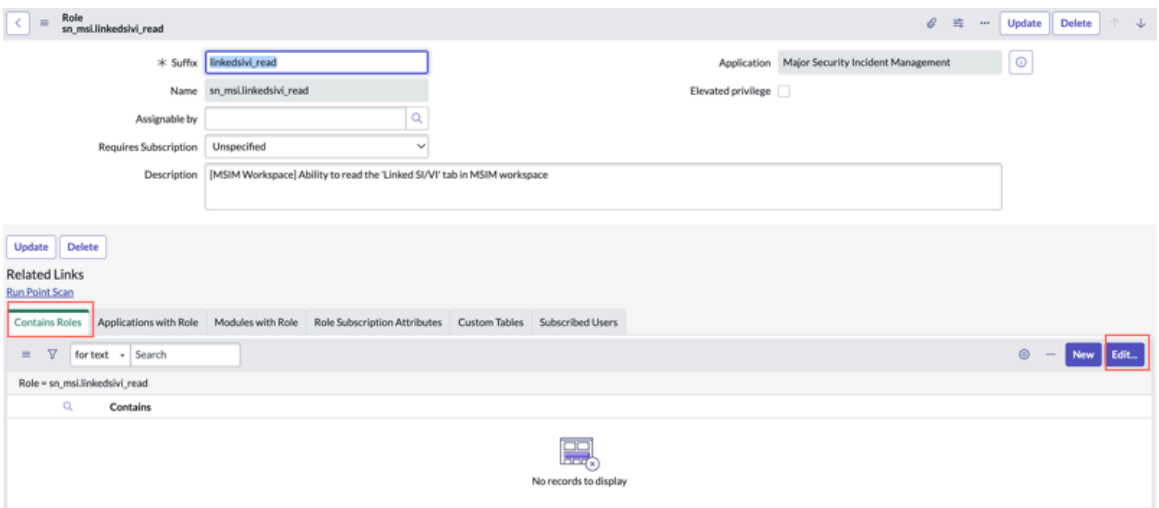
Gestão de incidentes graves de segurança persona contém a função sn_msi.linkedsivi_read.

1. sn_msi.workspace_admin (administrador do espaço do MSIM)
2. sn_msi.workspace_manager (Gerente do espaço do MSIM)
3. sn_msi.workspace_responder (respondente do MSIM Workspace)

Nota:
Para qualquer tabela de origem, você deve garantir que as funções necessárias sejam adicionadas à função sn_msi.linkedsivi_read.

Procedimento

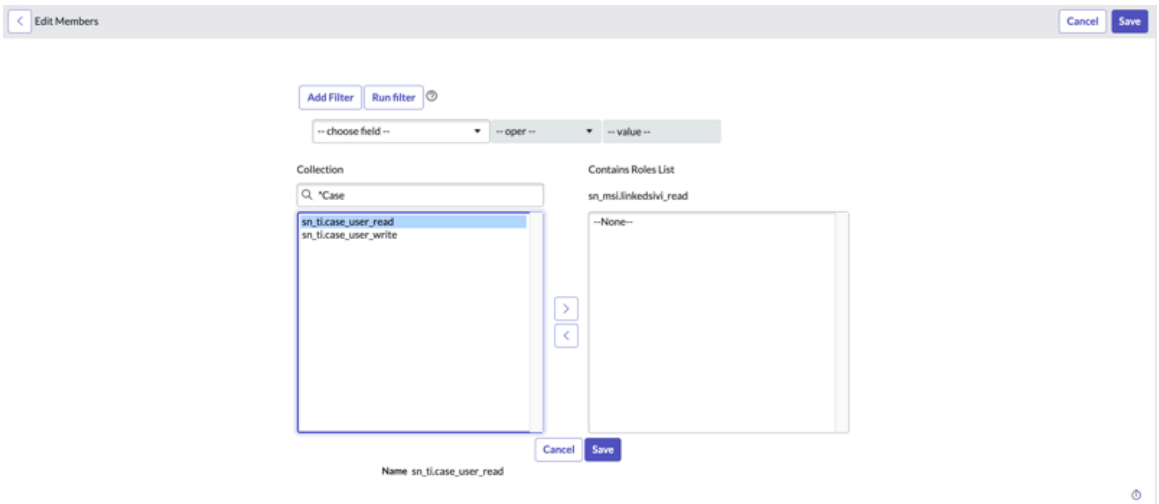
1. Navegar até **Administração de usuários** > **Funções** e pesquise a função **sn_msi.linkedsivi_read**.
2. Clique em **Editar** na seção da lista relacionada Contém funções.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Certifique-se de que as funções da tabela de origem sejam adicionadas na seção Contém funções.
   A página Editar membros é exibida para configurar as funções necessárias para um caso de segurança.



4. Pesquise as funções da tabela de origem na seção Coleções.
   Selecione as funções necessárias que permitem o acesso de leitura e gravação na tabela de origem para um caso de segurança.

Nota:

- Para um caso de segurança, são necessárias duas funções separadas para leitura e gravação.
- Acesso de gravação em tabelas para a capacidade de selecionar o registro de origem do Gestão de incidentes graves de segurança modal de registro vinculado ao espaço.

5. Clique em **Salvar** para adicionar funções.
6. Verifique se as funções foram adicionadas com sucesso à seção da lista relacionada **Contém funções**.

Etapa 6. Criar regras de negócios para um caso de segurança

Crie regras de negócios necessárias para um caso de segurança.

Antes de Iniciar
Função necessária: administrador

Crie as três regras de negócios a seguir para o novo caso de segurança da tabela de origem (sn_ti_case). Essas regras de negócios são necessárias para manter a consistência no comportamento com a tabela de origem fornecida pronta para uso, como Incidente de segurança (sn_si_incident).

Regras de negócios para a nova tabela de origem:

1. **Desativar link quando inativo**: depois que o caso de segurança for encerrado, as informações relacionadas não serão mais mostradas na Gestão de incidentes graves de segurança página do espaço.
2. **Sincronizar informações da equipe na atualização**: a guia de detalhes do incidente de segurança grave mostra as informações sobre todas as equipes ativas e usuários que trabalham em tarefas diferentes. Depois que atualizarmos o atribuído ao usuário ou o grupo de atribuição for alterado no caso de segurança, precisamos atualizar as informações da equipe do caso de segurança na seção da equipe ativa do incidente de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

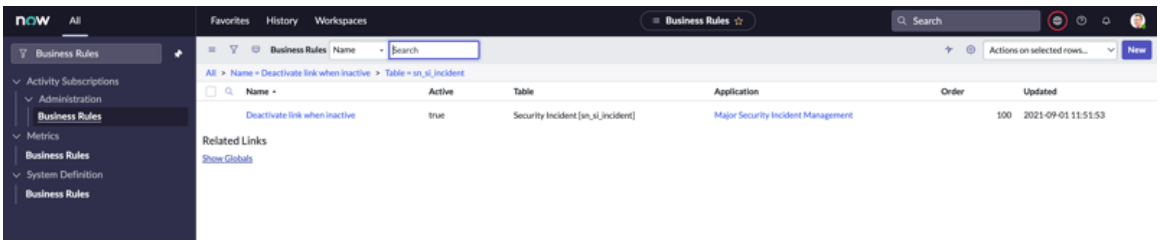
segurança grave. Essas regras de negócios atualizarão o novo usuário atribuído e o grupo de atribuição na seção de equipe ativa.

3. **Sincronizar informações da equipe ao excluir**: a guia de detalhes do incidente de segurança grave mostra as informações sobre todas as equipes ativas e usuários que trabalham em tarefas diferentes. Depois de encerrarmos o caso de segurança, não precisaremos mais mostrar as informações da equipe do caso de segurança na seção da equipe ativa do Incidente de segurança grave. Essas regras de negócios removerão o usuário atribuído e o grupo de atribuição da equipe ativa.

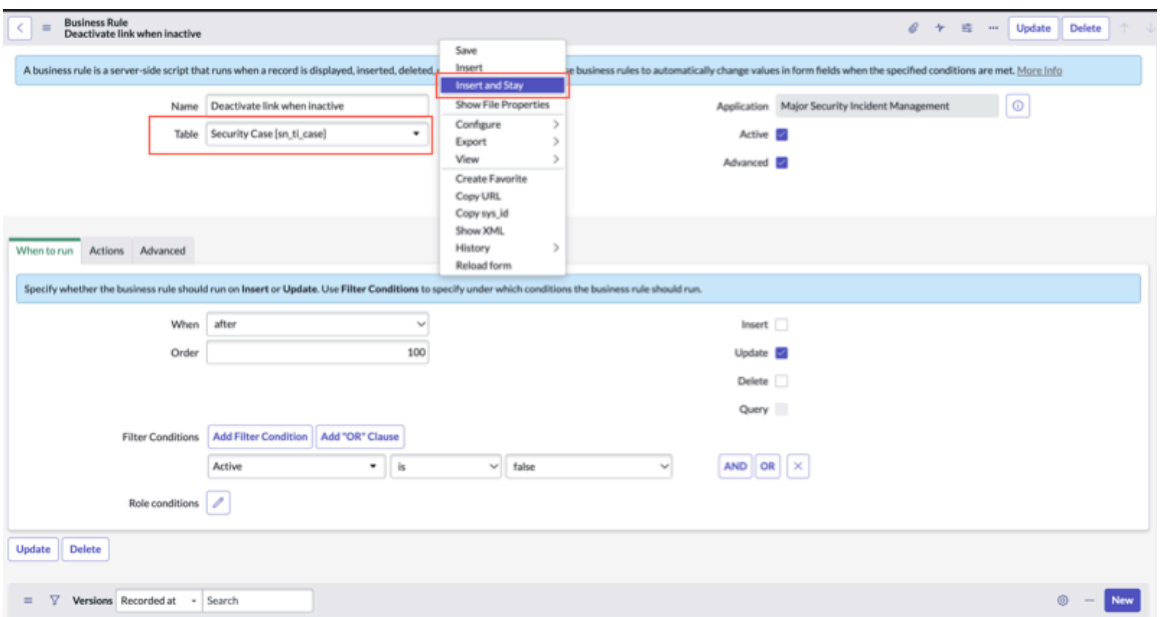
Crie regras de negócios para a nova tabela de origem:

Procedimento

1. Navegar até **Definição do sistema** > **Regras de negócios**.
2. Execute a opção de filtro para filtrar os critérios de regras de negócios com as informações abaixo:
   - **Nome**: Desativar link quando inativo
   - **Tabela**: sn_si_incident



3. Abra o registro e mude o nome da tabela para uma nova tabela de origem: sn_ti_case.
4. Clique com o botão direito do mouse no menu da página e clique em **Inserir e permanecer** para criar o registro.



5. Repita o procedimento para outras duas regras de negócio.
   - Sincronizar informações da equipe ao excluir
   - Sincronizar informações da equipe na atualização

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Etapa 7. Criar configurações de registro de acúmulo

Crie uma configuração de registro de acúmulo para vincular e desvincular registros adicionais do MSI.

Antes de Iniciar

Função necessária: admin e sn_msi.workspace_admin

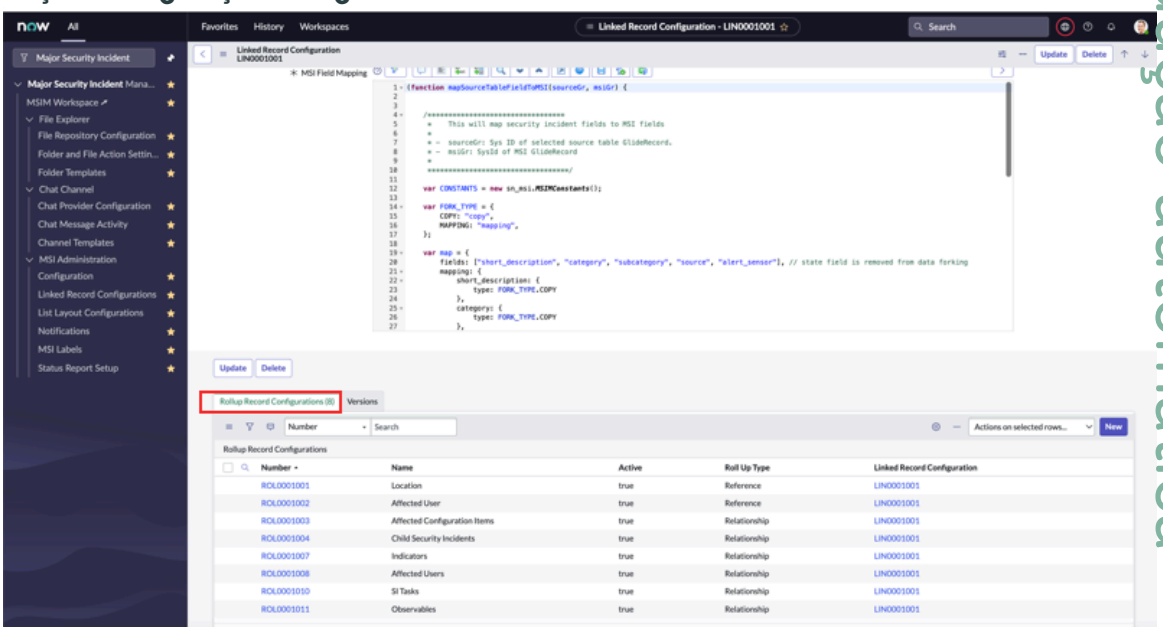
Nota:
O administrador do sistema pode criar o registro e o administrador do espaço do MSI pode atualizá-lo.

Para acumular informações, como itens de configuração, observáveis e indicadores de comprometimento relacionados a um caso de segurança, crie uma configuração de registro de acúmulo.

Procedimento

1. Navegar até **Security Incident Response grave** > **Configuração de registros vinculados**.
   A página Configurações de registro vinculado é exibida.
2. Selecione ou crie um novo registro vinculado e navegue até a seção **Configuração de registro** de acúmulo na mesma página.

Seção Configuração de registro de acúmulo



O que Fazer Depois

- Para obter informações mais detalhadas, consulte Configurar registros de acúmulo no Gestão de incidentes graves de segurança
- Para obter informações de exemplo de caso de segurança, consulteComo escrever um script para um caso de segurança

Como escrever um script para um caso de segurança

Gravar um script para um caso de segurança para acumular configuração de registro.

Antes de Iniciar

Função necessária: admin e sn_msi.workspace_admin

Tradução automática

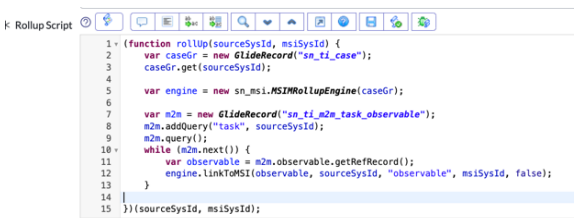
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
O administrador do sistema pode criar o registro e o administrador do espaço do MSI pode atualizá-lo.

Procedimento

1. Pesquise as configurações de registro vinculado usando a navegação à esquerda.
2. Navegar até **Administração do MSI** > **Configuração de registro vinculada**.
3. Abra o registro de configuração que foi criado para um caso de segurança.
4. A configuração do registro de acúmulo será exibida na seção Lista relacionada.
5. Clique em **Novo** para criar uma nova configuração de registro de acúmulo.

Abaixo está um registro de exemplo criado para acumular dados de observáveis relacionados ao caso de segurança que estamos tentando acumular com os valores de campo como:

Nome	Descrição
Acumular tipo	Relacionamento **Nota:** As informações do observável estão disponíveis em um formato de lista relacionada.
Script de Acúmulo	A entrada sourceSysId contém o SYS ID do caso de segurança e msiSysId contém o SYS ID do incidente de segurança grave.  ○ Line 2: As a first step, query for Glide Record for sourceSysId from **Security Case(sn_ti_case)** table. ○ Line 7: Next, query **sn_ti_m2m_task_observable** table using security case sys ID to figure out all the linked observables to a security case. ○ Line 10: Next, iterate over all the linked observables and link them to a Major Security Incident using the method:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	`MSIMRollupEngine.linkToMSI("entityGr", "sourceSysId", "fieldNameInLinkedRecordTable", "msiSysId", "isPrimaryRecord")`

Executar acúmulo atâmico sob demanda

A estrutura de acúmulo não pode lidar com atualizações nos registros vinculados existentes. Nesses casos, o acúmulo atâmico sob demanda deve acontecer para registros vinculados, o que pode ser obtido por meio de regras de negócio.

Para capturar atualizações para os registros vinculados, as regras de negócios devem ser criadas na tabela de origem.

Essas regras de negócios funcionam em operações de inserção, atualização e exclusão. Ao executar a inserção ou atualização, você precisa adicionar ou atualizar as informações acumuladas para MSI. Se você excluir, as informações acumuladas serão removidas de MSI.

Por exemplo, quando um incidente de segurança for vinculado a MSI, as informações relacionadas serão acumuladas automaticamente MSI. Mais tarde, porém, se você adicionar um novo observável a um MSI, o observável recém-adicionado também será acumulado para MSI. Aqui, a regra de negócios **observável de sincronização acumulada** captura a atualização e acumula o registro atualizado para MSI. Da mesma forma, a mesma regra de negócios também lida com a remoção dos observáveis acumulados existentes, se eles forem removidos do incidente de segurança.

Regras de negócio predefinidas

A seguir estão algumas regras de negócios predefinidas que ajudam você a entender como lidar com acúmulos atâmicos

Regra	Descrição
Sincronizar indicador acumulado (sn_ti_m2m_task_indicator)	Use esta regra de negócios para lidar com o acúmulo e a remoção do indicador de comprometimento do incidente de segurança, caso de segurança e tarefa de correção.
Sincronizar observável acumulado (sn_ti_m2m_task_observable)	Use esta regra de negócios para lidar com o acúmulo e a remoção de observáveis vinculados do incidente de segurança, caso de segurança e tarefa de correção.
Sincronizar usuário afetado acumulado (sn_si_m2m_task_affected_user)	Use esta regra de negócios para lidar com o acúmulo e a remoção de usuários afetados vinculados do incidente de segurança, caso de segurança e tarefa de correção.
Sincronizar IC afetado acumulado (task_ci)	Use esta regra de negócios para lidar com o acúmulo e a remoção de itens de configuração associados do incidente de segurança, caso de segurança e tarefa de correção.

Integrações do Security Incident Response

Todas as Security Operations aplicações principais e integrações de terceiros não essenciais estão disponíveis na ServiceNow Store. Esta integração permite que você obtenha recursos

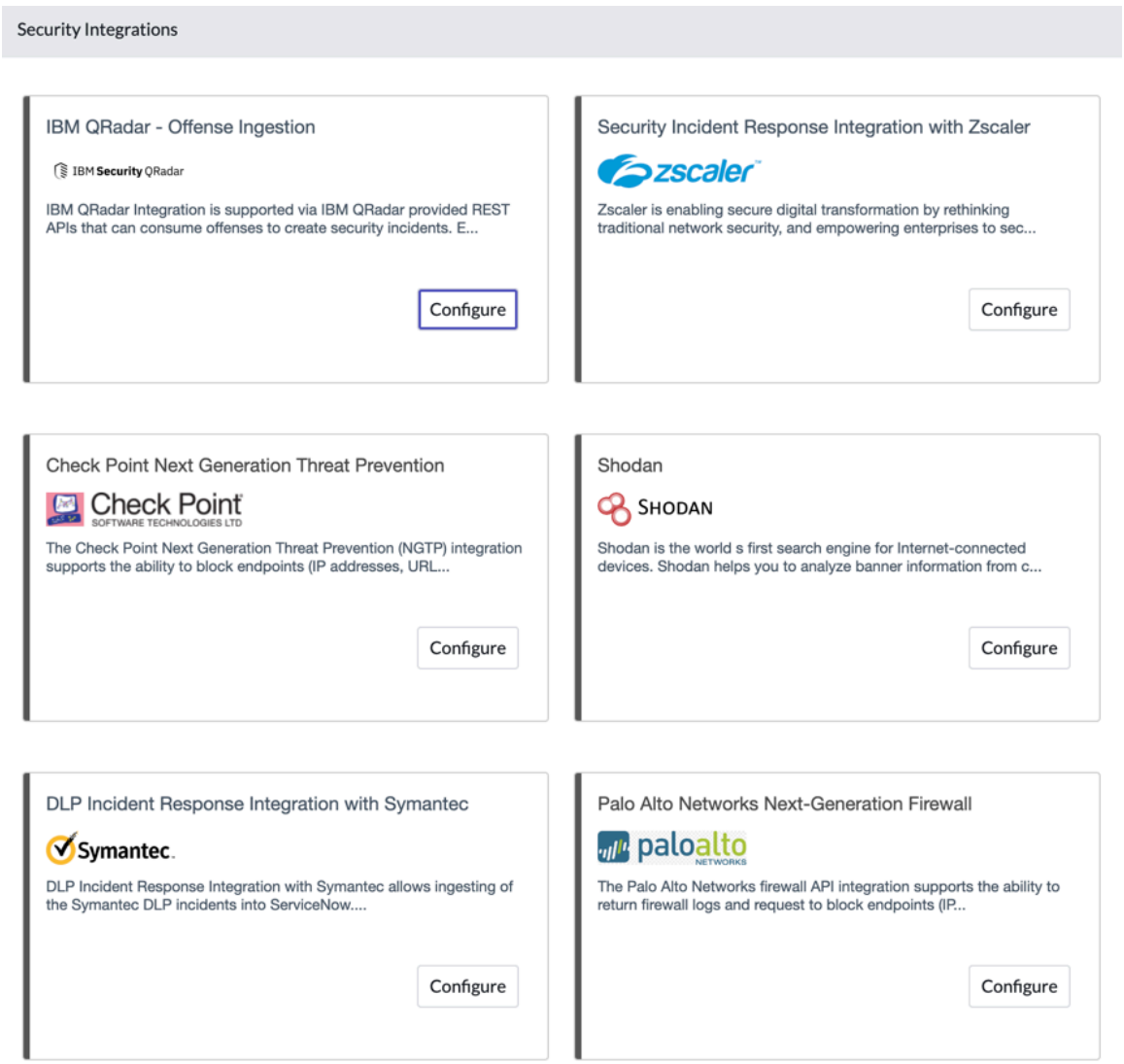
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

novos e atualizados com mais rapidez. Esta seção fornece instruções para ativar as integrações e configurar ServiceNow e integrações de terceiros. Também estão incluídas algumas diretrizes básicas para desenvolver suas próprias integrações, bem como detalhes sobre integrações específicas incluídas no sistema básico.

Configurações de Integração

O sistema básico inclui uma série de "cartões" para cada uma das implementações de integração que você pode ativar e usar. Além disso, os cartões são exibidos para todas as integrações publicadas na ServiceNow Store que têm dependências nos plug-ins Security Operations. Os cartões de integração podem ser exibidos selecionando **Security Operations** > **Configurações de Integração**.



Você pode filtrar as integrações visíveis usando o menu suspenso **Categoria**. O menu suspenso **Mostrar configurações** permite que você veja várias instâncias de implementações que permitem sua criação.

Botões em cartões de integração

Os cartões de integração exibem botões diferentes, dependendo do estado atual da integração e da origem do cartão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Botão	Descrição
Instalar Plug-in	Clique neste botão para instalar o plug-in aplicável para ativar a integração. Depois que o plug-in é instalado, o botão muda para **Configurar**.
Configurar	Clique neste botão para inserir informações para configurar a integração. Para algumas integrações, pode ser necessário inserir chaves de API ou URLs adquiridos no site da integração de terceiros.
Novo	Certas integrações, como Carbon Black e IBM QRadar, permitem que você defina várias implementações da mesma integração. Para essas integrações, clique em **Novo** depois que o plug-in for ativado. Os cartões permitem instalar plug-ins (quando aplicável) e configurar as implementações para uso.
Abrir página	No sistema de base, sua instância executa uma consulta na ServiceNow Store para todas as aplicações que tenham dependências de plug-ins Security Operations. Quando essas aplicações são encontradas e os plug-ins da aplicação associados são ativados, os cartões de integração deles são exibidos com os outros cartões de integração de segurança. Clique em **Abrir página** para acessar o site da aplicação de terceiros para configurar a integração. Depois de concluir a configuração, o botão **Abrir página** muda para **Configurar**.

ArcSight ESM Ingestão de eventos para integração Security Operations

A integração de ingestão de eventos ArcSight ESM com o produto Security Incident Response permite que os analistas de incidentes de segurança coletem eventos correlacionados e automatizem a criação de incidentes de segurança com a plataforma ServiceNow. Os dados são ingeridos continuamente com base em uma programação de pesquisa configurada e são usados por analistas para identificar e responder a possíveis ameaças à segurança cibernética.

Com esta integração, os eventos correlacionados que são candidatos a incidentes de segurança podem ser ingeridos periodicamente. Você pode mapear campos em eventos correlacionados para campos de incidente de segurança, visualizar a configuração de um evento como um incidente de segurança e configurar a ingestão programada de eventos para criar automaticamente incidentes de segurança de forma contínua.

Visão geral

Esta integração fornece a um analista do centro de operações de segurança (SOC) visibilidade para eventos de correlação em ArcSight ESM. Esses dados podem ser integrados a incidentes de segurança do Now Platform Security Incident Response (SIR) para investigação e correção adicionais. Os perfis são criados na sua instância Now Platform para lidar com diferentes tipos de evento de correlação que são criados e disponibilizados por meio de visualizadores de consulta de correlação em ArcSight ESM. Esses perfis personalizam como diferentes ArcSight ESM campos de evento correlacionados são exibidos em incidentes de segurança SIR.

Principais recursos

Esta integração inclui os seguintes recursos principais:

- Crie vários perfis de ingestão de eventos para criar SIR incidentes de segurança para tipos específicos de ameaças, como malware e tentativas de acesso não autorizado.
- Mapeamento de arrastar e soltar de valores de campo de evento de correlação ArcSight ESM] para campos de incidente de segurança SIR associados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Uma visualização do layout do incidente de segurança SIR com base em eventos de correlação de amostra para validar os detalhes do mapeamento de eventos.
- Inclua eventos de correlação históricos, bem como novos eventos notáveis em intervalos configuráveis.
- Filtrar eventos de correlação que não atendem a SIR critérios de geração de incidentes, por exemplo, eventos de baixa prioridade
- Agregue eventos a incidentes de segurança SIR existentes com base em valores de campo correspondentes para evitar incidentes de segurança duplicados.
- Atualize eventos de correlação com base na criação de incidentes SIR e/ou condicionais de fechamento por meio de uma interface bidirecional.

Now Platform Versões compatíveis

Esta integração é compatível com as versões New York Patch 6 e Orlando Now Platform.

As seguintes aplicações do Security Operations devem ser instaladas e ativadas a partir de ServiceNow Store. Instale e ative um aplicativo de cada vez na ordem listada abaixo para garantir uma instalação sem problemas:

1. Security Integration Framework
2. Security Support Common
3. Security Incident Response
4. Ingestão de eventos e alertas para Security Operations
5. Plug-ins do Integration Hub
   a. ServiceNow Integration Hub Runtime
   b. Etapa de ação do Hub de integração da ServiceNow - REST

Para obter mais informações sobre como instalar as aplicações principais Security Operations, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

ArcSight ESM versões compatíveis

Esta integração foi testada com a versão 7.0.0.2436 do ArcSight ESM Manager. A integração oferece suporte a ambientes de serviço no local e em nuvem ArcSight ESM / hospedado.

MID Server

Esta integração requer um MID Server instalado e configurado em sua instância Now Platform® para se conectar ao serviço ArcSight ESM quando o servidor ArcSight ESM é implantado em sua rede corporativa. Se você estiver usando o serviço em nuvem ArcSight ESM, um MID Server não será necessário. Consulte o site de documentação do produto da ServiceNow para obter mais informações sobre MID Servers.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Referências

Referência	Identificador de documento	Título do Documento
1	ArcSight ESM documentação do produto	Documentação do produto ArcSight .
2	ServiceNow Site da documentação do produto	Site de documentação do produto da ServiceNow

Configure sua instância Now Platform® para a integração de ingestão de eventos ArcSight ESM

A seção a seguir lista as tarefas de configuração que você deve concluir em sua instância Now Platform® antes de instalar a aplicação do ServiceNow Store.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração sem problemas.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform® e Security Incident Response (SIR) necessárias.	As funções a seguir são necessárias para a instalação, configuração e uso da integração na sua instância Now Platform®. • Um usuário com a função de administrador Now Platform® (admin) instala a aplicação a partir do ServiceNow Store e atribui a função de administrador de incidente de segurança (sn_si.admin). • Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no Now Platform®: ◦ Nomeia, cria e edita perfis de evento. ◦ Seleciona e mapeia valores de ArcSight ESM eventos de correlação para incidentes de segurança. ◦ Visualiza os detalhes do incidente de segurança para precisão antes de finalizar a configuração. ◦ Programa a ingestão de eventos correlacionados em andamento. ◦ Habilita atualizações de eventos correlacionados quando um incidente de SIR é criado e encerrado. ◦ Atribui a função de analista de incidente de segurança (sn_si.analyst). ◦ Usuários com o sn_si.analyst trabalham com incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	Para obter mais informações sobre funções e atribuição de funções a usuários, consulte Funções no site de documentação do produto da ServiceNow .
Verifique se você está usando a versão 7.0.0.2436 ou posterior do ArcSight ESM Manager. Versões anteriores não são compatíveis.	Se você tiver acesso ao ArcSight ESM Visualizador de consulta, terá acesso à API necessária para esta integração. Não há nenhuma outra configuração especial necessária para a API.
Configure o Visualizador de consulta em ArcSight ESM.	Antes de ingerir eventos de correlação, você deve configurar o Visualizador de consulta no console ArcSight ESM. Consulte Configurar o Visualizador de consulta ArcSight ESM para mais detalhes.
Opcional Crie fases personalizadas em ArcSight ESM para atualizações de evento de correlação.	Um evento de correlação passa por várias fases em seu ciclo de vida antes de ser encerrado. ArcSight ESM fornece fases padrão como Inicial, Monitoramento, Em fila e Encerrado. Algumas dessas fases exigem entradas do usuário, mas outras fases são aplicadas automaticamente ao evento sem qualquer intervenção do usuário (o campo **Usuário obrigatório** está desmarcado no console ArcSight ESM. Você pode criar fases personalizadas que não exijam nenhuma intervenção do usuário e usá-las na sua instância Now Platform®. Consulte Opções adicionais: automatizar atualizações de eventos correlacionados e fechamento com base no SIR status do incidente para mais detalhes.
Verifique se você instalou e configurou uma aplicação do MID Server.	Aplicação do MID Server configurada Um MID Server em sua instância Now Platform® é necessário para se conectar ao serviço ArcSight ESM se o servidor ArcSight ESM for implantado em sua rede corporativa. Consulte Instalar e configurar a aplicação ServiceNow para a integração de ingestão de eventos ArcSight ESM para obter instruções sobre como configurar uma aplicação do MID Server. Consulte o MID Server para obter informações sobre MID Servers. Se você estiver usando um serviço hospedado ou em nuvem, que seja acessível pela Internet, um MID Server não será necessário.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas. **1.** Security Incident Response **2.** Security Integration Framework

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	3. Security Support Common **4.** Ingestão de eventos e alertas para Security Operations: esta aplicação requer: ○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub Runtime ○ com.glide.hub.action_step.rest => Etapa de ação do ServiceNow IntegrationHub - REST **5.** Threat Core Para obter mais informações sobre como instalar as aplicações principais Security Operations, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

O que Fazer Depois

Você configurou com sucesso sua instância Now Platform® para a integração. A próxima etapa é instalar a aplicação ArcSight ESM Security Event Ingestion for Security Operations a partir do ServiceNow Store para a integração.

Configurar o Visualizador de consulta ArcSight ESM

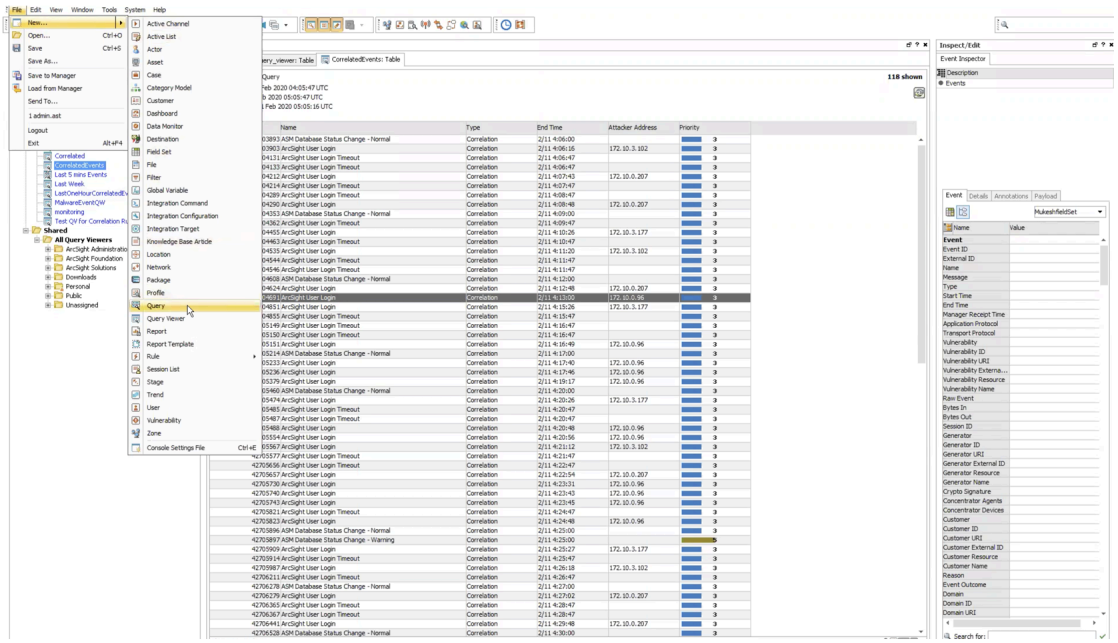
Crie um visualizador de consulta e defina filtros que incluirão eventos de correlação criados recentemente que serão ingeridos ServiceNow.

Antes de Iniciar

Função necessária: Administrador do ArcSight

Procedimento

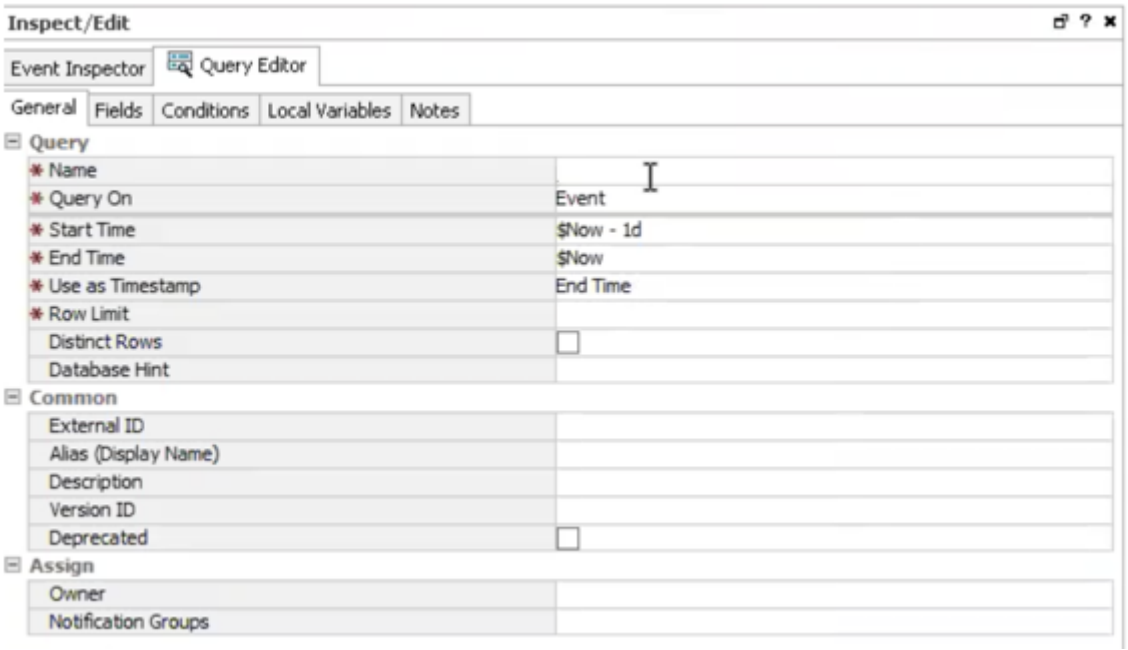
1. Faça login no console ArcSight ESM para criar um visualizador de consulta.
2. Para criar uma nova consulta, navegue até **Arquivo** > **Novo** > **Consulta**.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

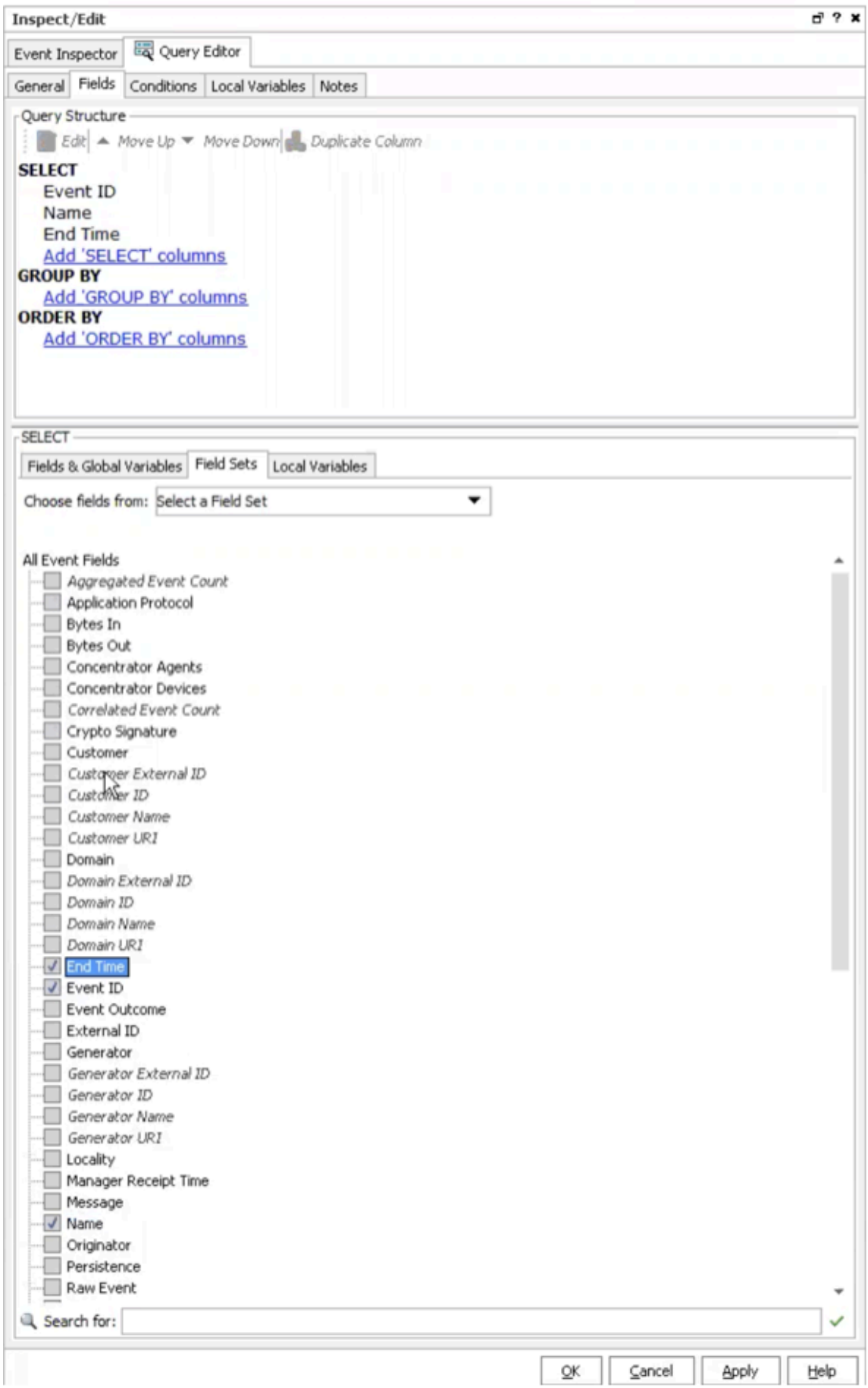
3. Defina condições para o Visualizador de consulta no painel **Inspecionar/editar**.



4. Clique na guia **Campos**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

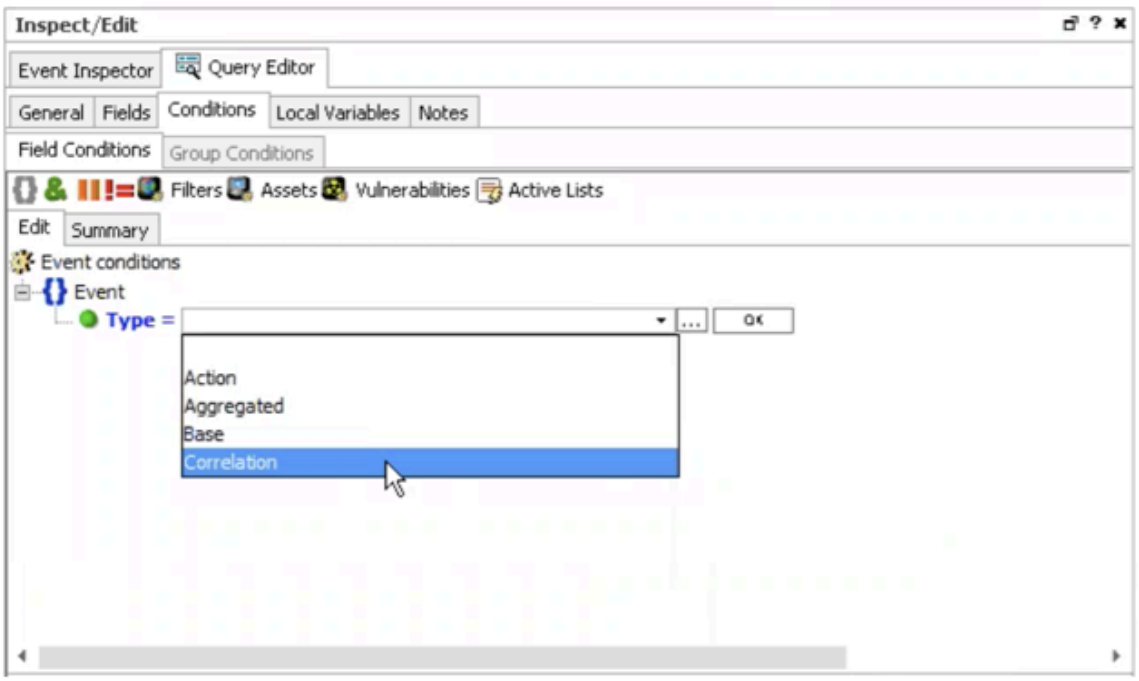


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione os campos que devem ser incluídos durante a ingestão.
   Você deve selecionar os campos *`ID do evento`*, *`Nome`* e *`Hora de término`* para que a ingestão seja bem-sucedida.
6. Clique no link **Adicionar colunas "ORDER BY"**, selecione o campo **ID do evento** e especifique a ordem de classificação como **Decrescente** para garantir que os eventos mais recentes sejam ingeridos.
7. Clique na guia **Condições**.
8. Clique com o botão direito do mouse em **Evento** em **Condições de evento** na seção **Resumo**.
9. Clicar **Nova condição** > **Raiz** > **Tipo** e selecione o Tipo de evento como **Correlação**.

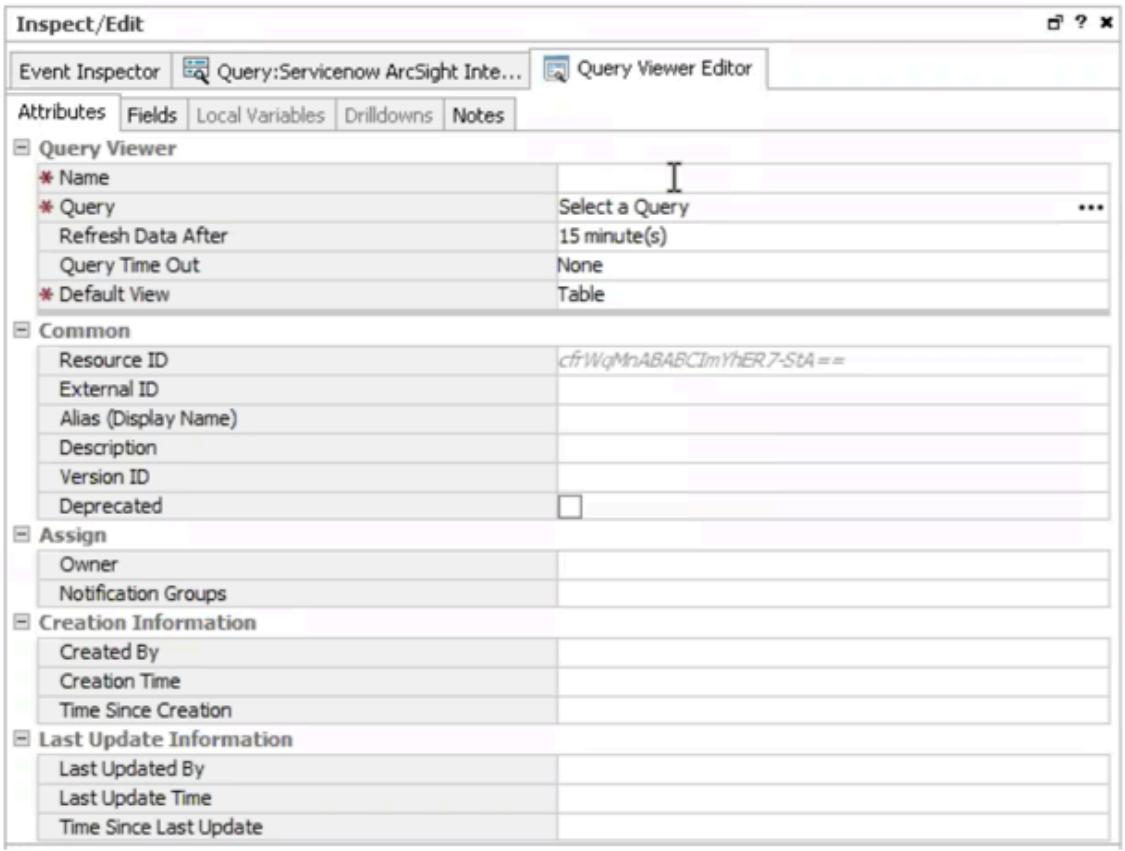
> **Importante:**
> Somente eventos de correlação serão recuperados; eventos de base para correlações não serão recuperados.



10. Clique em **OK** para salvar a consulta.
    A próxima etapa é criar um Visualizador de consulta para esta consulta.
11. Navegar até **Arquivo** > **Novo** > **Visualizador de consultas**.

Tradução automática

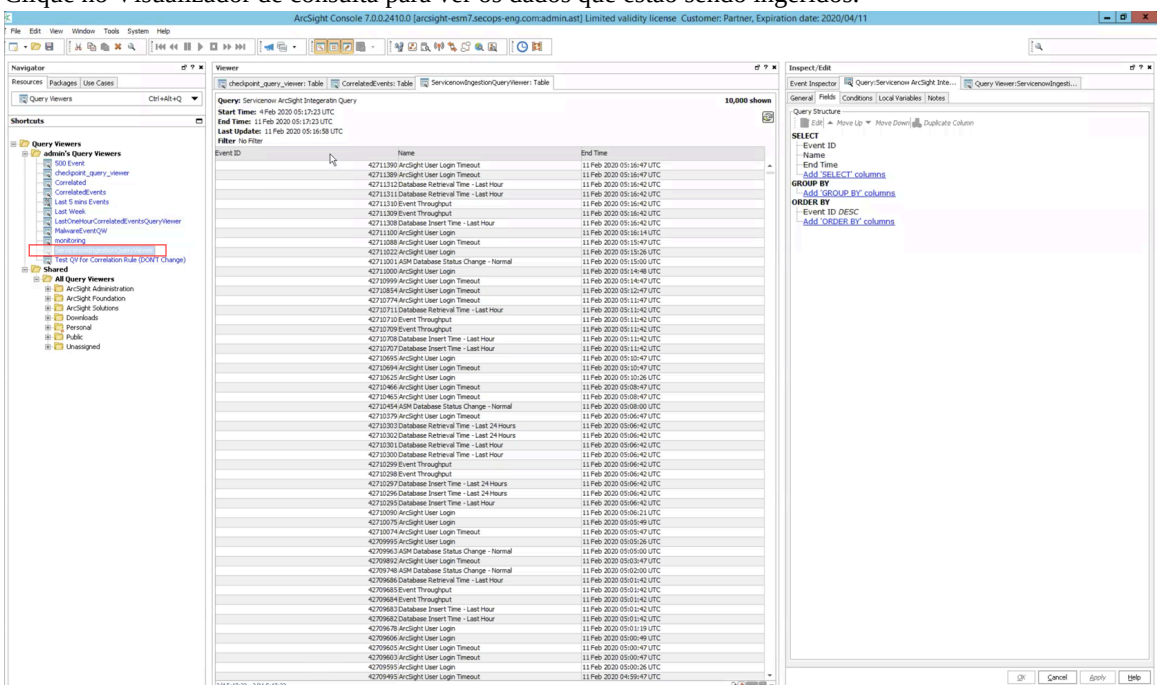
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



12. Clique na guia **Campos** e certifique-se de que os campos obrigatórios (*`ID do evento`*, *`Nome`*, *`Hora de término`*) especificados na consulta estejam selecionados.

13. Clique em **Aplicar** para salvar o Visualizador de consulta.
O novo Visualizador de consulta que você criou está listado na seção Visualizadores de consulta.

14. Clique no Visualizador de consulta para ver os dados que estão sendo ingeridos.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instalar e configurar a aplicação ServiceNow para a integração de ingestão de eventos ArcSight ESM

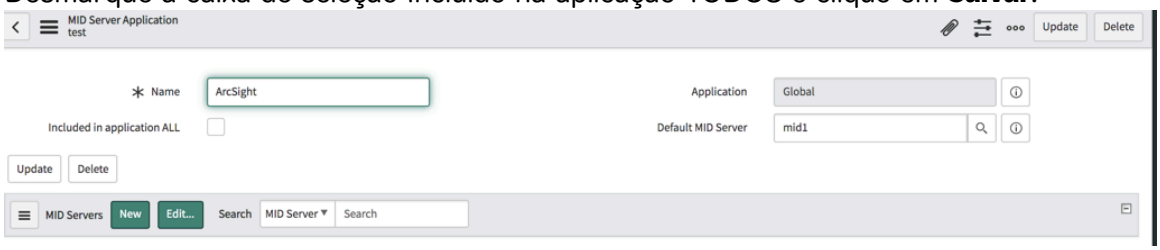
Antes de executar a integração na sua instância Now Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente aos produtos Security Incident Response e Security Operations na sua instância Now Platform.

Antes de Iniciar

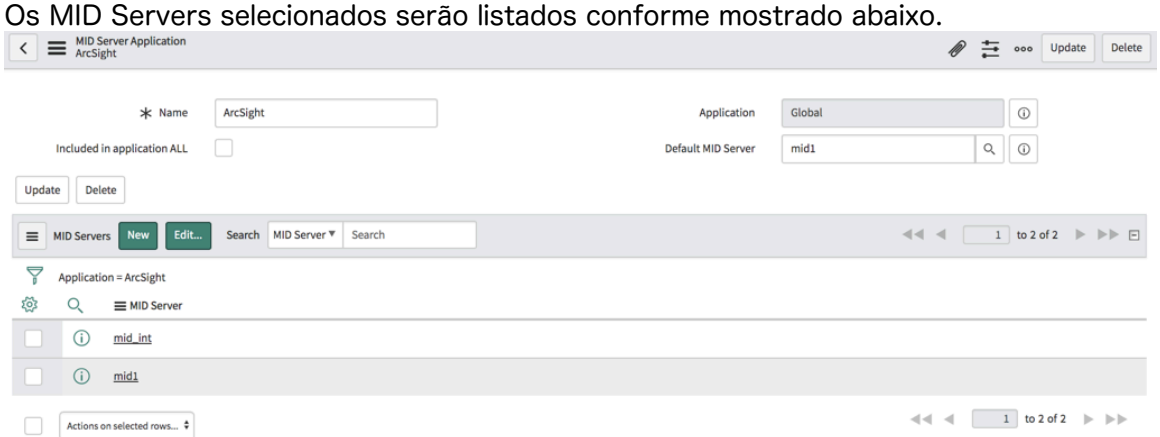
Função necessária: sn_si.admin

Procedimento

1. Se você não instalou a aplicação [ArcSight ESM de ServiceNow Store para a integração, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.
2. Depois de instalar a aplicação com êxito, navegue até **Integrações** > **Configurações de integrações** e localize o bloco ArcSight ESM.
3. Para configurar a aplicação, clique em **Novo**.
4. Como alternativa, se um botão **Configurar** for exibido em um bloco, clique nele para editar uma configuração existente.
5. No formulário, preencha os campos.
   Para criar uma nova aplicação do MID Server, siga estas etapas:
   a. Navegar até **MID Server** > **Candidaturas** e clique em **Novo**.
   b. Insira um nome para a aplicação do MID Server e selecione um MID Server a ser usado como padrão.
   c. Desmarque a caixa de seleção Incluído na aplicação TODOS e clique em **Salvar**.



   d. Clique em **Editar**. Na página **Editar Membros**, selecione todos os MID Servers disponíveis, mova-os para a Lista de MID Servers e clique em **Salvar**.
   e. Os MID Servers selecionados serão listados conforme mostrado abaixo.

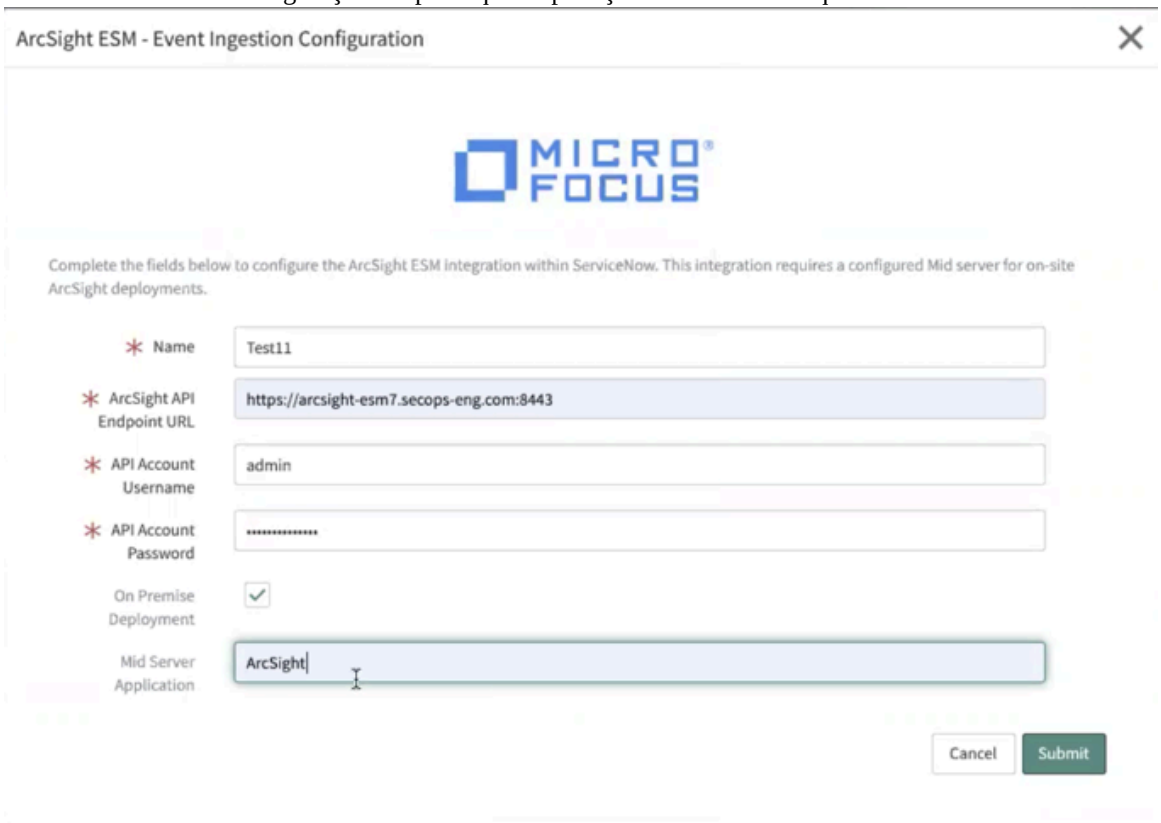


Dependendo da disponibilidade, um dos MID Servers configurados com a aplicação MID Server será usado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Insira os detalhes da configuração e especifique a aplicação do MID Server que você criou.



Cada evento de correlação que você ingere do console do gerenciador ArcSight ESM requer um perfil de evento exclusivo em sua instância. No entanto, a origem ArcSight ESM que você configura no formulário Configuração de ingestão de eventos pode ser reutilizada para vários perfis, desde que cada perfil inclua tipos de evento de correlação exclusivos.

7. Clique em **Enviar**.
   Depois de validada e enviada com sucesso, cada configuração de servidor ArcSight ESM é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista de seleção Mostrar configurações, clique em **Sim**.

O que Fazer Depois

Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar um perfil de evento.

Criar um perfil para integração de ingestão de evento de correlação ArcSight ESM

Como um usuário com a função sn_si.admin, você cria um perfil em sua instância Now Platform e determina quais eventos de correlação criam incidentes de segurança. Antes que os incidentes de segurança Now Platform Security Incident Response (SIR) sejam criados a partir de eventos de correlação, os valores de campo dos eventos são exibidos em um layout de um incidente de segurança Now Platform para que você possa visualizar como o incidente de segurança real será criado.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Os eventos de correlação são ingeridos automaticamente no ambiente Security Operations da sua instância Now Platform, dependendo do tipo de perfil definido. Um perfil é um encapsulamento de um tipo de evento de correlação, como tentativas de acesso não autorizado ou malware.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois que um evento de correlação tiver sido ingerido, você poderá mapear campos de evento de correlação individuais para campos correspondentes no incidente de segurança. Você pode filtrar eventos de correlação para especificar quais eventos criam incidentes de segurança. Por exemplo, você pode preferir filtros que criam incidentes de segurança somente para eventos de correlação identificados como de alto risco. Você também pode definir critérios adicionais de agregação de eventos para que os eventos de correlação duplicados de entrada sejam agregados a um incidente de segurança em aberto. Por fim, você pode definir uma programação de ingestão e ativar o perfil.

Os nomes dos perfis de evento na sua instância Now Platform devem ser exclusivos e só podem ser mapeados para um perfil de evento ativo por vez.

Criar e nomear o perfil para integração de ingestão de eventos ArcSight ESM

Você pode configurar um perfil para ingerir eventos de correlação.

Antes de Iniciar

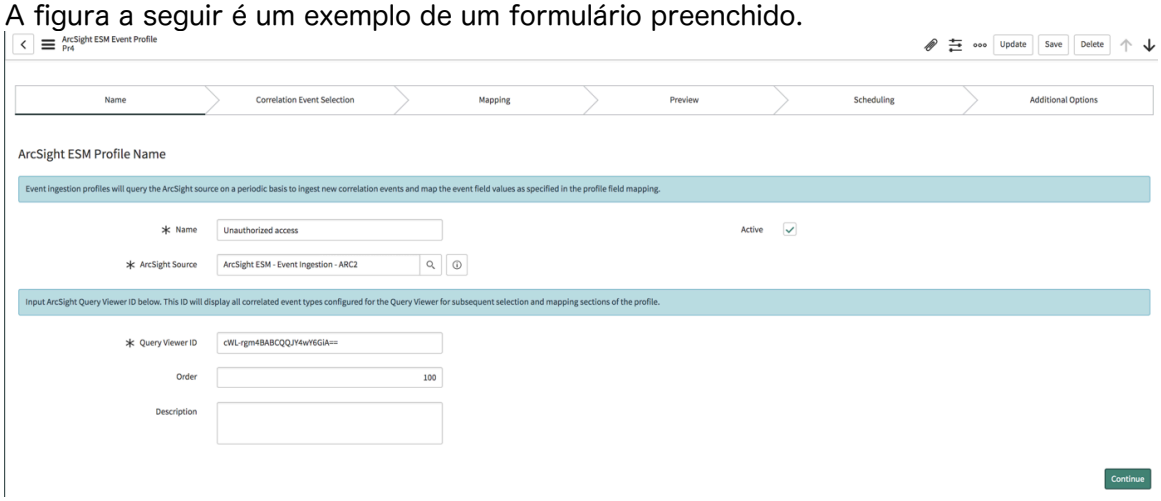
Função necessária: sn_si.admin

Procedimento

1. Para criar um perfil de evento para um evento de correlação em sua instância Now Platform, navegue até **Integração de ESM do ArcSight** > **Perfil de evento do ArcSight ESM**.
2. Clique em **Nova**.
3. Preencha os campos.

   Um exemplo de formulário preenchido segue a tabela.

   A figura a seguir é um exemplo de um formulário preenchido.

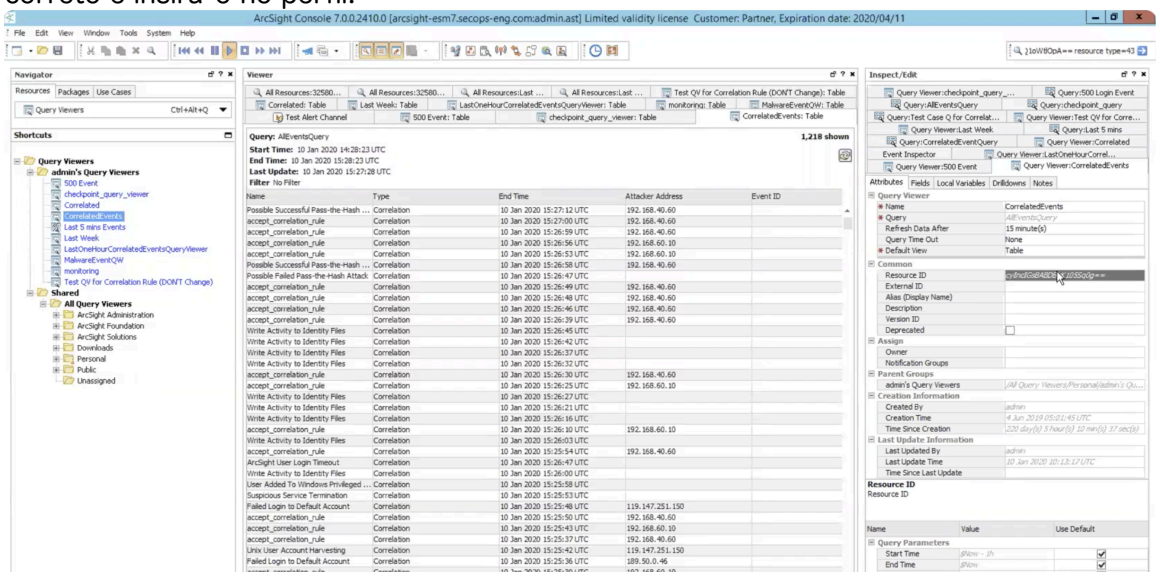


   Depois de inserir os detalhes do perfil, clique em **Continuar**. O ID do visualizador de consulta é validado e, se um ID de recurso correspondente estiver presente no ArcSight ESM Visualizador de consulta, o nome do visualizador de consulta será retornado conforme mostrado abaixo. Se a validação falhar, verifique se o ID do recurso existe no

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

console ArcSight ESM. Se o ID do recurso não for encontrado, encontre o ID de recurso correto e insira-o no perfil.



O que Fazer Depois

A próxima etapa é selecionar os tipos de evento de correlação para ingestão no Visualizador de consulta que foi selecionado na etapa anterior.

Selecionar eventos de correlação para integração de ingestão de eventos ArcSight ESM

Com base na origem ArcSight ESM e no Visualizador de consulta configurado, selecione uma regra de evento de correlação para o perfil.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Exiba os eventos de correlação disponíveis listados na Seleção de evento de correlação em sua instância da Now Platform para determinar quais eventos de correlação deseja ingerir e criar incidentes de segurança. Você só pode selecionar um tipo de regra de correlação na lista para cada perfil.

O ID do visualizador de consulta e o nome do visualizador de consulta conforme especificado no formulário do visualizador de consulta são exibidos. Selecione um evento de correlação na lista que você pode usar para criar um mapeamento de configuração para o evento correlacionado ingerido.

Clique na lista suspensa no campo Lista de eventos de correlação. Uma lista de eventos de correlação que estão presentes no ArcSight ESM Console do visualizador de consulta é exibida.

Clique em **Continuar** para prosseguir para a próxima etapa no assistente.

Mapeamento de campos de evento de correlação para a integração de ingestão de eventos ArcSight ESM

Depois de identificar a regra de evento de correlação específica na lista, a próxima etapa é mapear os campos de evento de correlação para os campos no formulário de incidente de segurança.

Visão geral

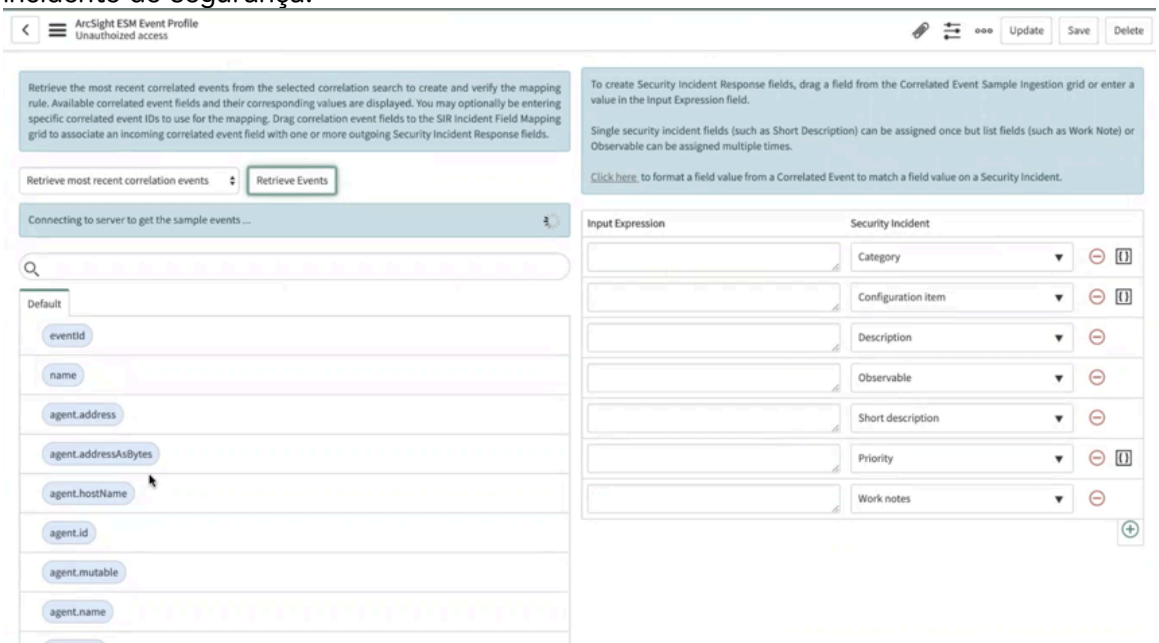
Para a etapa de mapeamento, você pode ingerir eventos de correlação de amostra para a regra de correlação selecionada. Durante esta fase de mapeamento, você pode garantir

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

que todos os dados de campo de evento de correlação relevantes sejam mapeados para o local apropriado no formulário de incidente SIR e, em seguida, visualizar o incidente SIR na seção de visualização.

A figura a seguir mostra a configuração de mapeamento padrão fornecida para criar o perfil de evento de correlação. Você pode personalizar os campos que preenchem o incidente de segurança.



Quando você clica em **Recuperar eventos**, os nomes do campo de evento de correlação e os valores correspondentes são preenchidos no lado esquerdo do formulário. Estes são os campos de evento de correlação ArcSight ESM que estão disponíveis para mapear para os campos de incidente de segurança.

Você pode preferir revisar alguns eventos de correlação de amostra no console para incluir na etapa de configuração de mapeamento de campo. Esta etapa é rotulada como Mapeamento na barra de andamento. Se esta página não for exibida, clique em **Mapeamento** na barra de andamento. Você pode ingerir até cinco eventos de correlação de amostra do gerenciador ArcSight ESM para a regra de correlação selecionada para ajudar no processo de mapeamento de campo. Há opções para ingerir os cinco eventos de correlação mais recentes para o Evento de Correlação selecionado ou ingerir até cinco eventos de correlação específicos com base nos IDs de evento.

Abaixo está um resumo das etapas necessárias para mapear eventos de correlação:

- Mapeamento de campo: edite a configuração de mapeamento arrastando os campos de evento de correlação do lado esquerdo e soltando-os na seção de mapeamento de incidente SIR à direita. O mapeamento à direita associa o campo de evento de correlação de entrada a um campo de incidente de segurança de saída.
- Experiência de mapeamento: personalize a grade de mapeamento adicionando ou removendo campos usando o ícone + na parte inferior da seção de mapeamento de campo de incidente SIR. Rastreie campos ignorados ou mapeados anteriormente com a codificação de cores fornecida (os campos mapeados ficam esmaecidos, os campos azuis não estão mapeados).
- Condições de geração de incidentes: depois que a seção de mapeamento estiver concluída, você poderá definir condições de filtro para filtrar quais eventos de correlação devem criar incidentes de segurança versus eventos de correlação que devem ser filtrados, por exemplo, eventos de correlação de prioridade baixa. Isso é feito na seção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condições de geração de incidentes localizada abaixo da seção Ingestão de amostra de evento de correlação.

- Critérios de agregação de eventos: defina critérios de agregação de eventos adicionais que agregam um evento de correlação de entrada a um incidente de segurança SIR existente em vez de criar incidentes semelhantes, potencialmente duplicados. Usando critérios de valor de correspondência de campo para cada perfil, essa capacidade de agregação adicional pode reduzir o número de incidentes de segurança ativos e sobrepostos, colocando todos os dados de evento notáveis de segurança relacionados em um único incidente de segurança.
- Tradução de campo de formato: em determinados casos, os valores de campo de evento no evento de correlação ArcSight ESM podem não ser traduzidos diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de script se quiser formatar valores semelhantes, mas não idênticos.

  Por exemplo, com o editor de script, um valor de categoria de Alerta de malware e Infecção de vírus pode ter valores de campo diferentes para a categoria de origem, mas ambos os valores podem ser convertidos em uma Atividade de código malicioso comum no campo Categoria no incidente de segurança SIR usando o Funcionalidade de tradução de campo de formato.

A próxima etapa é ingerir eventos de correlação de amostra e mapear valores para os campos de incidente de segurança SIR.

Criar mapeamentos para integração de ingestão de eventos ArcSight ESM

Nesta etapa, você ingere eventos de correlação de amostra e mapeia valores para os campos de incidente de segurança SIR.

Antes de Iniciar

Função necessária: admin, sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Como um usuário com a função sn_si.admin, você pode revisar até cinco eventos de correlação de amostra da coluna Ingestão de amostra de evento de correlação à esquerda do formulário para ajudar no mapeamento e na tradução de valores de campo de evento para os campos de incidente de segurança no Incidente de SIR Coluna Mapeamento de campo à direita.

Crie mapeamentos personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Os campos exibidos por padrão são normalmente campos importantes a serem preenchidos no formulário de resposta a incidentes de segurança. No entanto, esses campos podem ser removidos e quaisquer campos adicionais podem ser exibidos usando os botões + e -. Crie mapas personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Personalizar os campos permite mapear ArcSight ESM campos que não são exibidos na grade de mapeamento padrão no incidente de segurança.

Procedimento

1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Você pode extrair os eventos de correlação de amostra mais recentes para a regra de correlação selecionada ou fornecer os IDs de evento de correlação exclusivos para os eventos de correlação específicos que você deseja usar para sua experiência de mapeamento de evento de correlação.
3. Na lista suspensa, selecione um dos seguintes:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

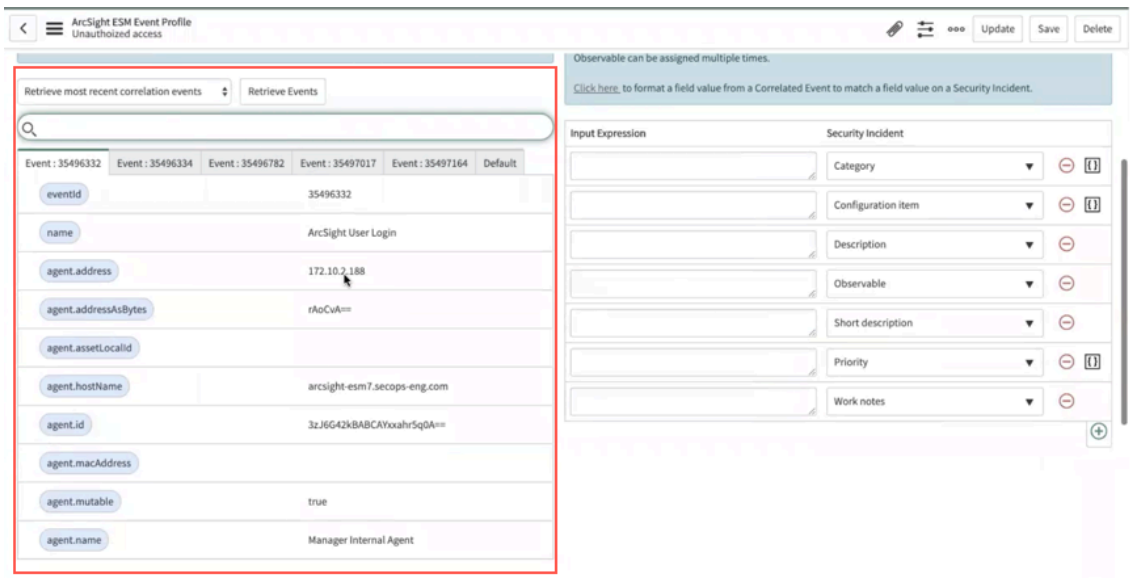
- Recuperar eventos de correlação mais recentes
- Selecionar eventos de correlação com base no ID do evento

Clique **em Recuperar eventos** para extrair os eventos de correlação de amostra mais recentes do console ArcSight ESM para a regra de pesquisa de correlação selecionada.

Os campos de evento de correlação e os resultados dos valores são exibidos como guias individuais.

A extração de eventos de correlação de amostra pode demorar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela.

Na figura a seguir, os pares de valor de nome de campo para o evento de correlação ingerido ou os eventos de amostra importados são exibidos no lado esquerdo deste formulário após a conclusão da extração de ingestão. Esses valores são os valores que você mapeia para os campos de incidente de segurança no lado do mapeamento de campo de incidente de SIR do formulário.



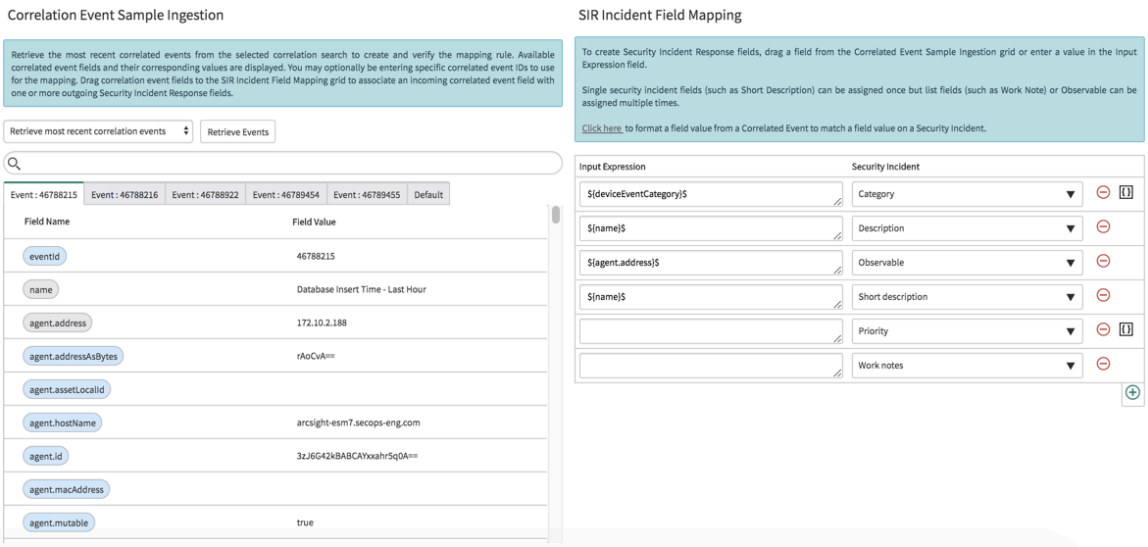
4. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e mantenha pressionado um nome de campo azul no lado esquerdo do formulário.
5. Arraste o nome do campo, por exemplo, agent.hostnamee solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.

   Para ajudar a garantir que nenhum campo de evento seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. Os campos azul claro à esquerda indicam que um campo de evento de correlação ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de correlação de entrada a mais de um campo em um incidente de segurança.

   Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação de cores ajuda a rastrear quais campos de evento já foram utilizados para futuros mapeamentos de campo de incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

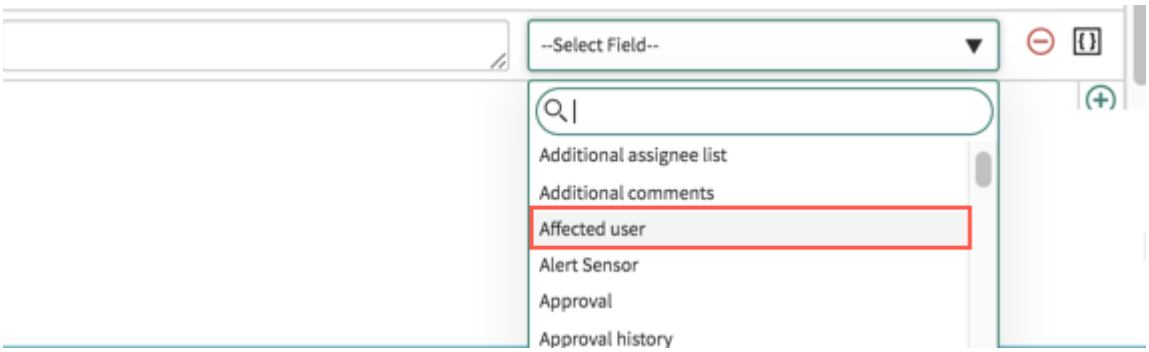


6. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas.

a. À direita do formulário na seção Mapeamento de campo de incidente de SIR, na parte inferior da grade, clique no ícone de adição.
Um novo campo é exibido.

b. Na coluna Incidente de segurança, expanda a lista de seleção exibida e selecione um campo.

Na lista de seleção expandida para o novo campo, alguns campos estão sombreados. Na figura a seguir, Usuário afetado tem um plano de fundo cinza porque foi mapeado no incidente de segurança. Semelhante à codificação de cores dos campos de eventos de correlação no lado esquerdo do formulário, essa codificação de cores para os campos de incidente de segurança à direita ajuda a rastrear os campos de incidente SIR já mapeados.



Nota:
Para que vários observáveis possam ser exibidos no mesmo incidente de segurança, o campo Observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho oferecem suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, será exibida uma mensagem de erro informando que não há nenhum valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista de seleção na qual você pode escolher várias opções e você tentar mapear uma opção para esse campo que não é exibido na lista de seleção, o campo não será preenchido no incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Como alternativa, digite um valor no campo Pesquisar da nova linha.

d. No lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar o **ID do evento** desejado no campo **Expressão de entrada**.
Com o recurso de arrastar e soltar, mapeie-o ao lado do novo campo.

7. Opcional: Abra o editor de script e continue editando.

(Optional) Para obter mais informações sobre o editor de script, consulte Use o editor de script para formatar valores de evento de correlação para integração ArcSight ESM.**Condições de filtragem de geração de incidentes**

8. Opcional: Depois de concluir as etapas de mapeamento de campo anteriores, você pode usar os mesmos valores de campo no construtor Condições de geração de incidente para definir critérios adicionais que um evento de correlação de entrada deve satisfazer para criar um incidente de segurança SIR.
Para definir condições de geração de incidentes, siga estas etapas.

a. Role até a seção Condições de geração de incidente no formulário e marque a caixa de seleção **Filtrar com base nas condições** para habilitar a opção.

(Optional) O construtor de Condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

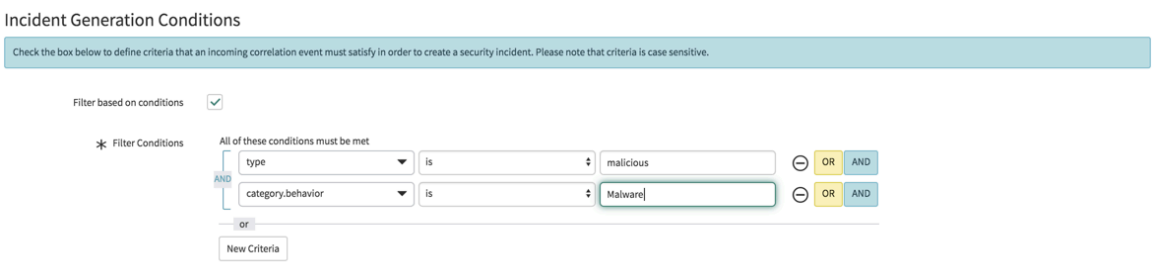
As opções nas listas de seleção para o primeiro campo no construtor de Condições de filtro correspondem aos campos exibidos na seção Ingestão de amostra de evento de correlação para os eventos que você ingeriu. Esses campos são dinâmicos e mudam dependendo dos eventos de correlação que você ingere. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas e devem corresponder exatamente aos valores do evento de correlação ArcSight ESM.

Usando as listas de seleção e os campos do construtor de condição, defina filtros para a primeira linha.

b. Para adicionar mais condições, à direita dos campos, clique em **E** ou **OU**.
Se **AND** for selecionado, todas as condições deverão ser correspondidas. Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida.

c. Opcional: Na segunda linha, defina uma segunda condição de filtro.

(Optional) A imagem a seguir é um exemplo com duas condições que devem ser correspondidas antes que os incidentes de segurança sejam criados.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

(Optional) Você definiu as condições de geração de incidentes para que os incidentes de segurança sejam criados somente quando ambas as condições de filtragem inseridas forem correspondidas.

Esse tipo de filtragem de condição de geração de incidente ajuda a restringir os eventos de segurança e limita o número de incidentes de segurança desnecessários que você cria sem modificar a pesquisa de correlação subjacente ou filtrar eventos em ArcSight ESM. Se critérios de filtragem adicionais forem definidos, somente os eventos de correlação que correspondam a todos os critérios serão mapeados para incidentes.

Nota:
Se algum dos nomes de campo de evento tiver caracteres especiais, como aspas (“), hifens ('), sublinhados (-) ou e comercial (@), talvez esses caracteres precisem ser substituídos para fins de tradução de mapeamento e possivelmente criar um evento duplicado nome. O mapeamento pode ser feito de forma apropriada, mas um sufixo numérico é anexado para diferenciar campos com nomes de evento duplicados. Por exemplo, se o primeiro campo de evento for `Events.event` e o segundo campo de evento for `Events.event`, esses campos não poderão ser identificados exclusivamente, pois os caracteres de texto padrão restantes são os mesmos. Nesse caso, um sufixo é adicionado ao segundo campo de evento e o campo é renomeado para `eventos@event(1)`.

Critérios de agregação de eventos para lidar com eventos de correlação semelhantes e evitar incidentes duplicados

9. **Opcional:** Para evitar a criação de incidentes de segurança duplicados, defina critérios de agregação de eventos adicionais para que os eventos de correlação de entrada sejam agregados a um incidente de segurança em aberto.
Para definir os critérios, siga estas etapas abaixo:

   a. Role até a seção **Critérios de agregação de evento** no formulário e marque a caixa de seleção Condições de agregação para habilitar essa opção.

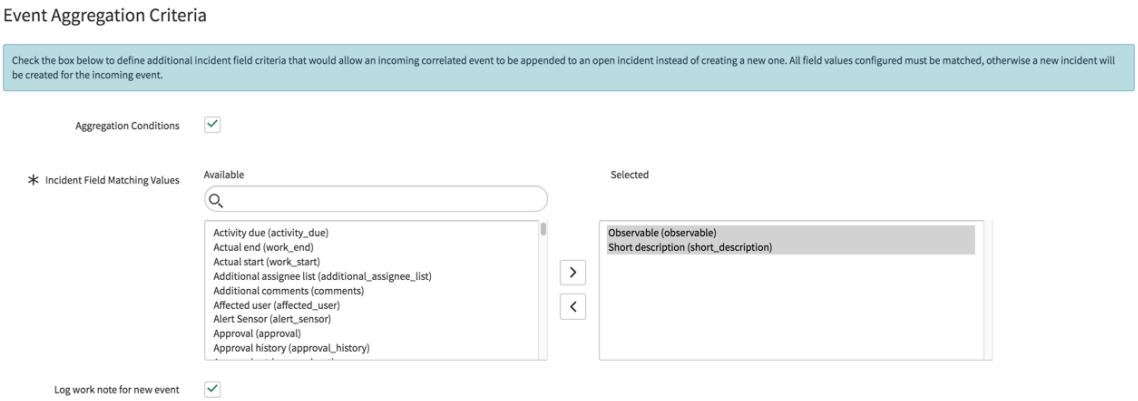
   (Optional) As colunas Valores correspondentes do campo de incidente são exibidas. Esses nomes de campo são os campos no incidente de segurança que incluem todos os campos personalizados que estão configurados no incidente de segurança SIR.

   b. Na lista Disponível, selecione os valores de campo que você deseja corresponder aos incidentes de segurança existentes no seu Now Platform e mova-os para a lista Selecionado.

   (Optional) Todos os valores de campo selecionados devem ser correspondidos para anexar este evento de correlação de entrada a um incidente de segurança existente. Isso inclui campos, como observáveis e itens de configuração, que podem ter vários valores de campo de evento de correlação mapeados para eles. Todos os valores devem corresponder. Se apenas um subconjunto dos valores for correspondido, as condições de agregação de evento não serão atendidas e um novo incidente de segurança será criado. Veja a captura de tela abaixo para mapeamento de campo de vários valores.

Tradução automática

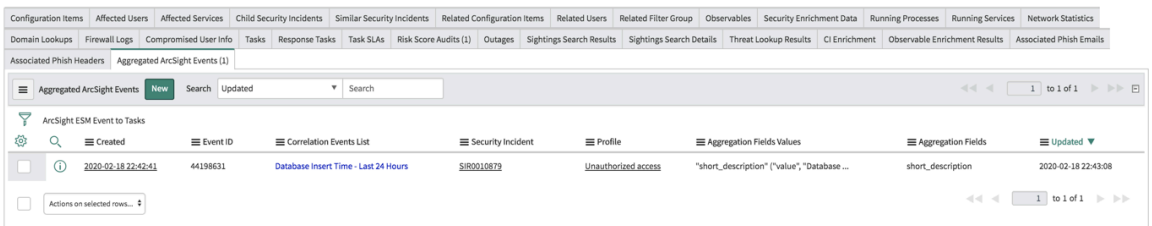
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se um novo evento de correlação corresponder a todos os valores selecionados nas condições de campo de agregação na etapa de mapeamento, o novo evento de correlação será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como analista do SOC que trabalha com incidentes de segurança, você pode exibir todos os eventos de correlação agregada adicionados em uma lista relacionada em um incidente de segurança. Todos os eventos de correlação agregados em um incidente de segurança são exibidos na lista relacionada de **eventos do ArcSight agregados**. Esta lista detalha os carimbos de data/hora associados e os valores de campos agregados. Essas informações ajudam a entender por que esses eventos de correlação estão sendo agregados a incidentes de segurança existentes. Se esta guia não for exibida, role até o lado esquerdo do registro em **Links relacionados** e clique no link **Mostrar todas as listas** relacionadas.

Nota:
Se você não vir esta lista relacionada, siga estas etapas:

- Clique com o botão direito do mouse no cabeçalho do formulário Incidente de segurança e clique em **Configurar** > **Listas relacionadas**.
- Selecione **Eventos do ArcSight agregados** na lista Disponível, mova para a lista Selecionado e clique em **Salvar**.
- Clique **em Mostrar listas relacionadas**. Agora você verá a guia **Eventos do ArcSight agregados** na seção Lista relacionada.



c. Opcional: Para registrar uma anotação de trabalho para cada vez que um evento for agregado ao incidente de segurança, marque a caixa de seleção para habilitar esta opção.
A anotação de trabalho registra que um novo evento correlacionado foi adicionado junto com um link para os detalhes do evento correlacionado.

Você mapeou com sucesso valores de um evento de correlação para campos em um incidente de segurança SIR. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem de geração de incidentes. Você também agregou eventos de correlação a incidentes de segurança SIR existentes quando os valores do campo de evento correspondem aos critérios de agregação configurados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

10. Escolha um para continuar com a configuração do perfil.

Visualizar o incidente de segurança para a integração de ingestão de eventos ArcSight ESM

Depois de concluir a etapa de mapeamento, visualize os valores mapeados em um incidente de segurança Now Platform Security Incident Response (SIR). Esta etapa de visualização permite que você verifique se mapeou todos os campos de correlação que deseja exibir no incidente de segurança.

Antes de Iniciar

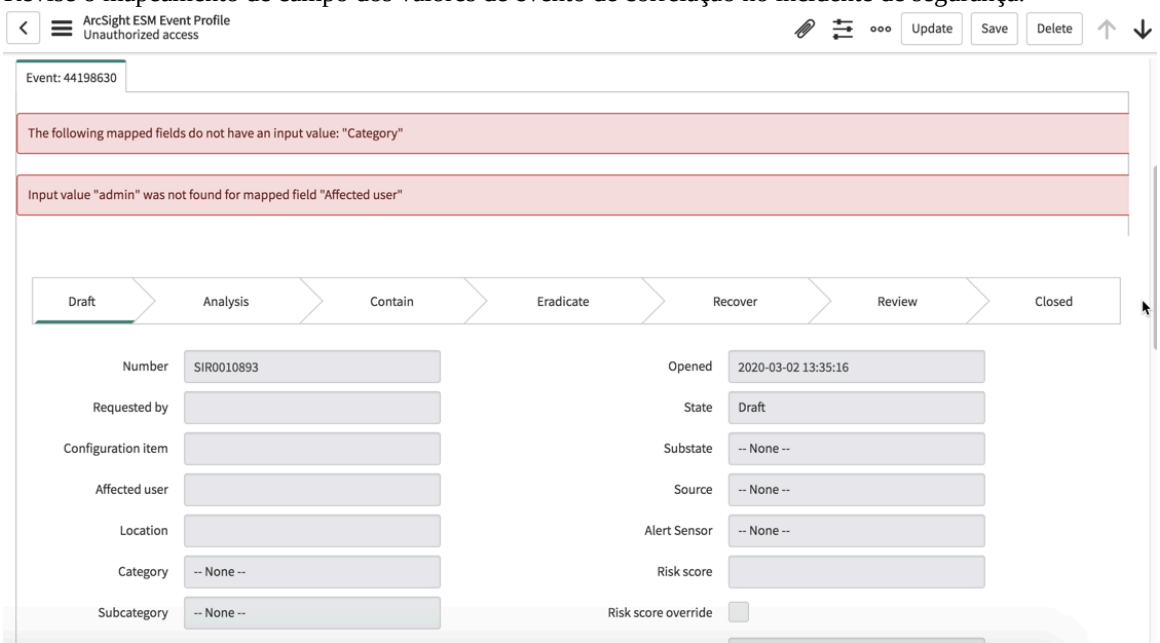
Função necessária: sn_si.admin.

Por Que e Quando Desempenhar Esta Tarefa

Como um usuário com a função sn_si.admin, visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou para preencher quaisquer dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. As visualizações de incidentes de segurança não são salvas como incidentes reais no produto Security Incident Response.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualizar** na barra de andamento.
2. Na lista de seleção IDs de evento de amostra, selecione um item.
   O incidente de segurança é exibido. Não altere nenhuma informação nos campos. Esta exibição é somente leitura e um registro deste incidente de segurança não é salvo.
3. Revise o mapeamento de campo dos valores de evento de correlação no incidente de segurança.



   A imagem anterior é um exemplo de uma visualização com um erro de mapeamento. Neste exemplo, um valor de campo do evento de correlação não tem um valor aceitável para o campo de referência no formulário de incidente SIR. Uma mensagem de erro é exibida indicando que um valor de entrada não foi encontrado para o campo Categoria, que é um campo de referência com um conjunto específico de valores. Como resultado, este valor de campo mapeado não aparecerá no formulário de incidente de segurança SIR sem modificação adicional.

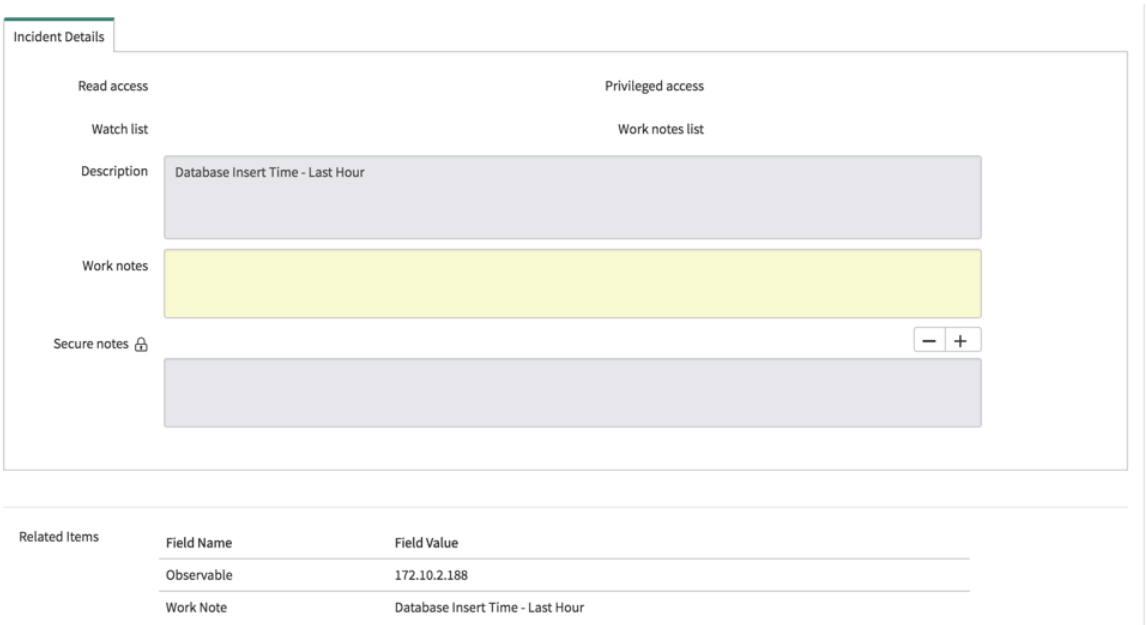
4. Para resolver esse erro, clique em **Mapeamento** na barra de andamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Edite o mapeamento para corrigir valores incorretos ou preencha os dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir os erros descritos nas mensagens de erro.

A figura a seguir é um exemplo da guia Detalhes do incidente na metade inferior de um incidente de segurança depois que todas as mensagens de erro são resolvidas. Para este exemplo, os campos Descrição e Anotações de trabalho foram mapeados e esses campos são preenchidos com os valores dos pares de valores extraídos das amostras de evento de correlação ArcSight ESM.



O que Fazer Depois

Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campo no incidente de segurança, a próxima etapa é definir a programação.

Criar uma programação para ingestão de ingestão de eventos ArcSight ESM ingestão

Você pode definir a pesquisa ou a programação de extração para novos eventos correlacionados. Durante esta etapa, você pode verificar as configurações existentes para recuperação de evento de correlação ou modificar a programação conforme necessário. Esta etapa também permite recuperar eventos de correlação históricos usando um intervalo de datas.

Antes de Iniciar

Função necessária: sn_si.admin.

Por Que e Quando Desempenhar Esta Tarefa

Você pode escolher se deseja ingerir eventos de correlação histórica durante a etapa de Programação. Você também escolhe com que frequência pesquisará novos eventos de correlação futuros que correspondam à configuração do perfil.

Como um usuário com a função sn_si.admin, você configura esses intervalos de pesquisa por perfil. O desempenho da integração de ingestão de evento de correlação ArcSight ESM pode ser afetado pelos diferentes intervalos de pesquisa. Ao programar, talvez você prefira equilibrar a redução da sobrecarga de pesquisa no servidor ArcSight ESM com o desejo de ser notificado o mais rápido possível quando um evento for criado ou atualizado. Um valor padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração para um minuto, se necessário.

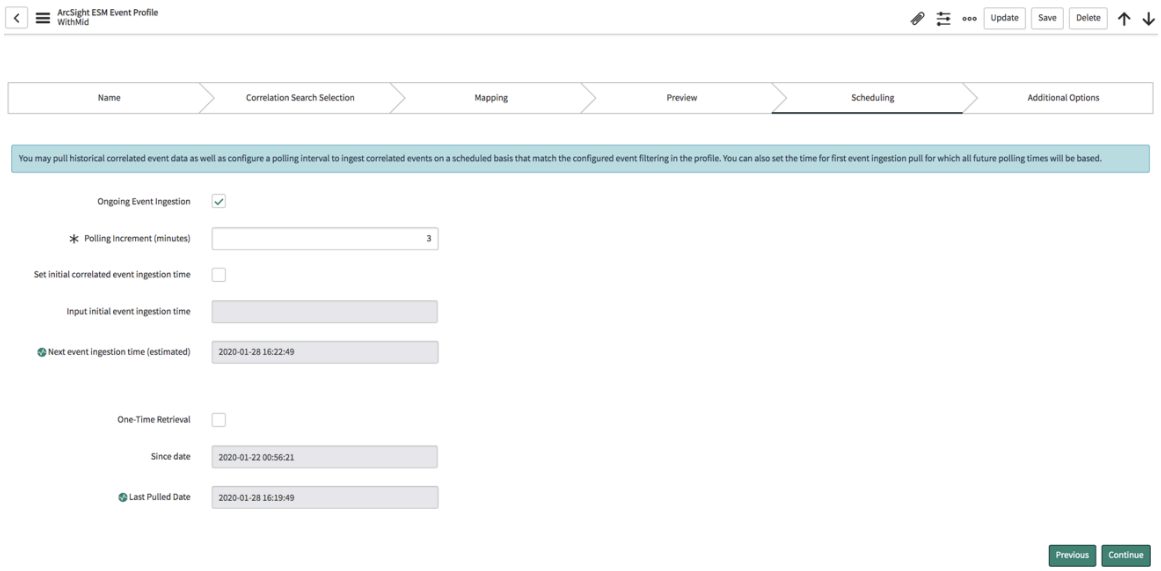
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Extraindo eventos de correlação novos e atualizados

Procedimento

1. Se a página Programação na barra de andamento não for exibida, selecione **Programação**.
2. Escolha um para programar como e quando os eventos de correlação são extraídos do<ArcSight> console.



Como exemplo para programar um tempo de ingestão de evento de correlação inicial, se você tiver uma verificação de segurança diária ArcSight ESM que é executada uma vez por dia às 4h no horário local, é possível configurar o perfil de evento de correlação correspondente em sua instância Now Platform para ser executado às 4 :05 hora local para capturar o evento de falha de segurança imediatamente e criar um incidente de segurança. Insira `04 05 00` no campo Ingestão de evento inicial. No campo Incrementar (minutos), insira `1440` (24 horas) para programar a próxima ingestão de evento por 24 horas a partir da ingestão de evento inicial. O tempo de ingestão do evento inicial e o tempo de ingestão do próximo evento são exibidos nos campos.

3. Para definir as configurações deste exemplo, siga estas etapas.

   a. Com a página Programação exibida, marque a caixa de seleção **Ingestão de evento em andamento** para habilitar esta opção.

   b. No campo Incrementar (minutos), insira `1440` (24 horas).

   c. Clique na caixa de seleção **Definir tempo de ingestão de evento correlacionado inicial** para habilitar a edição dos campos Ingestão de evento inicial e Próxima ingestão de evento.

   d. No campo Tempo de ingestão de evento inicial, insira `04 05 00`.
   No campo Tempo de ingestão do próximo evento (estimado), a hora da próxima ingestão de evento é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Continuar** para navegar até a página Opções adicionais.

> **Nota:**
> O número padrão de incidentes de segurança que podem ser criados e agregados em um dia e o período de fluxo são definidos nas ArcSight ESM Configurações de integração. Você pode modificar essas configurações, se necessário. Consulte ArcSight ESM Configurações de integração para integração de ingestão de eventos para mais detalhes.

Opções adicionais: automatizar atualizações de eventos correlacionados e fechamento com base no SIR status do incidente

A integração ArcSight ESM tem uma interface bidirecional que permite que ambos os eventos de correlação criem incidentes de segurança, bem como a capacidade de atualizar os eventos de correlação depois que o incidente de segurança é criado e/ou encerrado com detalhes relevantes do incidente, como o número do incidente de segurança , grupo de atribuição, SIR URL de incidente e assim por diante.

Antes de Iniciar
Função necessária: sn_si.admin

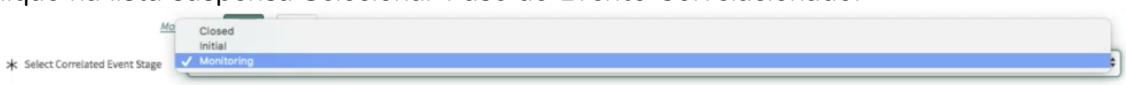
Procedimento

1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais**.
2. Siga as instruções abaixo para concluir a configuração para atualizar eventos correlacionados quando o incidente de segurança for criado.

   Fase de evento correlata não configurada: se você não configurou nenhuma fase de evento correlata na sua instância Now Platform, verá somente **Atribuir fase - Configuração inicial** na lista de seleção Atualização de fase de evento correlata. Para configurar a fase, siga estas etapas:

   - Insira um ID de recurso no campo Inserir ID de recurso de fase e clique em **Enviar**. O ID do recurso é validado no console ArcSight ESM e a tela a seguir é exibida.

   - Clique em **Salvar** para salvar a nova fase (**Monitoramento**).
   - Clique na lista suspensa Selecionar Fase de Evento Correlacionado.



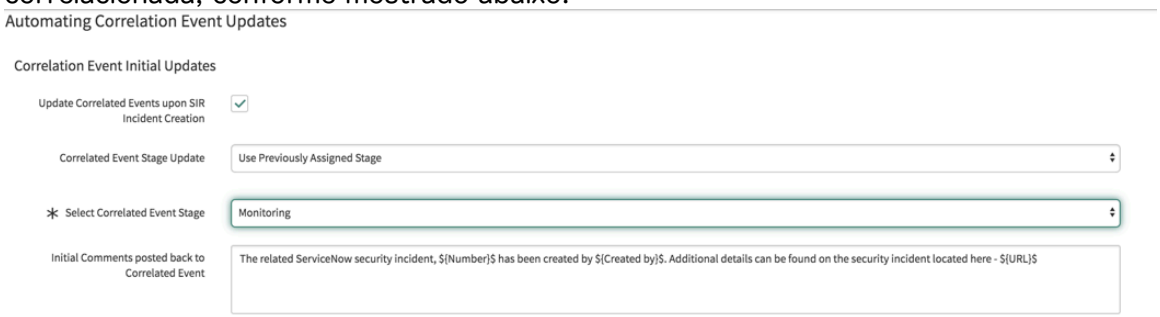
   - Você pode selecionar a fase recém-criada na lista.

   Fase de evento correlata já configurada: se você já configurou a fase de evento correlata, siga estas etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Selecione **Usar fase atribuída anteriormente** na lista de seleção Atualização de fase de evento correlata.
- Selecione uma fase existente na lista de seleção Selecionar fase de evento correlacionada, conforme mostrado abaixo.

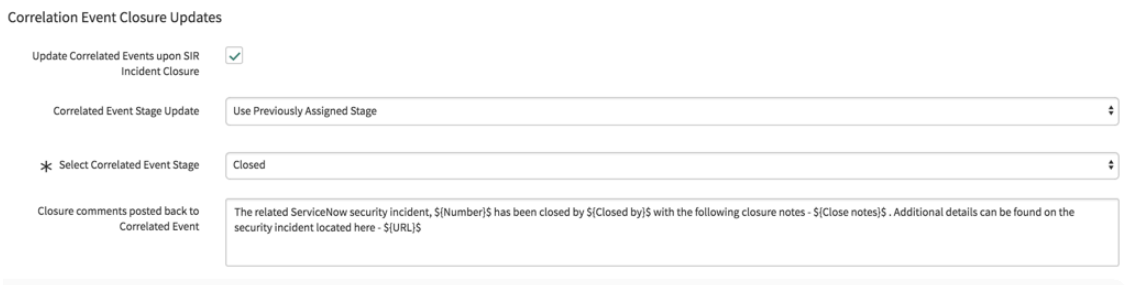


- Comentários iniciais publicados no evento correlacionado: além de atualizar o valor da fase do evento de correlação, você também pode publicar comentários nas anotações da fase de correlação. Conforme indicado nas instruções, você pode editar o texto padrão exibido na seção de comentários, incluindo a adição ou modificação das variáveis de substituição usando o formato ${field name}$ para qualquer campo no formulário de incidente do Security Incident Response.

Nota:
Você pode usar as fases padrão definidas no console ArcSight ESM ou criar suas próprias fases personalizadas. Para criar uma nova fase, siga estas etapas:

- No console ArcSight ESM, selecione **Arquivo** > **Novo** > **Fase**. A guia Inspecionar/editar é exibida.
- Defina a nova fase e não marque a caixa de seleção **Usuário obrigatório**. Certifique-se de que a fase esteja definida corretamente e na posição correta no ciclo de vida do evento.

3. Na seção Automatizando fechamento de evento correlacionado, você pode definir como atualizar o incidente de segurança quando ele é fechado.
4. No formulário, preencha os campos.



5. Clique em **Concluir** para concluir a configuração.
Uma caixa de diálogo de confirmação é exibida. Você concluiu com êxito a instalação e a configuração da integração. Ative este perfil para extrair eventos de correlação do console ArcSight ESM com base em sua programação.

ArcSight ESM Configurações de integração para integração de ingestão de eventos

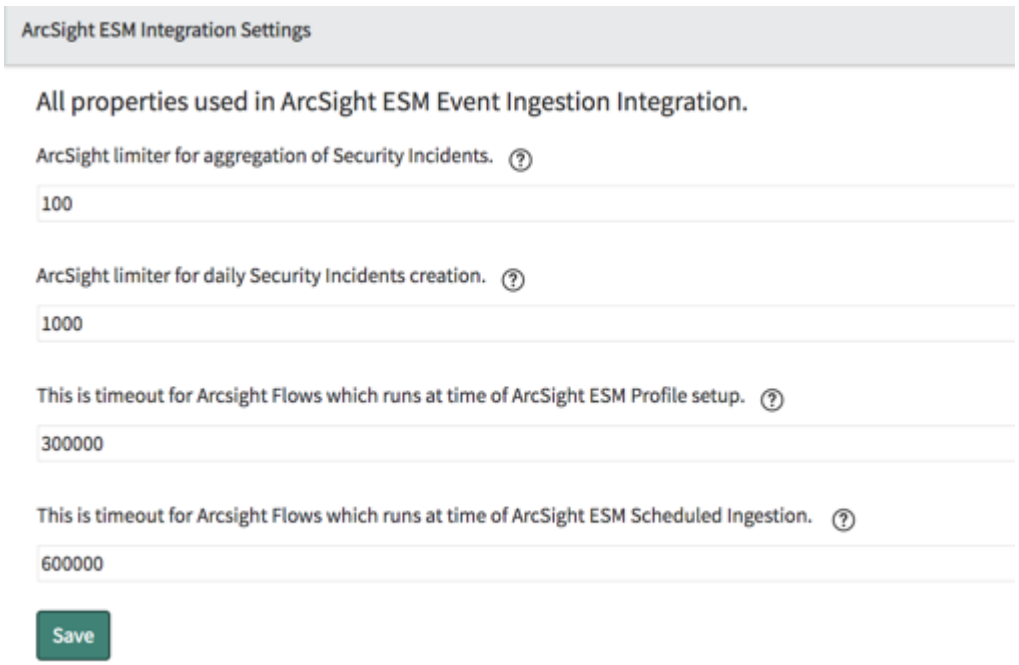
Use esta opção para modificar as ArcSight ESM configurações de ingestão padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para modificar as propriedades do sistema, faça login como um usuário com a função *sn_si.admin* e navegue até **Integração de ESM do ArcSight** > **Configurações de integração do ArcSight ESM**.

As definições de configuração padrão são exibidas. Você pode modificar essas configurações, se necessário.

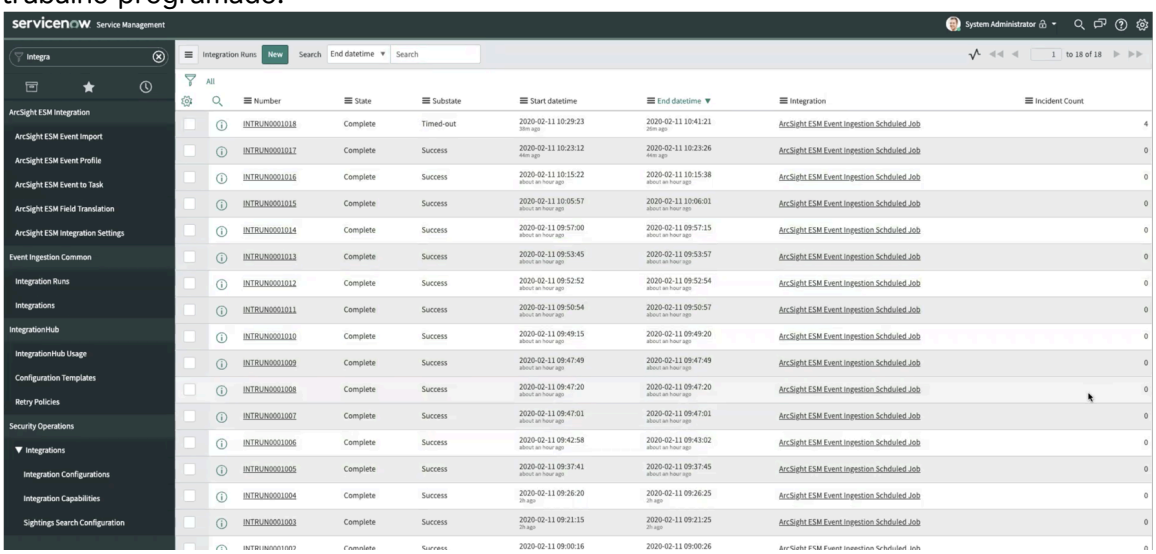


Solução de problemas da integração de ingestão de eventos ArcSight ESM

Esta seção fornece informações sobre como solucionar problemas de erros que podem ocorrer durante a ingestão de eventos.

Execuções de integração

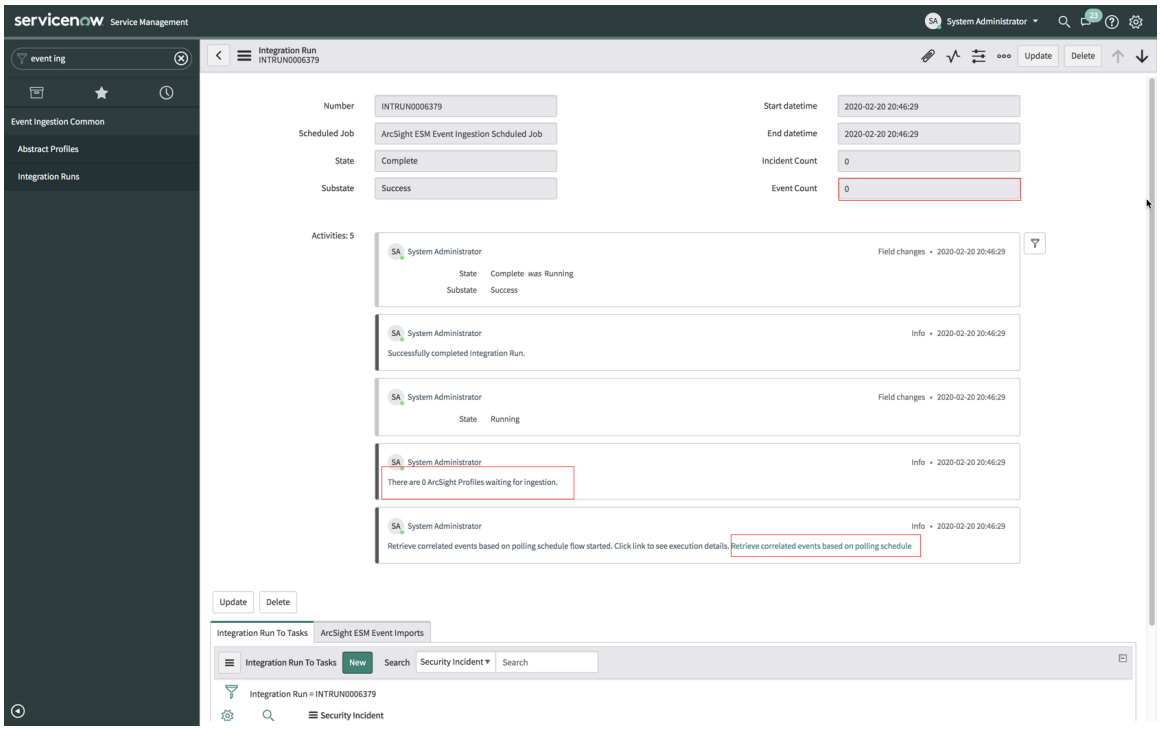
Navegar até **Ingestão de evento comum** > **Execuções de Integração**. Uma execução de integração ocorre a cada minuto e captura detalhes sobre os eventos ingeridos durante o trabalho programado.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode ver a lista de execuções de integração e o status de cada execução (Êxito, Tempo esgotado, Aguardando) e o número de incidentes de segurança que foram criados. Clique no link Número para expandir a página Execução de integração detalhada.



Você pode exibir detalhes como o número de eventos que foram ingeridos, o status, qual evento foi transformado em um incidente de segurança e as diferentes tarefas realizadas durante a ingestão. Além disso, você pode clicar no link para exibir os detalhes da execução do fluxo.

Detalhes do fluxo de execução

Clique no link de detalhes da execução para ver o fluxo associado à ingestão de eventos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode exibir uma execução passo a passo do fluxo detalhando as várias ações e subfluxos que foram executados como parte do fluxo.

Copiar perfil ArcSight ESM para integração de ingestão de eventos

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, convém copiar os perfis para economizar tempo.

Antes de Iniciar

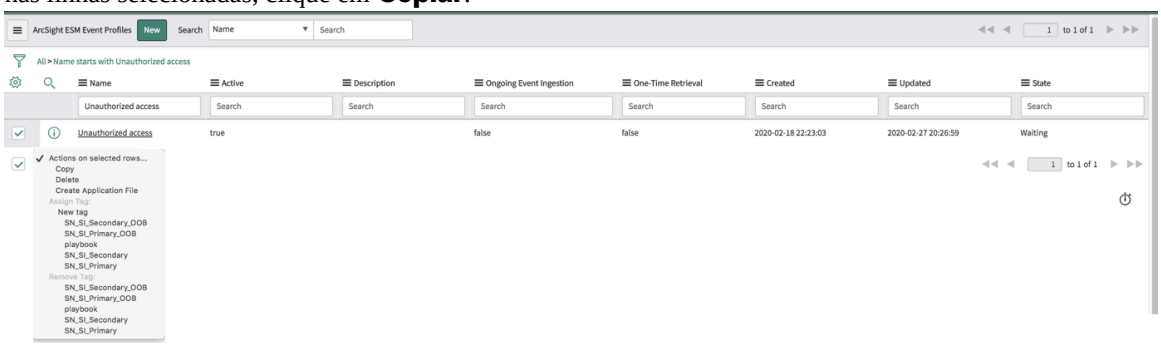
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

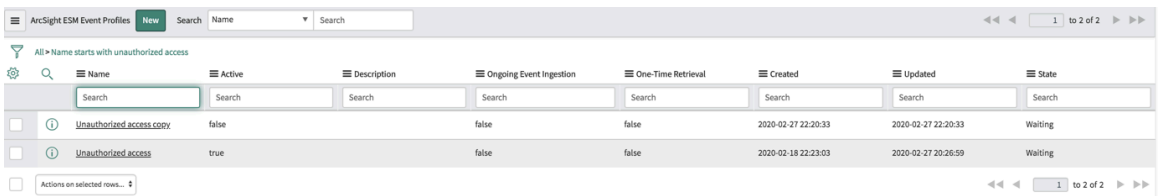
Como um usuário com a função sn_si.admin, se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado está desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Procedimento

1. Navegar até **Todos** > **Integração de ESM do ArcSight** > **Perfil de evento do ArcSight ESM**.
2. Na lista Perfis do ArcSight exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Copiar**.



O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo o mapeamento e a configuração de programação. O nome do perfil contém cópia. Embora o perfil original esteja habilitado (verdadeiro), a cópia está desabilitada neste ponto (falso). Você pode editar os valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil, conforme necessário.



Você copiou com sucesso as configurações de um perfil existente para um novo perfil. Observe que o status da coluna **Ativa** está definido como falso, pois o perfil precisa ser ativado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use o editor de script para formatar valores de evento de correlação para integração ArcSight ESM

Além dos campos mapeados diretamente dos valores de evento de correlação ingeridos, use o editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

O editor de script muda os valores de um campo de evento de correlação ArcSight ESM para que os valores compatíveis com o incidente de segurança Now Platform SIR sejam mapeados para a Categoria, Item de configuração (IC), Observável e outros campos de incidente de segurança.

Em determinados casos, os valores de evento de correlação ArcSight ESM são mapeados para campos de referência, como Categoria, Item de configuração (IC) e campos Observável no incidente de segurança. Como um usuário com a função sn_si.admin, talvez você prefira editar os valores de campo de evento mapeados para traduzir o formato ou os valores de dados para conformidade com os formatos de campo de incidente e valores esperados. Se você quiser traduzir o valor de um evento de correlação ArcSight ESM para um valor que seja compatível com esses campos no incidente de segurança SIR, use o editor de script.

Procedimento

1. Com o formulário de mapeamento exibido, clique no link para abrir o editor de script.
2. Na lista de seleção, selecione um campo de destino para o valor que você deseja editar.
3. Como alternativa, na seção Mapeamento de campo de incidente de SIR, clique no ícone de colchete [{}] ao lado de um campo para abrir o editor de script desse campo.

   Em determinadas instâncias, uma inclusão de script pode ser apropriada para o campo Item de configuração. Para um evento de correlação, por exemplo, um valor para o Item de configuração pode não ser correspondido.

   Conforme mostrado na figura a seguir, se uma correspondência para um nome de host não puder ser encontrada no Now Platform CMDB para o campo Item de configuração, você poderá editar a regra para que, se um endereço IP for encontrado, ele preencha o campo Item de configuração.

   O editor é aberto com o campo exibido no Campo de destino.
4. Insira as mudanças no script e clique em **Atualizar** para salvar as mudanças.
   A tabela ArcSight ESM Traduções de campo é exibida.
5. Feche a tabela para retornar ao formulário de mapeamento.

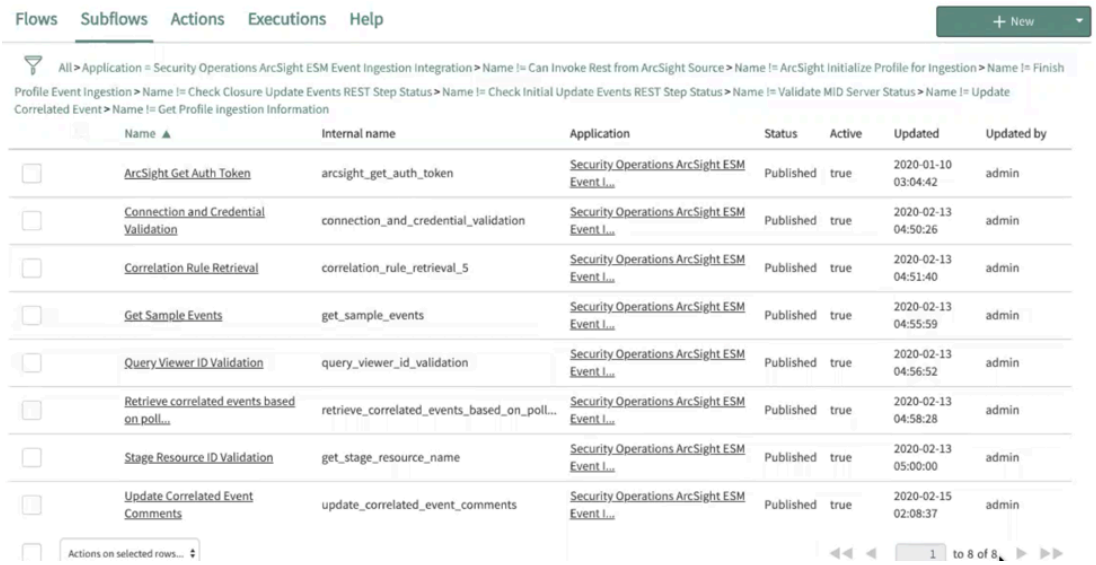
Uso do Flow Designer com integração de ingestão de eventos ArcSight ESM

Usando o Integration Hub e o Flow Designer, vários fluxos, subfluxos e ações estão disponíveis com a integração ArcSight ESM.

Para exibir esses subfluxos, navegue até **Flow Designer** > **Designer** e clique na guia **Subfluxos**. A figura abaixo mostra os subfluxos importantes usados durante a criação do perfil e o trabalho de ingestão programado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



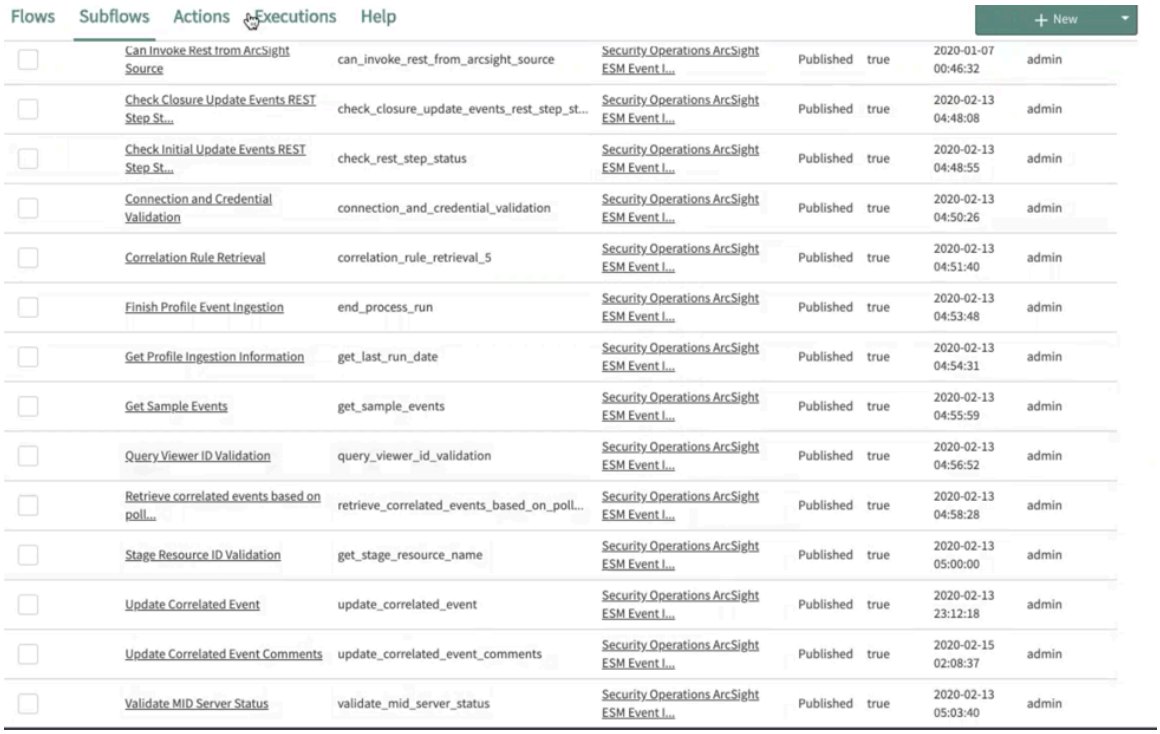
Esses subfluxos são listados na sequência em que são executados abaixo:

- **Validação de conexão e credencial**: este subfluxo valida a conectividade ServiceNow com o servidor ArcSight ESM e as credenciais especificadas. Este subfluxo é usado quando você clica no botão **Configurar** no bloco **ArcSight ESM - Ingestão de eventos**no **Security Operations** > **Integrações** > **Configuração de integrações** página.
- **Obter token de autenticação do ArcSight**: este subfluxo gera o token de autenticação ArcSight ESM do nome de usuário e senha usando o serviço de login ArcSight ESM. O serviço de login fornece o token de autenticação que pode ser usado para chamar qualquer outro endpoint ArcSight ESM. Este subfluxo é usado em todos os outros subfluxos.
- **Validação de ID do visualizador de consulta**: este subfluxo verifica se o ID do visualizador de consulta especificado durante a criação do perfil está presente no servidor ArcSight ESM.
- **Recuperação de regra de correlação**: este subfluxo recupera as regras de correlação com base no ID do visualizador de consulta.
- **Obter evento de amostra**: este subfluxo busca os eventos de correlação de amostra do servidor ArcSight ESM. Esses eventos de amostra são mapeados para os campos de incidente de segurança na seção Mapeamento do perfil.
- **Validação do ID do recurso da fase**: este subfluxo valida o ID do recurso da fase especificado no console ArcSight ESM e busca o nome do recurso.
- **Atualizar comentários do evento correlacionado**: este subfluxo atualiza os comentários do evento correlacionado nas seções Inicial e Fechamento do incidente na página Opções adicionais do perfil.
- **Recuperar eventos correlacionados com base na programação de pesquisa**: este subfluxo executa o trabalho programado que busca os eventos correlacionados com base no intervalo de pesquisa.

Durante a execução, os subfluxos acima também acionam vários outros subfluxos e ações, direta ou indiretamente, conforme mostrado abaixo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Can Invoke Rest from ArcSight Source	can_invoke_rest_from_arcsight_source	Security Operations ArcSight ESM Event I...	Published	true	2020-01-07 00:46:32	admin
Check Closure Update Events REST Step St...	check_closure_update_events_rest_step_st...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:08	admin
Check Initial Update Events REST Step St...	check_rest_step_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:55	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:50:26	admin
Correlation Rule Retrieval	correlation_rule_retrieval_5	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:51:40	admin
Finish Profile Event Ingestion	end_process_run	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:53:48	admin
Get Profile Ingestion Information	get_last_run_date	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:54:31	admin
Get Sample Events	get_sample_events	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:55:59	admin
Query Viewer ID Validation	query_viewer_id_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:56:52	admin
Retrieve correlated events based on poll...	retrieve_correlated_events_based_on_poll...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:58:28	admin
Stage Resource ID Validation	get_stage_resource_name	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:00:00	admin
Update Correlated Event	update_correlated_event	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 23:12:18	admin
Update Correlated Event Comments	update_correlated_event_comments	Security Operations ArcSight ESM Event I...	Published	true	2020-02-15 02:08:37	admin
Validate MID Server Status	validate_mid_server_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:03:40	admin

Carbon Black - Integração de aprimoramento de incidente

Use a integração Carbon Black para investigar e responder a incidentes de segurança usando APIs para consultar e interagir com endpoints associados a incidentes de segurança.

Localizar recursos de integração do Carbon Black - Incidente Aprimoramento

- Introdução ao Carbon Black - Integração de aprimoramento de incidente
- Fluxo de trabalho do Security Operations Carbon Black Integration - Obter processos em execução
- Security Operations Carbon Black Integration - Isolar fluxo de trabalho de host
- Fluxo de trabalho Security Operations Carbon Black Integration - Remover isolamento de host
-

Entenda os conceitos de integração

- Tipos de ServiceNow integrações fornecidas
- Security Operations gatilhos de fluxo de trabalho

Obtenha ajuda de recursos ServiceNow

- Faça ou responda perguntas na comunidade do Security Operations
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente
- Fazer upgrade para Madri

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Introdução ao Carbon Black - Integração de aprimoramento de incidente

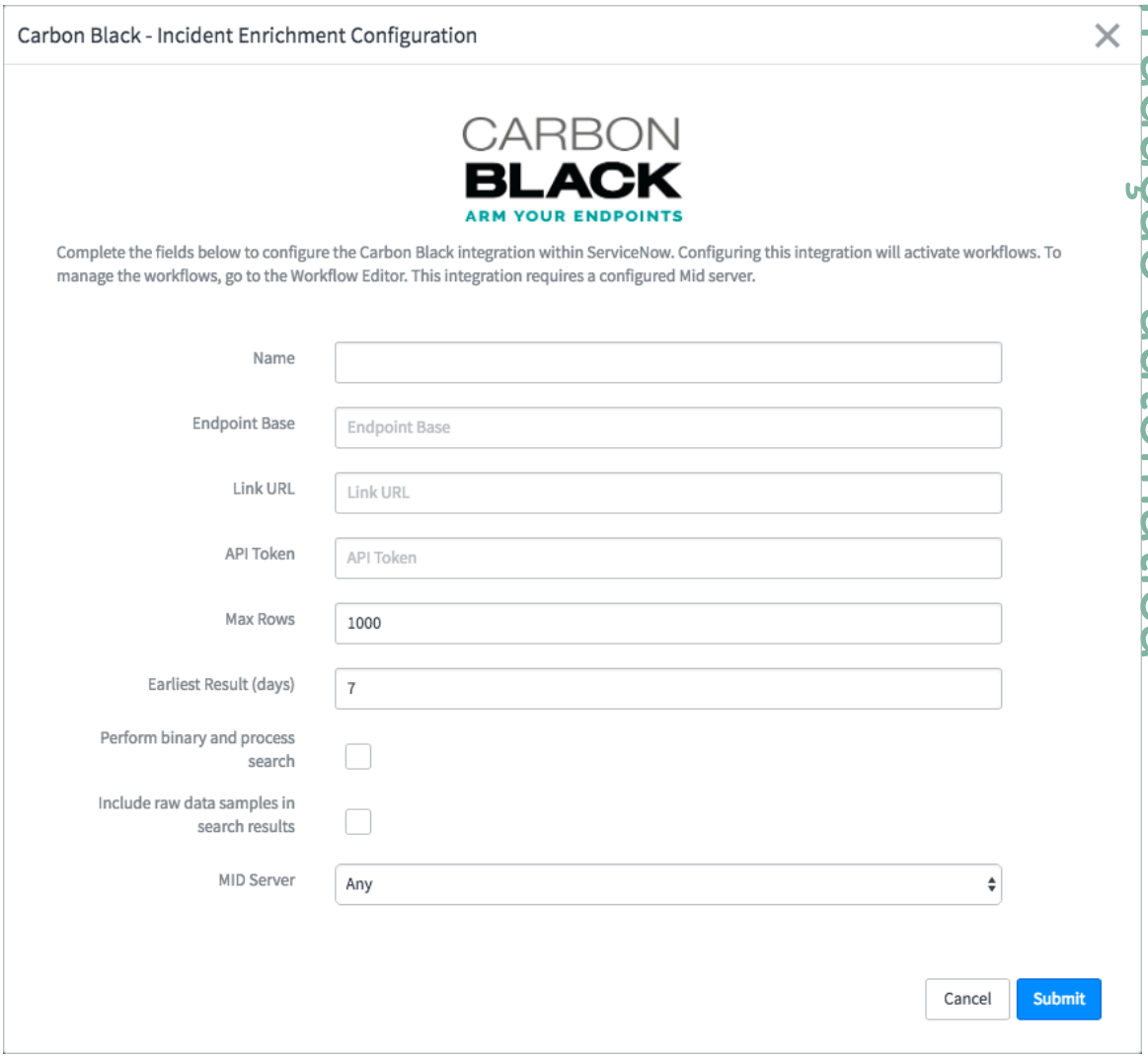
O aprimoramento de incidente do Carbon Black facilita a investigação de um incidente de segurança, consultando os logs em busca de indicadores potencialmente maliciosos. Antes de usar a integração Carbon Black - Incident Enrichment, você deve baixá-lo do ServiceNow Store e adicionar o URL base do endpoint e o MID Server apropriados.

Antes de Iniciar

Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando o download estiver concluído, acesse o site Carbon Black e obtenha o URL base do endpoint e o Token de API no seu perfil.
3. Em sua instância, navegue até **Security Operations** > **Integrações** > **Configuração de Integração**.
4. No cartão Carbon Black - Aprimoramento de incidente, clique em **Configurar**.



5. Preencha os campos, conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	O nome desta configuração.
Base do endpoint	O URL do endpoint que você adquiriu no site do Carbon Black.
URL do Link	A URL do link que vincula a uma instância do Carbon Black, quando disponível.
Token de API	O token de API que você adquiriu no site Carbon Black.
Máx. de Linhas	O número máximo de linhas que você deseja pesquisar. O padrão é 1000 linhas.
Resultado Mais Antigo (dias)	Os resultados mais antigos que você deseja ver em número de dias.
Executar pesquisa binária e de processo	Selecione esta opção para executar pesquisas binárias para encontrar arquivos binários, como hashes de arquivo, e pesquisas de processo para processos .exe que podem ter sido executados.
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados da pesquisa de detecções. A quantidade de dados retornados depende da configuração na propriedade do **número de linhas de dados brutos** nas propriedades do Security Incident Response.
MID Server	Selecione **Qualquer** para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota:
Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho.

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Integração do Carbon Black

A integração Carbon Black permite que você investigue e responda a incidentes de segurança usando APIs para consultar e interagir com endpoints associados a incidentes de segurança.

Explorar

- Integrações do Security Incident Response
- Carbon Black - Integração de aprimoramento de incidente

Configurar

Introdução à integração do Carbon Black

Usar

- Security Operations gatilhos de fluxo de trabalho
- Exibir itens afetados por um incidente de segurança

Desenvolver

- ServiceNow Security Operations diretrizes de desenvolvimento de integração
- Dicas para escrever integrações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Security Operations - Obter fluxo de trabalho de processos em execução
- Fluxo de trabalho do Security Operations Carbon Black Integration - Obter processos em execução
- Exibir itens afetados por um incidente de segurança
- Executar bloqueio de solicitação
- Integração do Security Operations - Fluxo de trabalho de solicitação de bloqueio
- Executar Isolar Host
- Security Operations Carbon Black Integration - Isolar fluxo de trabalho de host
- Fluxo de trabalho Security Operations Carbon Black Integration - Remover isolamento de host

- Desenvolver treinamento
- Desenvolver documentação
- Localizar componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Faça ou responda perguntas na comunidade do Security Operations
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Introdução à integração do Carbon Black

Carbon Black é um sistema de segurança avançado que se integra facilmente com Security Operations. Antes de usar a integração Carbon Black, você deve baixar a integração do ServiceNow Store e adicionar a Base de endpoint apropriada e o Token de API.

Antes de Iniciar

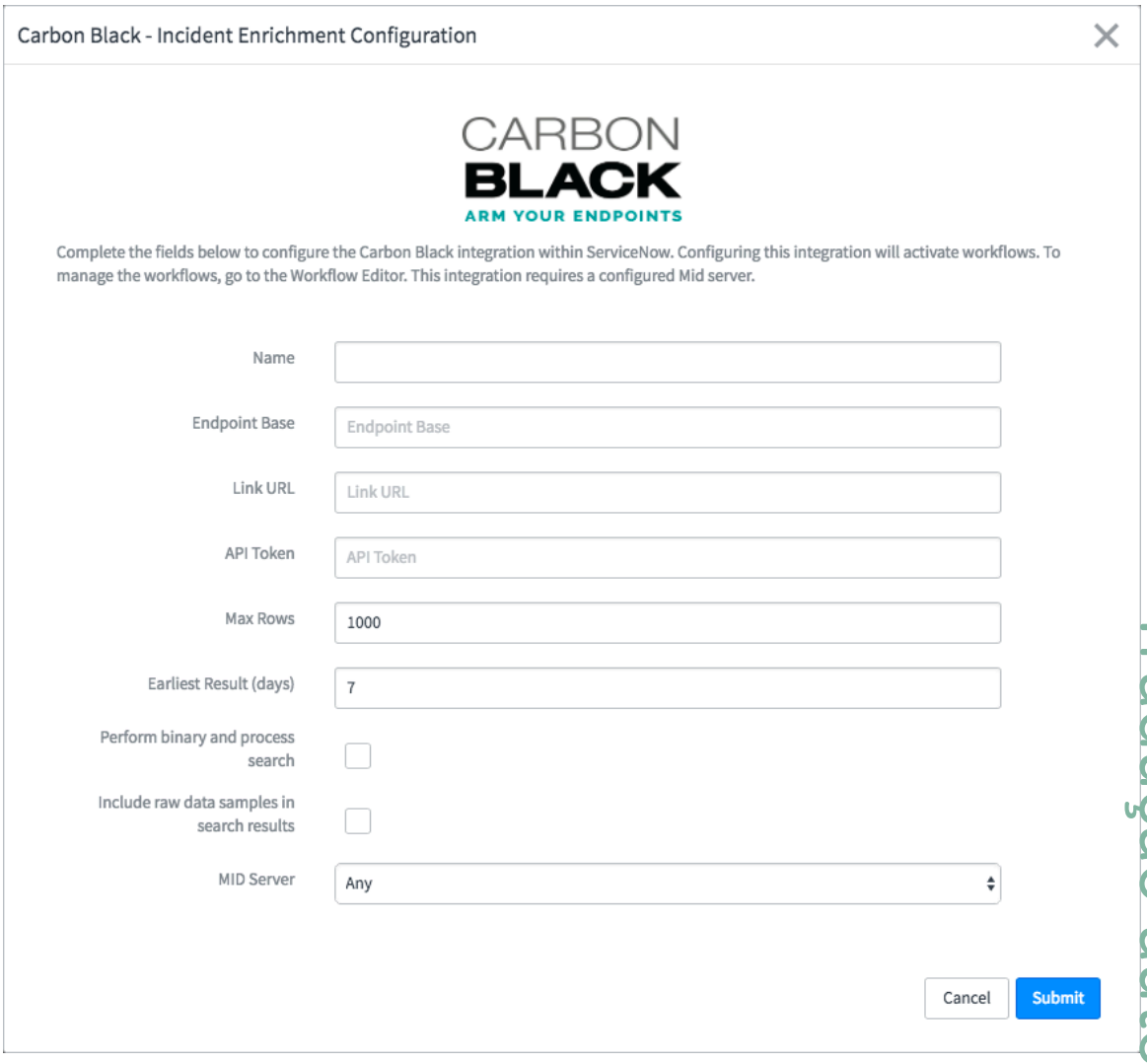
Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse o site Carbon Black e obtenha o URL base do endpoint e o Token de API no seu perfil.
3. Em sua instância, navegue até **Security Operations** > **Integrações** > **Configurações de Integração**. As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão Carbon Black, clique em **Novo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
Base do endpoint	A base de endpoint que você adquiriu no site do Carbon Black.
Token de API	O token de API que você adquiriu no site Carbon Black.
Usar MID Server	Marque esta caixa de seleção se ela ainda não estiver marcada.
MID Server	Selecione **Qualquer** para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.
Ativar Isolar Host	Marque esta caixa de seleção para permitir que os itens de configuração selecionados sejam isolados da guia da lista relacionada **Itens de configuração** em um incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho.

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Antibot Check Point - Integração do analisador de e-mails

Anti-bot Check Point - A integração do analisador de e-mail é compatível com um analisador de e-mail que consome notificações por e-mail do Anti-bot Check Point para criar incidentes de segurança e gerar fluxos de trabalho de aprimoramento e resposta.

Configurar a integração do analisador de e-mails do Antibot Check Point

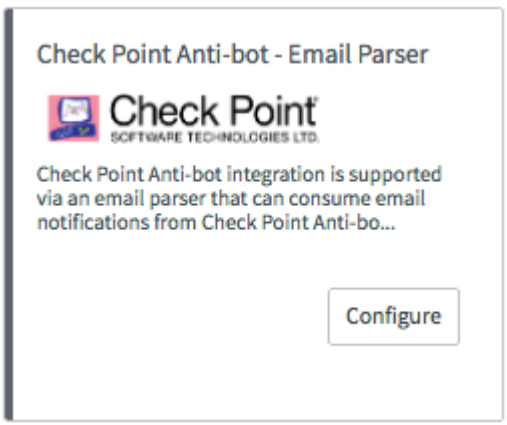
A integração do analisador de e-mail anti-bot Check Point usa notificações por e-mail para direcionar fluxos de trabalho de aprimoramento e de resposta.

Antes de Iniciar
Função necessária: sn_si_admin

Por Que e Quando Desempenhar Esta Tarefa
Um modelo de analisador de e-mail anti-bot Check Point é fornecido para uso na integração. Ele deve ser configurado e ativado antes que a integração ocorra. Atualizar o analisador o ativa.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.



2. No cartão Analisador de e-mail antibot Check Point, clique em **Configurar**.
3. Na caixa de diálogo **Configuração do analisador de e-mail do Antibot Check Point**, clique no link **Configurar analisador de e-mail**.
4. Clique no link **Anti-bot Check Point** para editar as configurações no analisador de e-mail do modelo fornecido.
   Preencha pelo menos o campo O e-mail é de. Para criar um analisador de e-mail, consulte Criar analisadores de e-mail no Security Operations.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Marque a caixa **Ativa**.
6. Clique em **Atualizar** no formulário **Analisador de e-mail**.
   O analisador de e-mail está ativo. Você não precisa retornar para **Configurações de integração**.

Integração de Check Point Next Generation Threat Prevention

Este documento descreve as etapas necessárias para integrar os recursos de Prevenção de ameaças de última geração (NGTP) do Check Point com ServiceNow® Security Incident Response (SIR) para que as aplicações funcionem corretamente juntas.

Depois de instalado e configurado, o analista de incidentes de segurança usa essa integração para bloquear endereços IP mal-intencionados, URLs e domínios usando os recursos da Lista de solicitações de bloqueio com os produtos ServiceNow Security Incident Response (SIR). Esta Lista de Solicitações de Bloqueio está configurada nos Gateways do Check Point como um Feed de Inteligência Personalizado. O recurso Feeds de inteligência personalizados fornece a capacidade de adicionar feeds de inteligência cibernética personalizados ao mecanismo de prevenção de ameaças de última geração. Ele permite a busca de feeds de um servidor de terceiros, neste caso, a aplicação ServiceNow Security Incident Response, diretamente para o gateway de última geração do Check Point a ser aplicado pelos blades Antivírus e Antibot. O analista de resposta a incidentes de segurança cria entradas para a Lista de bloqueios do Check Point a partir de observáveis determinados como mal-intencionados em ServiceNow incidentes de segurança SIR.

Para a maioria das implementações, uma Lista de Solicitações de Bloqueio é um arquivo csv que está hospedado em um servidor Web externo. Para esta integração, este servidor web é sua instância da Now Platform, o que permite que o mecanismo de prevenção de ameaças de última geração do Check Point busque a lista de endereços IP, URLs e domínios a serem bloqueados.

Para impor os observáveis de bloqueio no gateway do Check Point, certifique-se de que a política de prevenção de ameaças esteja configurada com os blades antibot e antivírus ativados. Conforme as entradas da Lista de bloqueios são modificadas, o Mecanismo de prevenção de ameaças importa dinamicamente a lista no intervalo configurado e aplica a política sem uma mudança de configuração ou uma confirmação no firewall. Para esta integração, a Now Platform criou uma tabela contendo entradas da Lista de Bloqueios que são recuperadas pelo Gateway de última geração do Check Point autorizado nos intervalos de recuperação configurados.

A integração inclui os seguintes recursos:

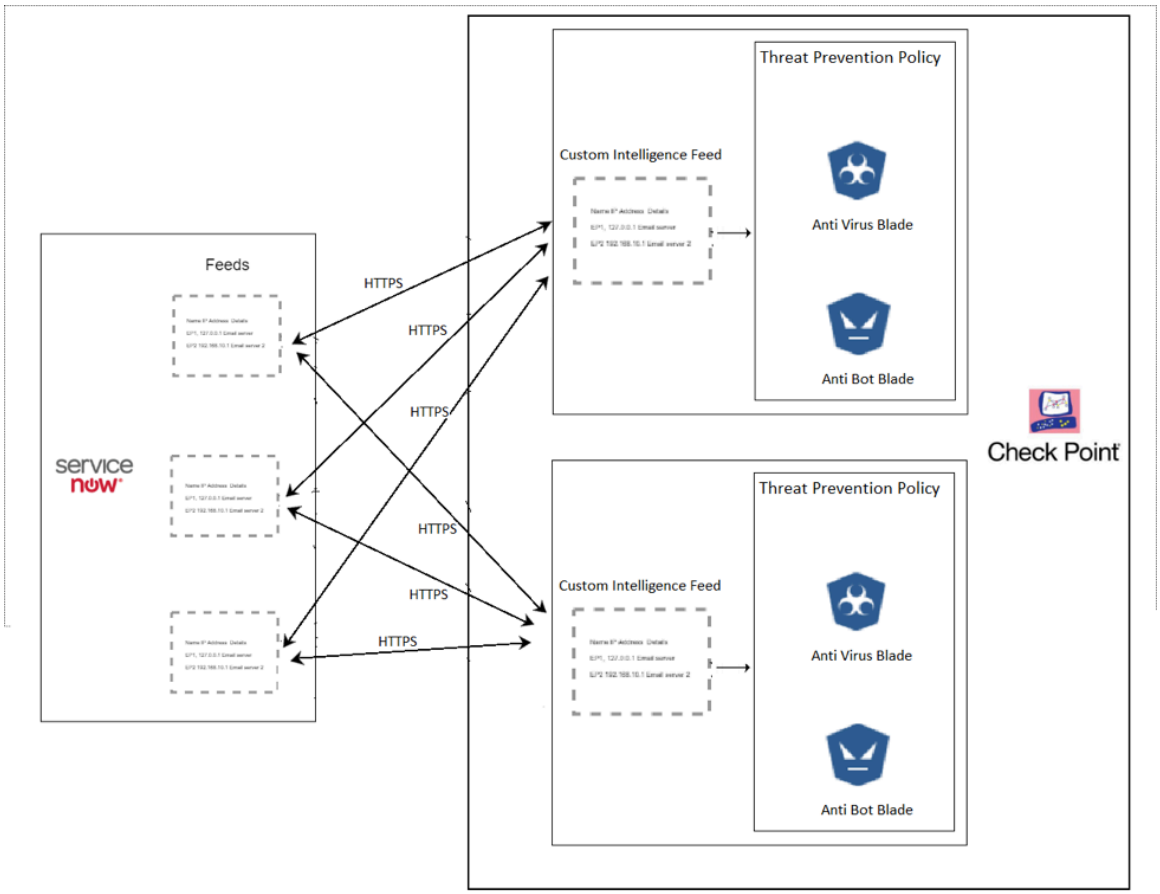
- Flexibilidade para criar várias Listas de bloqueio que se aplicam a vários Check Point Gateways.
- Relatórios detalhados sobre os tipos de sites que estão sendo bloqueados (phishing, malware e sites permitidos listados).
- Marcação de incidentes de segurança da Now Platform com entradas da Lista de Bloqueios por tipo de observável (URL, domínio, endereço IP).
- Configurar períodos de expiração da Lista de Bloqueios para manter o tamanho da Lista de Bloqueios expirando ou removendo automaticamente as entradas mais antigas.
- Pesquisando entradas da Lista de Bloqueios entre diferentes Listas de Bloqueios.
- Vincular entradas da Lista de bloqueios a registros observáveis e incidentes de segurança que incluem resultados de inteligência contra ameaças e detalhes sobre o motivo pelo qual uma entrada está bloqueada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Diagrama da arquitetura de integração

Abaixo está o diagrama de arquitetura de alto nível que descreve os componentes envolvidos e os pontos de integração entre a NOW Platform e a Check Point Systems.



Nota:
O logotipo da Check Point Systems, a imagem do blade antivírus e a imagem do blade antibot são da Check Point Systems ©. Eles são propriedade da Check Point Systems.

Plug-ins

A integração requer que o plug-in Security Incident Response (com.snc.security_incident) seja ativado.

Para instalar plug-ins Security Incident Response :

1. Faça login na sua instância com suas credenciais HI.
2. Verifique se você tem a função de administrador (admin).
3. Navegue até System Definition>plug-ins em sua instância.
4. Selecione e clique em Security Incident Response.

Depois que esses plug-ins forem instalados, você poderá carregar o novo plug-in de integração do Check Point na ServiceNow Store e seguir as instruções de configuração a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versões de SO do Check Point compatíveis

Esta integração requer o Feed de inteligência personalizado do Check Point. Instale o hotfix do recurso Inteligência personalizada conhecido como Check Point R80.10 Jumbo HF, pegue 121 e acima. Consulte a seção de instalação da documentação do feed de inteligência personalizada do Check Point para obter mais informações sobre a matriz de compatibilidade do produto.

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Depois de instalar o hotfix, certifique-se de que os comandos abaixo estejam acessíveis no Check Point Gateway. SSH para o gateway e faça login no modo especialista.

```
[gw-93440b> expert
[Enter expert password:


Warning! All configurations should be done through clish
You are in expert mode now.

[[Expert@gw-93440b:0]# ioc_feeds --help
External indicators configuration

positional arguments:
  show, add, delete, modify
                        Select an action for the external indicators configurations

optional arguments:
  -h, --help            show this help message and exit
  --feed_name           Set feed name
  --transport           Set feed transport protocol: http, https, local_file, local_directory
  --resource            Set feed resource URL
  --state               Set feed enforcement Active / Inactive
  --feed_action         Set feed action: Prevent, Detect, Ask
  --proxy               Set feed proxy
  --proxy_user_name     Set feed proxy user name
  --user_name           Set user name for remote feed
  --test                Set test as true if feed is for testing purposes only
  --format [ [ ...]]    Enter format in order to fetch custom csv file
  --delimiter           Enter delimiter in order to fetch custom csv file
  --comment [ [ ...]]   Enter comment char in order to fetch custom csv file
Missing a few arguments.
[Expert@gw-93440b:0]#
```

Versões compatíveis da ServiceNow

A versão de lançamento San Diego ou posterior é compatível.

Referências

Abaixo estão algumas das referências do Check Point que são úteis na configuração dos pré-requisitos.

1. Recurso de Feeds de inteligência personalizados - https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193
2. Para configurar blades Anti-Bot e Anti-Virus, consulte o Guia do usuário do Check Point. http://downloads.checkpoint.com/dc/download.htm?ID=46534
3. Para configurar a Inspeção de HTTPS no Check Point, siga o link abaixo. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202

Permissões e funções

As funções da ServiceNow a seguir são necessárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Administrador (admin) para instalação do plug-in da aplicação de integração
- Administrador de incidentes de segurança (sn_si.admin) para criar listas de bloqueios na ServiceNow e aprovar solicitações para adicionar e desativar entradas da lista de bloqueios.
- Analista de segurança (também conhecido aqui como Analista SOC, sn_si.analyst) para criar e manter registros de Entrada da Lista de Bloqueios.

Para obter mais informações sobre como atribuir a função de analista de segurança, no site de documentação da ServiceNow , navegue até Operações de segurança>Security Incident Response> Atribuir analistas de segurança.

Configuração do Check Point NGTP

Antes de usar a integração Check Point NGTP, você deve criar uma conta de API, configurar políticas e ativar a integração.

Criar uma conta de API para a integração Check Point NGTP

Uma função de conta de API é necessária em sua instância da Now Platform para esta integração. O nome de usuário e a senha associados a esta conta são criados na Now Platform e inseridos no Check Point, portanto, o Check Point é autenticado com a Now Platform ao recuperar entradas da Lista de Bloqueios.

Antes de Iniciar

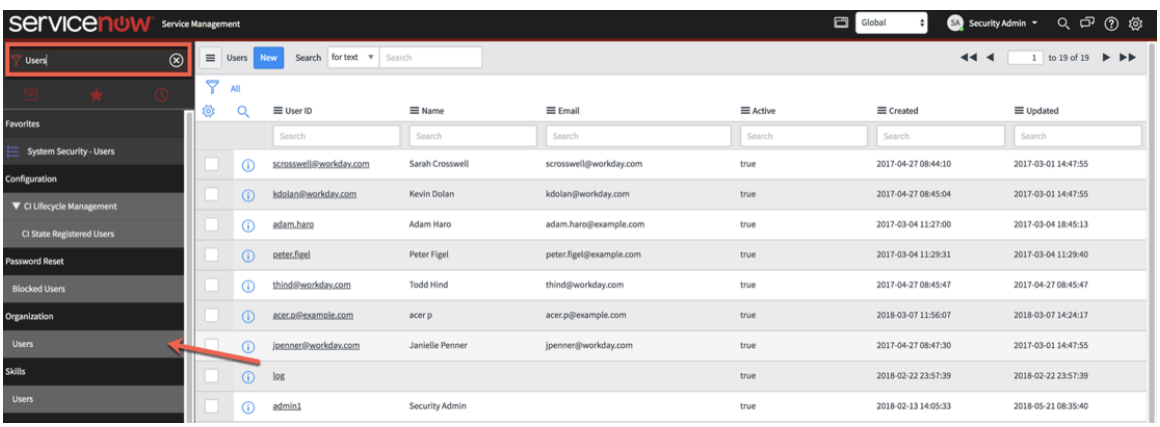
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

O administrador da Now Platform cria uma função de conta de API (sn_sec_checkpoint.api_account_access). Esta conta é usada exclusivamente para inserir as credenciais necessárias para autenticação no Check Point, para que o gateway possa recuperar listas de bloqueios da Now Platform. Esta conta é uma conta de usuário de API separada e exclusiva na instância da Now Platform e atribuída ao administrador do Check Point.

Procedimento

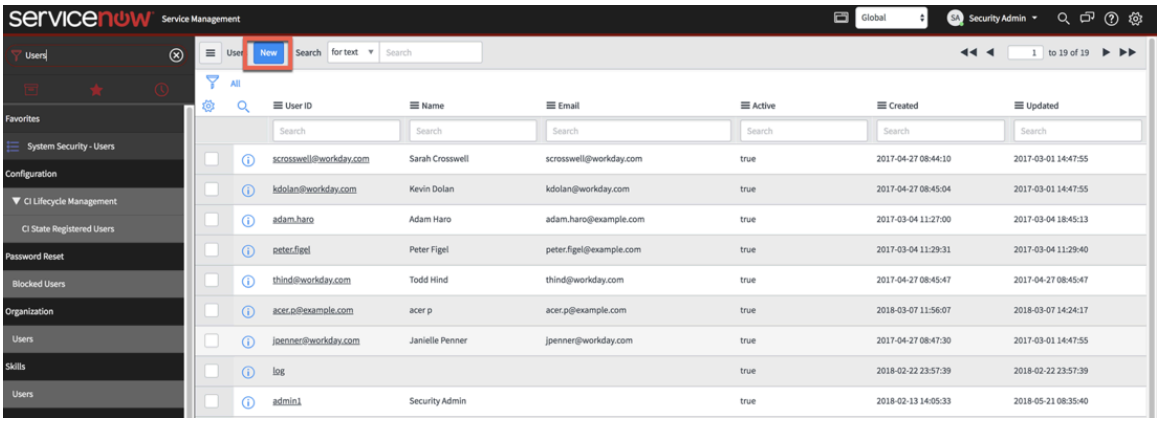
1. Navegar até **Todos** > **Organização** > **Usuários**.
2. Clique no módulo **Usuários**.



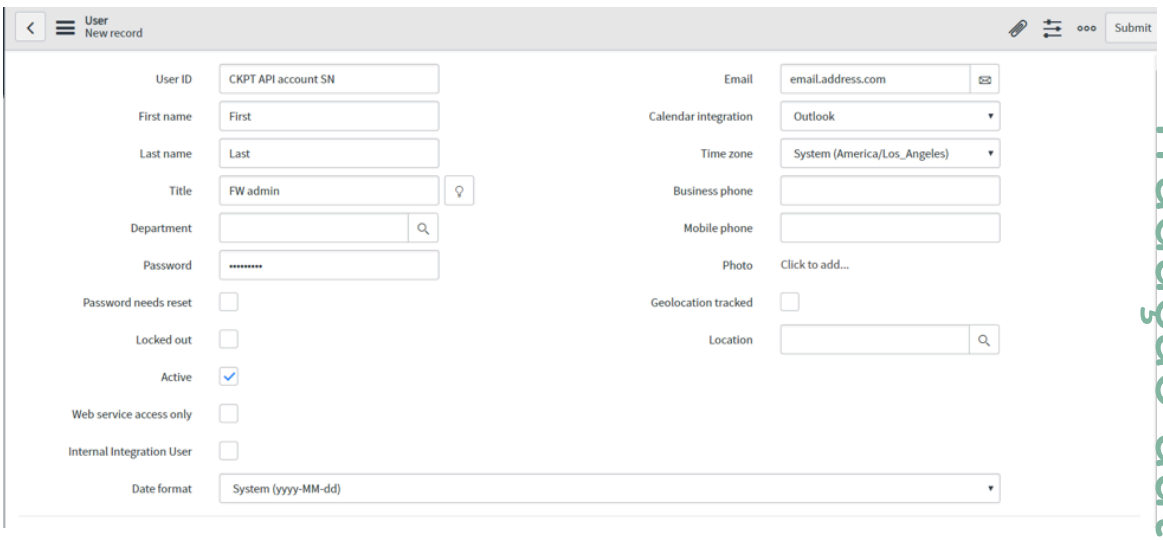
3. Na lista Usuários exibida, clique em **Novo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Um novo formulário será exibido.



4. Preencha o formulário, conforme necessário.

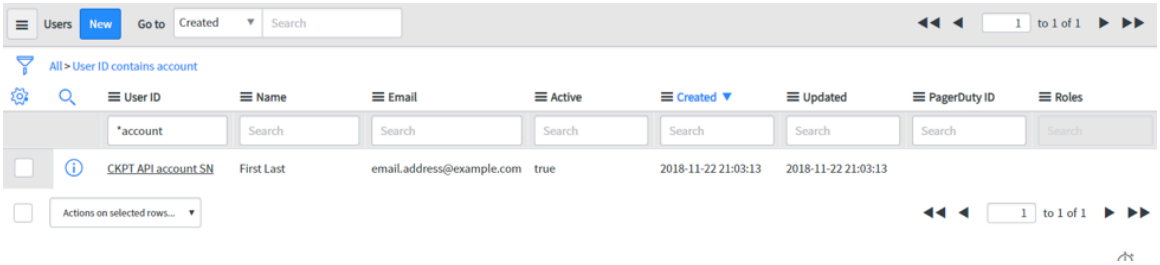
Nota:
Os valores do título do ID do usuário e do endereço de e-mail mostrados na tabela e na figura a seguir são valores de exemplo.

Campo	Descrição
ID do usuário	ID de usuário exclusivo para a função na sua instância da Now Platform. Este ID de usuário é inserido no campo **Nome** de usuário na seção **Autenticação de cliente** do gateway do Check Point da configuração da lista de bloqueios. Um exemplo é a conta da API do CKPT SN.
Nome	Pessoa que você está atribuindo
Sobrenome	Pessoa que você está atribuindo
Título	Cargo, por exemplo, administrador de FW.
Senha	Senha exclusiva criada para esta função. Essa senha é inserida no campo **Senha** na seção **Autenticação de cliente** da Configuração da lista de bloqueios no gateway do Check Point.
E-mail	Endereço de e-mail exclusivo

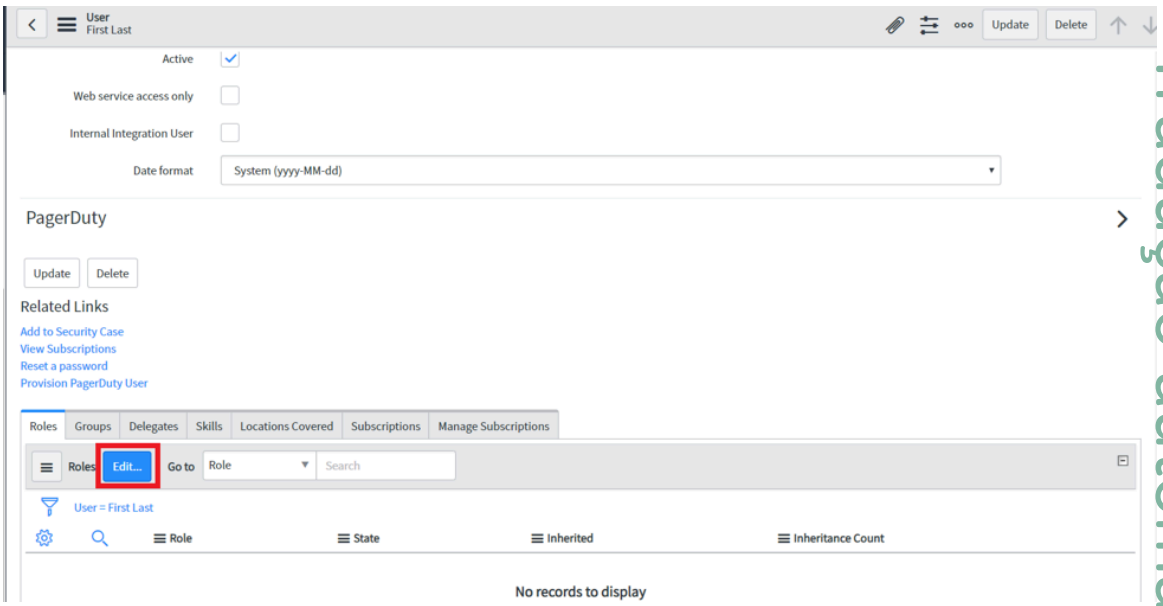
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Enviar**.
   Depois de enviado, você pode atribuir a função.
6. Na lista Usuários na coluna ID do usuário, clique no nome do ID do usuário inserido, por exemplo, SN da conta CKPTAPI.



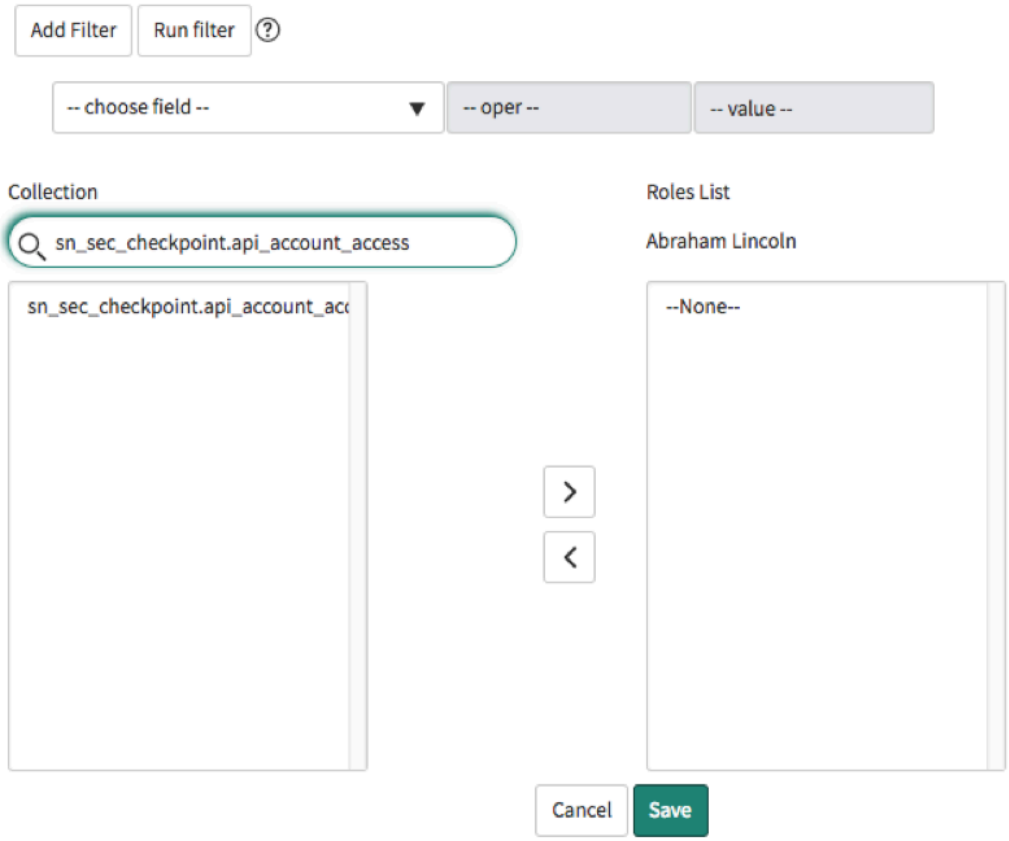
7. No registro aberto na seção Funções, clique em **Editar**.



8. No formulário **Editar membros** exibido, insira sn_sec_checkpoint.api_account_access no campo **Coleção**.

Tradução automática

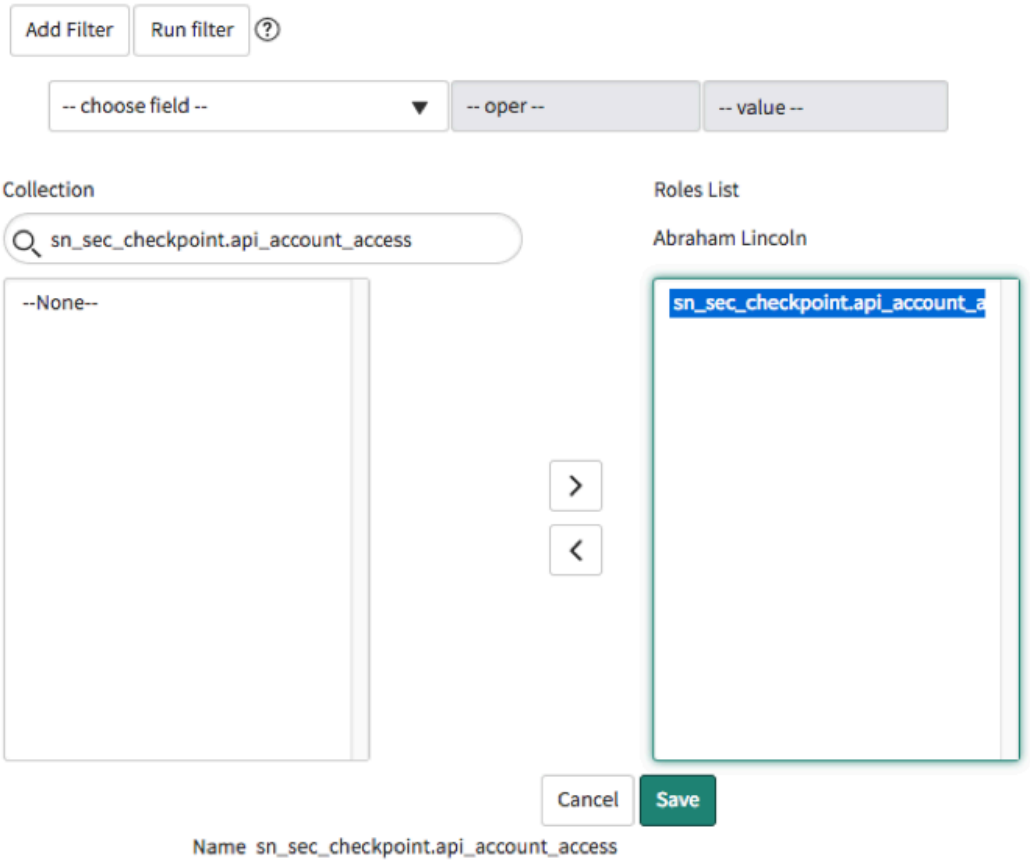
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Na coluna **Coleção**, selecione e mova sn_sec_checkpoint.api_account_access para a **Lista de funções**.
10. Clique em **Salvar**.
11. Navegue até **Usuários**e, na coluna **Usuário** na lista, clique no nome do ID que você criou para a função (SN da conta da API do CKPT).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



12. O registro do usuário é exibido. Este registro verifica se a conta do usuário foi atribuída.

Configurar a integração Check Point NGTP

Conclua as etapas a seguir para configurar a integração Check Point Next Generation Threat Prevention. Isso garantiria que os pré-requisitos para a integração funcionem.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Verifique se a Política de prevenção de ameaças está configurada com os Blades Antibot e Antivírus ativados. Consulte o Guia do usuário do Check Point mencionado na seção Referência para obter informações detalhadas sobre como configurar Blades Antibot e Antivírus.

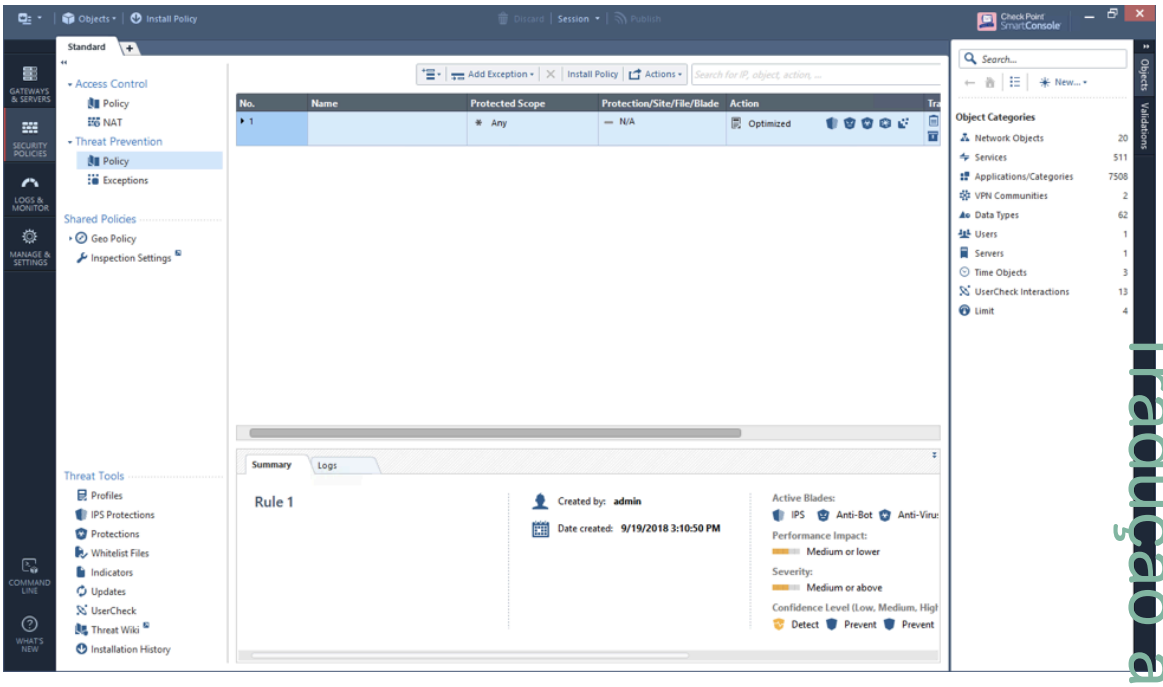
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

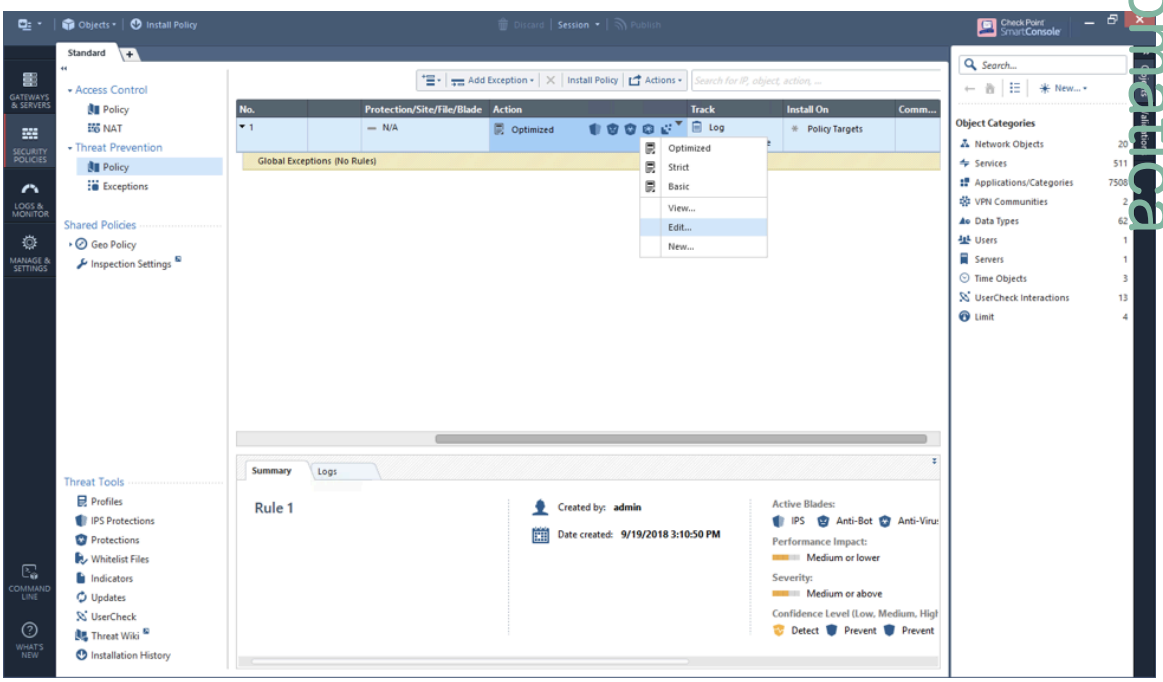
Nota:
As imagens neste tópico são privilegiadas e proprietárias e são usadas com permissão da Check Point Software Services, Ltd.

a. Faça login no **console inteligente**.

b. Navegar até **Políticas de Segurança** > **Prevenção de ameaças** > **Política**.



c. Abra a Política de prevenção de ameaças no modo de edição.



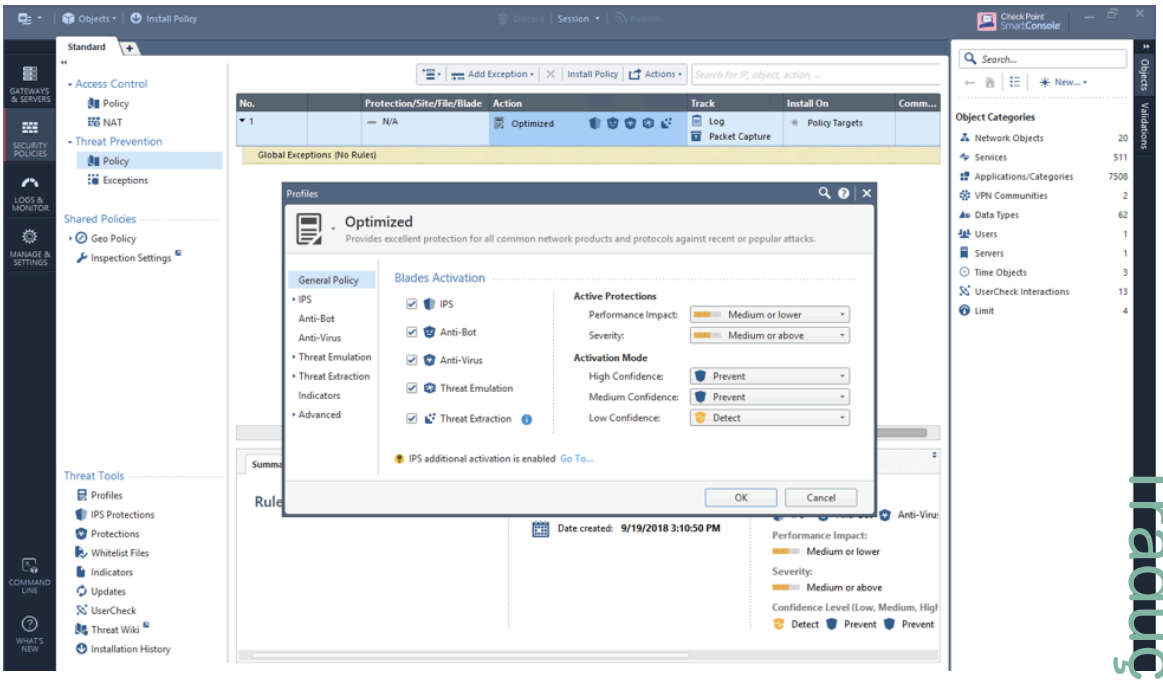
d. Proteções ativas # A severidade deve ser “Média ou superior”

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e. Modo de ativação # Confiança alta deve ser "Impedir"

f. Ativação de blades Antivírus e Antibot deve ser selecionado.



g. Publique as mudanças (se houver) e instale a política.

2. Se ainda não estiverem configurados, os Feeds de inteligência personalizados deverão ser adicionados após a ativação dos Blades Antibot e Antivírus.
Consulte a seção Instalação da documentação do recurso Feed de inteligência personalizada do Check Point.https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

3. Se ainda não estiver configurado, configure o Check Point Gateway para rotear todo o tráfego da Internet via proxy HTTP (se estiver configurando a Inspeção HTTPS).

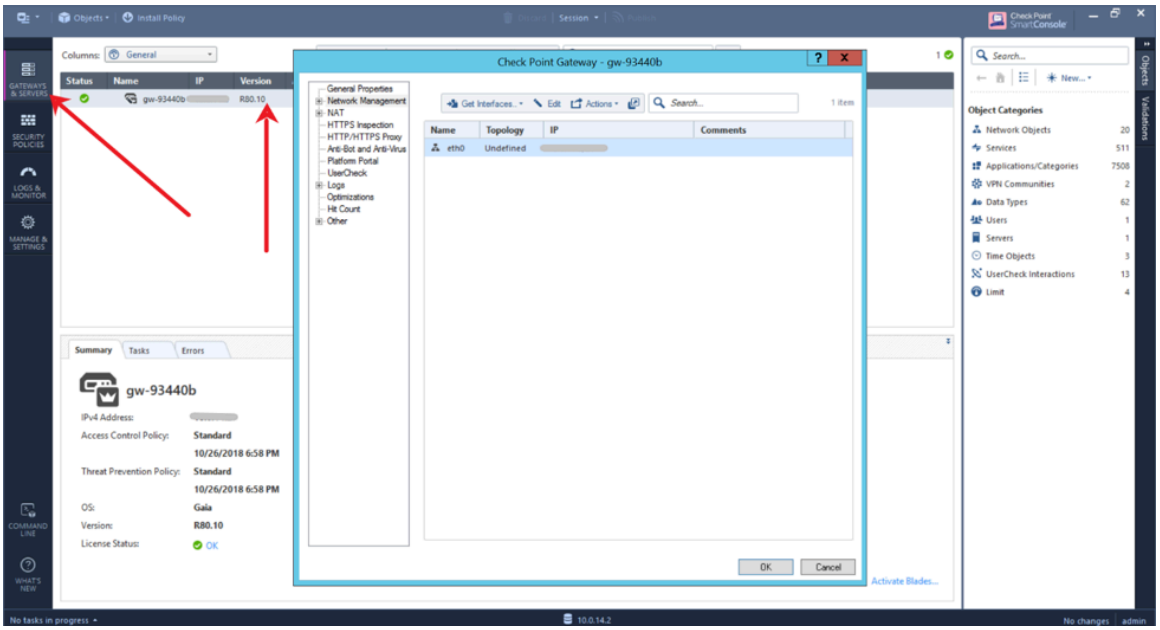
Nota:
Para o bloqueio de URL no NGTP do Check Point, há determinadas configurações que precisam ser garantidas. O tráfego de internet HTTPS usa o protocolo SSL (Secure Sockets Layer) e é criptografado para fornecer privacidade de dados. No entanto, o HTTPS pode ocultar o tráfego mal-intencionado que deveria ter sido bloqueado. Para que o Check Point Gateway obtenha a visibilidade do tráfego HTTPS, roteie o tráfego via proxy HTTP ou configure a Inspeção HTTPS (recomendado). Esta seção detalha as etapas a serem seguidas para configurar o proxy HTTP no Check Point Gateway.

a. Faça login no **console inteligente**.

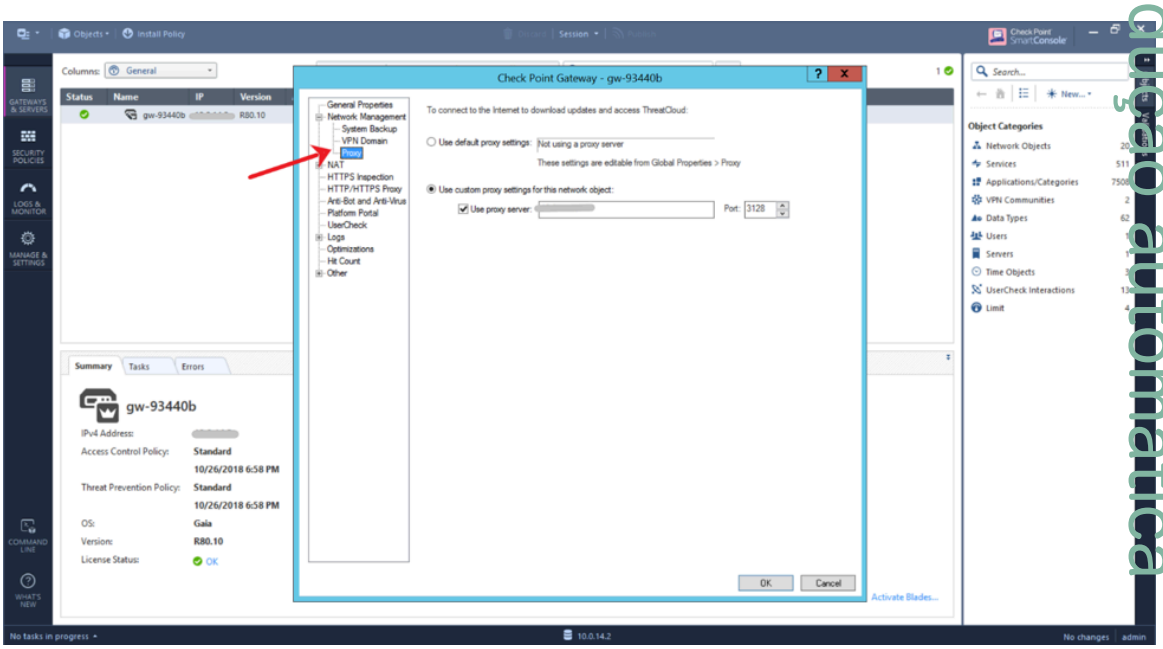
b. Navegue até **Servidores e gateways**e clique duas vezes no servidor aplicável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Navegar até **Gestão de redes** > **Proxy**.



d. Forneça os detalhes do proxy a serem usados para roteamento do tráfego HTTP.

e. Certifique-se de que as solicitações HTTP do endpoint do cliente sejam feitas por meio do proxy HTTP.

4. Se ainda não estiver configurado, habilite a inspeção de HTTPS (se o proxy HTTP estiver configurado). Quando a maior parte do tráfego for SSL, é recomendável usar o Blade de inspeção HTTPS. Isso torna o tráfego transparente para o GW. Habilite a Inspeção de HTTPS no Check Point Gateway da seguinte forma.

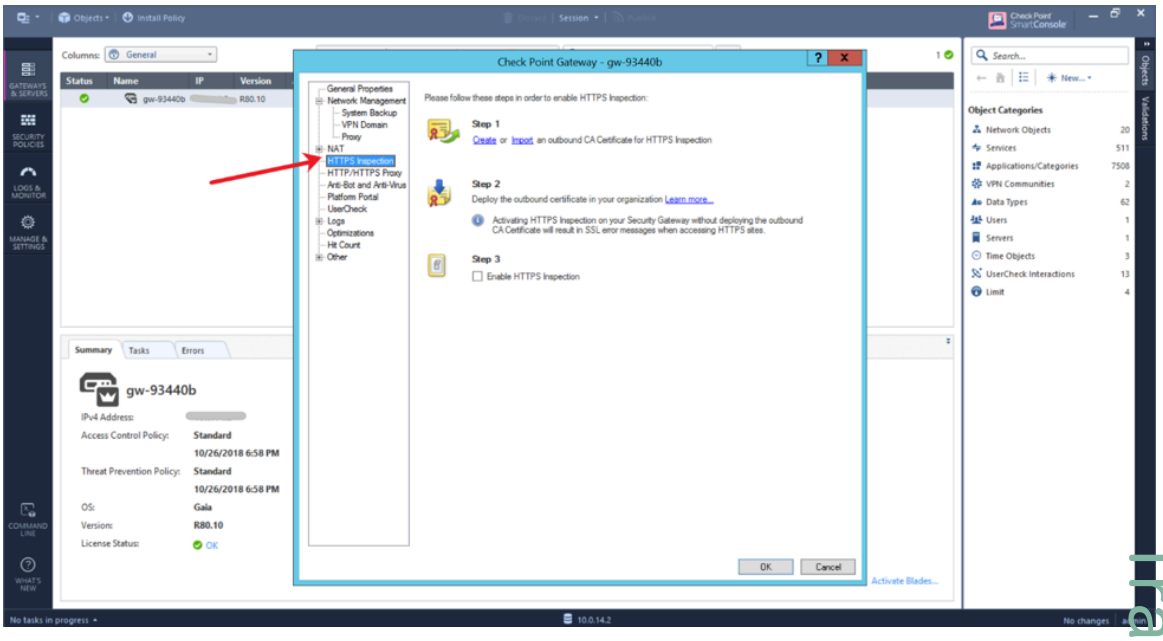
a. Faça login no **console inteligente**.

b. Navegue até **Servidores e gateways**e clique duas vezes no servidor aplicável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Navegue até **Inspeção de HTTPS**.



d. Siga as etapas para configurar a Inspeção de HTTPS no Guia do usuário do Check Point.

Ativar a integração Check Point NGTP

Se você não instalou o aplicativo, siga as instruções para instalá-lo.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Faça login na instância em que você deseja instalar a aplicação.
2. Navegar até **Aplicações do sistema** > **Candidaturas**.
3. Clique na guia **Downloads**.
   Uma lista de aplicações disponíveis para instalação é exibida.
4. Localize a aplicação Check Point Next Generation Threat Prevention, selecione-a e clique em **Instalar**.
   Sua aplicação é instalada automaticamente na sua instância.

Trabalhando com listas de bloqueio

A integração ServiceNow Check Point Next Generation Threat Prevention oferece suporte a listas de bloqueios que aceitam IP, URL e observáveis de domínio.

ServiceNow A lista de bloqueios configurada é um arquivo csv que está hospedado em um servidor Web externo, que para esta integração é a instância da Now Platform. O Feed de inteligência personalizado é configurado no Check Point Gateway, que extrai os endereços IP, URLs e domínios da Now Platform em intervalos pré-configurados.

Esta integração oferece suporte a três tipos de listas de bloqueio:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Endereço IP (inclui um endereço IP individual (somente IPv4) para a lista de bloqueios e blocos CIDR (intervalos) de endereços para a lista de permissões).
- URL
- Domínio

Observáveis compatíveis com a integração Check Point NGTP

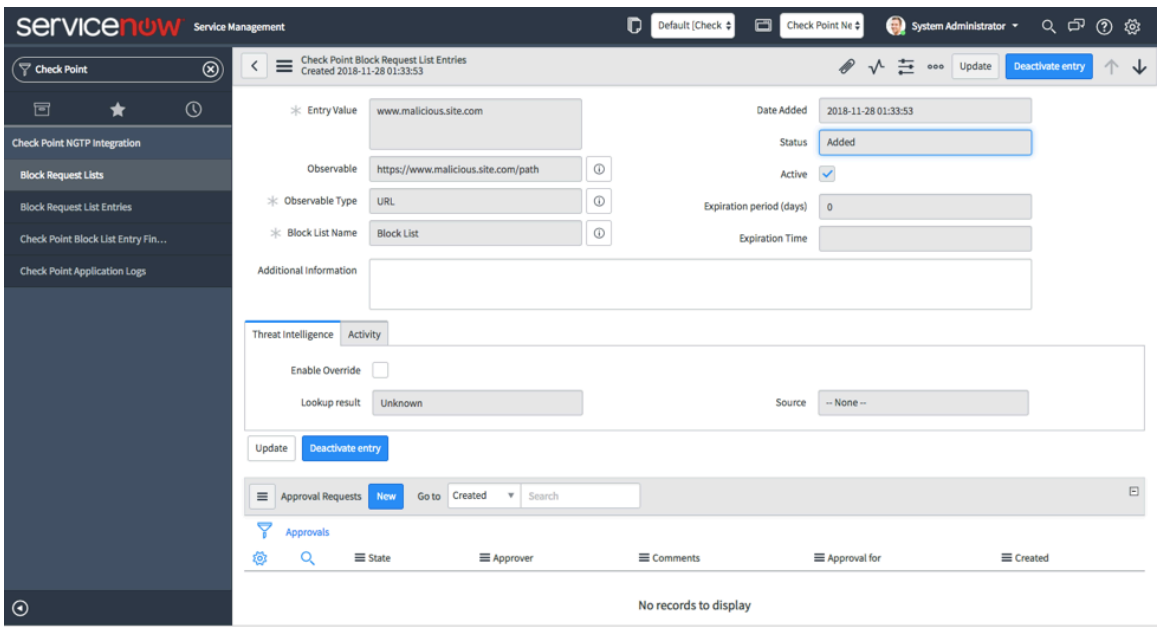
A seção lista as descrições dos observáveis compatíveis com esta integração e formatos de exemplo para cada tipo.

Tipo de Observável	Exemplos	Descrição
Domínio	• example.com • mail.exemplo.com	Caracteres curinga não são compatíveis.
Endereço IP	95.153.103.54 (IPv4)	Representa um endereço de interface único e distinto. A integração é compatível somente com os formatos IPv4 e CIDR (o formato CIDR só é compatível para fins de listagem de permissões). Para fins de lista de permissões, a integração tem suporte para observáveis de endereço IP, incluindo intervalos CIDR (Roteamento entre domínios sem classe), por exemplo, 95.153.100.0/22. **Nota:** Uma mensagem de erro é exibida quando você tenta anexar um único endereço IP a uma Lista de Bloqueios que você já permitiu listar como parte de um intervalo CIDR. Por exemplo, o endereço único 95.153.103.54 faz parte do intervalo CIDR representado por 95.153.100.0/22 (95.153.100.0-95.153.103.255).
URL	• https://www.exemplo.com • http://www.example.com	Descrição — A URL HTTPS é formatada pela aplicação para aparar o caminho da URL e reter somente o nome do domínio. O Check Point NGTP depende da solicitação HTTP CONNECT para avaliar o tráfego da Web

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

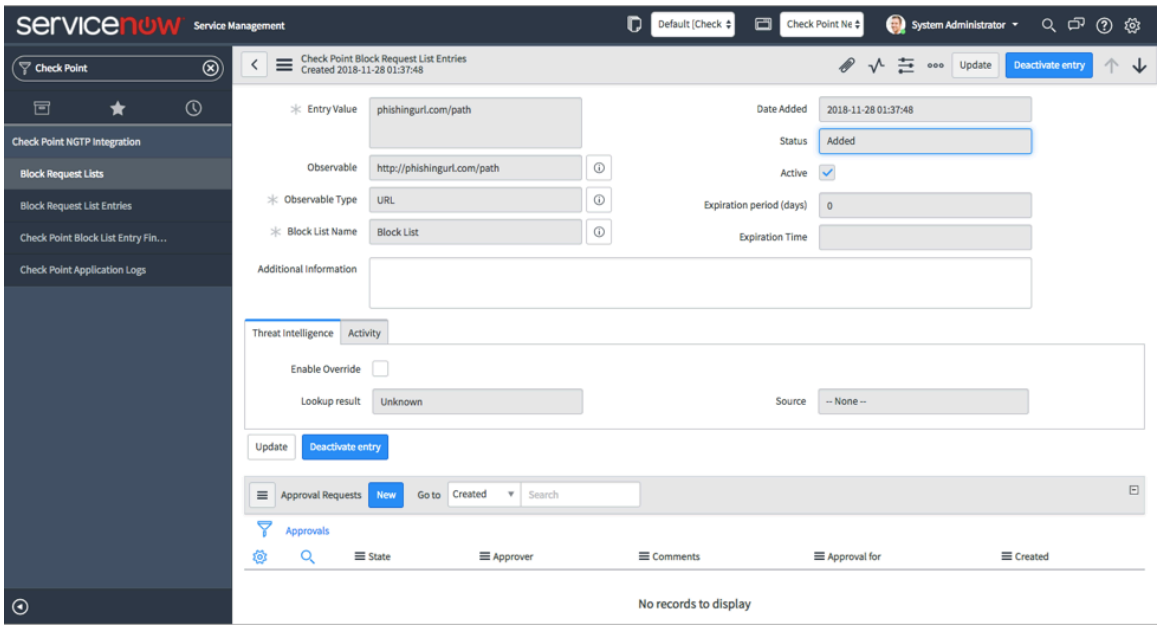
Tipo de Observável	Exemplos	Descrição
		e impor o bloqueio. Para a solicitação HTTPS CONNECT, o URL inteiro não está visível na solicitação e somente o nome do domínio está visível. Quando um usuário bloqueia qualquer URL HTTPS com um caminho específico (por exemplo: https://www.example.com/path), a aplicação recorta o caminho automaticamente (www.example.com). A aplicação mantém o relacionamento entre o observável original e o URL formatado. Abaixo está a captura de tela da entrada da lista de bloqueios que mostra o URL formatado e o observável original.



Para URLs HTTP com um caminho específico (por exemplo, http://www.example.com/path), o Check Point bloquearia o URL especificado, pois o URL inteiro está visível na solicitação CONNECT.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Criar uma lista de bloqueios para a integração Check Point NGTP

Crie uma lista de bloqueios em sua instância da Now Platform. Depois de aprovado e ativado, você pode criar entradas para essas Listas de bloqueios a partir de observáveis determinados como mal-intencionados em incidentes do Now Platform Security Incident Response (SIR) e solicitar aprovação para bloqueá-los.

Antes de Iniciar

Função necessária: Administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

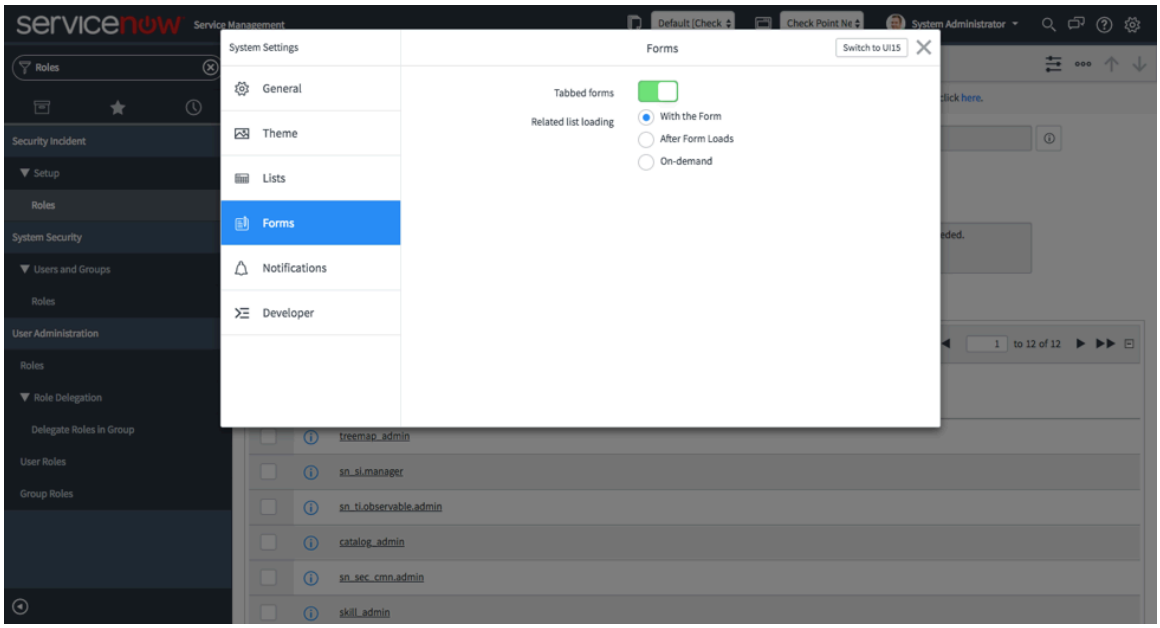
Crie a Lista de bloqueios na sua instância da Now Platform para que o Check Point possa importar objetos (endereços IP, URLs, domínios) incluídos na lista. O Feed de inteligência personalizado é configurado no Check Point Gateway, que extrai os endereços IP, URLs e domínios da Now Platform em intervalos pré-configurados. Para garantir o bloqueio dos observáveis, a política de prevenção de ameaças deve ser configurada com os blades antibot e antivírus ativados.

Nota:

Os números neste tópico são mostrados com os **formulários** com guia desmarcados em Configurações do sistema.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Procedimento

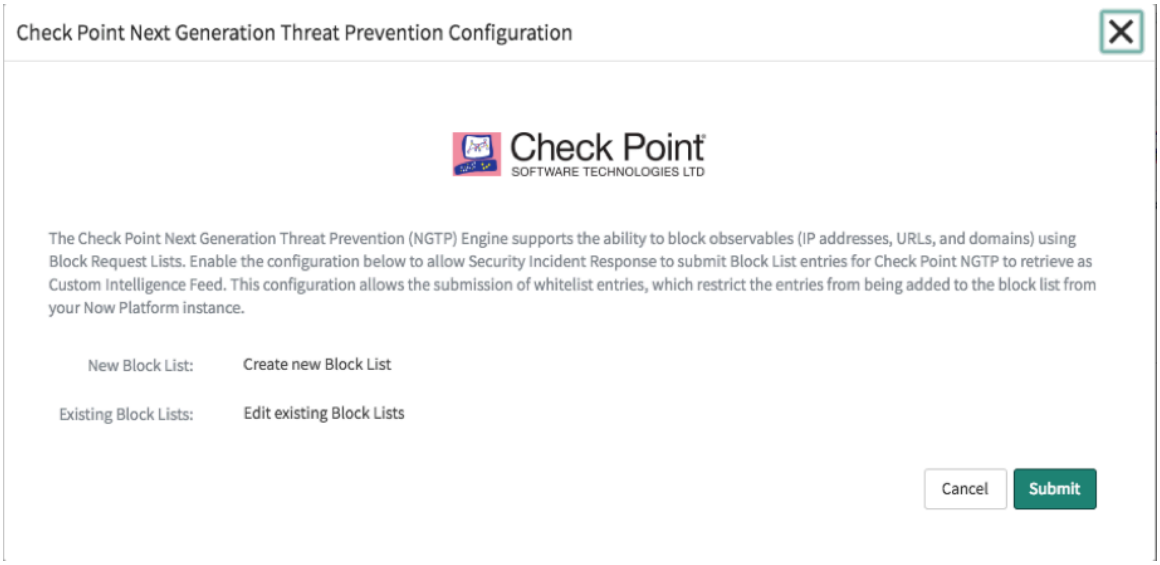
1. Após a conclusão da instalação da aplicação, navegue até **Integrações** > **Configurações de Integração**.
2. Localize o cartão **de Prevenção de ameaças de última geração do Check Point** e clique em **Configurar**.

Nota:
Conteúdo privilegiado e proprietário usado com permissão da Check Point Software Services, Ltd.

3. Clique **em Criar nova lista de bloqueios**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome da lista de solicitações de bloqueio do ponto de verificação. Inclua o tipo de observável (URL, IP, domínio) neste campo para que o analista de segurança possa reconhecer facilmente a intenção da Lista de Bloqueios pelo nome. O nome também deve indicar claramente para qual política de firewall esses objetos da Lista de bloqueios estão mapeados. Alguns exemplos de nomes de Lista de bloqueios são IP de malware de saída ou URL de phishing de saída.
Ativo	Essa caixa de seleção está desmarcada por padrão para indicar que a Lista de bloqueios está inativa. Quando inativa, a Lista de Bloqueios não pode receber entradas adicionais. Quando a caixa de seleção está marcada (quando a solicitação de mudança é fechada ou a solicitação de mudança não é gerada), a Lista de bloqueios é ativada e fica disponível para entradas da Lista de bloqueios.
Marcador de exibição	A caixa de seleção é marcada por padrão para marcar automaticamente o observável e o registro de incidente de segurança associado se o observável estiver bloqueado na Lista de bloqueios. Quando selecionado, o campo "Marcador para observáveis" fica disponível no formulário. **Nota:** Um nome de marcador é criado por padrão a partir do valor inserido no campo Nome com um prefixo de Check Point, por exemplo, Check Point-Malware OutBound IP. Você pode mudar o nome e a cor do marcador. O nome do marcador é exibido no campo "Marcador para observáveis" depois que a Lista de bloqueios é salva. Quando a caixa de seleção está desmarcada, nenhum marcador é criado e o campo "Marcador para observáveis" não está disponível no formulário.
Tipo de Observável	Selecione um tipo de observável que esta Lista de Bloqueios aceita na lista: Endereço IP (incluindo CIDR para lista de permissões), URL ou domínio.

Tradução automática

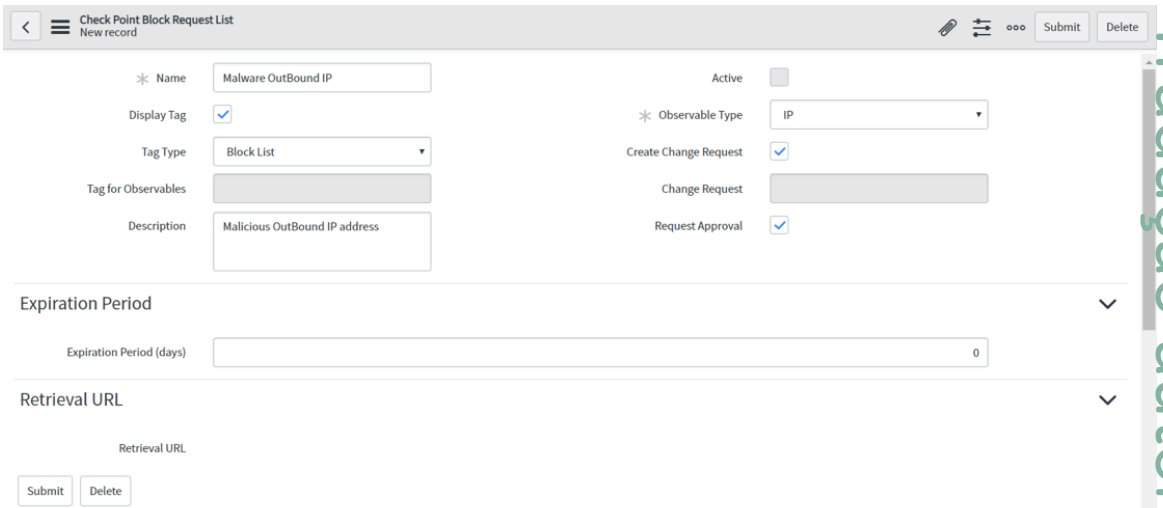
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo de marcador	Marcadores que estão disponíveis na lista. Uma lista de bloqueios é uma lista de observáveis que você deseja que a Prevenção contra ameaças de última geração do Ponto de verificação bloqueie. Uma lista de permissões é uma lista de observáveis que você não deseja bloquear na Prevenção contra ameaças de última geração do Check Point. Por padrão, a cor do marcador da lista de bloqueios é preta e a cor do marcador da lista de permissões é cinza. Você pode mudar a cor.
Criar solicitação de mudança	Esta caixa de seleção é marcada por padrão para criar automaticamente uma solicitação de mudança e tarefas de mudança em sua instância da Now Platform, que são anexadas ao registro da Lista de Bloqueios. A solicitação de mudança é usada para configurar o URL de recuperação da Lista de Bloqueios no gateway de firewall do Check Point Next Geration. Esta opção será recomendada se o administrador do firewall também estiver usando a Now Platform para políticas de firewall ou mudanças de regra. Se você criar uma solicitação, depois que ela for fechada, a Lista de bloqueios será ativada automaticamente. Desmarque a caixa de seleção para ativar manualmente a Lista de Bloqueios depois de receber aviso por e-mail do administrador do firewall de que o Feed de Inteligência Personalizado foi configurado em todos os Gateways do Check Point. Quando a caixa de seleção de Criar solicitação de mudança está desmarcada, o campo Solicitação de mudança fica indisponível.
Solicitar Aprovação	Esta caixa de seleção é marcada por padrão para solicitar aprovações para ativar/remover entradas da Lista de Bloqueios das Listas de Bloqueios. A aprovação é solicitada aos usuários que têm a função de Administrador de incidentes de segurança (sn_si.admin). A solicitação de aprovação será enviada por e-mail aos aprovadores. Depois que a aprovação for aceita, a entrada será ativada nessa Lista de Bloqueios. Quando a caixa de seleção não estiver marcada, as entradas dessa Lista de Bloqueios não seguirão o fluxo de trabalho de aprovação e serão ativadas diretamente na lista de bloqueios.
Marcador do observável	Este campo será exibido somente se a caixa de seleção Exibir marcador estiver marcada. O campo é preenchido automaticamente depois que a Lista de bloqueios é salva com um valor padrão do campo Nome. Se a Lista de bloqueios for criada com o nome "URL do malware", o nome do marcador derivado será "Lista de bloqueios - URL do malware"
Solicitação de Mudança	Quando a caixa de seleção Criar solicitação de mudança está marcada, o número da solicitação de mudança é exibido na instância da Now Platform depois que a Lista de bloqueios é salva. Quando a caixa de seleção Criar solicitação de mudança está desmarcada, este campo não é exibido.

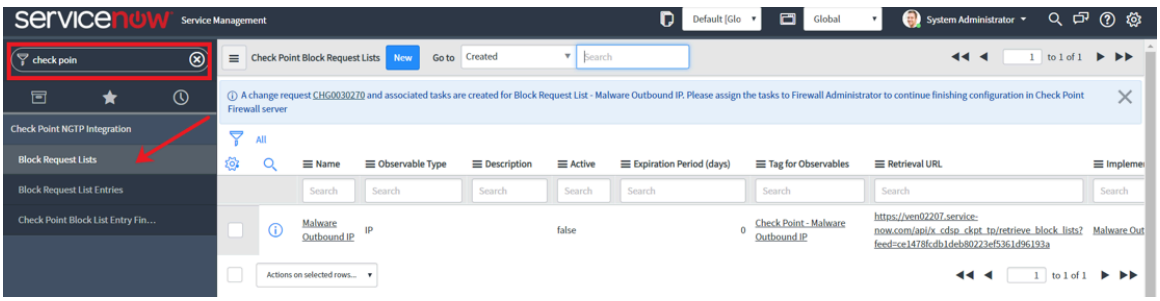
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Descrição da Lista de Bloqueios do Check Point. O nome geralmente contém os tipos de sites e observáveis que você esperaria estar nesta Lista de Bloqueios e você pode usar este campo para obter mais detalhes.
Período de Expiração (dias)	Período de expiração da Lista de Bloqueios. 0 (o padrão) indica que a entrada da Lista de bloqueios nunca expira. Se você alterar este valor, esta entrada ficará ativa para o número de dias inseridos. Você pode inserir um valor mínimo de 1, que é de 24 horas, e não há valor máximo.
URL de recuperação	O URL de recuperação será gerado automaticamente, depois que a Lista de Bloqueios for salva. Para configurar esta Lista de Bloqueios em Gateways do Check Point, você deve usar este URL. Depois que este URL estiver configurado, o Check Point buscará observáveis a serem bloqueados no formato csv.



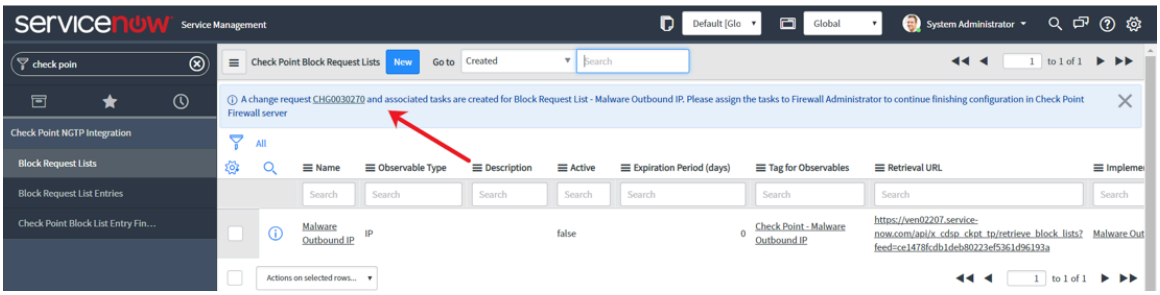
5. Clique em **Enviar**.
6. Se a Lista de Solicitações de Bloqueio do Ponto de Verificação não for exibida, navegue até **Integração de NGTP do Ponto de Verificação** > **Lista de solicitações de bloqueio**.



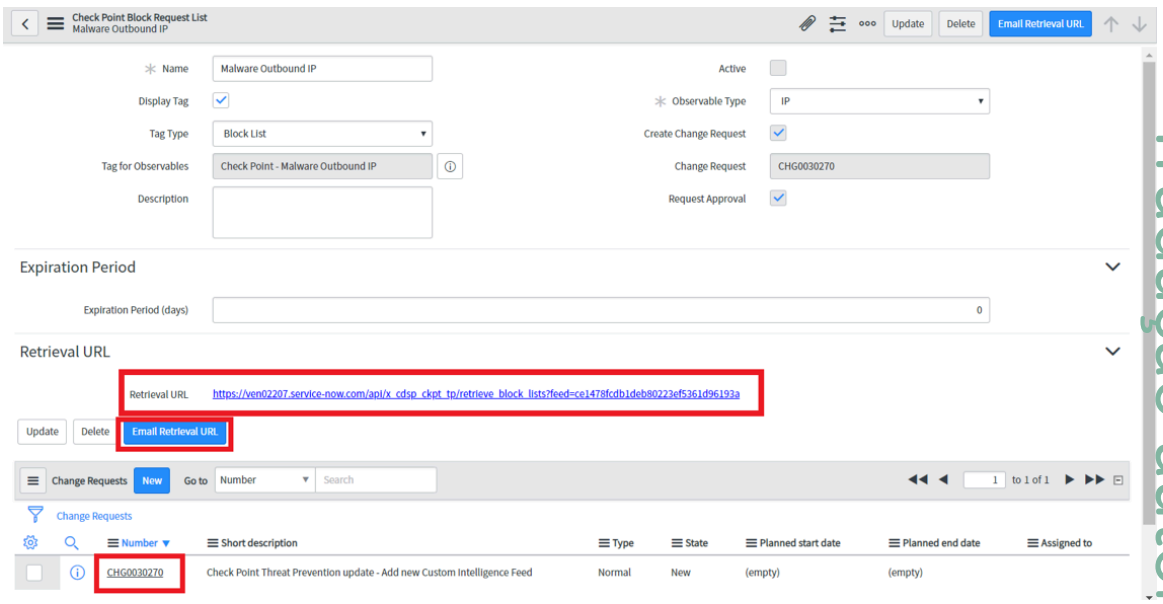
A nova Lista de bloqueios é exibida. O status da Lista de Bloqueios ainda está inativo (falso), o que significa que a Lista de Bloqueios não está disponível para aceitar entradas. Se Criar solicitação de mudança tiver sido configurada, uma mensagem será exibida indicando que uma solicitação de mudança e tarefas foram criadas em sua instância da Now Platform.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Na coluna **Nome**, clique em um item para abrir o registro.
   O registro da Lista de Bloqueios é exibido. Este exemplo mostra uma Lista de Bloqueios de IP de Saída de Malware. Os campos, opções e links a seguir são exibidos no novo registro após o envio e descritos na tabela a seguir.



Campo	Descrição
URL de recuperação de e-mail	Envia por e-mail um aviso de que o link do bloco está disponível para configuração para o administrador do firewall do Check Point.
URL de recuperação	Este URL é usado para configurar o Feed de inteligência personalizado nos gateways do Check Point. **Nota:** Se você tiver as Configurações do sistema definidas como Formulários com guias, este link será exibido na guia Informações de recuperação da lista de bloqueios na parte inferior do registro.
Solicitação de mudança da Now Platform	Um link para o registro de solicitação de mudança é exibido na seção Solicitações de mudança quando configurado, e o número da solicitação é exibido no campo Solicitação de mudança.
Atualizar	Modifique os dados e atualize os campos editáveis.
Deletar	Exclua o registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Crie e adicione mais Listas de Bloqueios conforme necessário.
   As Listas de Bloqueios são exibidas na Página de Listas de Solicitações de Bloqueio do Check Point.

O que Fazer Depois

Ative a Lista de Solicitações de Bloqueio manualmente ou com uma solicitação de mudança da Now Platform.

Ativar uma lista de bloqueios para a integração Check Point NGTP

Depois que a Lista de bloqueios tiver sido criada na Now Platform e o URL estiver disponível, o administrador do Check Point configura a Lista de bloqueios como Feed de inteligência personalizado em todos os Gateways de última geração do Check Point. Antes de aceitar entradas da Lista de Bloqueios, a Lista de Bloqueios deve ser configurada no Check Point e ativada na Now Platform.

Antes de Iniciar

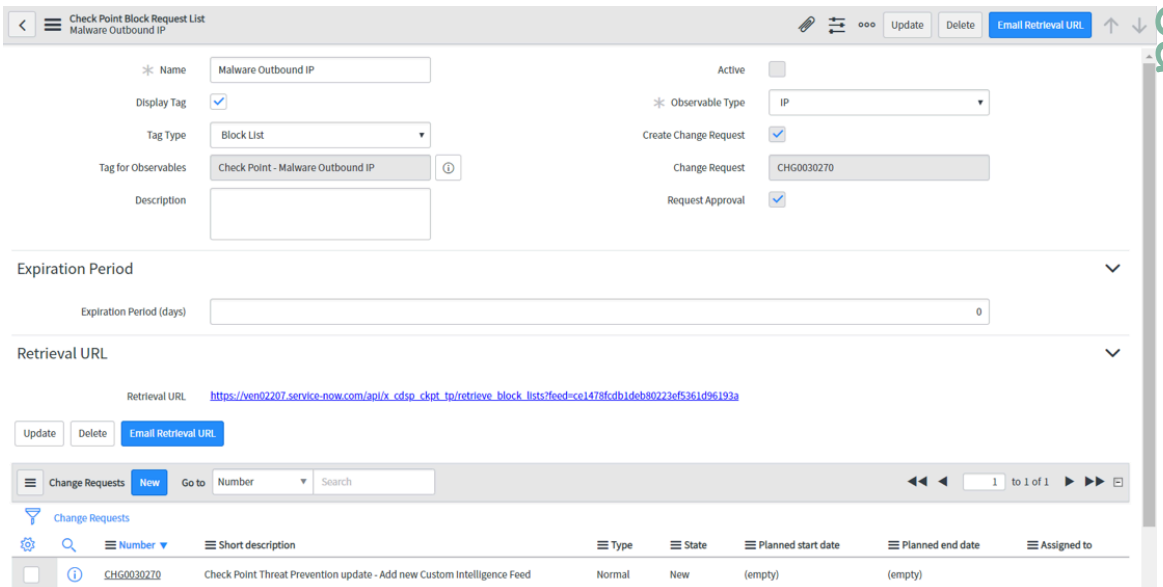
Função necessária: Administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

Depois que a Lista de bloqueios for configurada, como administrador de incidentes de segurança, você poderá ativar a Lista de bloqueios manualmente ou a Lista de bloqueios será ativada automaticamente após a conclusão de uma solicitação de mudança da Now Platform. A Solicitação de Mudança deve ser aprovada e movida do estado inativo para o estado ativo antes que possa aceitar entradas da Lista de Bloqueios.

Procedimento

1. Navegar até **Todos** > **Integração de NGTP do Ponto de Verificação** > **Lista de solicitações de bloqueio**e selecione o módulo **Listas de solicitações de bloqueio**.
2. Na lista **Listas de solicitações de bloqueio do Check Point** exibida, selecione sua nova Lista de bloqueios na coluna **Nome**.
3. No registro exibido, observe o botão da **URL de recuperação de e-mail**, o link da URL de recuperação da lista de bloqueios ativa e, se configurado, a solicitação de mudança da Now Platform na seção Solicitações de mudança.
   Observe também que a caixa de seleção Ativo está desmarcada.

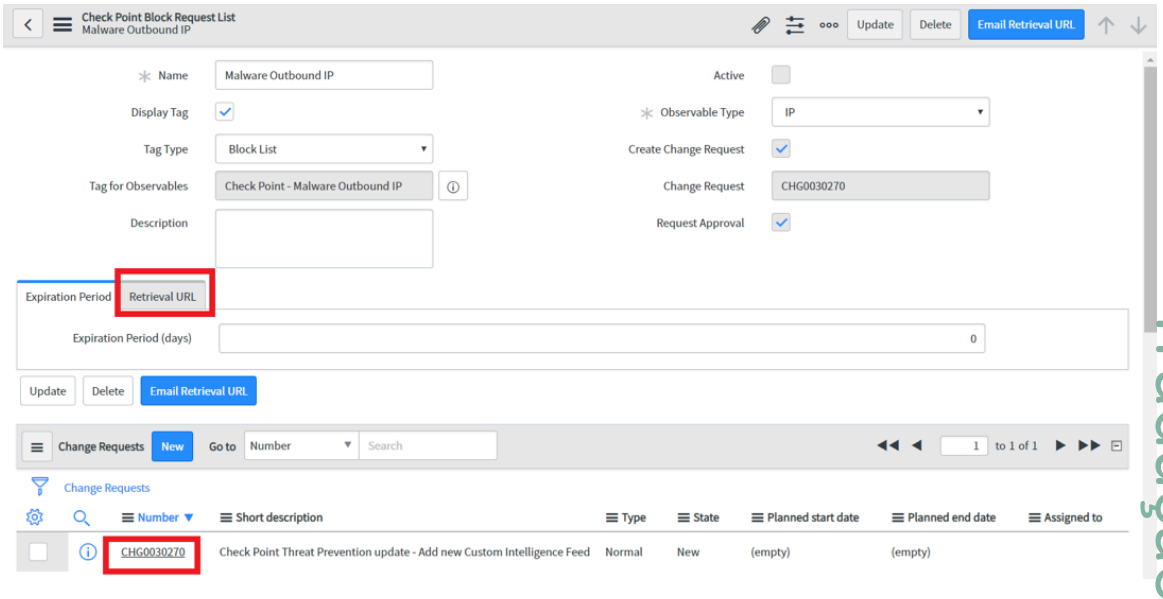


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Com os formulários com guia desmarcados nas configurações do sistema, o URL de recuperação da lista de bloqueios aparece na seção URL de recuperação.

4. Clique na guia **URL de recuperação da lista de bloqueios** para exibir o URL de recuperação.
A figura a seguir mostra o URL de Recuperação da Lista de Bloqueios exibido como uma guia com os formulários com guia selecionados nas configurações do sistema. O link para a solicitação de mudança (CH0030270) também é exibido.



5. Para concluir a configuração e mover a Lista de Bloqueios de inativa para ativa, você deve escolher uma das opções a seguir para notificar o administrador do firewall de que o URL de recuperação está disponível.

Opção	Descrição
Clique em URL de recuperação de e-mail.	URL de Recuperação da Lista de Bloqueios de E-mail diretamente para o administrador do firewall. Esta opção permite que o administrador do firewall conclua a configuração na plataforma Check Point. Escolha esta opção se o administrador do firewall não estiver usando a Now Platform.
Conclua a solicitação de mudança da Now Platform e atribua as tarefas de configuração ao administrador do firewall.	Esta opção estará disponível somente se o administrador de firewall do Check Point também estiver usando a Now Platform e os processos de aprovação e gestão de mudanças da Now Platform estiverem configurados. **Nota:** Usuários com a função de administrador de incidentes de segurança (sn_si.admin) podem aprovar a solicitação de mudança da Now Platform. Depois que as tarefas de configuração forem concluídas e a solicitação de mudança for encerrada, a Lista de bloqueios será ativada automaticamente.

O que Fazer Depois

Depois de notificar o administrador do firewall de que o URL de recuperação está disponível e de confirmar que a Lista de bloqueios foi configurada no Check Point, como administrador de incidentes de segurança, a próxima etapa é ativar a Lista de bloqueios. Você ativa a Lista de bloqueios manualmente ou, se configurado, usa o formulário de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

solicitação de mudança da Now Platform para ativar a Lista de bloqueios. A Lista de bloqueios é ativada automaticamente quando a solicitação de mudança é fechada.

Configurar uma lista de bloqueios como um feed de inteligência personalizado na integração Check Point NGTP

O administrador do firewall deve configurar o Feed de inteligência personalizado correspondente à Lista de bloqueios criada na plataforma NOW.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Esta tarefa precisa ser realizada em cada um dos gateways NGTP do Check Point. O administrador do firewall precisaria do acesso SSH dos servidores de gateway. Se sua organização tiver processos de aprovação e gestão de mudanças da Now Platform, verifique se a capacidade de envio/recebimento de e-mail está habilitada.
O administrador do firewall precisaria do URL de recuperação da Lista de bloqueios e das credenciais do usuário da ServiceNow com a função de acesso à conta da API do Check Point (sn_sec_checkpoint.api_account_access).

Se o administrador do firewall não estiver usando a plataforma NOW, o administrador de incidentes de segurança NOW poderá fornecer as informações necessárias por e-mail. Como alternativa, se o administrador do firewall estiver usando a plataforma NOW, a solicitação de mudança associada à lista de bloqueios poderá ser atribuída ao administrador do firewall. Esta solicitação de mudança tem as informações necessárias para configurar o feed de inteligência personalizado.

Para obter mais informações sobre como configurar o Feed de inteligência personalizado em gateways do Check Point, consulte: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Procedimento

1. Verifique se a capacidade de envio/recebimento de e-mail está habilitada em sua instância da Now Platform navegando até **Propriedades do e-mail** > **Administração** > **Propriedades do E-mail**.
2. Em Configuração de e-mail de saída, verifique se **Envio** de e- **mail** e Recebimento de e-mail estão selecionados.
3. Modifique o SSH para o gateway do Check Point com o modo especialista.
4. Execute o comando para adicionar o Feed de inteligência personalizado.
   A execução do comando é interativa e solicita o formato do feed e a senha.
   - Quando solicitado a informar o formato do feed, insira "cp_csv"
   - Quando solicitada a senha do usuário da plataforma NOW com acesso à API.

   A execução do comando avisaria sobre o certificado do servidor (plataforma NOW) que não é confiável para a máquina e solicitaria a adição do certificado de segurança do servidor ao armazenamento confiável da máquina. Insira **Y**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A mensagem "Status:Succeed" será exibida, confirmando que o feed foi adicionado com sucesso.

```
[Expert@gw-93440b:0]# ioc_feeds add --feed_name phishing_url --transport https --resource https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/
retrieve_block_lists?feed=<feed_id> --user_name <now_ckpt_api_user> --feed_action Prevent
Enter feed format. Should be cp_csv/stix_1.x: cp_csv
Only Check Point's csv format files will be loaded
Enter Password
Password: <now_ckpt_api_password>

Default value for active is: true

Feed Name: phishing_url
Feed is Active
File will be fetched via HTTPS
Resource: https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/retrieve_block_lists?feed=<feed_id>
Action: Prevent
User Name: admin

[============================================================] 100.0% ...Getting file from the server
The server security certificate is not trusted by your machine.
SHA256 Fingerprint=SHA256 fingerprint of the NOW instance.

Do you want to trust it for this specific feed?  [y/n]: y
Fetching active feeds

Update summary
##############
feed: phishing_url. Status: Succeed
##############
Activating Scheduler

[Expert@gw-93440b:0]#
```

Enviar entradas da lista de bloqueios de um incidente de segurança para a integração Check Point NGTP

Os observáveis anexados a um registro de incidente de segurança são enviados para aprovação como entradas da Lista de bloqueios para diferentes Listas de bloqueios. Um processo de aprovação opcional para entradas da Lista de bloqueios faz parte do fluxo de trabalho pré-configurado. O gateway importa entradas da Lista de bloqueios (endereços IP, URLs, domínios) que estão incluídas nas Listas de bloqueios.

Antes de Iniciar

Função necessária:

- Analista de incidentes de segurança (sn_si.analyst) para enviar entradas da lista de bloqueios.
- Administrador de incidentes de segurança (sn_si.admin) para aprovar entradas da lista de bloqueios. Esta autoridade pode ser atribuída conforme exigido pela sua organização.

Por Que e Quando Desempenhar Esta Tarefa

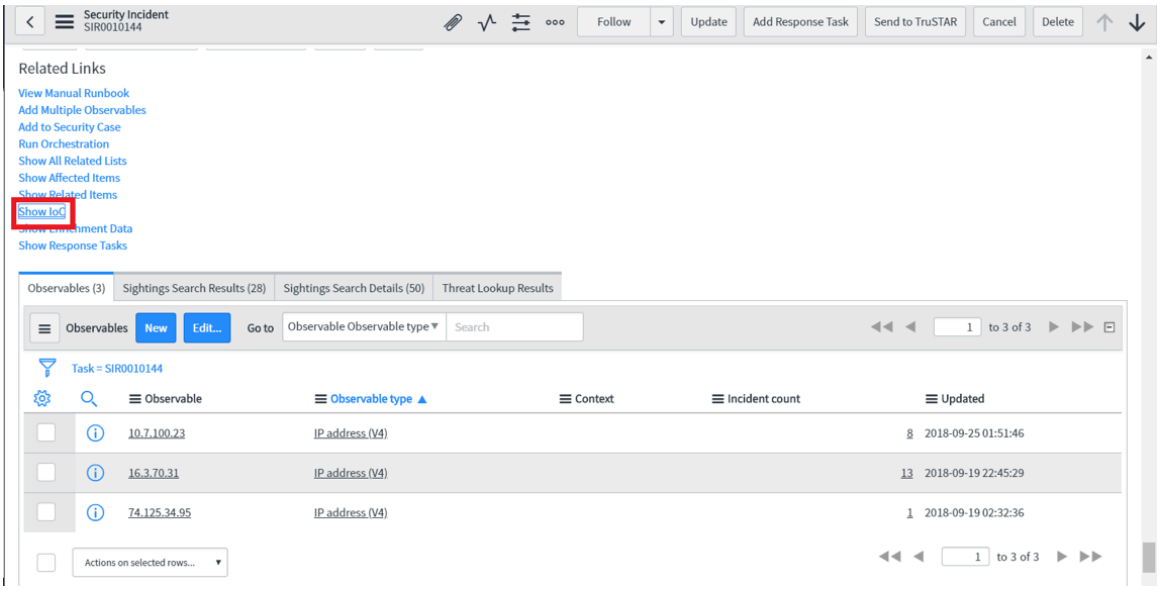
Usuários com a função sn_si.analyst enviam entradas de bloqueio solicitando um bloqueio em observáveis anexados a um registro de incidente de segurança. Depois de enviada, uma entrada da Lista de Bloqueios com um status Pendente é gerada e enviada para aprovação. O exemplo a seguir mostra uma solicitação de bloqueio para um observável de URL.

Procedimento

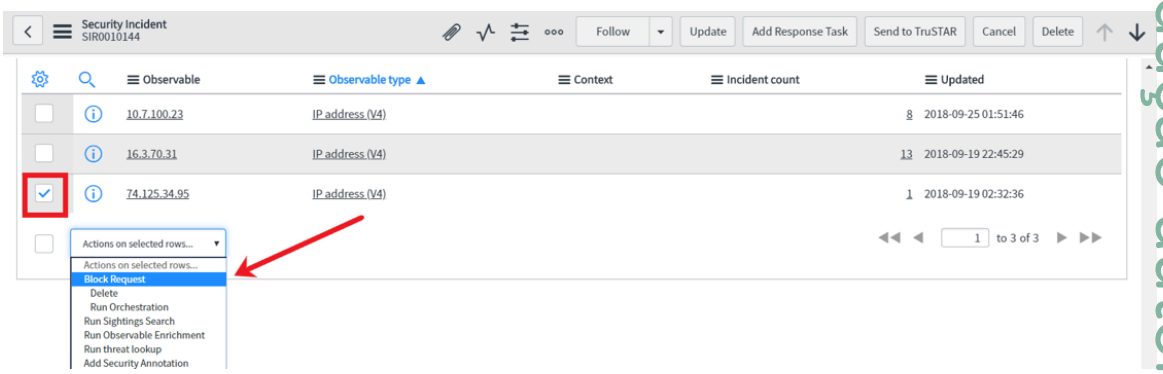
1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar Todos os Incidentes**e clique em um registro de incidente de segurança para abri-lo.
2. Clique no link relacionado **Mostrar IoC**.

Tradução automática

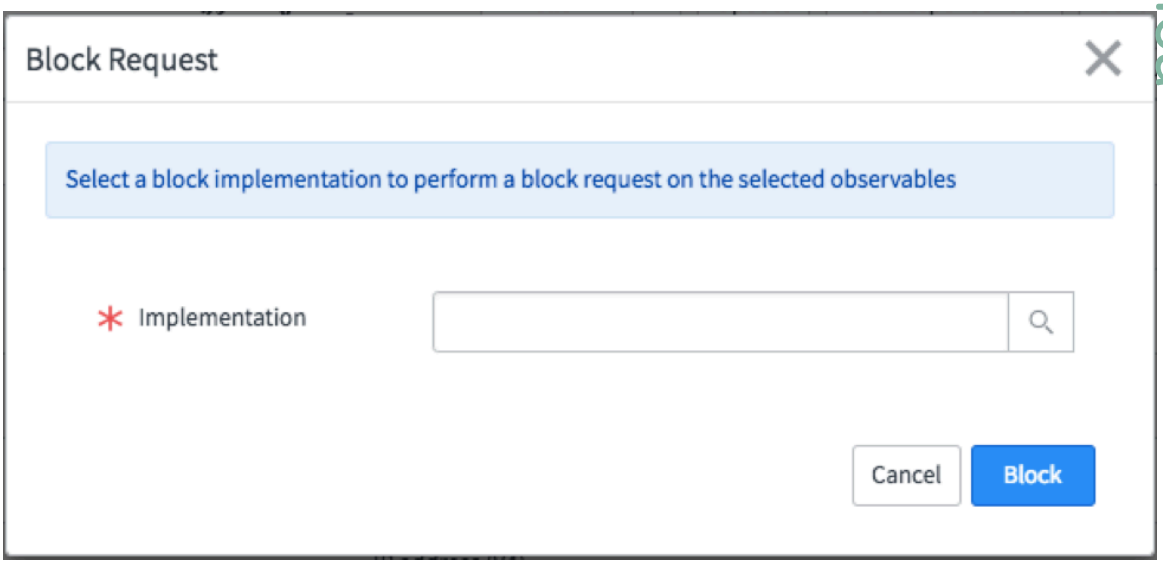
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Na lista relacionada Observáveis, selecione os observáveis que você deseja bloquear e, na lista **Ações nas linhas selecionadas**, selecione **Solicitação de bloqueio**.



4. Na caixa de diálogo exibida, clique no ícone de pesquisa (ícone)

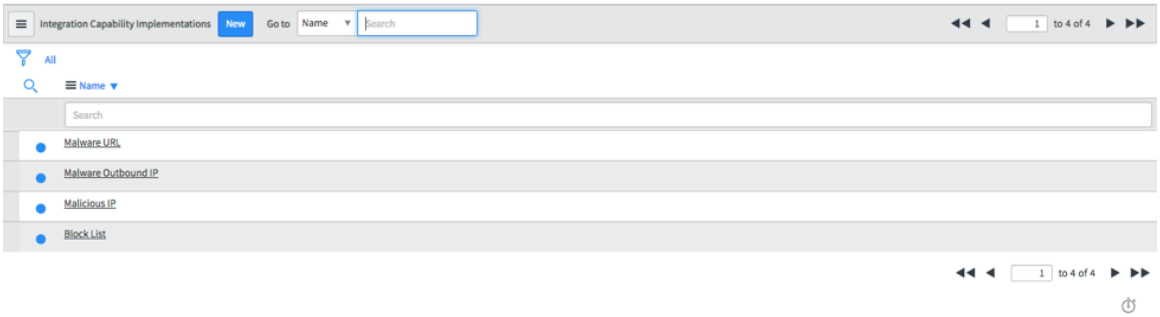


5. Na lista, selecione a Lista de bloqueios à qual você deseja anexar esta entrada.

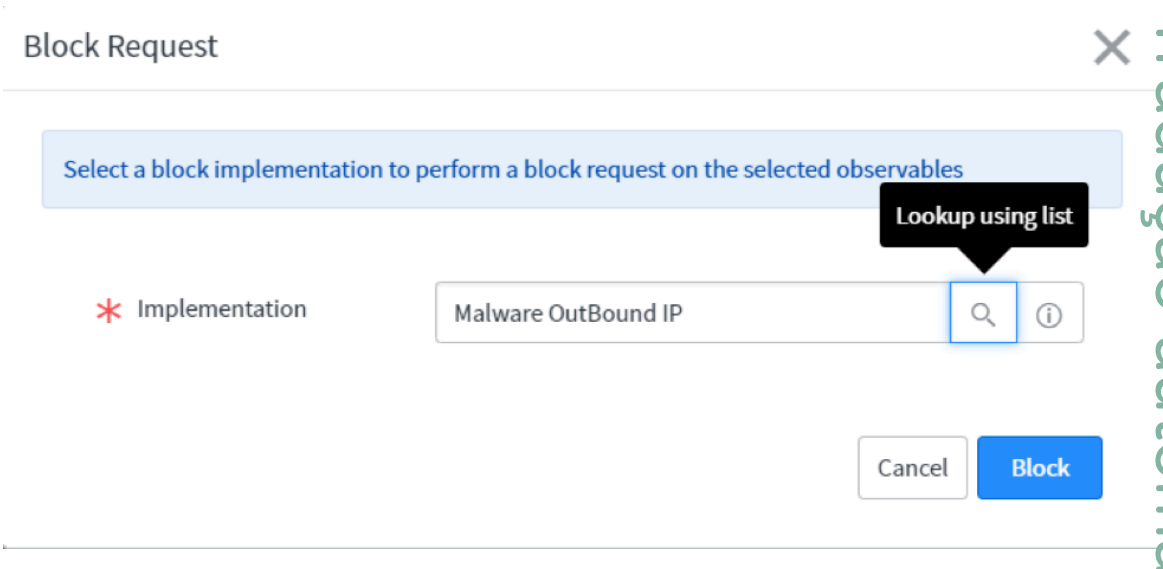
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Para este exemplo, o tipo de observável (IP) de entrada deve corresponder ao tipo de observável (IP) Lista de Bloqueios.

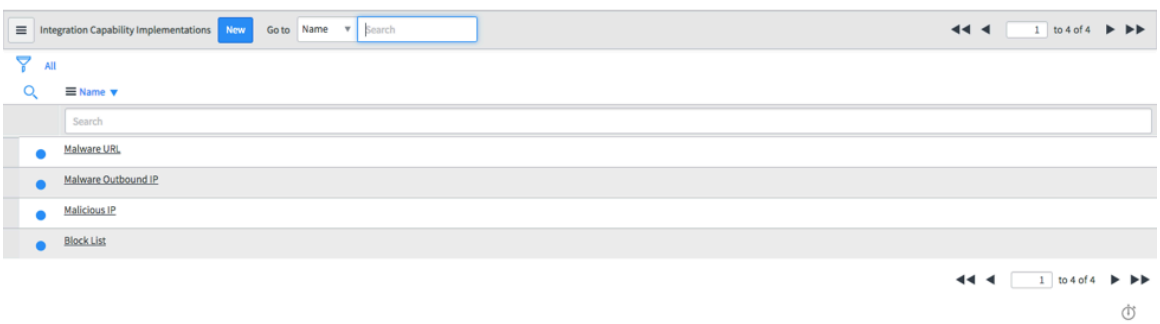


6. Na caixa de diálogo Solicitação de Bloqueio com o nome da Lista de Bloqueios exibido no campo Implementação, clique em **Bloquear**.



7. Na lista exibida, selecione a Lista de bloqueios à qual você deseja anexar esta entrada.

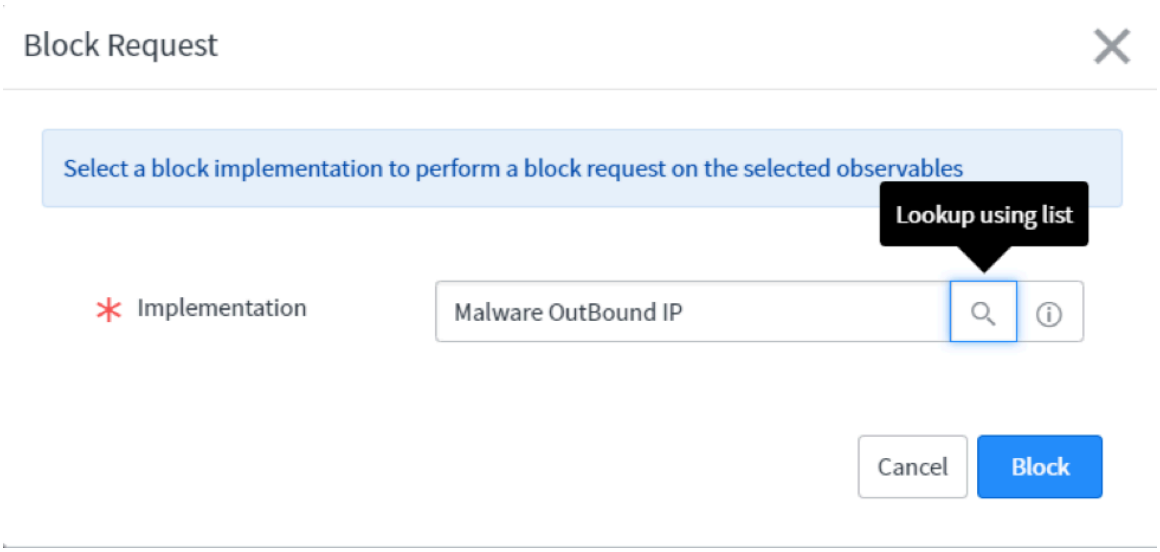
Nota:
Para este exemplo, o tipo de observável (IP) de entrada deve corresponder ao tipo de observável (IP) Lista de Bloqueios.



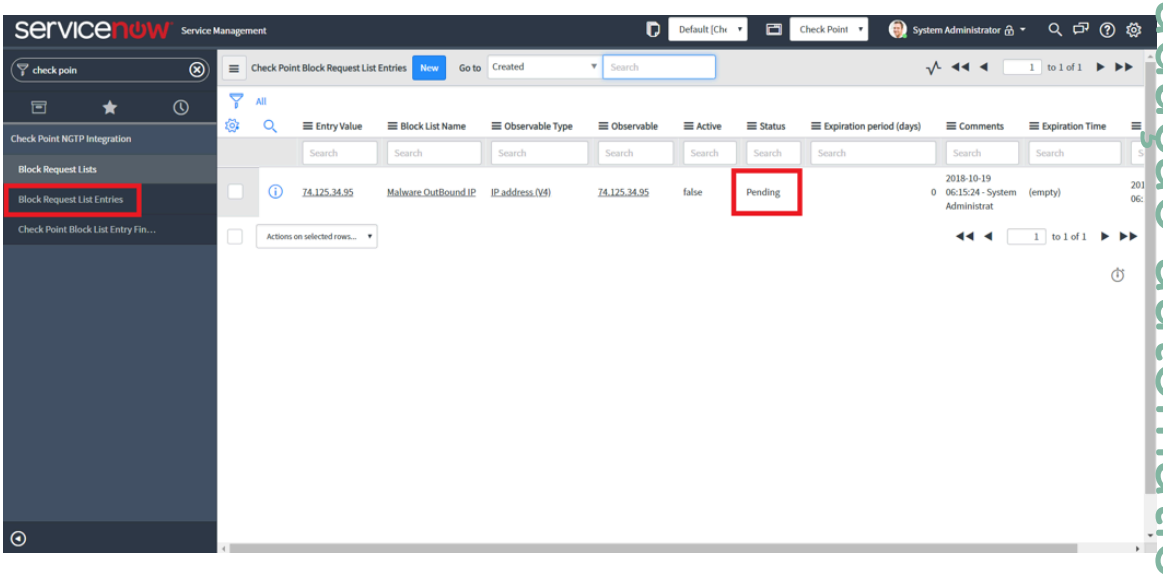
8. Na caixa de diálogo Solicitação de Bloqueio com o nome da Lista de Bloqueios exibido no campo **Implementação**, clique em **Bloquear**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



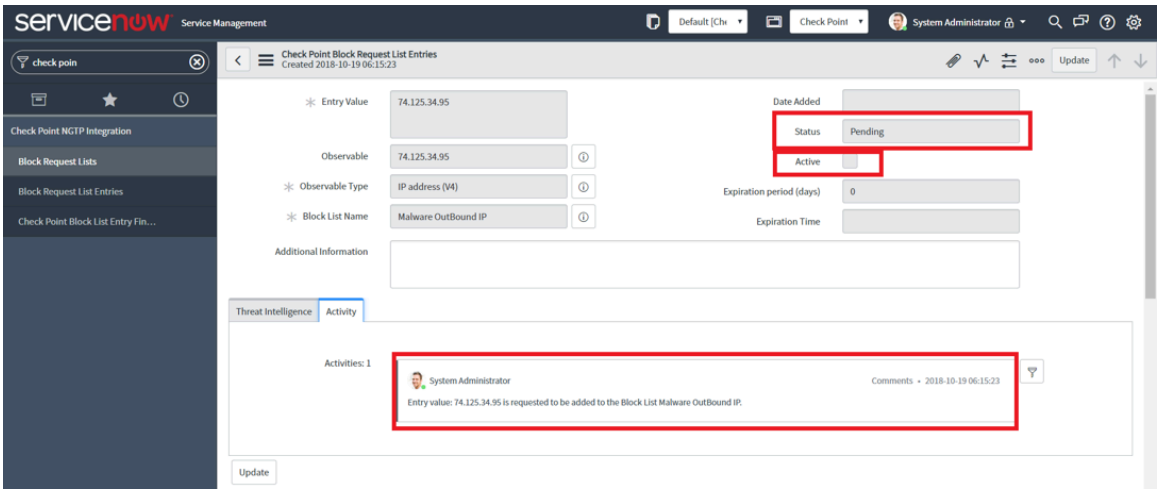
9. Navegar até **Integração de NGTP do Ponto de Verificação** > **Bloquear Entradas da Lista de Solicitaçõe**s e clique em **Bloquear entradas da lista de solicitações**.



10. Na lista Entradas da Lista de Solicitações de Bloqueio do Ponto de Verificação, clique no seu observável na coluna **Valor de entrada** para abrir o registro.
Para este exemplo, o registro de **74.125.34.95** é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O status é Pendente, a caixa de seleção Ativo está desmarcada e as anotações de trabalho mostram que há uma solicitação para adicionar o observável. Esta solicitação de Entrada da Lista de Bloqueios está pronta para aprovação.

O ícone ao lado do campo Observável é um link para a tabela Observável da Now Platform.

O valor no campo Observável (74.125.34.95) é vinculado à tabela Observável e corresponde ao formato que foi trazido do evento de acionamento de incidente do Security Incident Response.

Enviar entradas da lista de bloqueios diretamente da Tabela de Entrada da Lista de Bloqueios

Para observáveis determinados como mal-intencionados e não associados a um incidente de segurança específico da Now Platform, você envia entradas da Lista de bloqueios da lista de bloqueios.

Antes de Iniciar

Função necessária: Administrador de incidentes de segurança (sn_si.analyst)

Por Que e Quando Desempenhar Esta Tarefa

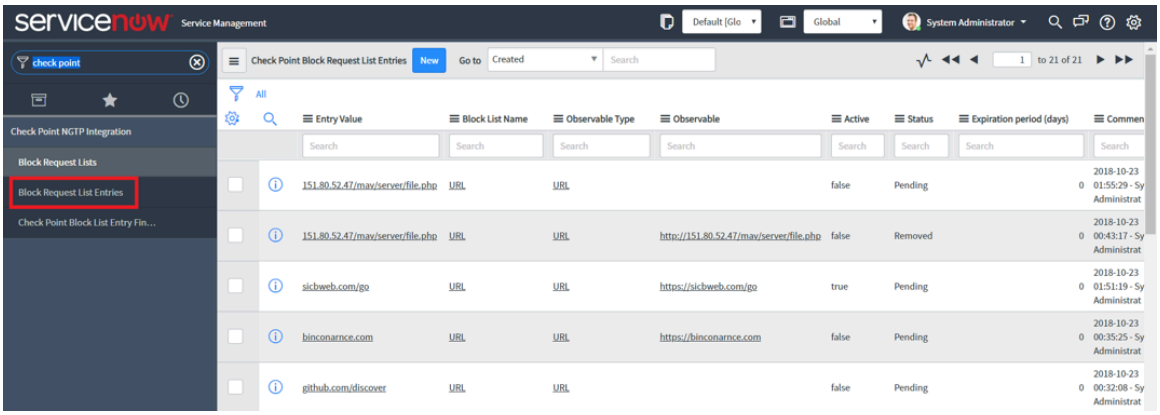
Quando você quiser bloquear um observável que você determinou que é malicioso ou permitir que um observável que você determinou não seja malicioso e o observável não estiver associado a um registro de incidente de segurança específico da Now Platform, envie entradas da Lista de Bloqueios diretamente da lista de bloqueios. Exemplos desses tipos de entradas da Lista de Bloqueios podem ser URLs ou domínios para sites específicos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

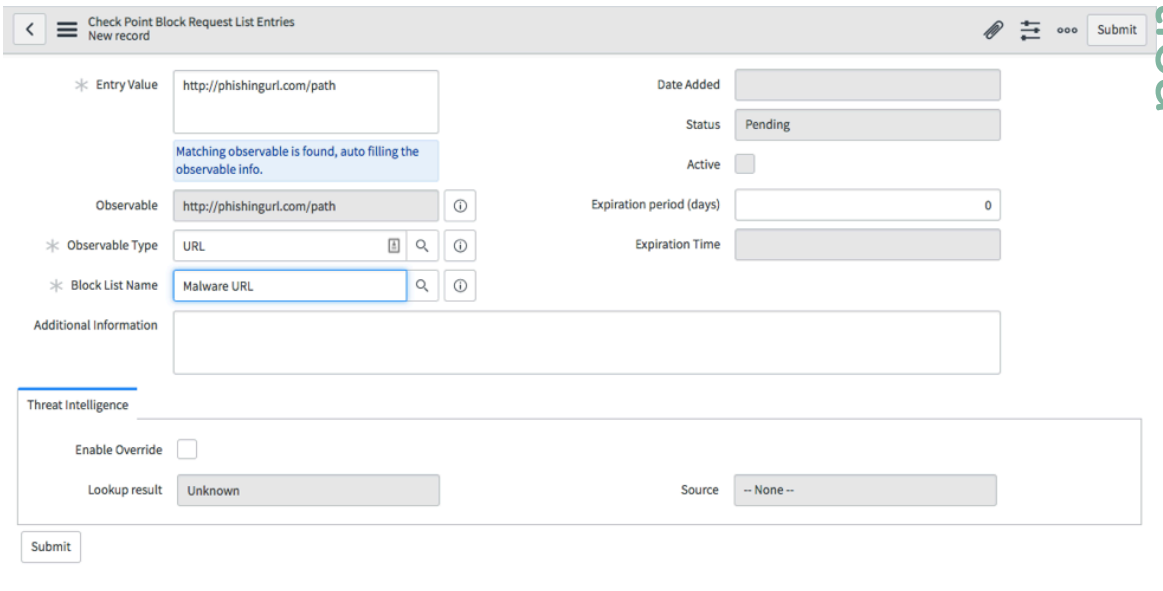
Procedimento

1. Navegar até **Todos** > **Integração de NGTP do Ponto de Verificação** > **Entradas de Solicitação de Bloqueio**.



2. Clique no módulo **Listas de Solicitações de Bloqueio**.
3. Na lista Entradas da lista de solicitações de bloqueio do Check Point, clique em **Novo**.
4. No campo **Valor de entrada**, insira um valor para o seu observável.
   Os dois resultados possíveis desta entrada:
   - Os campos restantes no formulário são preenchidos automaticamente.
   - Um observável correspondente é encontrado e uma mensagem é exibida informando que existe um observável correspondente. Selecione a Lista de Bloqueios à qual você deseja anexar esta entrada e clique em Enviar. Selecione a Lista de Bloqueios à qual você deseja anexar esta entrada antes de definir o período de Expiração.

   Uma mensagem será exibida instruindo você a preencher o formulário. Um observável correspondente não foi encontrado e você deve preencher o formulário. Depois de concluí-la, selecione a Lista de bloqueios à qual você deseja anexar o observável e clique em Enviar. Um registro observável é criado. A figura a seguir mostra um exemplo de um observável de domínio existente e como os campos são preenchidos automaticamente.

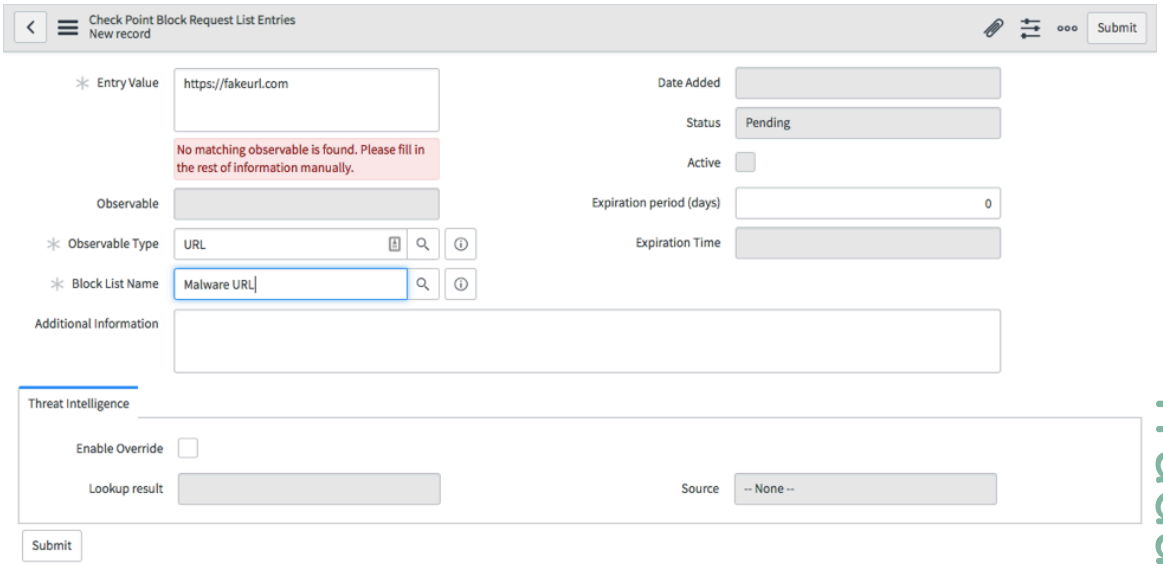


5. Clique no ícone de pesquisa para selecionar a Lista de Bloqueios à qual você deseja anexar a entrada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Enviar**.
7. Se você tiver a aprovação por e-mail configurada em seu fluxo de trabalho, uma solicitação de e-mail de aprovação será enviada.
   Se for exibida uma mensagem solicitando que você preencha o restante das informações manualmente, preencha os campos.



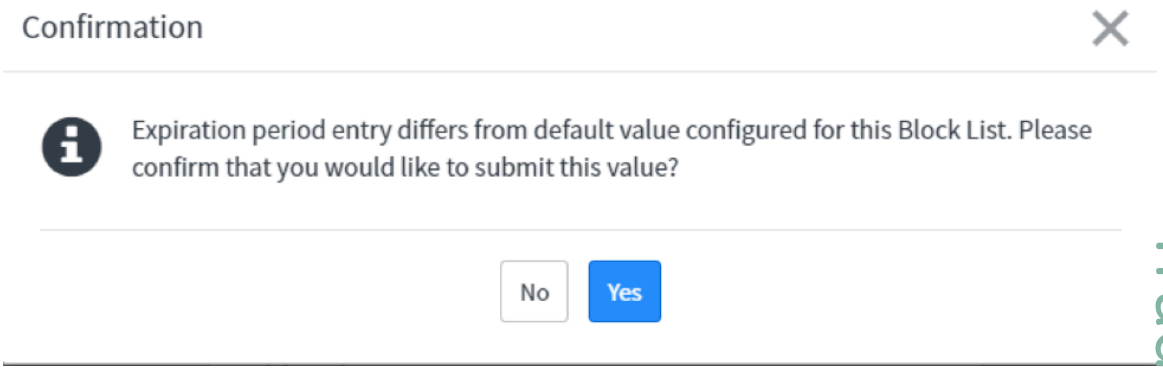
Campo	Descrição
Tipo de observável	Tipo de observável compatível com a caixa de diálogo.
Nome da Lista de Bloqueios	Lista de bloqueios para a qual você deseja a entrada. **Nota:** Selecione a Lista de Bloqueios à qual você deseja anexar a entrada antes de definir o Período de expiração.
Habilitar substituição (o padrão é selecionado)	Origem ou resultado da pesquisa. Quando configurado, permite que você insira um resultado de pesquisa e a origem usada para encontrar os resultados. Esses campos são normalmente preenchidos quando um registro de incidente de segurança é criado. Nesse caso, não há resultado de pesquisa ou origem e você preenche esses campos manualmente.
Resultado da pesquisa	Selecione **Desconhecido** ou **Mal**-intencionado.
Origem	Origem que executa uma pesquisa de ameaça na entrada da Lista de Bloqueios, por exemplo, ThreatCrowd etc.
Período de expiração	O período de expiração herdado da Lista de Bloqueios por padrão. Você pode substituir este valor, mas somente durante a criação da entrada. 0 indica que a entrada da Lista de Bloqueios nunca expira. Se você alterar este valor, esta entrada ficará ativa para o número de dias inseridos. Você pode inserir um valor mínimo de 1 e não há valor máximo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

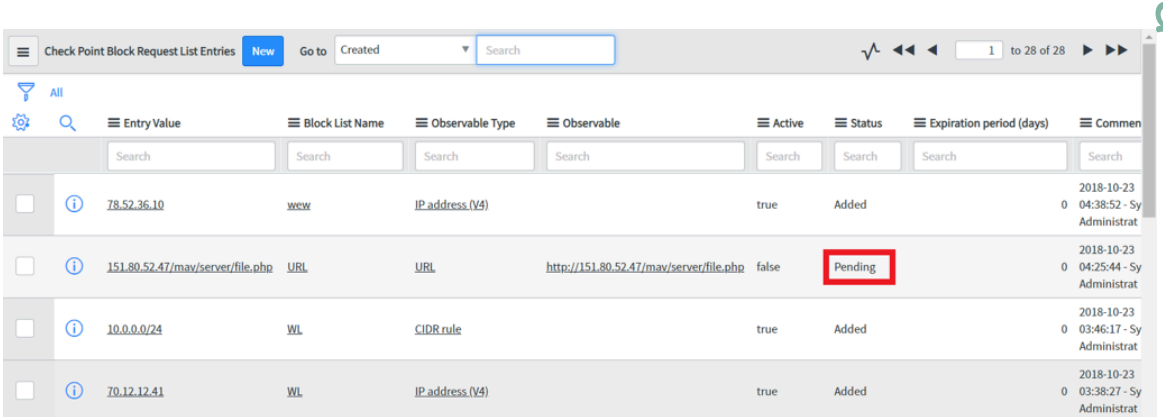
Campo	Descrição
	Por exemplo, se você inserir 30 dias às 14h01 de 1º de maio, a entrada da Lista de bloqueios expirará às 14h01 de 31 de maio. No entanto, o programador verifica se há entradas expiradas às 00:00 todos os dias e muda o estado da entrada para "expirado" às 00:00 de 1º de junho.

8. Clique em **Enviar**.
   Se você alterou o período de expiração padrão da entrada da Lista de bloqueios, uma caixa de diálogo de confirmação de aviso será exibida indicando que o período é diferente da Lista de bloqueios selecionada.



Opção	Descrição
Sim	Confirma sua substituição de expiração, salva o registro e retorna para as Entradas da Lista de Bloqueios do Ponto de Verificação. Se você tiver a aprovação por e-mail configurada em seu fluxo de trabalho, uma solicitação de e-mail de aprovação será enviada.
Não	Cancela a substituição. Neste ponto, você pode alterar o valor do **período de expiração**. Depois de alterar o valor, clique em Enviar para retornar à lista Entradas de bloco do ponto de verificação.

9. Se não for exibido, navegue até **Check Point Block Request List Entries**e observe que o status da entrada é **Pendente**.



A entrada está pronta para aprovação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aprovar entradas da lista de bloqueios para a integração Check Point NGTP

Um processo de aprovação para entradas da Lista de bloqueios faz parte do fluxo de trabalho pré-configurado. Você aprova as entradas da Lista de Bloqueios antes que as entradas sejam ativadas nas Listas de Bloqueios. Depois de aprovar a entrada da Lista de bloqueios, o gateway recupera a entrada e seu observável é bloqueado a partir desse ponto.

Antes de Iniciar

- A aprovação de entradas da Lista de bloqueios é atribuída ao Administrador de incidentes de segurança (sn_si.admin) por padrão, mas essa autoridade pode ser atribuída conforme exigido pela sua organização. No exemplo a seguir, o administrador da Now Platform tem autoridade de aprovação.

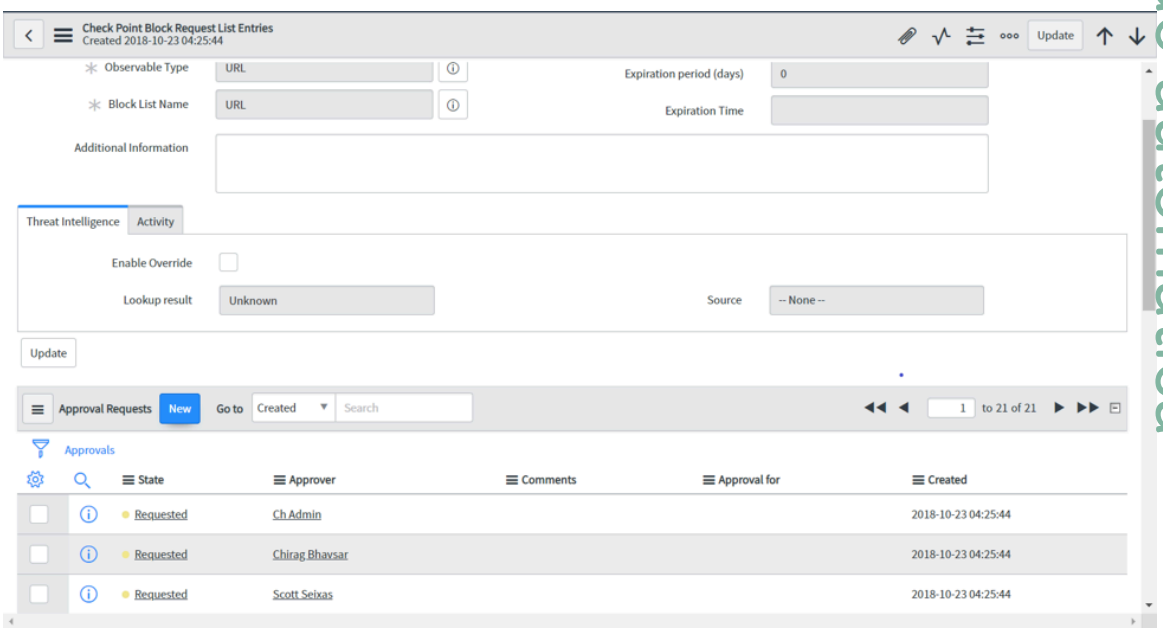
Função necessária: sn.si.admin

Por Que e Quando Desempenhar Esta Tarefa

Quando o processo de aprovação está habilitado, uma entrada da Lista de bloqueios não é ativada ou desativada na Lista de bloqueios até que seja aprovada.

Procedimento

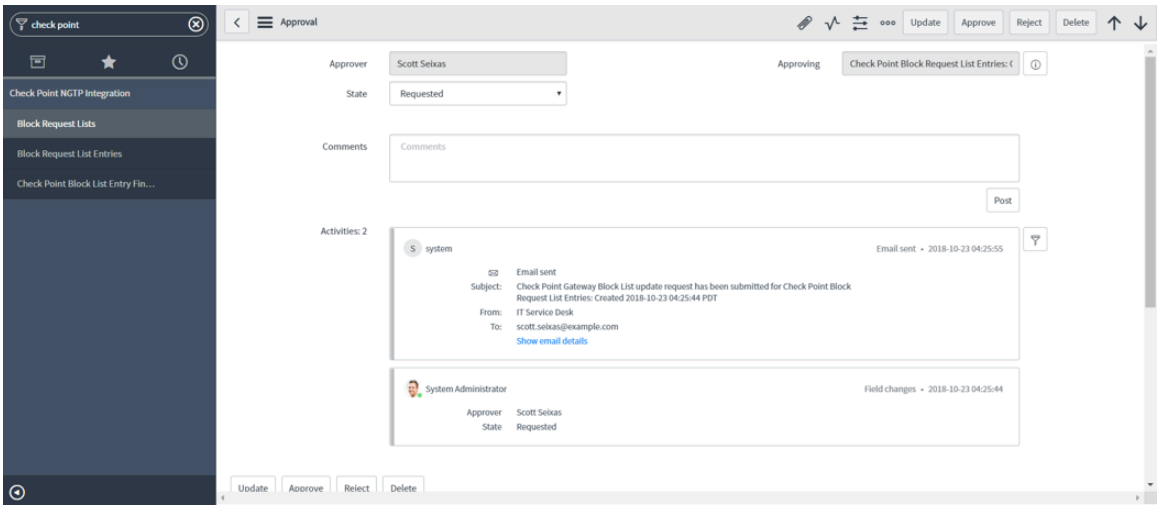
1. Navegar até **Todos** > **Integração de NGTP do Ponto de Verificação** > **Bloquear Entradas da Lista de Solicitações**e abra o registro de Entrada da Lista de Bloqueios.
2. No registro de entrada da lista de bloqueios, role até a seção **Solicitações de aprovação**.



3. Em Solicitações de aprovação, clique em um item na coluna **Estado** para abri-lo.
   O registro de aprovação é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



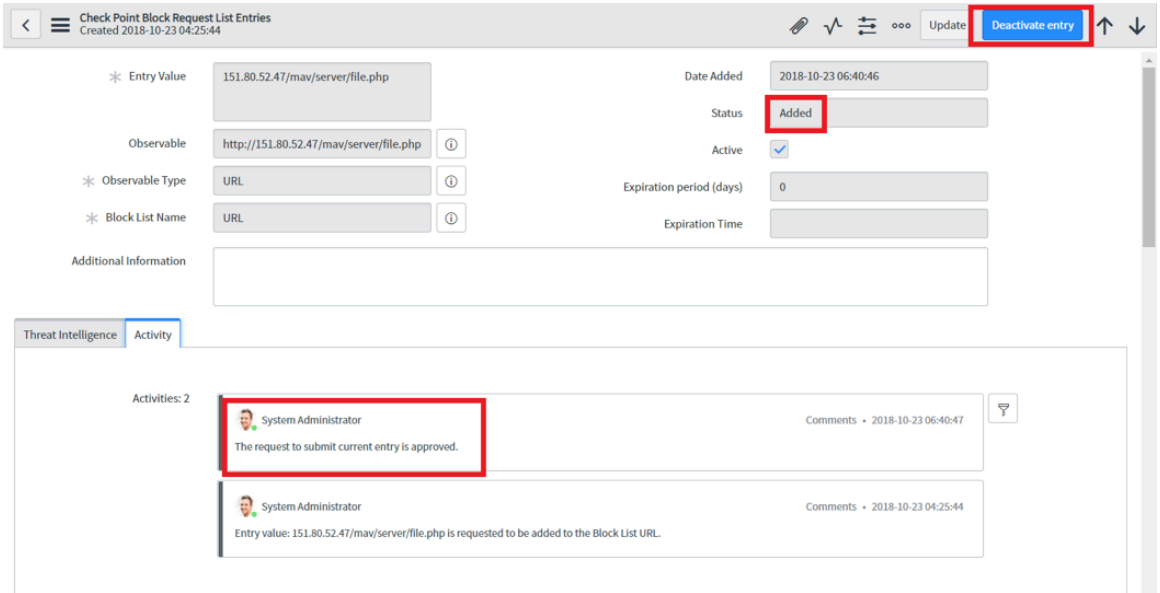
4. Escolha uma opção para aprovar a entrada da Lista de Bloqueios.

Opção	Descrição
Aprovar	No registro de entrada, o campo Status muda para Adicionado e a caixa de seleção Ativo é marcada. O botão Desativar é exibido e ativo. As anotações de trabalho mostram que a solicitação da entrada da Lista de bloqueios foi aprovada.
Rejeitar	No registro de entrada, o campo Status muda para Rejeitado e a caixa de seleção Ativo é desmarcada, indicando que a entrada não está bloqueada no Gateway. As anotações de trabalho mostram que a solicitação da entrada da Lista de bloqueios foi rejeitada.

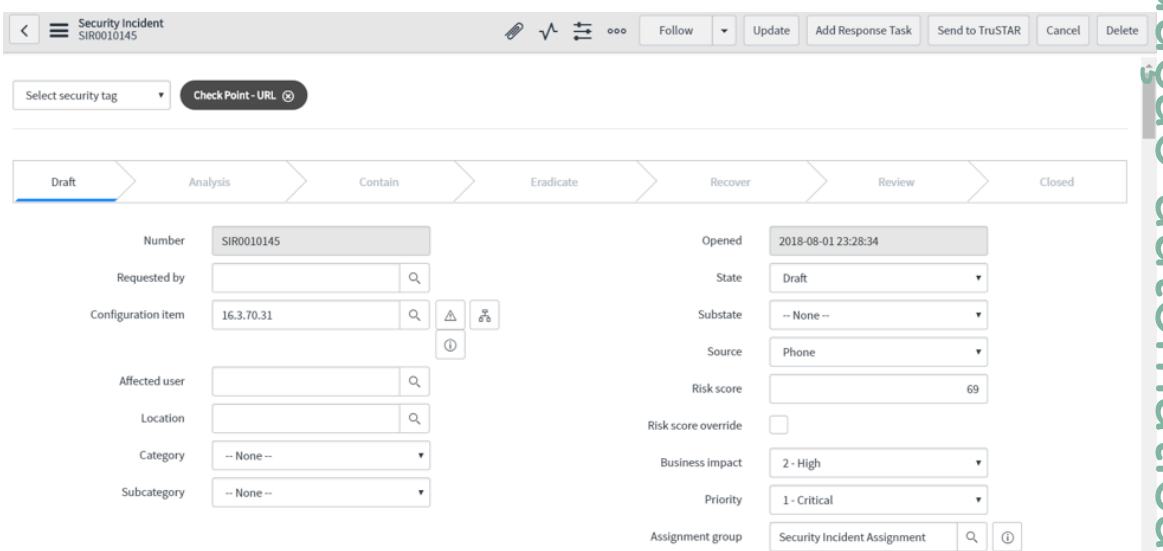
Depois de aprovar a entrada da Lista de Bloqueios e ativá-la, o firewall de última geração do Check Point recupera a entrada da Lista de Bloqueios após o próximo intervalo de recuperação. Depois que a entrada é recuperada, o observável é bloqueado desse ponto em diante. Na figura a seguir, observe que a caixa de seleção Ativa está marcada, o status é Adicionado e as anotações de trabalho indicam que a solicitação foi aprovada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



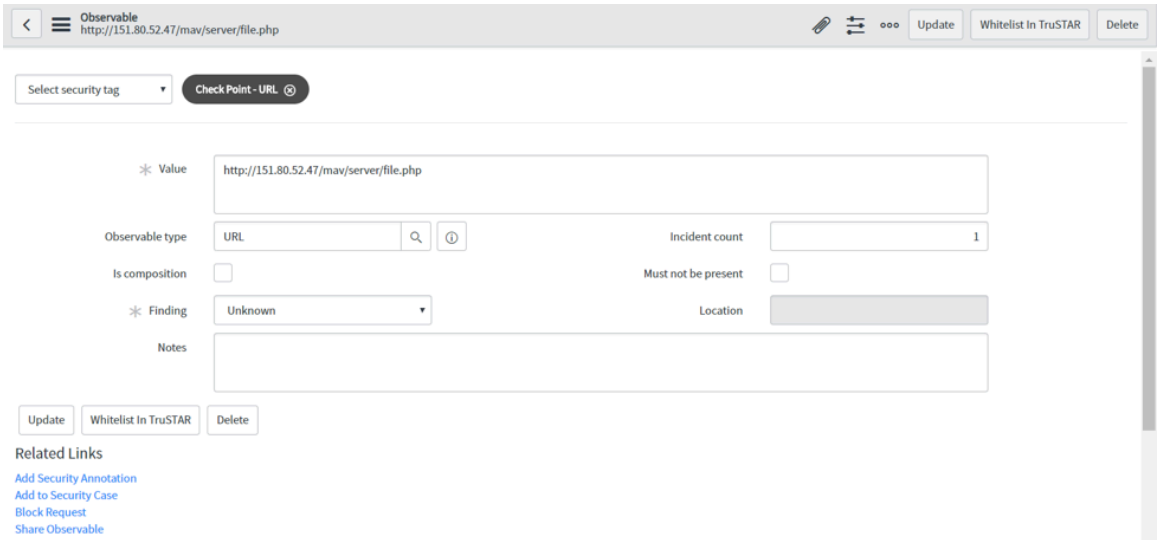
Depois que a entrada da Lista de bloqueios é aprovada e ativada, o registro do incidente de segurança é marcado com um marcador de segurança. O marcador é exibido na parte superior do registro.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O marcador de segurança também é exibido no registro observável.



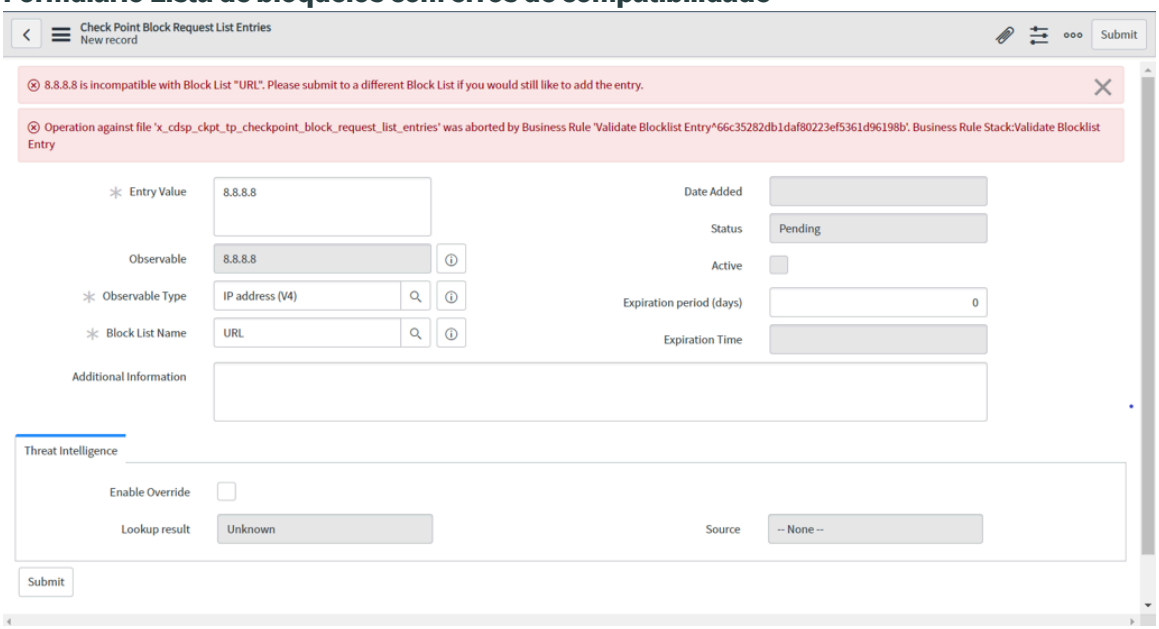
Exceções de entrada da lista de bloqueios para a integração Check Point NGTP

Há restrições para adicionar entradas da Lista de Bloqueios às Listas de Bloqueios. Se houver conflitos duplicados, de compatibilidade ou de CIDR (roteamento entre domínios sem classe) ao tentar adicionar entradas da Lista de bloqueios às Listas de bloqueios, serão exibidas mensagens de erro que ajudarão a resolver esses erros.

Exceção de compatibilidade

Cada lista de bloqueios aceita somente entradas compatíveis com seu tipo de observável. Se você criar uma Lista de Bloqueios de Domínio e tentar anexar um endereço IP observável a ela, uma mensagem de erro incompatível será exibida. Por exemplo, uma lista de bloqueios de domínio só pode aceitar observáveis de domínio, conforme ilustrado na figura a seguir.

Formulário Lista de bloqueios com erros de compatibilidade

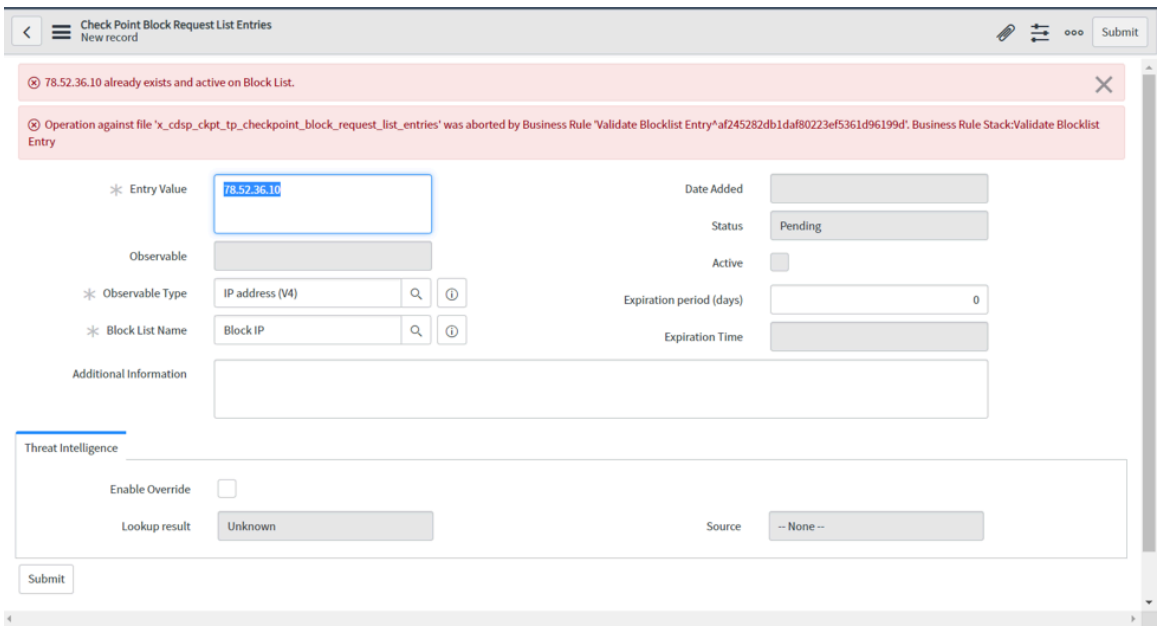


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

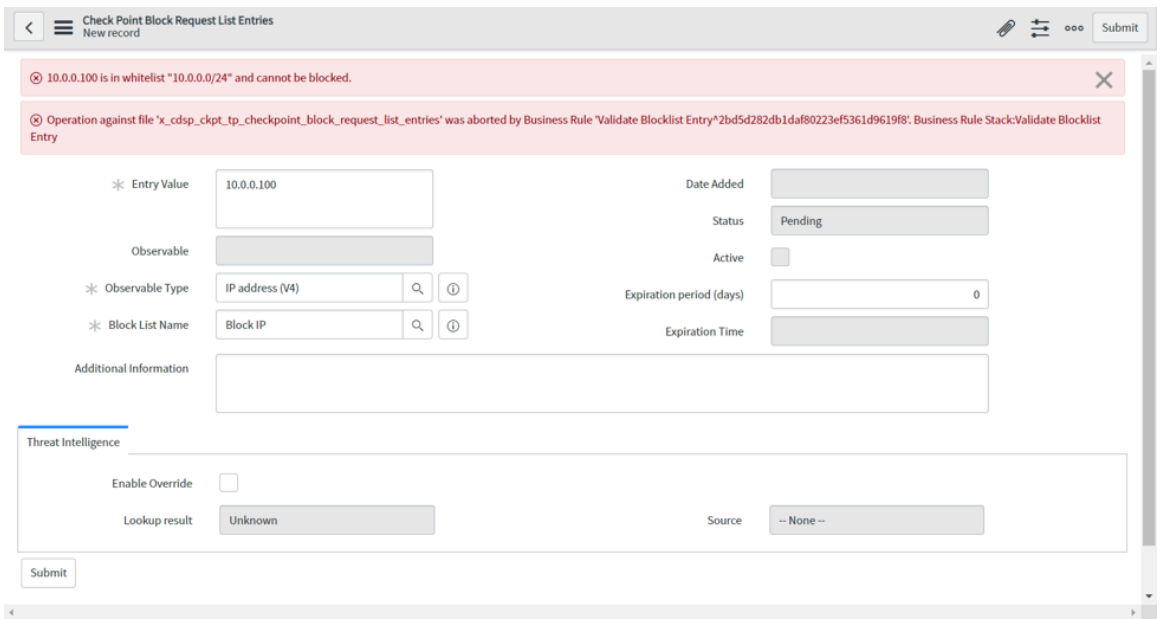
Exceção de duplicação

Um observável não pode ser ativado em várias Listas de bloqueios do mesmo tipo de observável. Se um observável de URL já estiver ativado em uma Lista de Bloqueios de URL e você tentar ativar o mesmo observável em uma Lista de Bloqueios de URL de Phishing, uma mensagem de erro de duplicação será exibida.



Exceção de CIDR (roteamento entre domínios sem classe)

Se você tentar anexar um único endereço IP a uma lista de permissões e esse endereço IP fizer parte de um observável CIDR que já está em uma Lista de bloqueios/Lista de permissões, um erro de conflito de CIDR será exibido. Este erro indica que o único endereço IP já está incluído na lista de bloqueios ou na lista de permissões como parte do observável CIDR. Por exemplo, 192.168.24.25 faz parte do bloco CIDR 192.168.0.0/22.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Editar o nome do marcador de segurança para a integração Check Point NGTP

Se a caixa de seleção Exibir marcador estiver marcada ao criar o registro da Lista de Bloqueios, você poderá editar os nomes e as cores dos marcadores de segurança. Os marcadores de segurança ajudam a rastrear observáveis que já estão bloqueados.

Antes de Iniciar

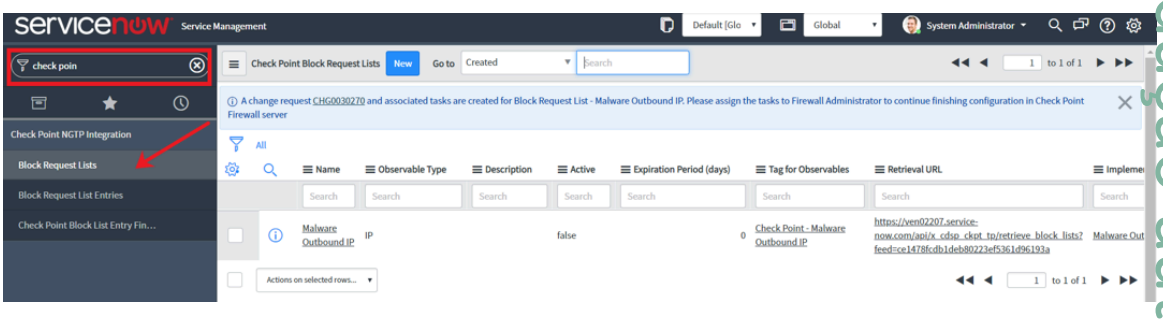
Função necessária: sn.si.admin

Por Que e Quando Desempenhar Esta Tarefa

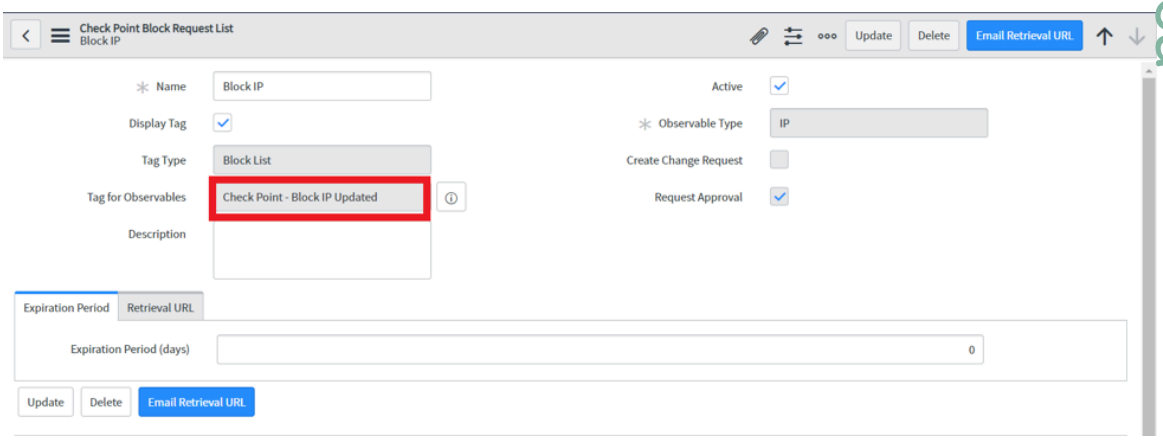
Os marcadores de segurança ajudam a identificar rapidamente quais incidentes de segurança têm observáveis em uma lista de bloqueios. Os marcadores também ajudam a identificar se um observável já está bloqueado ou se foi removido de uma Lista de Bloqueios. Por padrão, a cor do marcador de segurança é preta para entradas da lista de bloqueios e cinza para entradas da lista de permissões. Você pode mudar os nomes e as cores dos marcadores para ajudá-lo a reconhecer determinados marcadores com mais facilidade.

Procedimento

1. Navegar até **Todos** > **Integração de NGTP do Ponto de Verificação** > **Configuração da Lista de Solicitações de Bloqueio**.



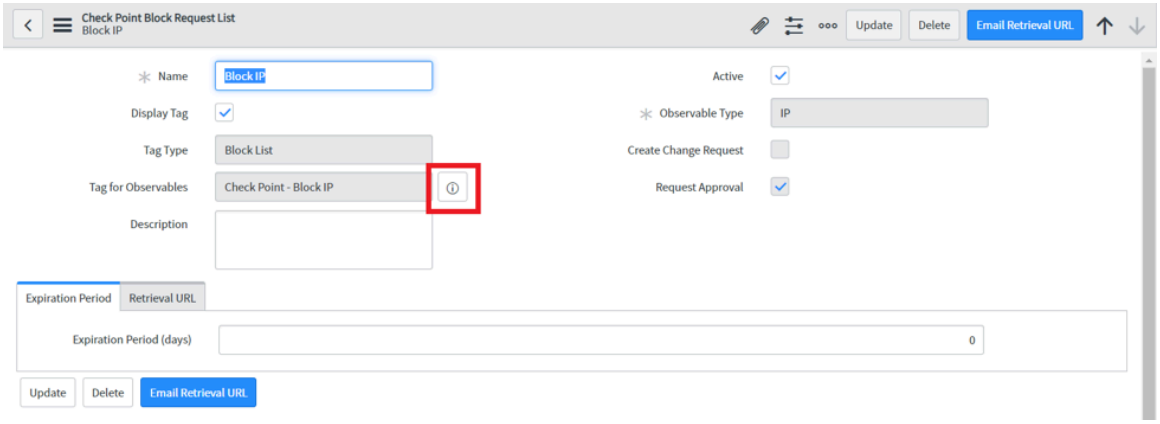
2. Clique em um item na coluna **Nome** para abri-lo.
   O registro da Lista de Bloqueios é exibido. Por padrão, o nome do marcador de segurança é o mesmo valor que você inseriu no campo Nome da Lista de Bloqueios ao criá-lo. Por padrão, o nome também inclui um prefixo de Lista de bloqueios, por exemplo, Lista de bloqueios - URLs maliciosos de malware.



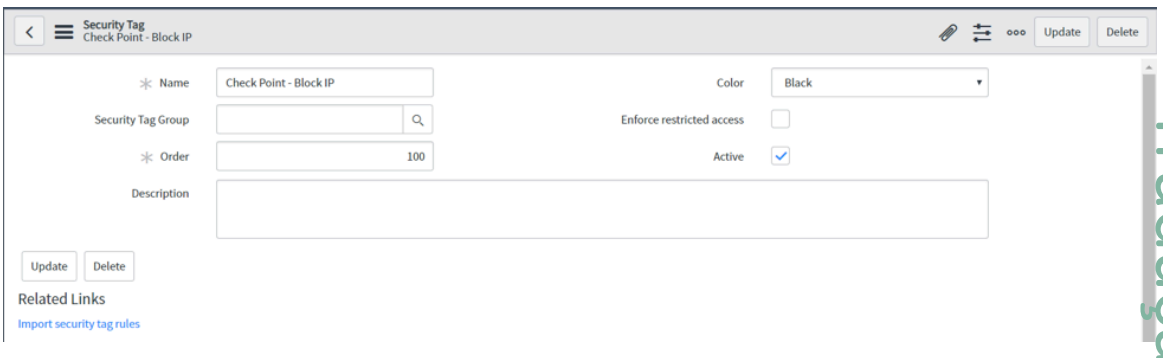
3. Clique no ícone de informações ao lado do marcador de observáveis e em Abrir registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

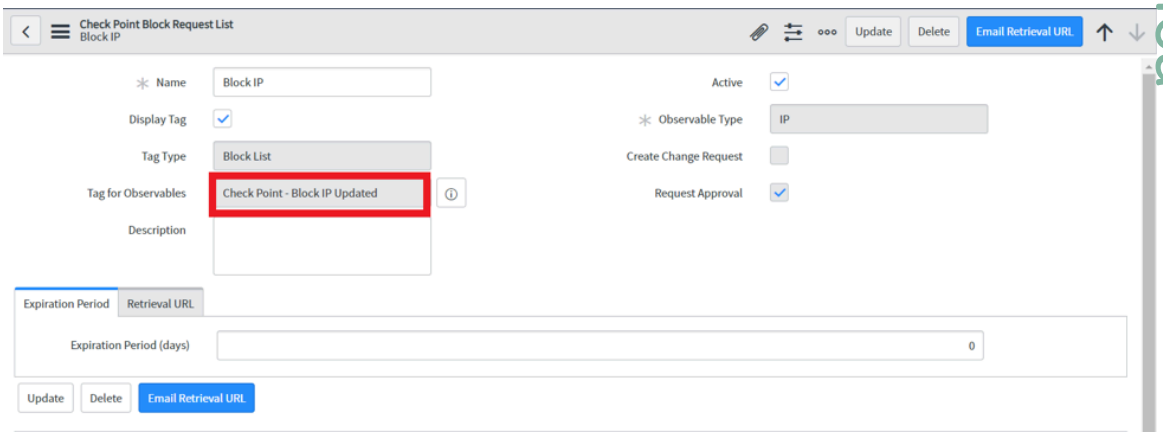


O formulário de marcador de segurança é exibido.



4. No campo **Nome**, modifique o nome do marcador de segurança.
5. Clique em **Atualizar**.
   O registro da Lista de bloqueios atualizado é exibido com o nome do marcador modificado.

Nota:
No exemplo a seguir, Saída foi adicionada ao nome do marcador. Mantenha o prefixo do Check Point no novo nome do marcador para ajudá-lo a identificar que o marcador está associado à integração de firewall de última geração do Check Point.

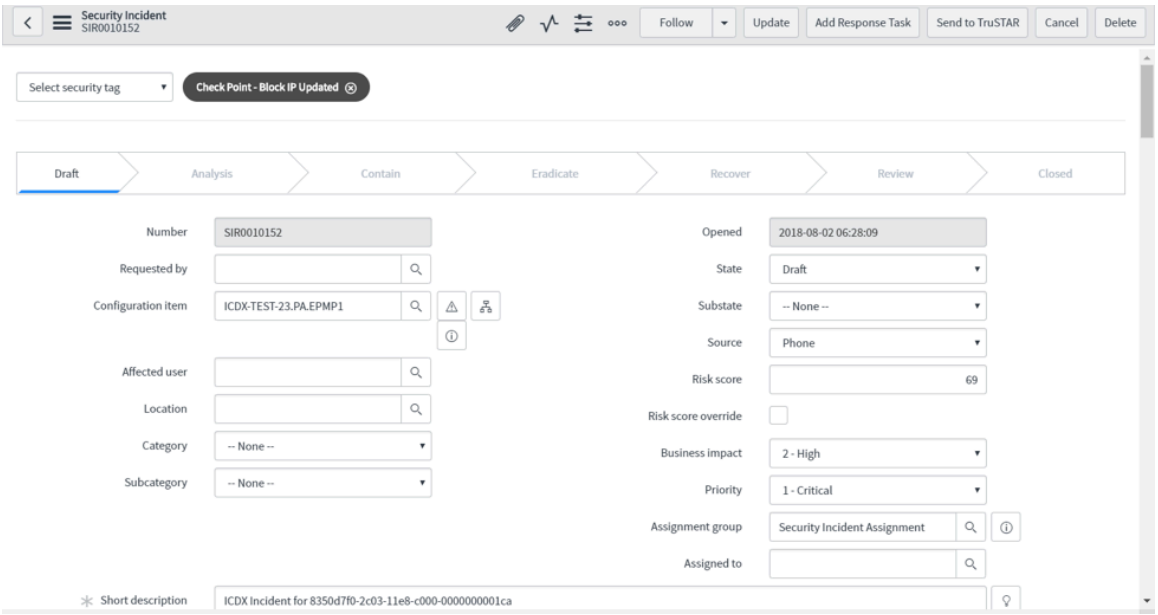


Os marcadores de segurança são exibidos para cada tipo de observável (IP, URL, domínio) no registro de Incidente de segurança e no registro de Observável sempre que esse observável é adicionado à Lista de bloqueios.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado



Se um observável já tiver sido adicionado a uma Lista de bloqueios e um marcador de segurança for exibido em um incidente de segurança para esse observável, o marcador de segurança da Lista de bloqueios também será exibido automaticamente em todos os registros de incidente de segurança subsequentes que forem criados. Essa duplicação informa que o observável já está em uma lista de bloqueios. Você não precisa adicionar este observável e bloqueá-lo novamente.

Quando um observável não está mais bloqueado, um marcador de segurança não é exibido no registro do incidente de segurança ou no registro do observável. Nesta instância, nenhum marcador de segurança indica que a data de expiração do observável pode ter passado ou que o observável foi desabilitado de uma lista de bloqueios.

Desinstalar a integração Check Point NGTP

Se você quiser desinstalar a integração Check Point NGTP da sua instância da Now Platform e remover todos os resquícios da integração, consulte o site de documentação da ServiceNow para obter instruções sobre como desinstalar aplicações.

Antes de Iniciar
Função necessária: administrador

Integração do CrowdStrike Falcon Host

A integração CrowdStrike Falcon Host permite que você insira observáveis em um incidente de segurança em uma lista de observação, tornando-os capazes de gerar alertas adicionais. Esta integração é uma implementação do fluxo de trabalho CrowdStrike Falcon Host - Publicar na lista de observação.

Explorar Integrações do Security Incident Response	Configurar Introdução à integração CrowdStrike Falcon Host
Usar	Desenvolver

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

• Realizar pesquisas em observáveis • Atividade Publicar na lista de observação	• ServiceNow Security Operations diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Faça ou responda perguntas na comunidade do Security Operations • Pesquise artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Introdução à integração CrowdStrike Falcon Host

O recurso Configuração de integração permite que você ative e configure rapidamente integrações de segurança de terceiros, incluindo a integração CrowdStrike Falcon Host. Antes de usar a integração CrowdStrike Falcon Host, você deve baixá-la do ServiceNow Store e adicionar um nome de usuário e senha.

Antes de Iniciar

- Se você estiver atualizando a integração CrowdStrike Falcon Host de uma versão anterior, deverá excluir a configuração existente e definir uma nova configuração. A nova integração oferece suporte à autenticação OAUTH2. Esta atualização requer que você insira o **ID do cliente** da **API e o segredo do cliente** da API para autenticar e concluir a configuração.
- Nos CrowdStrike Falcon Host**Escopos de API**do portal, habilite a configuração de **Leitura** e **Gravação** para **IOCs (Indicadores de compromisso)**.

Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Security Operations** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão CrowdStrike Falcon Host, clique em **Configurar**.
4. No formulário, preencha os campos para concluir a configuração:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração do CrowdStrike Falcon Host

Campo	Descrição
Nome	Nome da integração, por exemplo, `demo-1`.
ID do cliente da API	O ID de cliente que você obtém na seção de configurações do perfil da sua conta no portal CrowdStrike Falcon Host.
Segredo do cliente de API	A chave secreta do cliente que você obtém na seção de configurações do perfil da sua conta no portal CrowdStrike Falcon Host.

5. Clique em **Enviar**.

Resultado

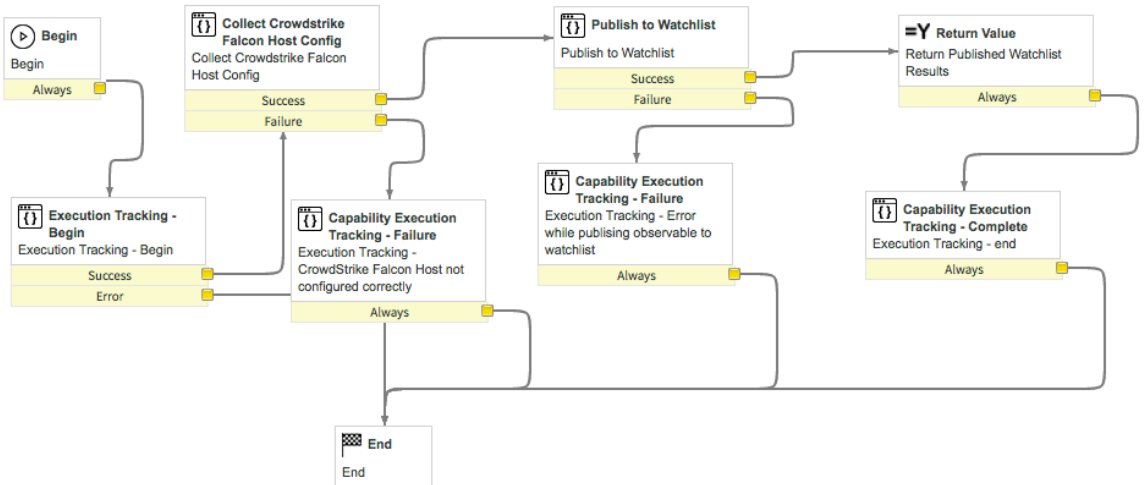
Depois de configurada, a integração CrowdStrike Falcon Host pode ser selecionada para publicar observáveis em listas de observação em Security Incident Response.

CrowdStrike Falcon Host do Security Operations – Fluxo de trabalho de Publicar na lista de observação

O fluxo de trabalho **CrowdStrike Falcon Host do Security Operations - Publicar** na lista de observação é usado para especificar a lista de observação para gerar alertas ou eventos. Os alertas e eventos são exibidos no sistema CrowdStrike Falcon Host com base em como ele está configurado.

Fluxo de trabalho Publicar na lista de observação

Este fluxo de trabalho é acionado pelo Integração do Security Operations - Capacidade de publicar na lista de observação quando você seleciona um ou mais observáveis associados a um incidente de segurança e usa a ação de IU Publicar na lista de observação para enviar os observáveis para uma lista de observação. Os observáveis podem ser usados para gerar alertas adicionais. Para obter mais informações, consulte Publicar observáveis em uma lista de observação de terceiros.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividades específicas para esta integração são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Atividade Coletar configurações do CrowdStrike Falcon Host

A atividade de fluxo de trabalho **Coletar configurações do CrowdStrike Falcon Host** reúne informações de configuração para usar no fluxo de trabalho.

A **atividade Coletar configuração do CrowdStrike Falcon Host** pode ser usada com qualquer fluxo de trabalho para coletar as definições de configuração do CrowdStrike Falcon Host.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida. .
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
user_name	Nome de usuário do CrowdStrike Falcon Host
password	Senha do CrowdStrike Falcon Host

Atividade Publicar na lista de observação

A atividade de fluxo de trabalho **Publicar na lista de** observação insere observáveis em um incidente de segurança em uma lista de observação para gerar alertas ou eventos. Os alertas e eventos são exibidos no sistema CrowdStrike Falcon Host com base em como ele está configurado.

A atividade **Publicar na lista** de observação pode ser usada com qualquer fluxo de trabalho para publicar observáveis em uma lista de observação.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida. .
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
observáveis	A lista de observáveis de Security Incident Response.
user_name	O nome de usuário do indivíduo responsável pela integração do CrowdStrike Falcon Host.
password	A senha do indivíduo responsável pela integração do CrowdStrike Falcon Host.
task_sys_id	O identificador do sistema para este trabalho de publicação na lista de observação.
capacidadeExecutionId	O nome da capacidade associada.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status	O status da atividade de publicação.

CrowdStrike Falcon Insight para integração Security Operations

Com a integração CrowdStrike Falcon Insight para Security Operations, você pode fazer ações de correção nos endpoints em tempo real, usar perfis para coletar detalhes sobre o host e fazer consultas ou ações específicas no endpoint usando o produto Now Platform Security Incident Response.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

A integração CrowdStrike Falcon Insight para Security Operations funciona com o Now Platform para que você possa obter informações adicionais sobre o escopo de um incidente. O CrowdStrike Falcon Insight captura todas as atividades de evento de endpoint relevantes. Você pode usar o Now Platform para se concentrar em investigações e ações de correção.

Conheça esta integração

Identificador de documento	Título do documento
ServiceNow site da documentação do produto	Site de documentação do produto da ServiceNow
CrowdStrike Falcon Insight para Security Operations	Introdução à integração CrowdStrike Falcon Insight

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Introdução à integração CrowdStrike Falcon Insight

Você pode ativar e configurar o CrowdStrike Falcon Insight para interagir com sua instância [Now Platform e produto Security Incident Response.

Antes de Iniciar

Função necessária: administrador

Antes de usar CrowdStrike Falcon Insight para a integração Security Operations, você deve baixá-lo do ServiceNow Store.

Por Que e Quando Desempenhar Esta Tarefa

Check-list

Configuração de tarefa	Descrição
Atribua e verifique as funções Now Platform e Security Incident Response.	Essas funções são necessárias para configuração e verificação dos resultados esperados: • A função de administrador instala a integração do ServiceNow Store e atribui a função sn_si.admin. • A função sn_si.admin configura a integração, cria e ativa perfis e, em seguida, atribui a função sn_si.analyst. • A função sn_si.analyst responde a incidentes de segurança, inicia perfis manualmente e pode enviar solicitações para ações como isolar o host e remover o isolamento do host para um grupo aprovado.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de configurar esta integração.	O plug-in ServiceNow IntegrationHub Enterprise Pack Installer [com.glide.hub.integrations.enterprise] é necessário. Este plug-in permite a execução de ações e fluxos do IntegrationHub: O plug-in Security Incident Response (com.snc.security_incident) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar os outros aplicativos Security Operations que são necessários para a integração. Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se essas aplicações ainda não estiverem instaladas, você deverá instalar e ativar cada aplicação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	uma de cada vez na seguinte ordem para garantir uma instalação sem problemas: **1.** Security Incident Response Dependência (com.snc.si_dep) **2.** Security Integration Framework **3.** Security Support Common **4.** Orquestração de suporte de segurança **5.** Inteligência contra ameaças Suporte Comum **6.** Trusted Security Circles **7.** Security Operations Assistente de configuração **8.** Security Incident Response
Configure um grupo de aprovação.	Uma capacidade de aprovação opcional está disponível para isolar máquinas host, restaurá-las para a rede e iniciar pesquisas de vistas. Para habilitar esta opção, você precisa de aprovação prévia da função sn_si.admin antes que as máquinas host sejam isoladas e restauradas em sua rede ou quando as pesquisas de vistas forem realizadas. Se você precisar de um nível extra de controle sobre essas ações, habilite a opção **Requer aprovação** ao configurar o perfil. A autoridade de aprovação é atribuída ao usuário com a função sn_si.admin. Você também pode reatribuir esta autoridade de aprovação a um grupo de aprovação.
Atribua e verifique as funções da plataforma CrowdStrike Falcon.	As funções a seguir são necessárias na plataforma CrowdStrike Falcon para a configuração de integração: • A função de administrador do Falcon é necessária para exibir, criar ou modificar clientes ou chaves de API. • A função de Respondente em tempo real - Administrador é necessária para criar e executar scripts personalizados. • A função de Respondente em tempo real - Respondente ativo é necessária para criar e executar scripts personalizados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Verifique se as funções e permissões de scripts personalizados estão habilitadas na plataforma CrowdStrike Falcon.	Esta integração usa scripts personalizados do CrowdStrike para alguns dos recursos de aprimoramento. • Verifique se as funções de Respondente em tempo real - Administrador e Respondente em tempo real - Respondente ativo estão disponíveis. • Verifique se a opção **de política Padrão (Windows)** está habilitada em Configuração > Políticas de resposta na IU do CrowdStrike Falcon. • Verifique se a **resposta em tempo real** e **os scripts personalizados** na funcionalidade em tempo real estão habilitados na IU do CrowdStrike Falcon.
Gere clientes de API e chaves na CrowdStrike Falcon Platform.	Crie clientes ou chaves de API do CrowdStrike na plataforma CrowdStrike Falcon para usar na configuração de integração Now Platform.

Criar cliente de API do CrowdStrike e gerar chaves

Crie o cliente da API do CrowdStrike e gere o ID e a chave do cliente, que você usa para configurar a integração CrowdStrike Falcon Insight.

Antes de Iniciar

Função necessária: administrador do CrowdStrike Falcon

Procedimento

1. Na plataforma CrowdStrike Falcon, navegue até **API Clients and Keys**.
2. Na tabela Clientes de API do OAuth2, clique em **Adicionar novo cliente de API**.
3. Insira os seguintes detalhes para definir seu cliente de API:

Campo	Descrição
Nome do cliente	Insira o nome do cliente. Este campo é obrigatório.
Descrição	Insira a descrição do nome do cliente.
Escopos de API	É necessário definir os escopos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Importante: Certifique-se de habilitar a conta da API e de que os seguintes escopos estejam habilitados para a conta da API: ○ Habilitar escopos de leitura e gravação para API de hosts ○ Habilitar escopo de leitura para API de indicadores

4. Clique em **Adicionar** para salvar o cliente de API e gerar o ID do cliente e a chave secreta.

Instalar e configurar CrowdStrike Falcon Insight

Instale e configure a aplicação CrowdStrike Falcon Insight para Security Operations da ServiceNow Store na sua instância Now Platform.

Antes de Iniciar

Função necessária: administrador

Nota:
Você pode associar uma capacidade a apenas um perfil. Você não pode associar uma capacidade a vários perfis. Ao configurar os servidores do CrowdStrike, você não pode reutilizar uma funcionalidade do CrowdStrike com vários perfis que compartilham o servidor do CrowdStrike. Seus perfis podem ter o mesmo recurso do CrowdStrike. Cada perfil deve usar seu próprio servidor CrowdStrike.

Procedimento

1. Baixe o CrowdStrike Falcon Insight para integração do Security Operations do ServiceNow Store e instale-o.
2. Navegar até **Security Operations** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco de integração CrowdStrike Falcon Insight para Security Operations e clique em **Configurar**.
4. No formulário, preencha os campos para concluir a configuração:

Configuração do CrowdStrike Falcon Insight

Campo	Descrição
Nome	Nome da integração, por exemplo, `demo-1`.
URL da API do CrowdStrike Falcon Insight	URL base que hospeda a API do CrowdStrike. Insira o URL com o protocolo HTTPS. Por exemplo, https://api.crowdstrike.com.
ID de cliente	O ID do cliente que você obtém na seção de configurações do perfil da sua conta no portal CrowdStrike Falcon Insight.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Segredo do Cliente	A chave secreta do cliente que você obtém na seção de configurações do perfil da sua conta no portal CrowdStrike Falcon Insight.

5. Clique em **Enviar**.

Resultado

Depois que a integração é validada e enviada com sucesso, ela é salva na página Integrações de segurança como um bloco. Você pode exibir o módulo CrowdStrike Falcon Insight no navegador de aplicações.

Criar um grupo de aprovação

Crie um grupo de aprovação para a integração CrowdStrike Falcon Insight para Security Operations que pode aprovar solicitações para isolar máquinas host, restaurá-las para a rede e iniciar pesquisas de vistas.

Antes de Iniciar

Você não pode reatribuir a autoridade de aprovação a um grupo, a menos que um grupo de aprovação esteja disponível em sua instância.

Nota:
A opção de aprovações na configuração do perfil aparece somente para as capacidades Isolar Host e Remover Isolamento de Host.

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Grupos**.
2. Na lista de grupos, clique em **Novo**.
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de grupo de aprovação

Campo	Descrição
Nome	Nome do grupo que você vê ao enviar uma solicitação de aprovação.
E-mail do grupo	Lista de distribuição de e-mail do grupo ou o endereço de e-mail do ponto de contato, como o gerente do grupo.
Gerente	Nome do gerente do grupo. Clique no ícone de pesquisa para exibir a lista.
Primário	Nome do grupo primário, se associado a um primário.
Tipo	Categorias de grupos.
Fornecedores	vendor_manager que você atribui aos usuários no processo de gestão de fornecedores da sua organização.
Descrição	Informações adicionais sobre o grupo.

4. Clique em **Enviar**.
   O novo grupo é exibido na lista Grupos.

   Este grupo está disponível para processar solicitações quando você habilita a opção **Requer aprovação** durante a configuração deste perfil.

   Para monitorar e processar solicitações enviadas por usuários com a função sn_si.analyst, cada membro do grupo de aprovação navega até a guia **Minhas aprovações** no Now Platform.

O que Fazer Depois

A próxima etapa é instalar e configurar a aplicação CrowdStrike Falcon Insight da ServiceNow Store.

Criar um perfil de capacidade para a integração CrowdStrike Falcon Insight

Crie um perfil e selecione os recursos CrowdStrike Falcon Insight que você deseja que o perfil execute.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Considere por que você deseja criar um perfil antes de adicionar recursos CrowdStrike Falcon Insight a ele. A tabela a seguir lista os recursos que você deve adicionar a um perfil quando quiser que o perfil execute determinadas consultas ou ações.

Você pode criar um único perfil que executa consultas para obter detalhes do sistema, lista usuários conectados, busca serviços em execução, busca processos em execução, busca estatísticas de rede, isola o host e remove o host isolado. Como alternativa, você pode criar vários perfis, cada um com seu próprio recurso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
As capacidades Isolar host, remover isolamento e obter arquivo não podem ser mescladas com nenhuma outra capacidade ao criar um perfil.

Tipos de perfil e capacidades necessárias do CrowdStrike Falcon Insight

Finalidade do perfil	Recursos do CrowdStrike
Reunir detalhes do host e usuários conectados	• **Obter detalhes do host** • **Obter usuários conectados**
Buscar as estatísticas de rede, processos e serviços em execução para um host	• **Obter Estatísticas de Rede** • **Obter processos em execução** • **Obter serviços em execução**
Isolar um host	**Isolar Host**
Remover isolamento de um host	**Remover isolamento**
Obter um arquivo de um endpoint de host	**Obter arquivo**

Procedimento

1. Navegar até **Todos** > **Integração com CrowdStrike Falcon Insight** > **Perfis de capacidade do CrowdStrike**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

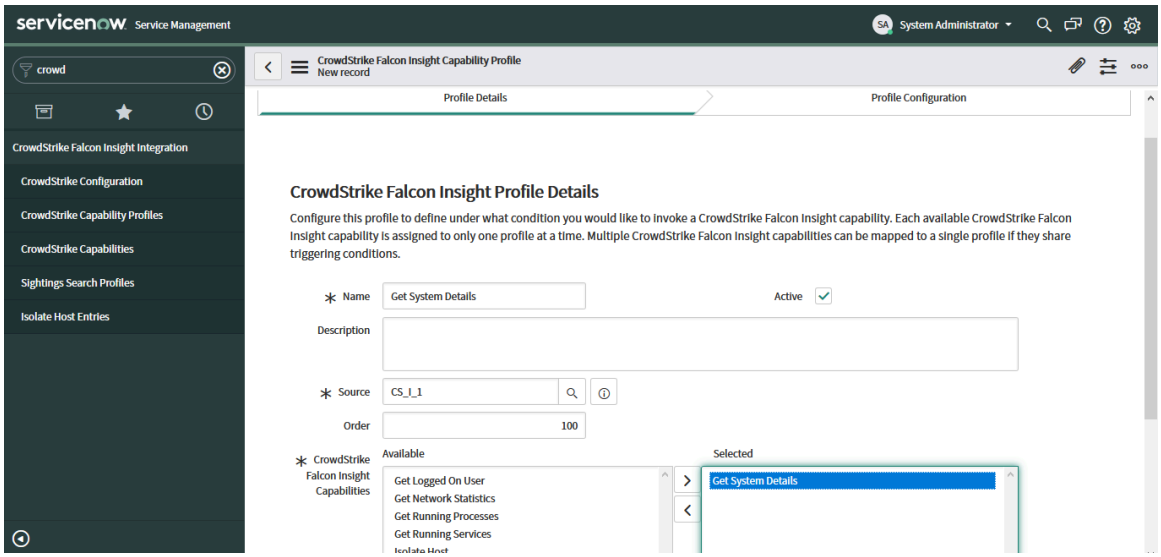
Campo	Descrição
Nome	Nome do novo perfil de recurso. Este nome ajuda a identificar o tipo de perfil e também é o nome padrão do marcador de segurança associado a este perfil.
Ativo	Indica se o perfil está ativo ou não. Quando o perfil está ativo, ele é acionado automaticamente quando um incidente de segurança é criado que corresponde às condições de filtragem que você especificou na configuração.
Descrição	Descrição exclusiva do perfil de recurso.
Origem	Nome do servidor. Você só pode exibir os servidores configurados anteriormente na lista.
Ordem	Prioridade de fluxo. O valor deste campo indica a ordem em que os fluxos são

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	executados quando dois ou mais perfis compartilham condições de gatilho. O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300, 400. Padrão: 100
Capacidades do CrowdStrike Falcon Insight	Capacidades do perfil do CrowdStrike Falcon Insight. Selecione os recursos desejados para este perfil na coluna **Disponível** até **Selecionado**.

O exemplo a seguir mostra um formulário completo para um perfil com o recurso Obter detalhes do sistema.



4. Clique em **Avançar**.

O que Fazer Depois

Agora você podeconfigurar seu perfil. Certifique-se de ter revisado os conceitos de configuração de perfis e condições do gatilho antes de configurar o perfil.

Configurar perfis e incidentes de segurança para a integração CrowdStrike Falcon Insight

Defina as configurações de perfil para que o perfil seja acionado somente nas condições que você definir.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Defina as condições que acionam automaticamente os recursos CrowdStrike Falcon Insight que você selecionou para o perfil. Você também pode selecionar um campo de entrada alternativo para o campo Item de Configuração (IC). Neste campo alternativo, você pode

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

definir condições de filtragem para que somente os incidentes de segurança relacionados ao evento de acionamento acionem automaticamente o perfil.

Nota:
Navegue até a página Configuração de perfil somente depois de inserir os detalhes do perfil. Para obter mais informações, consulte Criar um perfil de capacidade para a integração do CrowdStrike Falcon Insight.

Procedimento

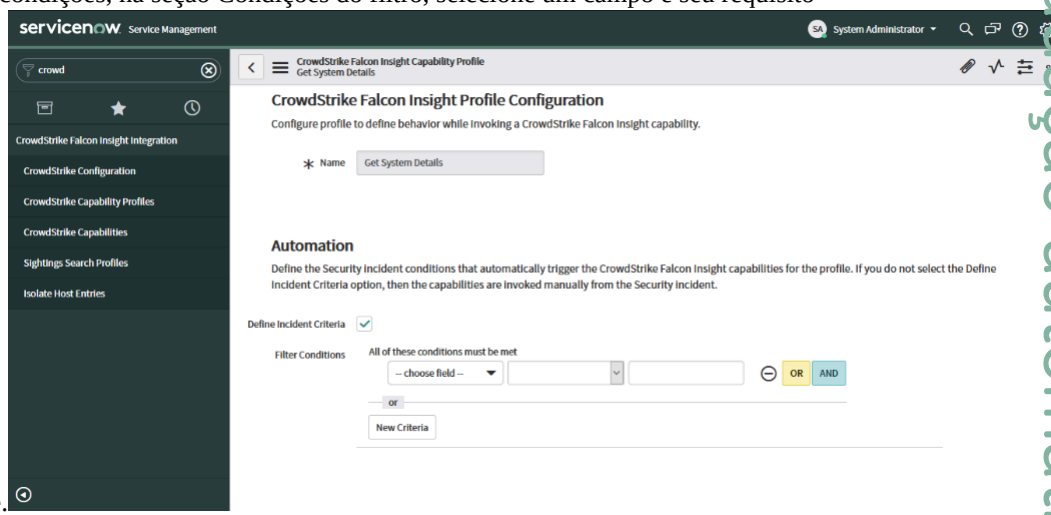
1. Na página Configuração de perfil, revise e configure as seguintes seções:

Definir critérios de incidente (automação)

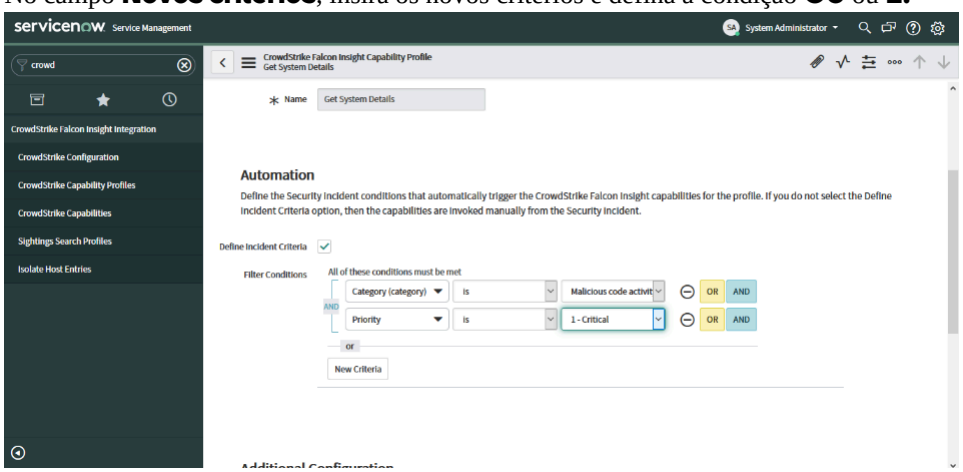
Defina as condições de incidente de segurança que acionam automaticamente os recursos CrowdStrike Falcon Insight para o perfil. Se você não selecionar a opção **Definir critérios de incidente**, os recursos serão invocados manualmente a partir do incidente de segurança.

a. Selecione a opção **Definir critérios de incidente**.

b. Para definir as condições, na seção Condições do filtro, selecione um campo e seu requisito correspondente.



c. No campo **Novos critérios**, insira os novos critérios e defina a condição **OU** ou **E.**



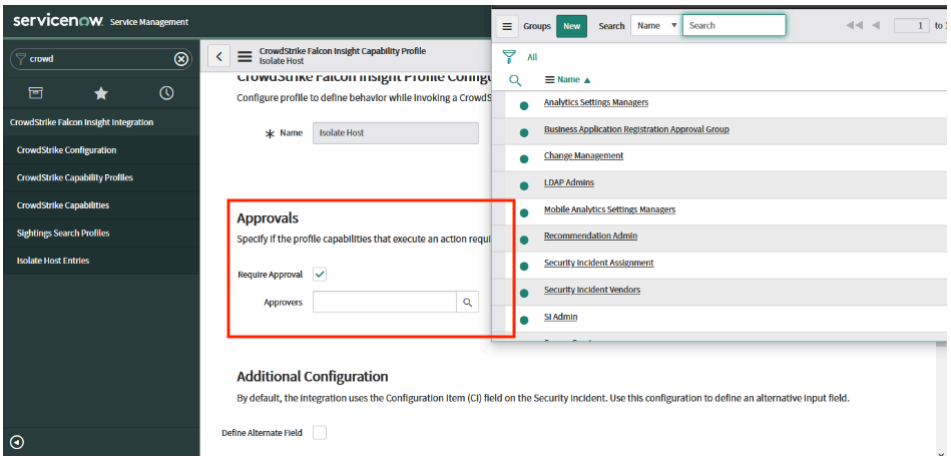
Aprovações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para fornecer um nível extra de controle ao usar os recursos do CrowdStrike Falcon Insight, selecione a opção **Requer aprovação**. A opção de aprovações na configuração do perfil aparece somente para os recursos Isolar Host e Remover Isolamento de Host.

Nota:
A autoridade de aprovação é atribuída ao usuário com a função sn_si.admin. Você também pode reatribuir esta autoridade de aprovação a um grupo de aprovação. Para obter mais informações, consulte configuração de um grupo de aprovação.



Configuração adicional

Selecione um campo alternativo no incidente de segurança para exibir todos os dados de IC correspondentes que você encontrar ao verificar seus ativos. Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança.

a. Selecione a opção **Definir campo** alternativo.

b. No **campo Gatilho de IC alternativo**, selecione um campo de entrada.

Nota:
Para obter mais informações, consulte Entenda como as condições do gatilho funcionam com um item de configuração para um perfil.

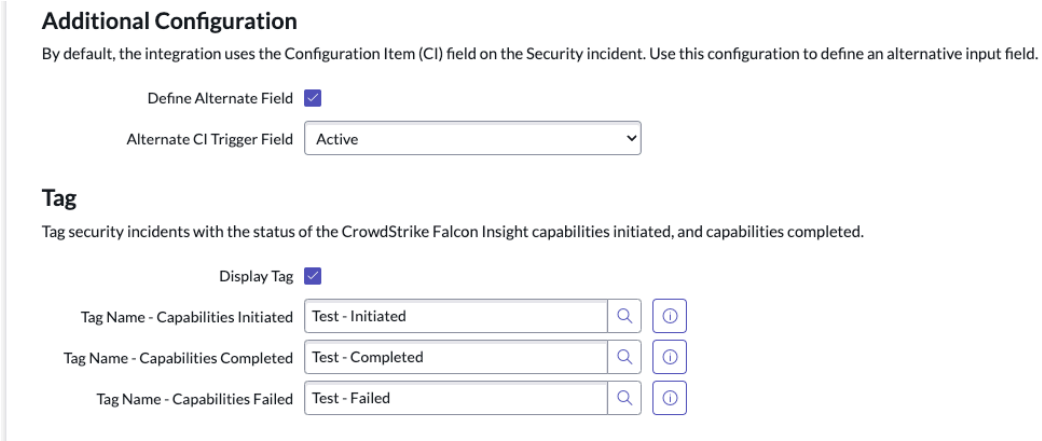
Marcadores

Para marcar os incidentes de segurança com os marcadores CrowdStrike Falcon Insight Capacidades-Iniciadas, Capacidades-concluídas e Capacidades-falhas, selecione a opção **Exibir** marcadores. Por padrão, esta opção está desabilitada para todos os perfis.

Nota:
Esses marcadores são fornecidos com o sistema de base. Você pode criar seus próprios marcadores, se necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Clique em **Concluído**.

Como as condições do gatilho funcionam com um item de configuração para um perfil

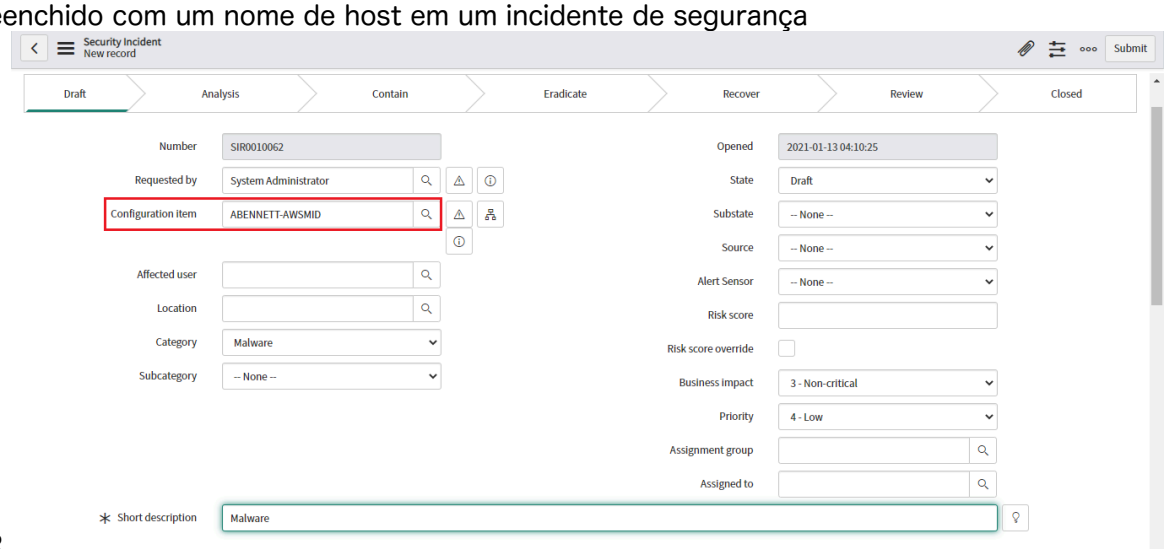
Você pode definir as configurações de perfil para que um perfil seja executado somente quando um conjunto de condições específicas for atendido ou pode configurar um perfil para pesquisar valores de campo específicos em um incidente de segurança.

Depois de criar um perfil e selecionar os recursos CrowdStrike Falcon Insight nos quais deseja que o perfil seja executado, você pode definir condições do gatilho para que seu perfil seja executado automaticamente quando os valores de campo padrão corresponderem ao incidente de segurança Now Platform.

Por padrão, a integração usa o campo **Item de configuração** (IC) em um incidente de segurança. Este campo é usado para corresponder seus IDs de ativo às informações armazenadas no banco de dados Now Platform. Quando um incidente de segurança SIR é criado por um evento de segurança e um perfil é ativado, seus ativos são verificados quanto a um valor correspondente no nome do host ou em um endereço IP.

Quando um valor correspondente é encontrado no banco de dados, esses dados são coletados do console CrowdStrike Falcon Insight e são inseridos na sua instância Now Platform, onde são exibidos nas listas relacionadas de um incidente de segurança.

O exemplo a seguir mostra um campo Item de configuração que é preenchido com um nome de host em um incidente de segurança SIR.



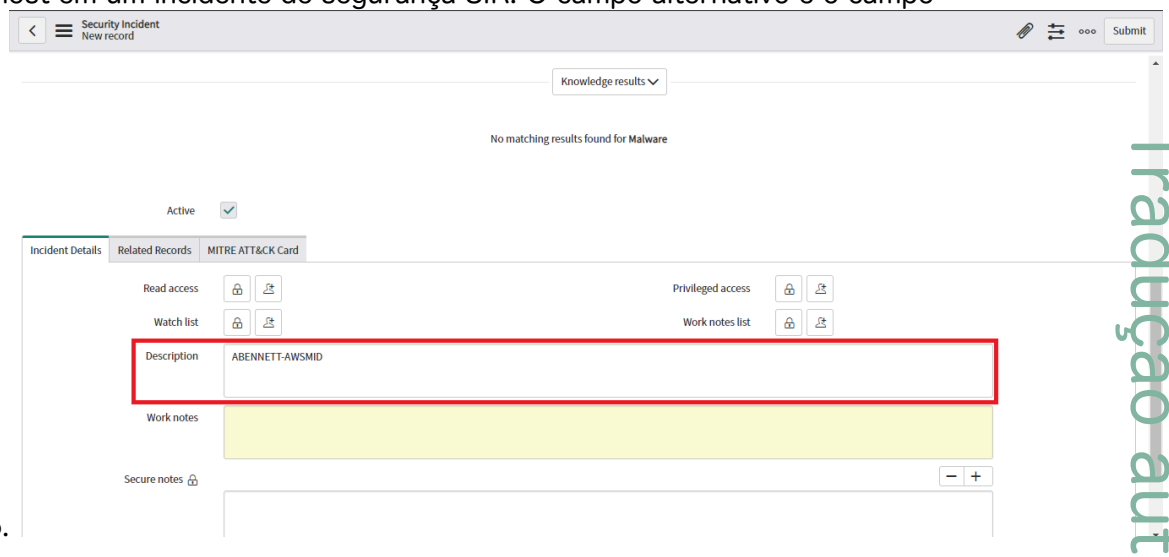
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando o campo **Item de configuração** (IC) não estiver preenchido com um nome de host ou um endereço IP que corresponda ao banco de dados, você poderá selecionar outro campo no incidente de segurança para exibir todos os dados de IC correspondentes encontrados ao verificar seus ativos.

Ao definir a configuração do perfil, você pode selecionar um campo de **gatilho de IC** alternativo para identificação do endpoint para garantir que os dados de IC da pesquisa CrowdStrike Falcon Insight sejam preenchidos no incidente de segurança associado. Você pode selecionar qualquer campo no incidente de segurança como um campo de gatilho de IC alternativo, incluindo campos personalizados que você cria. Se o campo de IC não estiver preenchido no incidente de segurança associado quando o incidente for criado, selecione o campo de IC alternativo para garantir que seus perfis sejam acionados.

O exemplo a seguir mostra um campo alternativo que é preenchido com um nome de host em um incidente de segurança SIR. O campo alternativo é o campo **Descrição**.



Verificar condições do gatilho de perfil CrowdStrike Falcon Insight

Teste o perfil e verifique se os filtros de condição do gatilho que você configurou funcionam conforme o esperado.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Ative o perfil que se baseia nas condições do gatilho configuradas que você especificou para que você possa exibir os resultados da consulta nos Now Platform incidentes de segurança.

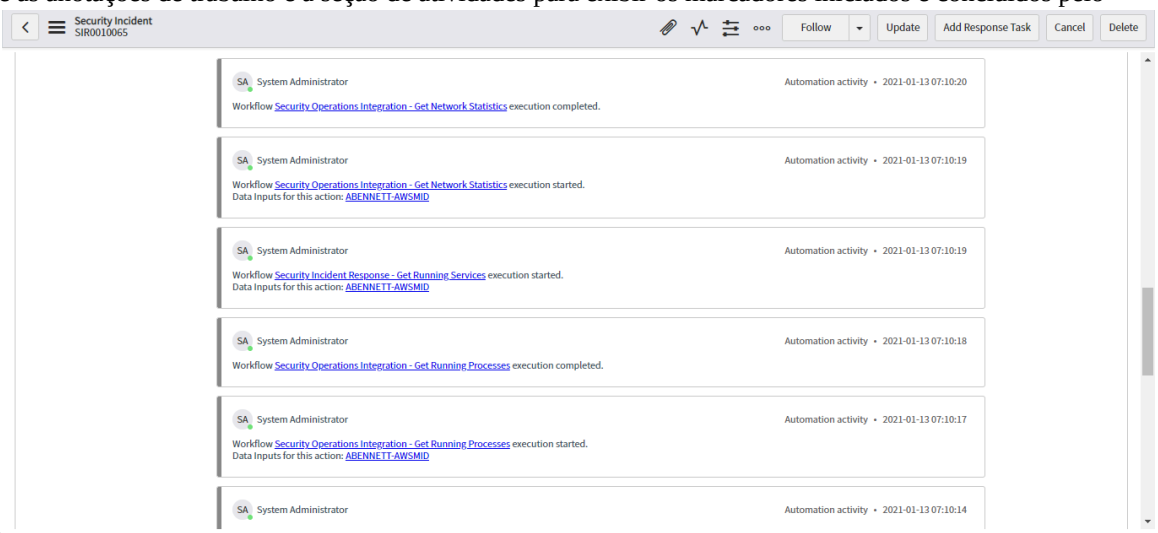
Procedimento

1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione **Novo** para criar um incidente de segurança.
3. Para criar um incidente de segurança, preencha as informações necessárias e clique em **Salvar**.

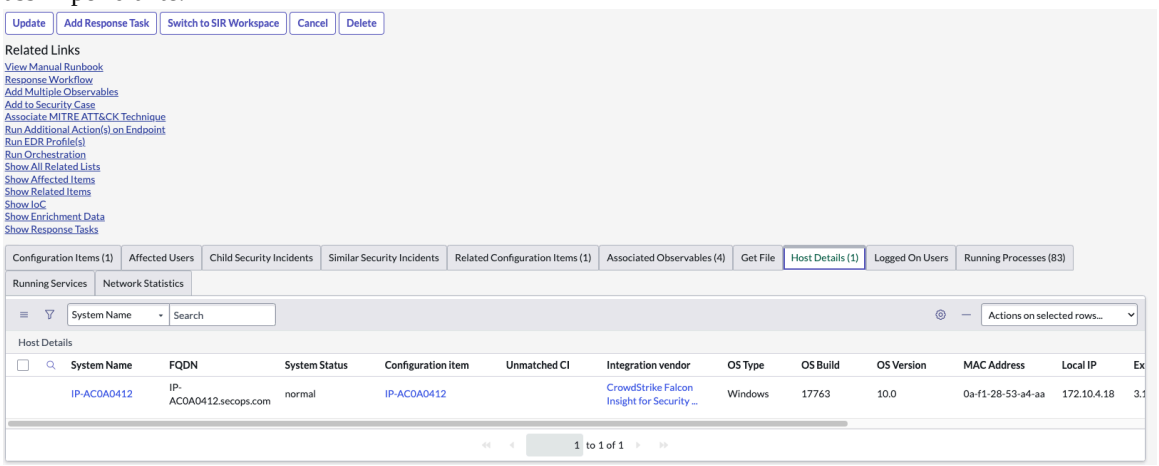
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Revise as anotações de trabalho e a seção de atividades para exibir os marcadores iniciados e concluídos pelo perfil.



5. Revise os detalhes nas listas relacionadas CrowdStrike Falcon Insight Detalhes, como Obter arquivo, Detalhes do host, Usuários conectados, Processos em execução, Serviços em execução, Estatísticas de rede e assim por diante.



Acionar um perfil CrowdStrike Falcon Insight manualmente a partir de um incidente de segurança

Acione um perfil manualmente depois de revisar um incidente de segurança.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Depois de ativar o perfil, com base nas condições do gatilho configuradas, você pode exibir os resultados da consulta nos Now Platform incidentes de segurança. CrowdStrike Falcon Insight também permite que você execute recursos individuais em itens de configuração (ICs) sem usar um perfil.

Procedimento

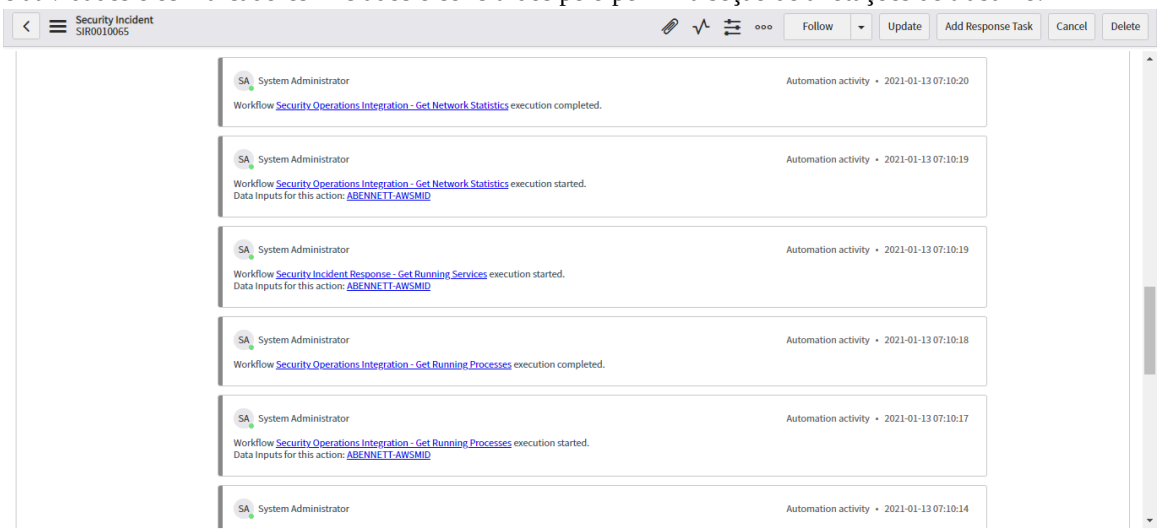
1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações CrowdStrike Falcon Insight.
3. Na seção de listas relacionadas, selecione **Executar perfil(is) de EDR**.
4. Procure e selecione um perfil na lista de perfis disponíveis.

Tradução automática

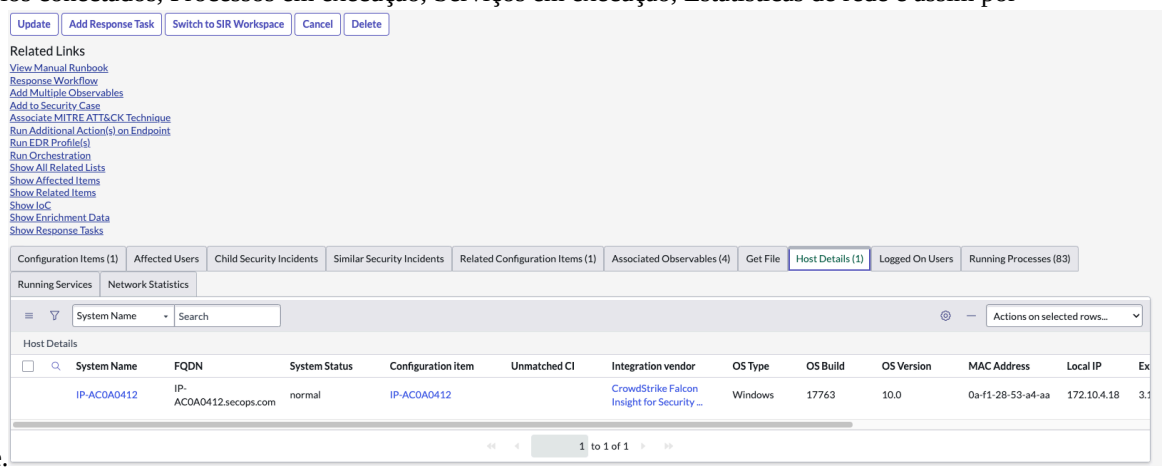
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione **Incluir IC relacionado** para executar este perfil em todos os ICs relacionados do perfil.
   Por exemplo, se houver cinco ICs associados ao incidente de segurança, o perfil selecionado será executado em todos os cinco ICs.

6. Clique em **Enviar**.
   O perfil selecionado é acionado manualmente. Você pode revisar a seção de anotações de trabalho e atividades e os marcadores iniciados e concluídos pelo perfil na seção de anotações de trabalho.



7. Os resultados aparecem na forma de listas relacionadas, como Obter arquivo, Detalhes do host, Usuários conectados, Processos em execução, Serviços em execução, Estatísticas de rede e assim por diante.



8. Para executar recursos individuais em um IC, execute as seguintes etapas:

   a. Na lista relacionada Itens de configuração, selecione o IC necessário.

   b. Clique na lista suspensa **Ações nas linhas selecionadas...** e selecione a capacidade necessária que você deseja executar para o IC selecionado.
      Por exemplo, Isolar Host.

   c. Pesquise a implementação da capacidade necessária para o IC usando a opção de pesquisa e selecione **Isolar host do CrowdStrike Falcon Insight**.

   d. Clique em **Isolar Host** para executá-lo no IC selecionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar e configurar um perfil para a pesquisa de vista

Use pesquisas de detecções para CrowdStrike Falcon Insight para localizar máquinas infectadas na rede da sua organização e para lidar com casos de resposta a incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Selecione um ou vários observáveis e execute uma pesquisa de vista manual em CrowdStrike Falcon Insight para determinar a predominância de uma ameaça ao longo do tempo.

Procedimento

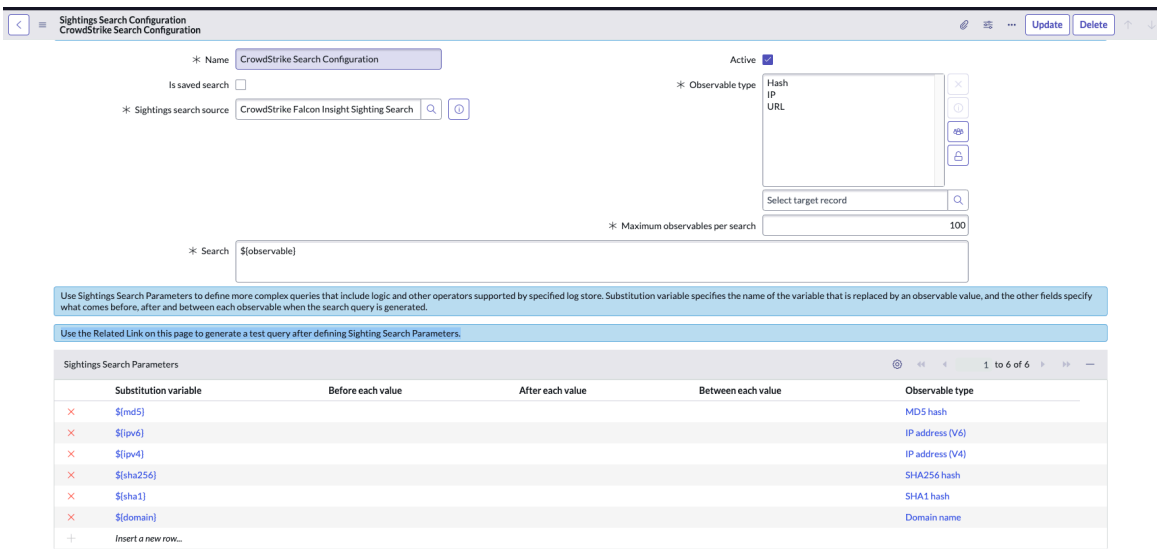
1. Navegar até **Todos** > **Integração com CrowdStrike Falcon Insight** > **Perfis de pesquisa de detecções**.
2. Clique em **Nova**.
3. Configure este perfil para determinar em quais servidores pesquisar uma capacidade de pesquisa específica do CrowdStrike Falcon Insight.
4. No formulário, preencha os campos:

Campo	Descrição
Nome	Nome do perfil de Pesquisa de detecções.
Pesquisa salva	A configuração de pesquisa salva será criada se você selecionar esta opção.
Origem de pesquisa de vistas	A origem da pesquisa de vistas. Selecione a Pesquisa de detecções do **CrowdStrike Falcon Insight** como a origem.
Ativo	Opção para indicar se o adicional está ativo ou não.
Tipo de observável	A integração do CrowdStrike Falcon Insight é compatível com os seguintes tipos de observável: ○ Hash ○ IP ○ URL A pesquisa de vista é compatível com os seguintes tipos de observáveis: ○ Nome do domínio ○ Endereço IP (V4) ○ Endereço IP (V6) ○ Hash MD5 ○ Hash SHA1 ○ Hash SHA256
Máximo de observáveis por pesquisa	Número máximo de observáveis que você pode exibir em uma consulta de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Pesquisar	A cadeia de caracteres de pesquisa padrão é `$(observable)`, mas você pode definir sua própria consulta de pesquisa especificando parâmetros compatíveis com a integração CrowdStrike Falcon Insight.
Parâmetros de Pesquisa de Vistas	Parâmetros para definir consultas mais complexas que incluem lógica e outros operadores compatíveis com o armazenamento de log especificado Você pode usar os Links relacionados na parte inferior da página para gerar uma consulta de teste depois de definir os Parâmetros de pesquisa de detecções.



5. Clique em **Enviar**.
   A configuração está concluída e você pode invocar a pesquisa de vistas do incidente de segurança Now Platform.
6. Para verificar a configuração e executar uma pesquisa de vista, execute as seguintes etapas:

   a. Abra um incidente de segurança, role até a parte inferior do incidente de segurança e clique em **Mostrar todas as listas relacionadas**.

   b. Se você selecionar um ou mais itens de configuração (IC) nas listas relacionadas a **Processos em execução**.

   > **Nota:**
   > Se você executar uma pesquisa de vista para um IC na lista relacionada Processos em execução, será somente uma pesquisa de vista de Hash de processo.

   c. Clique na lista suspensa **Ações nas linhas selecionadas...** e selecione **Executar pesquisa de detecções do CrowdStrike**.

   d. Pesquise o perfil de pesquisa de detecções necessário usando a opção de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

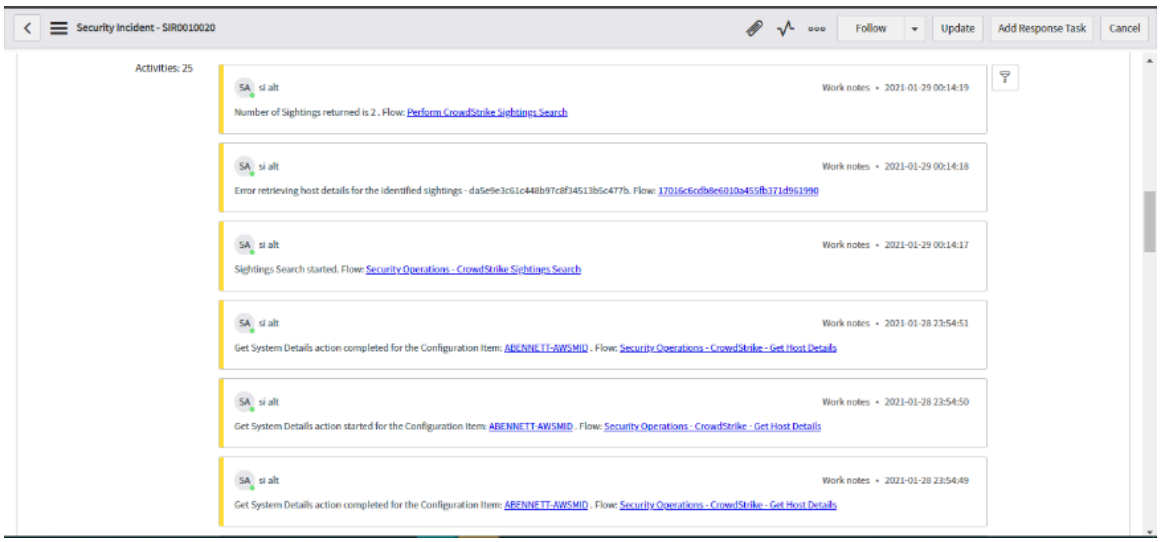
e. Selecione o perfil de pesquisa de detecções necessário e clique em **Enviar**.

f. Se você selecionar um ou mais observáveis nas listas relacionadas de **observáveis associados**.

g. Clique na lista suspensa **Ações nas linhas selecionadas...** e selecione **Executar pesquisa**de vistas .

h. No pop-up do intervalo de tempo, selecione qualquer valor aleatório e clique em **Pesquisar**.

i. Ao concluir a pesquisa, valide os resultados e os detalhes nas anotações de trabalho e nas listas relacionadas.



j. Selecione a guia **Vistas** para exibir os detalhes da vista.

k. Clique no ícone **Visualizar** ao lado do IC para exibir mais informações sobre os detalhes de vista do CrowdStrike.

l. Clique em **Detalhes da pesquisa** de detecções para exibir os detalhes da pesquisa de detecções e clique na guia **Resultados**da pesquisa de detecções para obter os resultados da pesquisa.

Configure e acione ações adicionais no CrowdStrike Falcon Insight

A integração CrowdStrike Falcon Insight oferece suporte à execução de ações adicionais, como expressão regular (regex). A integração CrowdStrike Falcon Insight fornece 40 ações adicionais com o sistema básico.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Integração com CrowdStrike Falcon Insight** > **Ações adicionais do CrowdStrike**.
2. Clique em **Novo** para criar sua própria ação adicional ou selecione uma ação existente que vem com o sistema básico.
   Por exemplo, vamos criar uma nova ação adicional.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

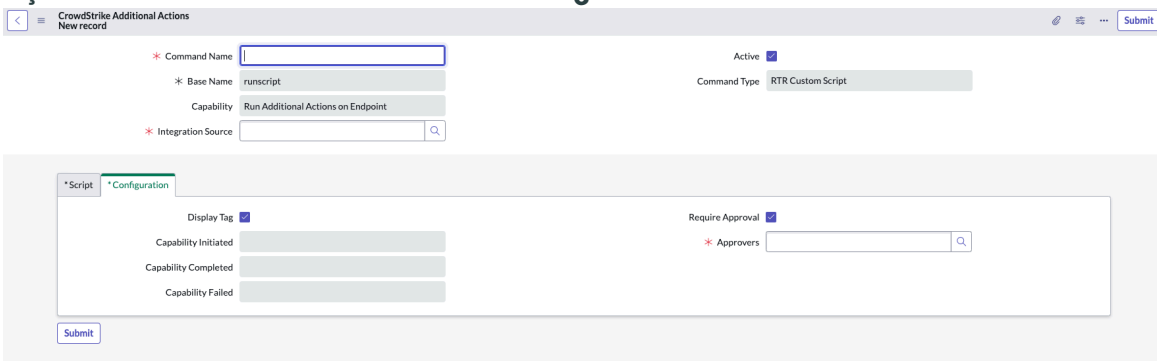
3. No formulário, preencha os campos.

Campo	Descrição
Nome do Comando	Nome do comando para a ação adicional. Por exemplo, reg set.
Nome base	Nome base da ação adicional. Este campo é definido por padrão. Por exemplo, reg.
Capacidade	Nome da capacidade da ação adicional. Este campo é definido por padrão. Por exemplo, Executar ações adicionais no endpoint.
Origem da integração	A origem da ação adicional. Por exemplo, CrowdStrike Falcon Insight Integration.
Ativo	Opção para indicar se o adicional está ativo ou não.
Tipo de Comando	Tipo de comando para a ação adicional. Este campo é definido por padrão. Por exemplo, Script personalizado de RTR.
Script	○ **Tipo de SO**: opção para selecionar o tipo de SO para o seu script. Selecione uma das seguintes propriedades: ▪ **Windows** ▪ **MAC OS X** ▪ **Linux** ▪ **Nenhum(a)** ○ **Script**: opção para inserir seu script se você selecionou um dos seguintes sistemas operacionais, exceto a opção Nenhum.
Configuração	○ **Exibir**marcador : opção para exibir o marcador da configuração. Você pode selecionar o marcador para os seguintes campos: ▪ Capacidade - Iniciada. Por exemplo, reg set - Initiated. ▪ Capacidade - Concluída. Por exemplo, reg set - Completed. ▪ Capacidade - Falha. Por exemplo, reg set - Failed. ○ **Requer aprovação**: opção para selecionar um aprovador ou grupo que precisa aprovar a configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

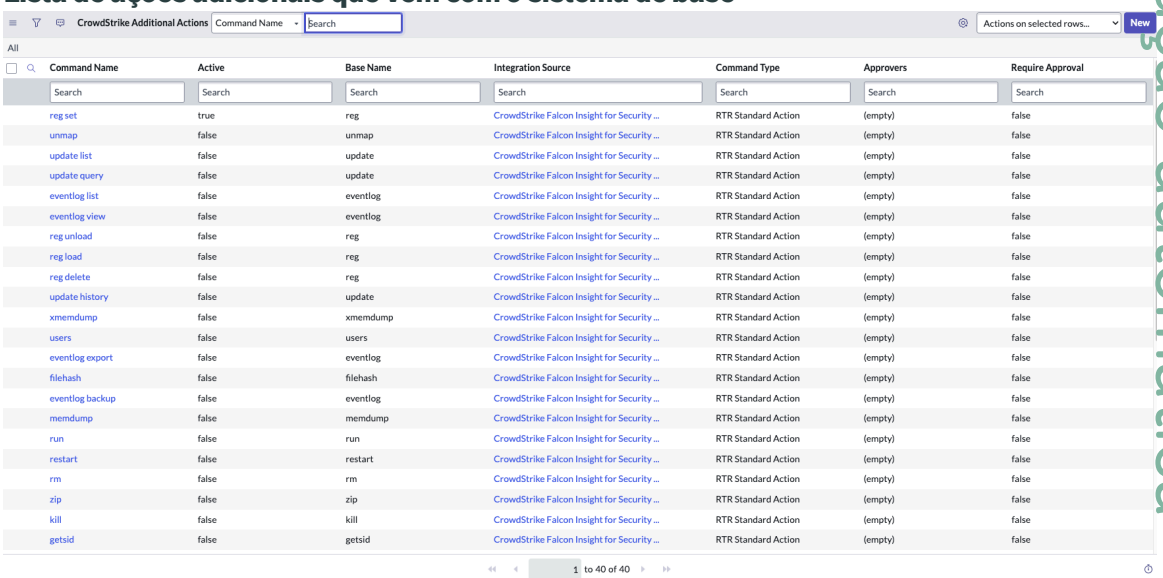
Ações adicionais do CrowdStrike Falcon Insight



4. Clique em **Enviar**.
5. Você também pode escolher entre as seguintes ações adicionais existentes.
   Existem 40 ações adicionais que vêm com o sistema de base, que você pode usar para executar configurações adicionais.

> **Nota:**
> Certifique-se de abrir a lista de ações adicionais do CrowdStrike e definir a ação adicional necessária como **verdadeiro**, caso contrário, a ação adicional não estará disponível no espaço.

Lista de ações adicionais que vem com o sistema de base



Command Name	Active	Base Name	Integration Source	Command Type	Approvers	Require Approval
reg set	true	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
unmap	false	unmap	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update list	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update query	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog list	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog view	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg unload	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg load	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg delete	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update history	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
xmemdump	false	xmemdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
users	false	users	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog export	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
filehash	false	filehash	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog backup	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
memdump	false	memdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
run	false	run	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
restart	false	restart	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
rm	false	rm	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
zip	false	zip	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
kill	false	kill	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
getsid	false	getsid	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false

1 to 40 of 40

6. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
7. Selecione o incidente de segurança que você deseja revisar com a execução de ações adicionais no endpoint.
   a. Na seção de links relacionados, clique em **Executar ações adicionais no endpoint**.
   b. Procure e selecione o recurso necessário.
      Por exemplo, clique na capacidade **do conjunto de registros**.
   c. Selecione **Incluir IC relacionado** para executar as ações adicionais em todos os ICs relacionados do endpoint.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. Você pode definir a **subchave** para executar as ações adicionais no endpoint.
Esta subchave pode ser uma chave HKLM/Software/nova.

8. Para iniciar a execução de ações adicionais no endpoint, clique em **Executar ação adicional**.
9. Exiba as atividades de automação da execução e valide-as.
10. Valide o status da ação nas Ações adicionais nas listas relacionadas ao endpoint.

Usando a integração CrowdStrike Falcon Insight no espaço do analista

Use a integração CrowdStrike Falcon Insight para aproveitar os recursos CrowdStrike Falcon Insight no espaço do analista de SIR.

Antes de Iniciar

Função necessária: sn_si.admin

Antes de usar a integração CrowdStrike Falcon Insight no espaço do Security Incident Response, você deve baixá-la do ServiceNow Store e configurá-la. Para obter mais informações, consulte Introdução à integração CrowdStrike Falcon Insight.

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar a integração CrowdStrike Falcon Insight para fazer ações de correção nos endpoints em tempo real, usar perfis para coletar detalhes sobre o host e fazer consultas ou ações específicas no endpoint usando o espaço Security Incident Response.

A integração CrowdStrike Falcon Insight permite que os analistas usem os seguintes recursos [CrowdStrike Falcon Insight no espaço do analista Security Incident Response :

- **Obter detalhes do host**
- **Obter usuários conectados**
- **Obter Estatísticas de Rede**
- **Obter processos em execução**
- **Obter serviços em execução**
- **Isolar Host**
- **Remover isolamento**
- **Obter arquivo**

Procedimento

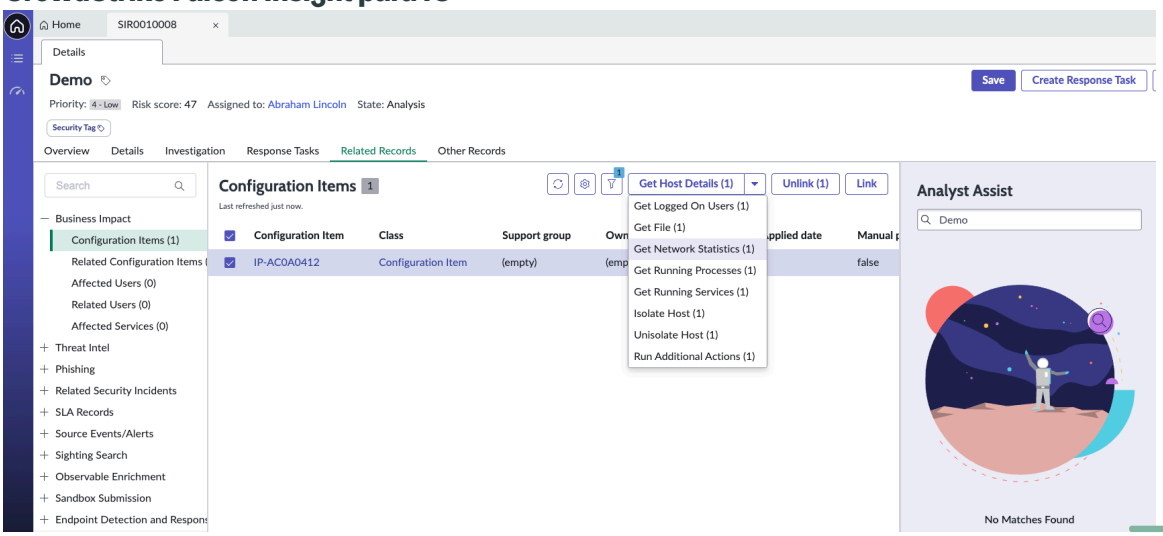
1. No espaço de SIR, abra o incidente de segurança necessário e selecione a guia **Registros relacionados**.
2. Você pode usar os recursos do CrowdStrike Falcon Insight na lista relacionada Impacto nos negócios para análise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Selecione um **Item de configuração**e escolha um recurso na lista suspensa.

CrowdStrike Falcon Insight para IC



b. Selecione a implementação do **CrowdStrike Falcon Insight** e clique em **Enviar**.
O recurso Obter estatísticas de rede é invocado no IC. Você pode exibir as anotações de trabalho dos resultados e descobertas.

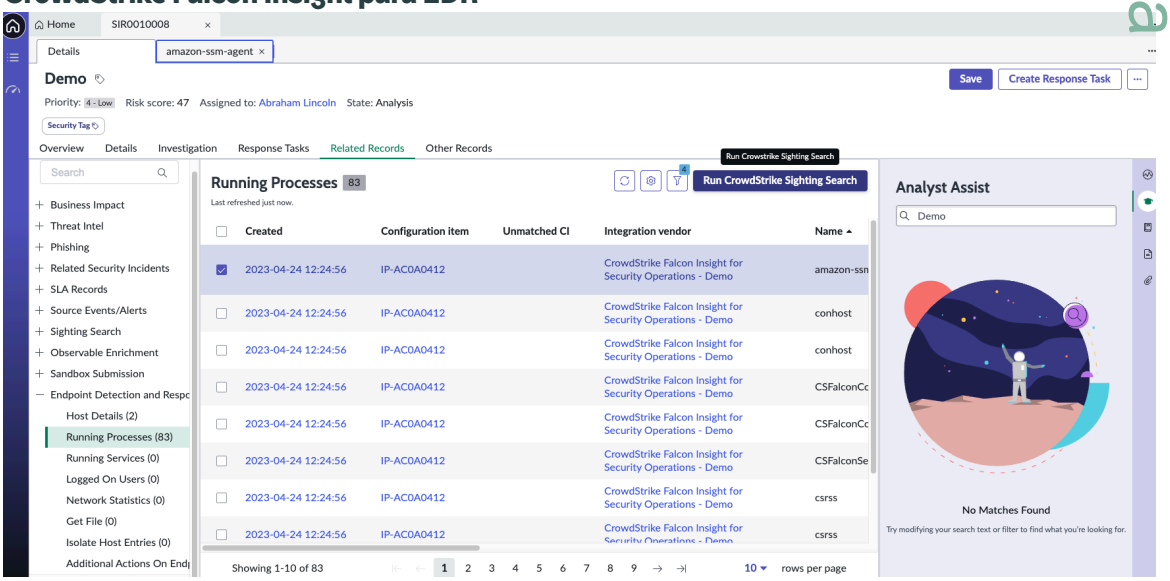
3. Você pode usar os recursos do CrowdStrike Falcon Insight na lista relacionada de **Detecção e resposta de endpoint (EDR)** para análise.

a. Na lista relacionada Detecção e resposta de endpoint (EDR), escolha um EDR na lista.

b. Clique em um processo em execução específico para exibir os detalhes do processo em execução do CrowdStrike Falcon Insight.

c. Para executar uma Pesquisa de detecções do CrowdStrike Falcon em um processo em execução específico, selecione o processo em execução e clique em **Executar CrowdStrike Sighting**.

CrowdStrike Falcon Insight para EDR



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

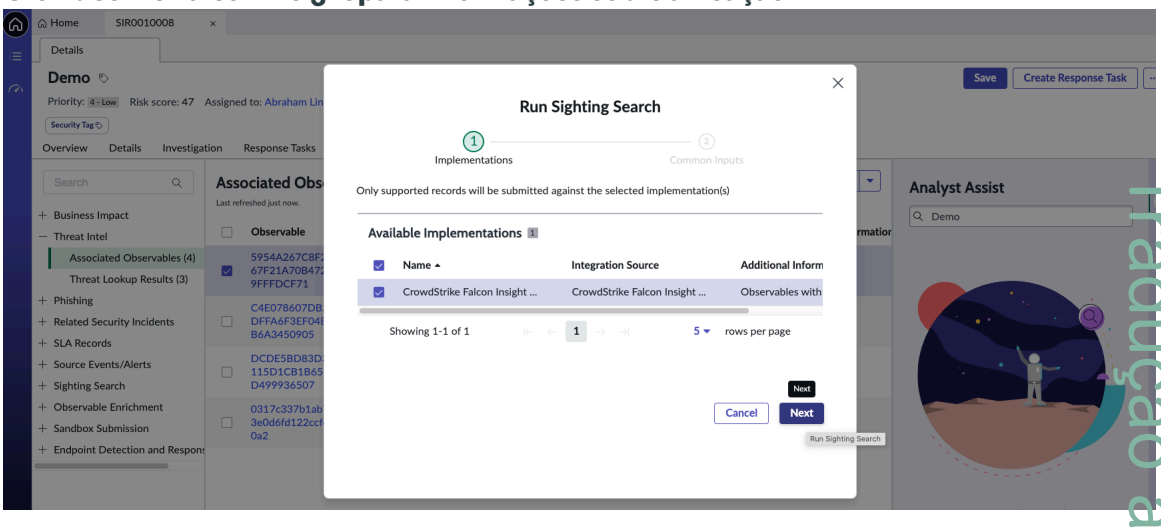
d. Selecione a implementação do **CrowdStrike Falcon Insight** e clique em **Executar pesquisa**.
Em seguida, uma pesquisa de vista de hash é executada no processo em execução selecionado. Você pode exibir as anotações de trabalho dos resultados e descobertas.

4. Você pode usar os recursos do CrowdStrike Falcon Insight na **Inteligência de ameaça** para análise.

a. No grupo Inteligência de ameaça, selecione um **Observável**e escolha uma capacidade CrowdStrike Falcon Insight na lista suspensa.

b. Selecione a implementação do **CrowdStrike Falcon Insight** e clique em **Avançar**.

CrowdStrike Falcon Insight para informações sobre ameaças



c. No pop-up Selecionar data/hora, selecione um valor aleatório e clique em **Enviar**.
Em seguida, uma pesquisa de vista é executada no observável selecionado. Você pode exibir as anotações de trabalho dos resultados e descobertas.

Integração do CrowdStrike Falcon X Sandbox para Security Operations

Com a integração CrowdStrike Falcon X Sandbox para Security Operations, você pode enviar arquivos e URLs como parte do processo de resposta do incidente de segurança para CrowdStrike Falcon X Sandbox para executar uma análise detalhada de malware e ameaça.

A integração CrowdStrike Falcon X Sandbox fornece um ambiente virtual isolado sob demanda, onde você pode executar a análise de malware e fornecer resultados para o incidente de segurança ServiceNow por meio da integração.

Quando você envia seus incidentes de malware, eles são retidos como parte do registro de incidentes de segurança. Você pode usar esses registros paraou resolução de incidentes adicionais e automatizar o envio de arquivos e URLs.

A integração oferece suporte à automação de playbooks de resposta de phishing e malware , o que permite que a equipe do centro Security Operations seja mais produtiva e eficiente ao responder a incidentes de segurança.

Principais benefícios

Com testa integração, você pode fazer o seguinte:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Automatize o envio de arquivos e URLs do usuário-relatou phishing (URP), mensagens de e-mail, anexos e outros incidentes de segurança.
- Envie ou reenvie manualmente arquivos e URLs analisados anteriormente para análise atualizada.
- Crie várias configurações de envio que aplicam automaticamente CrowdStrike Falcon X Sandbox parâmetros de envio, como sistema operacional, tipo de verificação e opções de tempo de execução.
- Analise o malware e os resultados da ameaça em um relatório no formato HTML no incidente SIR. Você pode exibir tresultados de pesquisa e o histórico do indicador de arquivos e URLs que foram analisados várias vezes.
- Marque ServiceNow incidentes com o status de processamento do envio, bem como os resultados da descoberta de ameaças.

Veja também

Identificador de documento	Título do documento
CrowdStrike Falcon X Sandbox	Perguntas frequentes do CrowdStrike Falcon Sandbox
ServiceNow site da documentação do produto	Site de documentação do produto da ServiceNow

Introdução à integração CrowdStrike Falcon X Sandbox

Ative e configure o CrowdStrike Falcon X Sandbox para interagir com sua instância [ServiceNow e produto Security Incident Response.

Antes de Iniciar

- Antes de usar o CrowdStrike Falcon X Sandbox para integração do Security Operations, você deve baixá-lo da ServiceNow Store.
- Revise a check-list de configuração a seguir e verifique se você concluiu todas as tarefas para uma integração sem problemas CrowdStrike Falcon X Sandbox.

Função necessária: admin, sn_si.admin

Check-list

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform e Security Incident Response.	As funções a seguir são necessárias para configuração e verificação dos resultados esperados: • O administrador (admin) instala a integração sandbox da loja de aplicativos da ServiceNow e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O sn_si.admin cria e edita a configuração e configurações globais e , então atribui

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	a função de analista de incidente de segurança (sn_si.analyst). • O analista de incidentes de segurança (sn_si.analyst) responde a incidentes de segurança, como enviar arquivos e URLs para a sandbox e analisar os resultados do envio.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de configurar esta integração.	Esta integração é compatível com as versões Paris e Orlando. Certifique-se de que esses plug-ins dependentes estejam instalados. Esses plug-ins permitem a execução de IntegrationHub ações e fluxos: • ServiceNow Etapa de ação do IntegrationHub - REST (com.glide.hub.action_step.rest) • ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) **Nota:** Se vocênão encontrar um plug-in, talvez seja necessário solicitá-lo ao ServiceNow pessoal. Para solicitar um plug-in, siga as etapas em Solicitar um plug-in . O plug-in Security Incident Response (com.snc.security_incident) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar os outros Security Operations aplicativos que são necessários para a integração. Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas. 1. Security Incident Response Dependência (com.snc.si_dep) 2. Security Integration Framework

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

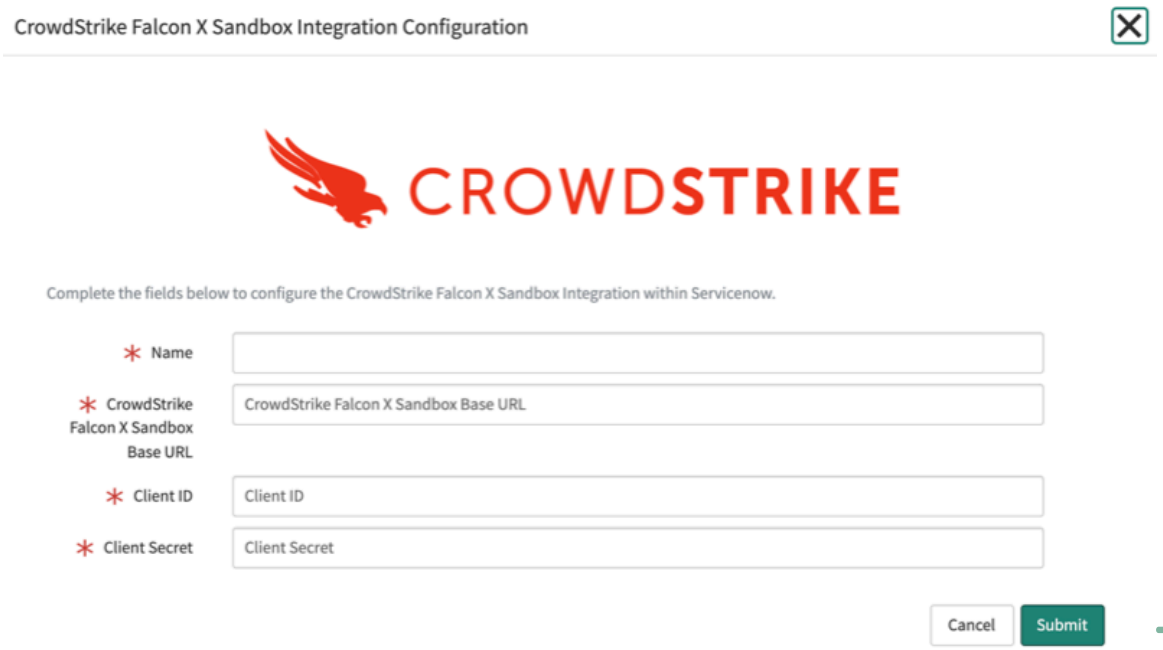
Configuração de tarefa	Descrição
	3. Security Support Common **4.** Orquestração de suporte de segurança **5.** Inteligência contra ameaças Suporte comum (necessário para usarse as capacidades de integração da área restrita) **6.** Trusted Security Circles **7.** Security Operations Assistente de configuração **8.** Security Incident Response Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte Obter direito de um produto ou aplicação do Security Operations e Ativar uma aplicação da ServiceNow Store.
Verifique se você está licenciado para a chave de API privada do Falcon Sandbox e ouobtenha a CrowdStrike Falcon X Sandbox chave de API completa.	Esta integração é compatível somente com o Falcon Sandbox Private Cloud. **Nota:** Esta versão não é compatível com a integração do Falcon X. CrowdStrike Falcon X Sandbox O oferece uma chave de API restrita autoassinada e uma chave de API completa atualizada. Use a chave de API completa para esta integração porque ela permite acesso irrestrito para envios automatizados. Para obter mais informações, consulte Base de conhecimento do CrowdStrike Falcon Sandbox .

Procedimento

1. Baixe a integração do CrowdStrike Falcon Sandbox for Security Operations na ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Security Operations** > **Integrações** > **Configurações de integração**.
3. Pesquise o bloco de integração CrowdStrike Falcon X Sandbox e clique em **Configurar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Insira os seguintes detalhes para concluir a configuração:

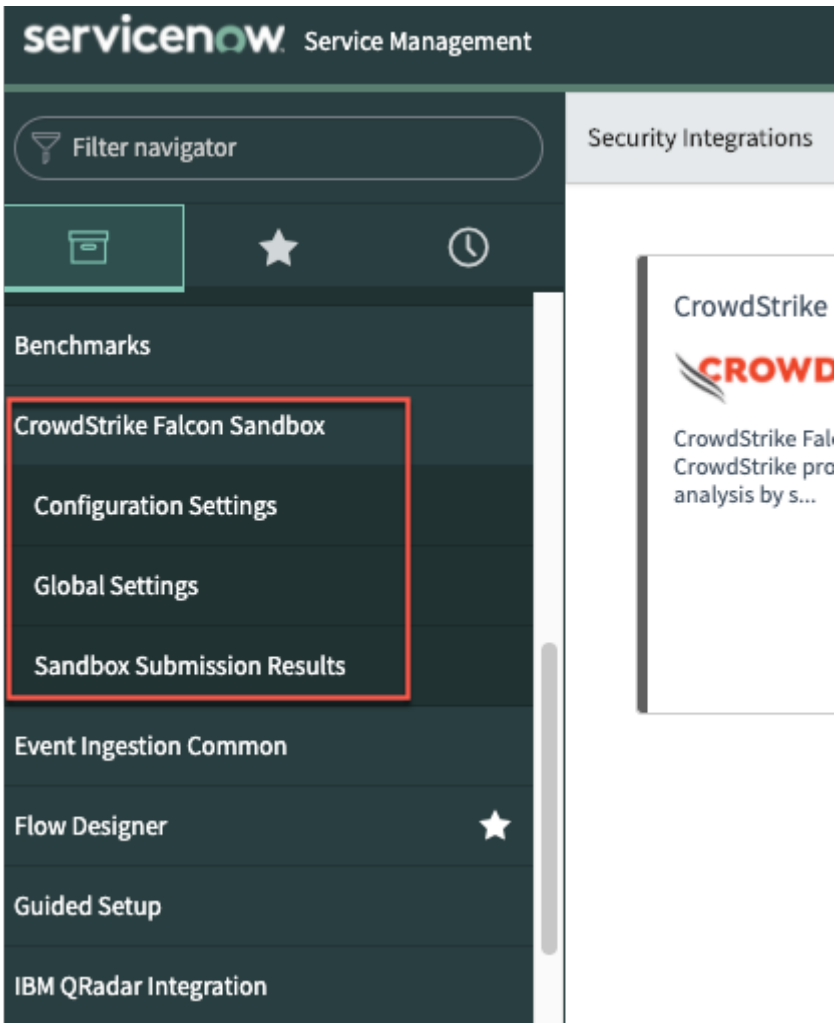
Campo	Descrição
Nome	Nome desta integração, por exemplo, `demo-1`. Embora este seja um nome exclusivo para identificar a configuração do sandbox, você só pode configurar uma integração por instância da ServiceNow.
URL base do CrowdStrike Falcon Sandbox	SURL base do andbox. Este URL está disponível depois de configurar a secaixa.Por exemplo, `https://servicenow.falcon-sandbox.com` é um URL base.
ID de cliente	ID do cliente da API do OAuth2. Para obter mais informações, consulte Clientes e chaves de API .
Segredo do Cliente	Chave secreta do cliente da API do OAuth2. Para obter mais informações, consulte Clientes e chaves de API .

5. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois que a área restrita for validada e enviada com sucesso, ele será salvo na página Integrações de segurança como um bloco. Agora você pode exibir o módulo Sandbox no navegador da aplicação .



Tradução automática

O que Fazer Depois

Depois de concluir com sucesso a integração, a próxima etapa é definir as configurações de envio da Sandbox.

Definir configurações de envio da área restrita

Defina a configuração Sandbox para definir o ambiente de análise e as opções de tempo de execução para os envios de registro de incidente de segurança para a análise de malware.

Antes de Iniciar

Função necessária: sn_si.admin

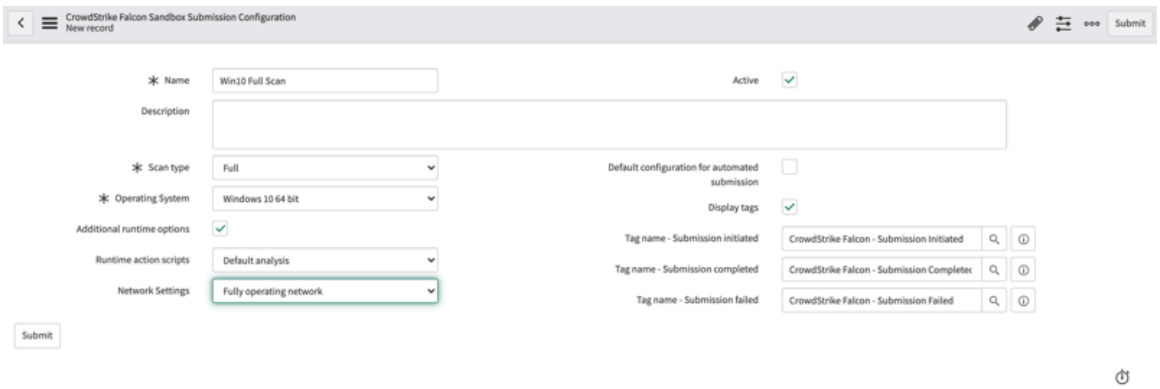
Por Que e Quando Desempenhar Esta Tarefa

Antes de enviar arquivos ou URLs para CrowdStrike Falcon X Sandbox usando a integração, você deve definir pelo menos uma configuração de envio. A configuração de envio define o sistema operacional Sandbox, o tipo de verificação, as opções de tempo de execução e outras características de manipulação de incidentes. Você pode criar várias configurações para usar as diferentes opções que estão disponíveis no ambiente CrowdStrike Falcon X Sandbox.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **CrowdStrike Falcon X Sandbox** > **Definições de Configuração**.
2. Clique em **Nova**.



3. Preencha os campos a seguir para criar uma configuração para um **tipo de verificação**completa .

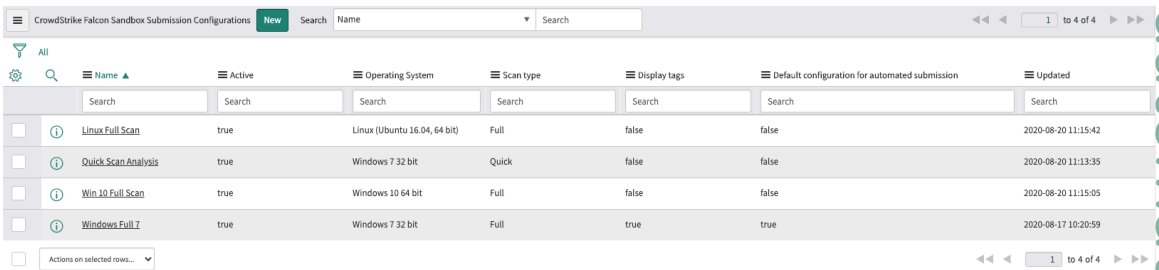
Campo	Descrição
Nome	Nome exclusivo para a configuração de envio. Este nome aparece para os analistas quando eles enviam um arquivo. É importante garantir que o nome seja descritivo e facilmente distinguível de outras configurações (por exemplo, Win 10 Full Scan). Se o nome não for exclusivo, será exibido um erro e os nomes de registro de configuração duplicados não serão salvos.
Tipo de verificação	Spode digitar como **Completo**. Um tipo de verificação **rápida** fornece uma análise de ameaça limitada.
Sistema operacional	Um ambiente de VM de análiseem que a caixae verifica o arquivo ou a URL.
Ativo	Option que você seleciona ao enviar arquivos ou URLs manualmente.
Configuração padrão para envio automatizado	Option que é limpo por padrão. Selecionar esta opção permite que esta configuração esteja disponível para automatizar os envios de análise de malware. **Nota:** Você pode ter apenas uma configuração de envio ativa como configuração padrão para envios automatizados.
Marcadores de exibição	Option que é limpo por padrão. Quando você seleciona esta opção, os marcadores são exibidos para fornecer o status de um arquivo ou envio de URL. A análise pode levar vários minutos para ser

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	processada. Os marcadores de exibição são envio iniciado, envio concluído, ou envio com falha.
Opções adicionais de tempo de execução	Option que é limpo por padrão. Ao selecionar esta opção, parâmetros de tempo de execução adicionais compatíveis com o Sandbox ficam disponíveis.
Scripts de ação de tempo de execução	Opção que permite usar um umscript de ação que simulas comportamento humano e interages com o arquivo ou URL durante a análise. https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/ Consulte a documentação CrowdStrike Falcon X Sandbox para obter mais detalhes.
Configurações de rede	Opção que permite selecionar o tipo de configurações de rede usadas ao enviar um URL ou arquivo para a área restrita.

4. Clique em **Enviar**.
   Depois de enviar a configuração, ela é salva na página Definições de configuração como um registro. A configuração deve estar **Ativa** para ser usada em envios de [eebox.



O que Fazer Depois

Depois de configurar os envios do andbox s, a próxima etapa é enviar manualmente arquivos ou ULRs para a área restrita

.

Enviar manualmente arquivos ou URLs para a área restrita

Você pode enviar manualmente um arquivo ou URL para uma área restrita quando determinados critérios de incidente, como a categoria é phishing, forem atendidos.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

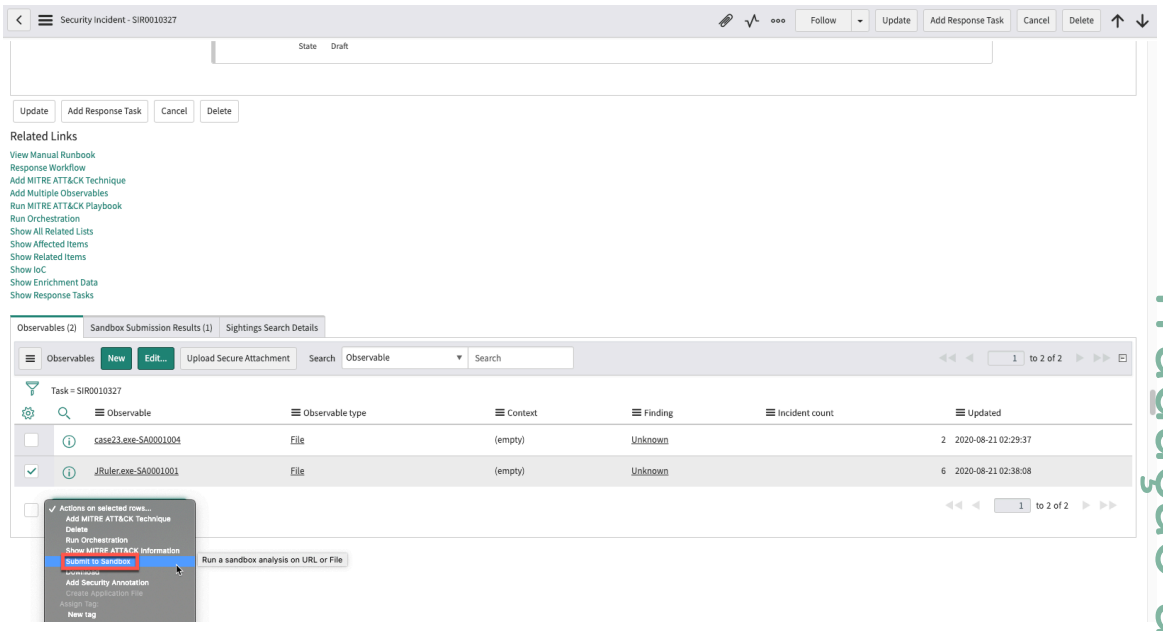
Depois de revisar o incidente de segurança e o arquivo ou URL, você pode selecionar a opção **Enviar para área restrita** para executar uma análise de malware.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

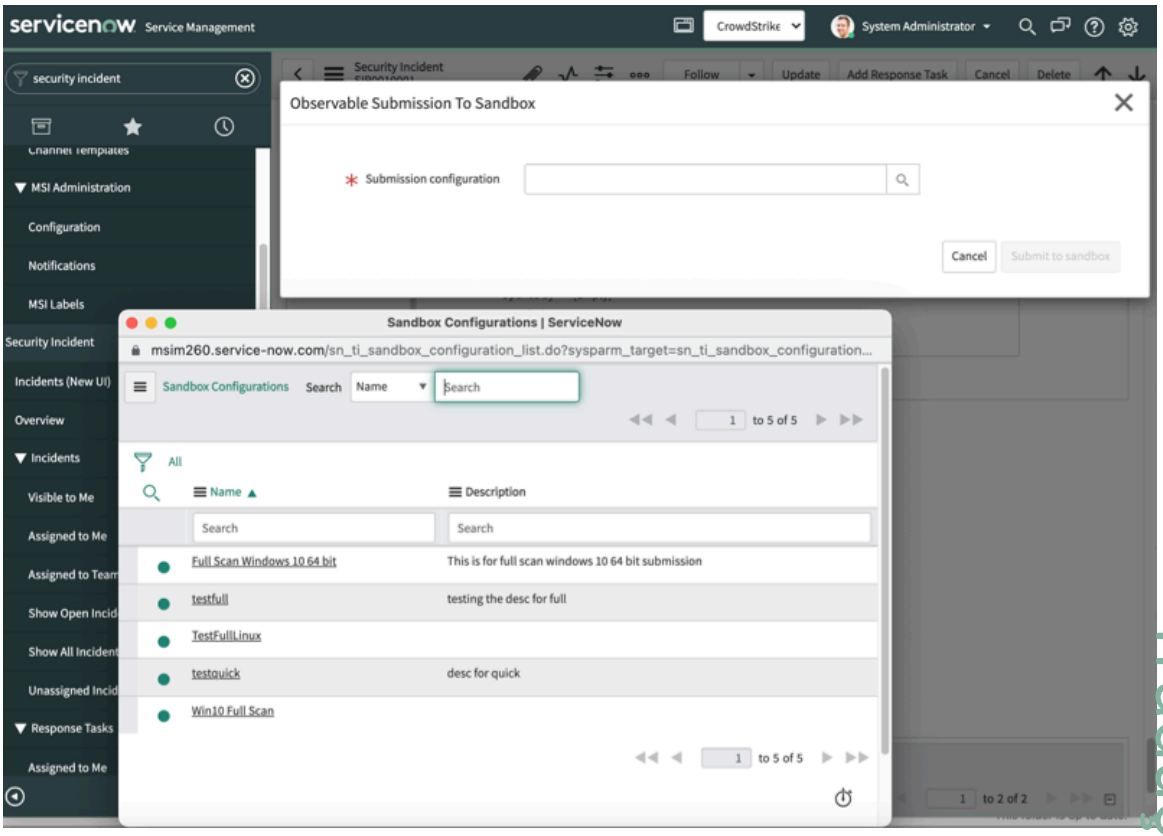
1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar Todos os Incidentes** e abra um incidente de segurança para o qual você deseja enviar um arquivo ou registro de tipo de observável de URL.
2. Clique no link relacionado **Mostrar IoC**.
3. Na guia **Observáveis**, selecione um ou vários registros para os quais você deseja executar a análise de malware ou ameaça e clique em **Enviar para área restrita**.



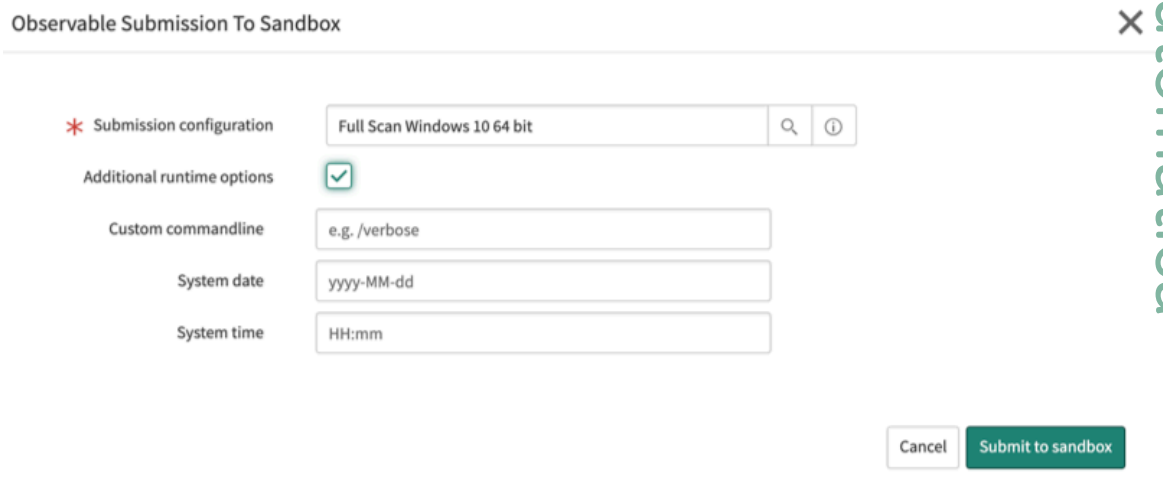
4. Quando o filtro Envio de arquivo for exibido, selecione sua configuração de área restrita preferencial em Configuração de **envio** e clique em **Enviar para área restrita**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. **Opcional:** Selecione **Opções adicionais de tempo de execução** se quiser fornecer mais opções personalizadas.



Campo	Descrição
Linha de comando personalizada	Linha de comando da aplicação regular ou uma operação especial.
Data do sistema	Data do sistema no formato aaaa-MM-dd.
Hora do sistema	Hora do sistema no formato HH:mm.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de iniciar o envio, você pode exibir as anotações de trabalho para ver o status do envio. Para obter mais informações sobre o status do envio ou para analisar os resultados, exiba os **Resultados de envio**da área restrita.

Nota:
No CrowdStrike Falcon X Sandbox, a verificação rápida não é compatível com URLs. Se as anotações de trabalho tiverem muitas informações, você poderá usar a opção Filtrar para ver as anotações de trabalho necessárias que são relevantes para você.

O que Fazer Depois
Ao enviar os observáveis para a área restrita para análise de malware, exiba os resultados do envio da área restrita para executar as próximas etapas em possíveis ameaças.

Automatizar CrowdStrike envios do Falcon Sandbox usando o Flow Designer

A integração CrowdStrike Falcon X Sandbox inclui modelos de fluxo criados usando o Flow Designer que funcionam com registros de incidentes de segurança.

Antes de Iniciar
- Verifique se você criou uma configuração de envio Sandbox e habilitou uma configuração como a **configuração padrão para envio automatizado**. Quando o fluxo é acionado, o envio da área restrita ocorre em sua configuração padrão.

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Esses fluxos foram projetados principalmente para iniciar quando você deseja automatizar envios de arquivo ou URL como parte do fluxo de trabalho de resposta do incidente.
Ao ativar um fluxo de amostra, seus anexos de arquivo de phishing serão enviados automaticamente se você definir os incidentes de segurança como phishing em seu fluxo de amostra. Como alternativa, você pode enviar todos os arquivos .exe quando este tipo de arquivo estiver anexado a um registro observável.

Você pode modificar esses fluxos de amostra para acionar um envio automatizado em diferentes condições, categorias, condições compostas e assim por diante.

A integração da área restrita consiste em dois fluxos do sistema de base que são desativados por padrão.

- **Enviar arquivo quando a categoria for phishing**: este fluxo envia um arquivo para a área restrita para análise de malware quando a categoria de incidente de segurança é definida como phishing. Você deve anexar um arquivo ao registro observável no incidente de segurança. Se você estiver usando a funcionalidade URP (User Reported Phishing), qualquer anexo de e-mail será analisado automaticamente e adicionado ao registro de incidente SIR como um registro observável. Nenhuma ação adicional é necessária para automatizar o envio.
- **Enviar quando o tipo de arquivo do observável for exe**: este fluxo envia um arquivo para a área restrita para análise de malware quando o observável do incidente de segurança for um exe. Semelhante ao fluxo de categoria de phishing, você deve anexar um arquivo a um registro observável no incidente de segurança. Você pode fazer isso manualmente, carregando o arquivo, ou automaticamente se um anexo de e-mail de phishing ou outro mecanismo que esteja criando o incidente estiver associado aos registros observáveis.

Quando os fluxos são configurados e as condições do incidente atendem aos parâmetros, os envios da área restrita são acionados automaticamente quando você revisa o incidente de segurança. Revise a anotação de trabalho que indica que um envio foi iniciado, um

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

marcador aparece se habilitado na configuração e um registro de resultados de envio pendentes.

A integração da área restrita também contém vários subfluxos. Os subfluxos são componentes internos dos recursos gerais de envio de integração. Você pode personalizar e editar os subfluxos para atender aos seus critérios de segurança.

Você pode consultar os subfluxos para solucionar problemas com envios da área restrita. Um registro de execução é criado sempre que você invoca um subfluxo. Este registro indica onde ocorreu um erro específico no fluxo e permite que você corrija o problema.

Sandbox Integration - Vários fluxos de trabalho

Flows | Subflows | Executions | Help | + New

All > Application Name contains Sandbox

Name ▲	Internal name	Application	Status	Active	Updated	Updated by
Search	Search	*Sandbox	Search	Search	Search	Search
Add submission status tag on SIR	add_submission_status_tag_on_sir	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 12:33:57	admin
Aggregate Additional Runtime Options	aggregate_additional_runtime_options	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 08:47:54	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-18 02:52:33	admin
CrowdStrike Falcon Sandbox Poll Submission	crowdstrike_falcon_sandbox_polling	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-02 05:11:53	admin
CrowdStrike Falcon Sandbox Submission	submit_file_to_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:17:57	admin
CrowdStrike Falcon Submission Results	crowdstrike_falcon_submission_results	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:30:16	admin
CrowdStrike Polling Quick/Full Scan	crowdstrike_polling_quickfull_scan	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 20:23:07	admin
Fetch Environment Ids from Sandbox	fetch_environment_ids_from_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-25 07:45:54	admin
Submit File or URL to CrowdStrike Quick ...	submit_fileurl_to_crowdstrike	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 19:04:42	admin
Submit File/URL to Sandbox	submit_fileurl_to_sandbox	Security Operations CrowdStrike Falcon S...	Draft	true	2020-05-25 07:50:18	admin
Submit Observable for Automated submission	submit_observable_for_automated_submission	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-06 06:15:35	admin

Actions on selected rows... | 1 to 11 of 11

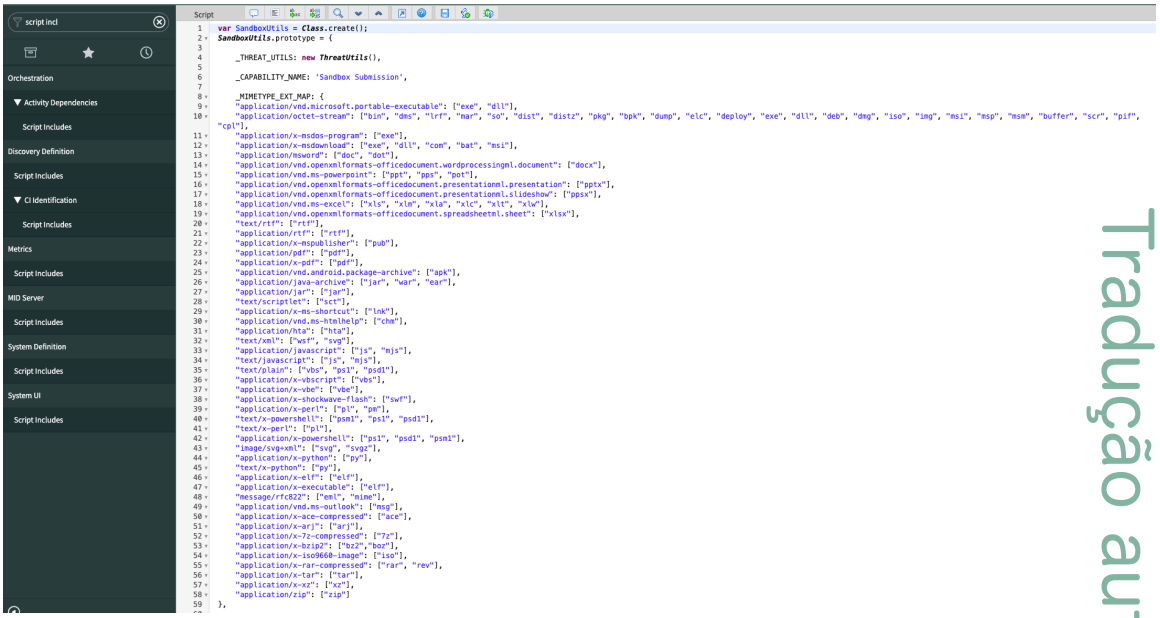
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

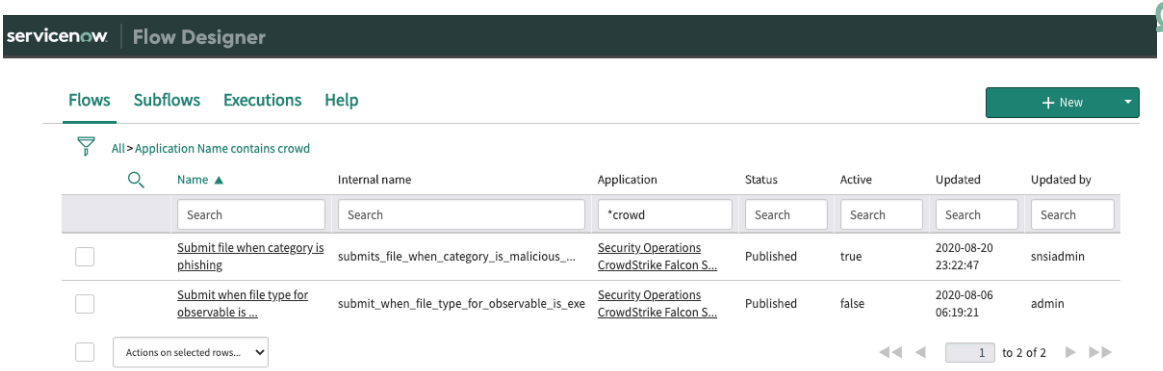
- Se você optar por personalizar os fluxos padrão, verifique se o subfluxo Enviar observável para envio automatizado está incluído no fluxo para acionar envios automáticos.
- Você pode personalizar e definir suas extensões de arquivo para um exe. Crie uma cópia do fluxo **Enviar quando o tipo de arquivo do observável for exe**e faça mudanças na cópia. O tipo de conteúdo e as extensões de arquivo são mapeados no script SandboxUtils. Para acessar as inclusões de script, navegue até **Definições do sistema > Inclusões de script** e pesquise por SandboxUtils.

Script SandboxUtils



Procedimento

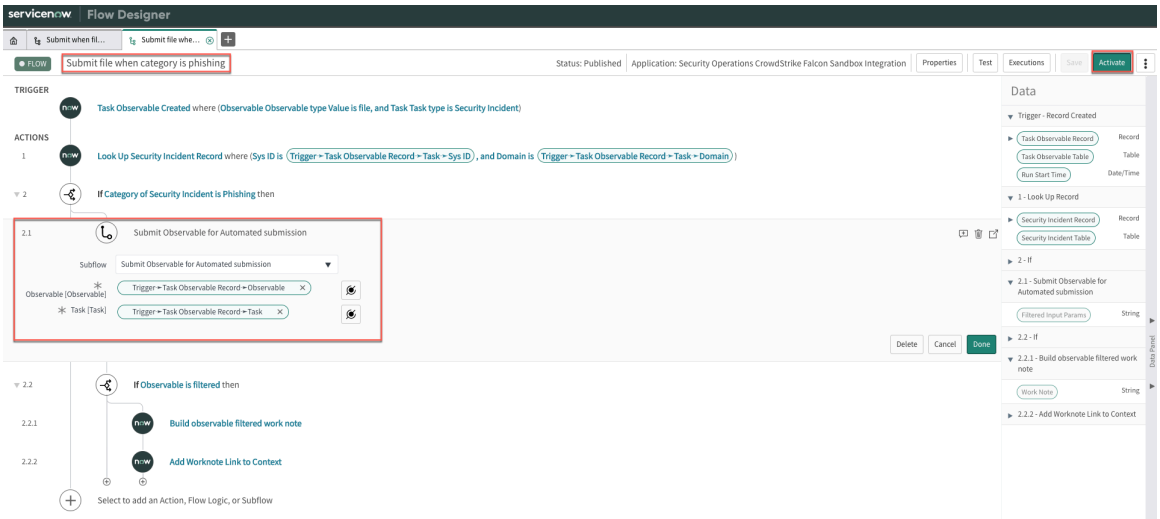
1. Navegar até **Todos** > **Flow Designer** > **Designer** > **Fluxos**.
2. Filtre os fluxos pelo tipo de **aplicação**.
   Por exemplo, *crowd filtra os dois fluxos CrowdStrike Falcon X Sandbox.



3. Selecione um fluxo para exibir os detalhes.
   O exemplo abaixo mostra o fluxo Enviar arquivo quando a categoria for phishing.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em **Ativar** e em **OK** quando a mensagem de confirmação for exibida.

O que Fazer Depois

Depois de configurar fluxos de envio automatizados, você pode Exibir os resultados de envio da área restrita para analisar quaisquer ameaças.

Monitorar os resultados de envio na área restrita

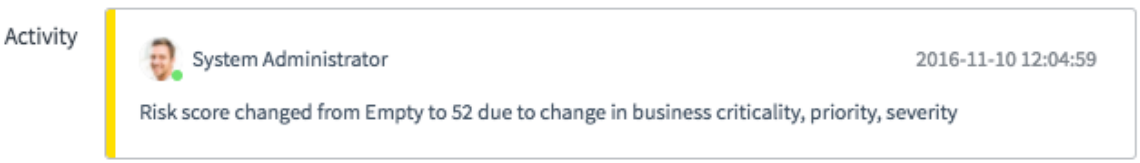
Os resultados de todos os envios do Sandbox são mostrados na guia **Resultados de envio do Sandbox** para cada incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

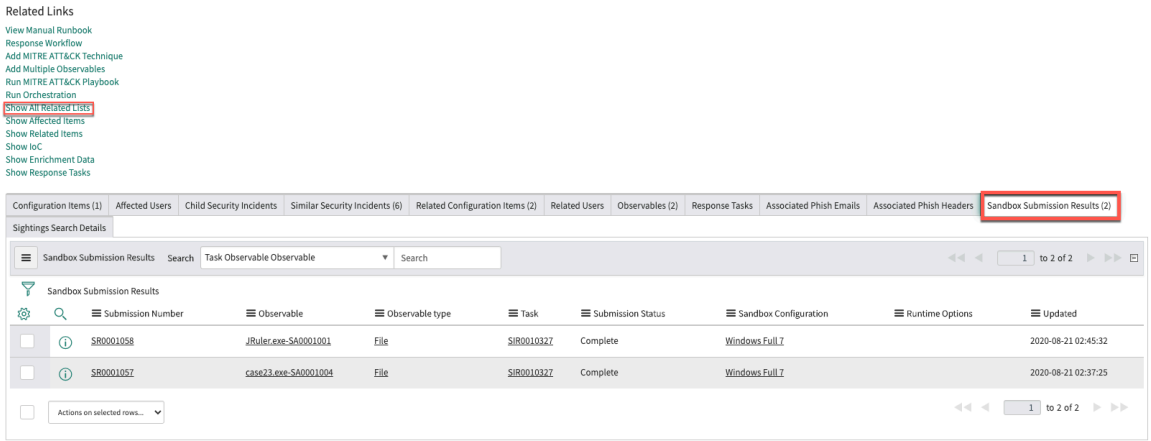
1. Abra o incidente de segurança com o qual você está trabalhando e verifique se o envio do sandbox foi bem-sucedido.



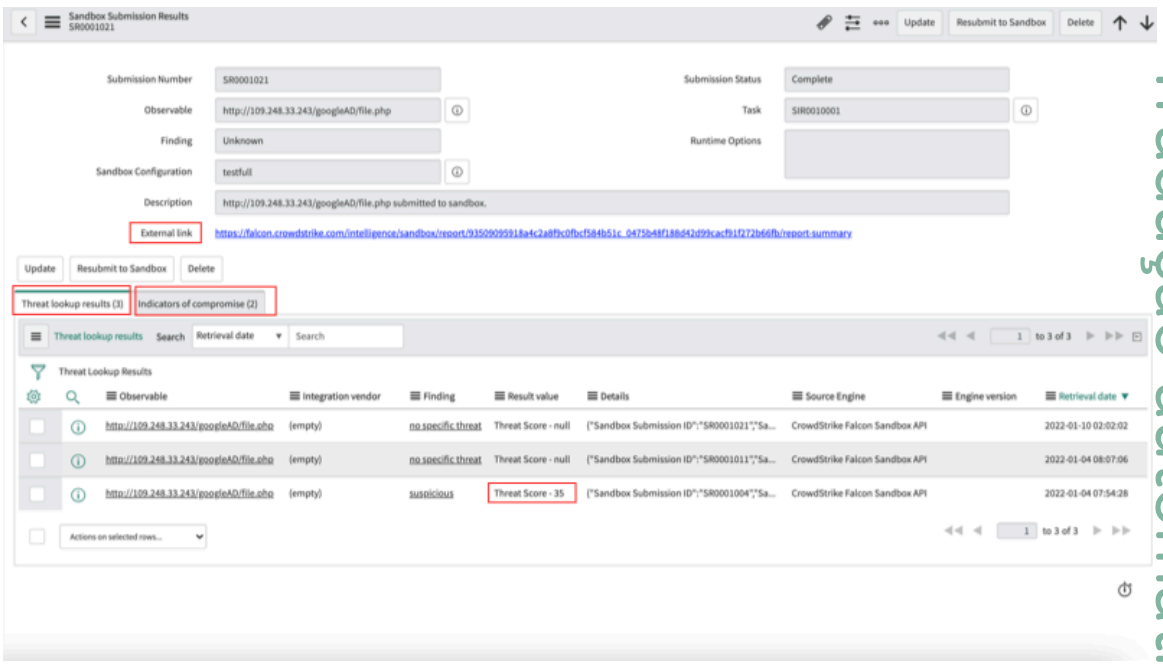
2. Revise as Wanotações de trabalho para obter mais informações e saiba como prosseguir se você puder't verificar se a verificação foi bem-sucedida.
3. Clique no link de resultados completos em Wnota de orks ou em na parte inferior do incidente de segurança, navegue até **Mostrar todas as listas relacionadas**> **Resultados de envio**da área restrita.
   Os resultados são exibidos na guia Resultados de envio da área restrita.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em abrir qualquer registro para exibir a análise completa da secaixa.



5. Opcional: Clique **em Reenviar para área restrita** para reprocessar o observável.

Resultado

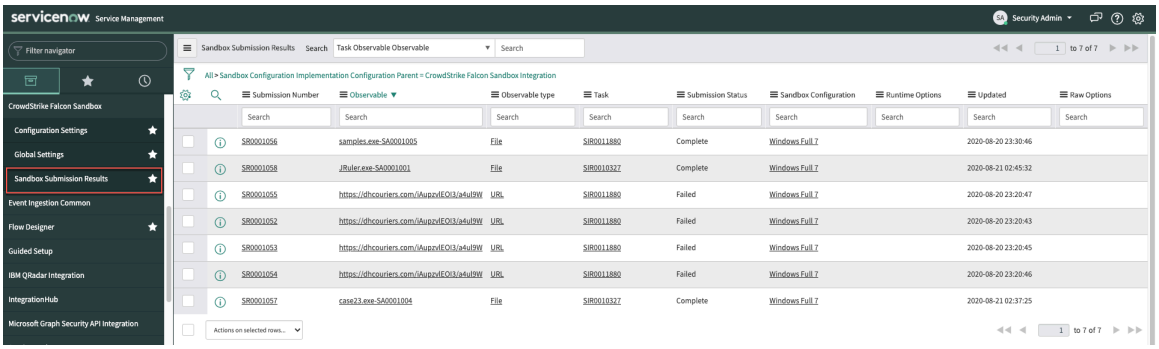
- A guia **Resultados de pesquisa de ameaças** fornece a avaliação da ameaça, incluindo descobertas mal-intencionadas, pontuações de ameaça e detalhes adicionais. Essesdetalhes são fornecidos na estrutura de formato de pesquisa de ameaças padrão para todas as integrações de pesquisa de ameaças ServiceNow.
- A guia **Indicadores de comprometimento** fornece os resultados maliciosos ou suspeitos dosecaixa com as pontuações de Confiança. As pontuações de confiança são semelhantes a outras informações do indicador armazenadas na plataforma ServiceNow. Os indicadores classificados como informativos não estão incluídos nesta guia.
- Clique em **Link externo** para exibir os resultados da Sandbox no portal CrowdStrike Falcon X Sandbox.

Nota:
Esta opção requer que você tenha a função [CrowdStrike Falcon X Sandbox para exibir os resultados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você também pode monitorar os resultados de envio do ebox para todos os incidentes de segurança, navegando até **CrowdStrike Falcon Sandbox** > **Resultados de envio de sandbox**.



Marcar incidentes de segurança com o status de envio da área restrita

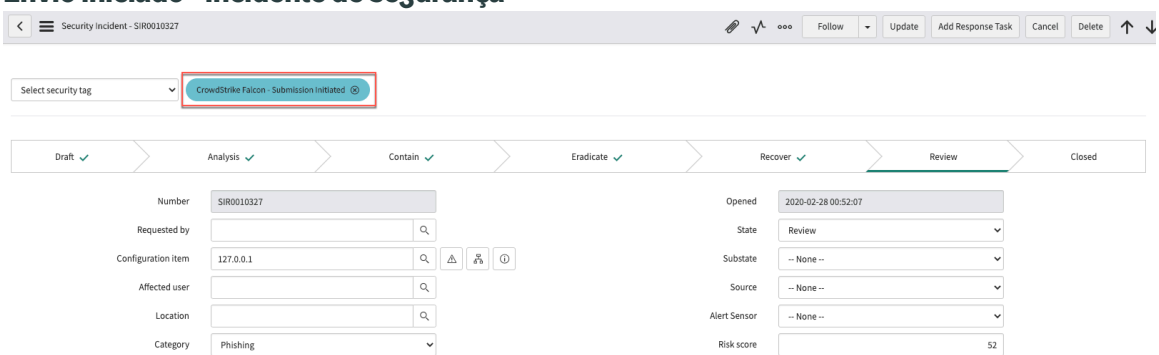
Opcionalmente, você pode marcar os incidentes de segurança com os marcadores Envio iniciado e Envio concluído.

Quando você seleciona a opção **Exibir marcadores** na configuração de envio da Sandbox, os marcadores são exibidos para fornecer o status de um envio de arquivo ou URL. Verificar o status dessa forma é útil porque a] análise da caixa e pode levar vários minutos para ser processada.

Os marcadores de exibição são chamados de envio iniciado, envio concluído e envio com falha.

O exemplo a seguir mostra um incidente de segurança em que o envio foi iniciado.

Envio iniciado - Incidente de segurança

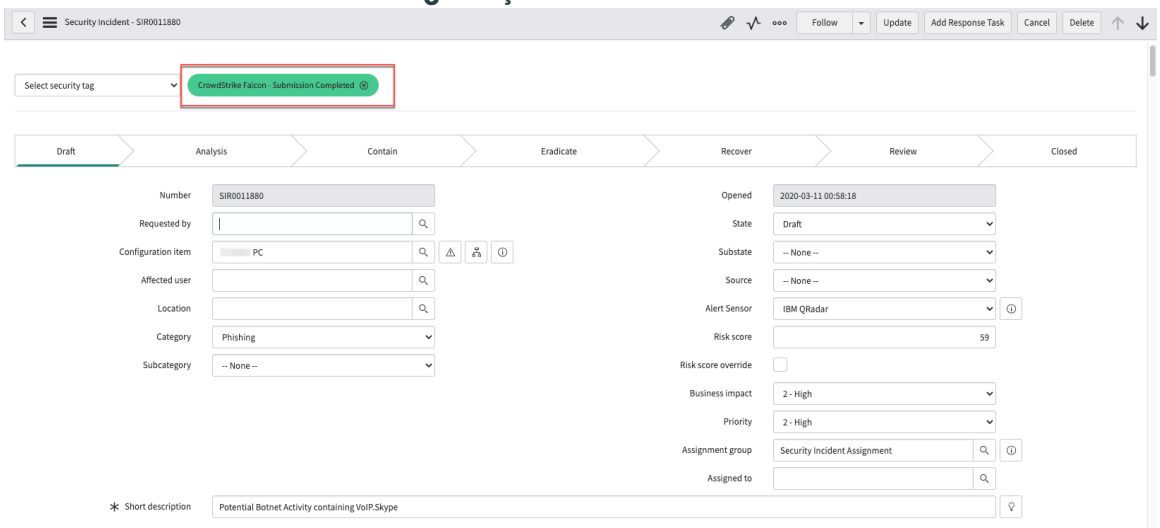


O exemplo a seguir mostra um incidente de segurança em que o envio foi concluído.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Envio concluído - Incidente de segurança



Revisar as configurações globais do andbox

Se você tiver problemas com os resultados de envio de arquivo ou URL, revise e modifique as configurações globais eecaixa.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Sandbox do CrowdStrike Falcon** > **Configurações globais**.
2. Revise e modifique as configurações conforme necessário.

Campo	Descrição
Limite de tamanho de arquivo (MB)	Limite de tamanho de arquivo de carregamento da área restrita em megabytes. **Nota:** O limite de tamanho de arquivo de 256 MB é configurado por padrão. Não aumente o valor para além de 256 MB. No entanto, convém reduzir o limite máximo de tamanho de arquivo para evitar o envio de arquivos grandes.
Tempo limite máximo para envio de resultados (minutos)	Tempo limite máximo para resultados de envio de a caixa se. **Nota:** O tempo limite padrão] é de 30 minutos. Se os resultados demorarem mais de 30 minutos, você poderá aumentar o tempo. Além disso, você pode exibir os resultados no portal [doandbox.

3. Clique **em Salvar** .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração do Elasticsearch Incident Enrichment

A integração Elasticsearch - Incident Enrichment pesquisa seus logs e adiciona informações de vista relevantes aos seus incidentes de segurança.

Explorar Integrações do Security Incident Response	Configurar • Introdução ao Elasticsearch - Incident Enrichment integration • Criar registros de configuração de pesquisa de vistas
Usar • Executar uma pesquisa de vistas • Integração do Security Operations - Fluxo de trabalho de pesquisa de detecções • Security Operations - Fluxo de trabalho de pesquisa de detecções do Elasticsearch	Desenvolver • ServiceNow Security Operations diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Faça ou responda perguntas na comunidade do Security Operations • Pesquise artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Tradução automática

Introdução ao Elasticsearch - Incident Enrichment integration

Elasticsearch é um mecanismo de pesquisa e análise RESTful distribuído que se integra facilmente com Security Operations. Antes de usar a integração Elasticsearch - Incident Enrichment, você deve baixá-la do ServiceNow Store e adicionar a URL base da API e as credenciais de login apropriadas.

Antes de Iniciar

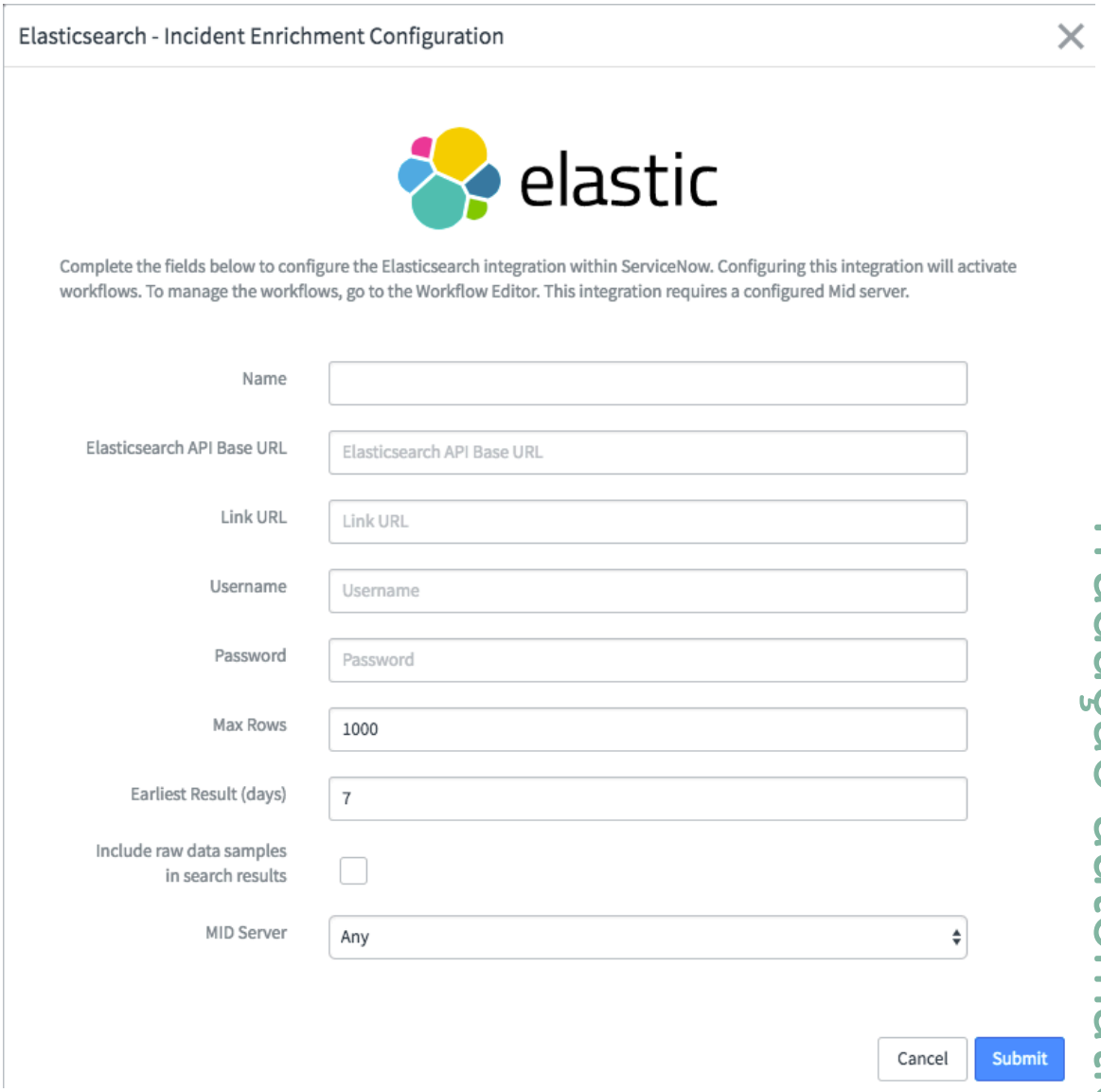
Função necessária: sn_si.admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse Elasticsearch e obtenha a URL base da API no seu perfil do Elasticsearch.
3. Em sua instância, navegue até **Security Operations** > **Integrações** > **Configurações de Integração**. As integrações de segurança disponíveis aparecem como uma série de cartões.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. No cartão Elasticsearch - Aprimoramento de incidente, clique em **Novo**.



5. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
URL de Base da API Elasticsearch	O URL base que você adquiriu no site Elasticsearch.
URL do Link	[Opcional] Links para uma instância do Kibana, quando disponíveis
Nome do usuário	Seu nome de usuário Intel Elasticsearch.
Senha	Sua senha Intel Elasticsearch.
Máx. de Linhas	O número máximo de linhas que você deseja pesquisar.
Resultado Mais Antigo (dias)	Os resultados mais antigos que você deseja ver em número de dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados da pesquisa de detecções. A quantidade de dados retornados depende da configuração na propriedade do **número de linhas de dados brutos** nas propriedades do Security Incident Response.
MID Server	Selecione **Qualquer** para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota:
Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho.

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
8. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Resultado

Depois de configurada, a integração Elasticsearch - Incident Enrichment pode ser selecionada para publicar observáveis em listas de observação no Security Incident Response.

Integração de segurança de endpoint do FireEye

O FireEye Endpoint Security (série HX) ajuda as organizações a inspecionar e analisar quais contêm ameaças conhecidas e desconhecidas em qualquer endpoint.

Os invasores qualificados hoje ignoram as defesas tradicionais nas quais a maioria das equipes de segurança conta há anos para proteger seus endpoints. Mesmo quando uma defesa tradicional interrompe uma ameaça conhecida, ela não pode determinar o que essa ameaça estava tentando fazer. FireEye HX O Endpoint Security ajuda sua equipe de segurança a localizar e interromper ameaças avançadas conhecidas e desconhecidas contra seus endpoints.

A integração do Gold Standard Security Incident Response com FireEye HXtorna mais fácil e eficiente para os analistas de segurança investigar e corrigir incidentes de segurança em um instante, sem precisar navegar entre as ferramentas. Você pode usar a contenção de rede para executar ações de correção nos endpoints, implementar perfis para coletar detalhes específicos sobre o host e executar consultas ou ações específicas no endpoint.

Principais recursos

- Capacidade de executar ações de aprimoramento de host para coletar mais detalhes sobre o endpoint, como detalhes do host, estatísticas de rede, detalhes do usuário, detalhes do arquivo, detalhes do processo e detalhes do serviço.
- Capacidade de executar a Pesquisa de segurança corporativa para detectar possíveis observáveis maliciosos nos endpoints e tomar ações de correção.
- Capacidade de coletar triagem e aquisição de dados para inspeção e análise detalhadas do endpoint.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Limitações

A seguir estão as limitações conhecidas desta integração:

1. O valor do campo da aplicação MID deve ser inserido manualmente.
2. Isolar Host e Obter Serviços em Execução não podem ser executados no agente Linux.
3. Remover isolamento não é compatível com o agente Linux.
4. A aquisição de triagem não é compatível com o agente do Linux.
5. Os usuários precisam configurar os links relacionados a Mostrar dados de aprimoramento. Ele não está disponível para uso imediato.
6. Para a pesquisa de Vistas, somente cinco pesquisas ativas podem estar presentes de uma só vez. O restante será enfileirado e começará após a conclusão de qualquer uma das vistas em andamento.
7. As vistas estão disponíveis prontas para uso, que serão ativas falsas por padrão.
8. O hash não é compatível com Obter processos em execução.

Configure sua instância do NowPlatform para integração do FireEye

Verifique e revise o procedimento de configuração a seguir para configurar a instância NowPlatform para integração FireEye.

Antes de Iniciar
Função necessária: administrador da Now Platform (sn_si.admin)

A seção a seguir lista as tarefas de configuração que devem ser concluídas em sua instância do NowPlatform antes de instalar a aplicação para a integração do FireEye.

Verifique se você concluiu as tarefas a seguir antes de instalar a aplicação da ServiceNow Store.

Tarefa	Descrição
Verifique se você atribuiu as funções necessárias do NowPlatform e do Security Incident Response (SIR).	As seguintes funções são necessárias: 1. O usuário com a função de administrador do sistema (admin) é necessário para instalar a aplicação para a integração. 2. O usuário com a função de administrador de incidentes de segurança (sn_si.admin) é necessário para configurar a integração, criar, ativar e remover perfis. 3. O usuário com a função de analista de incidentes de segurança (sn_si.analyst) é necessário para trabalhar com incidentes de segurança. Um usuário com esta função pode iniciar qualquer um dos recursos disponíveis na integração.
Verifique se você instalou e configurou um MID Server.	Configurar MID Server: um MID Server em sua instância NowPlatform é necessário para gerenciar arquivos e se conectar ao serviço FireEye implantado na rede da organização. Para obter mais

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	informações sobre MID servers, consulte https://docs.servicenow.com
Verifique se as aplicações principais da ServiceNow necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação.	As aplicações a seguir devem ser instaladas e ativadas na ServiceNow Store antes de instalar esta aplicação. Instale e ative um aplicativo de cada vez na ordem listada abaixo para garantir uma instalação sem problemas: **1.** Suporte do Security Incident Response **2.** Security Support Core **3.** Security Support Common **4.** Security Incident Response **5.** Comum de suporte de Inteligência contra ameaças **6.** Instalador do pacote Enterprise do Hub de integração da ServiceNow
Antes de habilitar a opção de aprovação para perfis, verifique se você criou um grupo de aprovação.	Um fluxo de trabalho de aprovação opcional está disponível para isolar máquinas host, restaurá-las na rede, obter o arquivo e executar ações adicionais no endpoint. Se sua organização deseja um nível extra de controle sobre essas ações, habilite a opção Requer aprovação durante a configuração dos perfis. Na ausência de um perfil, se uma capacidade for invocada diretamente da Lista relacionada, as Aprovações poderão ser tratadas no módulo de configuração padrão do FireEye. Como administrador de segurança, você pode configurar a aprovação ao configurar os perfis e as configurações padrão. Um grupo de aprovação deve estar disponível na lista Grupos em sua instância.

Tradução automática

Procedimento

1. Navegar até **Administração de usuários** > **Grupos**.

2. Clicar **Novo** na lista Grupos.

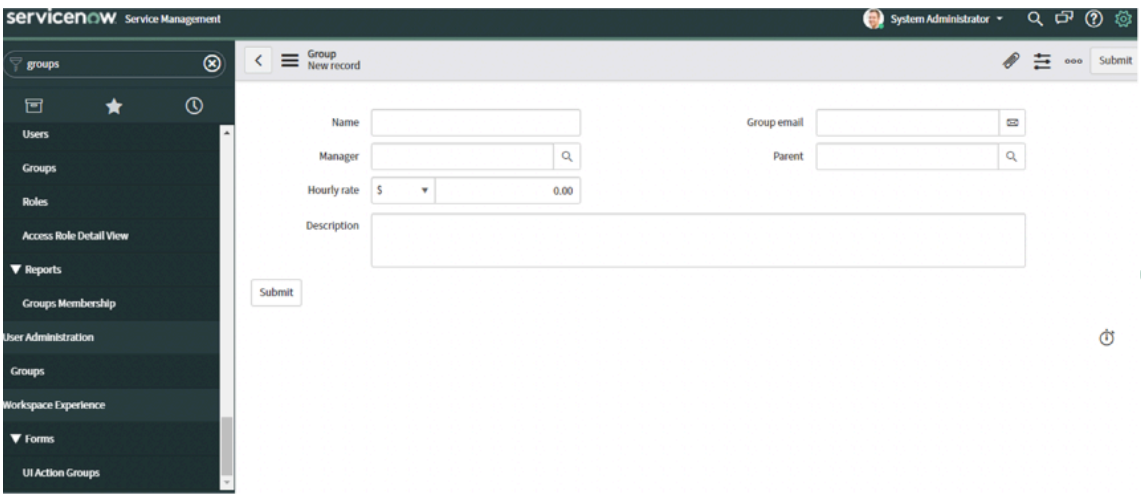
3. Preencha o formulário com os seguintes detalhes:

Campo	Descrição
Nome	Nome do grupo exibido quando uma solicitação de aprovação é enviada.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
E-mail do grupo	(Opcional) Lista de distribuição de e-mail do grupo ou o endereço de e-mail do ponto de contato, como o gerente do grupo.
Gerente	(Opcional) Nome do gerente do grupo. Clique no ícone de pesquisa para exibir a lista.
Primário	(Opcional) Nome do grupo primário, se associado a um primário.
Taxa por hora	(Opcional) O valor pago por hora trabalhada.
Descrição	(Opcional) Informações adicionais sobre o grupo.

4. Clicar **Enviar**.



O novo grupo é exibido na lista Grupos. Você criou com sucesso um grupo de aprovação. Adicione usuários ao novo grupo, conforme necessário, que possam aprovar as solicitações enviadas pelo analista de segurança. Um usuário herda funções de todos os grupos aos quais o usuário pertence. Você também pode atribuir funções diretamente a um usuário.

Para monitorar e processar solicitações enviadas por usuários com a função sn_si.analyst, cada membro do grupo de aprovação deve navegar até Minhas aprovações na Now Platform. Como alternativa, os aprovadores podem encontrar as solicitações enviadas especificamente para a integração do FireEye em Aprovações do FireEye.

O que Fazer Depois

A próxima etapa é instalar e configurar a aplicação da ServiceNow Store.

Como definir configurações de carimbo de data/hora para aquisição de triagem

Configure e verifique as configurações de carimbo de data/hora antes do procedimento de instalação.

Antes de Iniciar

Função necessária: administrador de incidentes do NowPlatform Security (sn_si.admin)

Antes de instalar a aplicação FireEye, existem alguns pré-requisitos que precisam ser realizados no FireEye.

A aquisição de triagem pode ser solicitada com uma entrada do campo "Em torno do carimbo de data/hora" ou do campo "Padrão". Informações de solicitações de carimbo de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

data/hora próximas coletadas durante um período especificado antes do carimbo de data/hora até um período especificado após o carimbo de data/hora. O carimbo de data/hora é a hora em que o evento que gerou o alerta ocorreu. Se você selecionar Padrão, o dispositivo Endpoint Security solicitará informações do host para todos os dados em torno de um evento.

Quando um usuário do Endpoint Security solicita uma coleta de triagem com base em uma data e hora específicas, o agente retorna informações para uma janela de tempo especificada antes e depois do alerta. As configurações de carimbo de data/hora controlam a duração da janela para a coleta de triagem. As configurações de carimbo de data/hora se aplicam somente a eventos de URL de agente (Eventos de monitor de URL) e eventos de chave de registro (Eventos de chave de registro).

Você pode usar a guia Configurações de carimbo de data/hora para especificar o período de tempo antes e depois do carimbo de data/hora durante o qual as informações são coletadas. As configurações de carimbo de data/hora podem variar de 0 a 86400 segundos. O padrão para ambas as configurações é 600 segundos.

Você pode usar a guia Configurações de carimbo de data/hora na página Configurações de triagem automática para especificar o período de tempo antes e depois do carimbo de data/hora durante o qual as informações são coletadas. O carimbo de data/hora é a hora em que o evento que acionou o alerta ocorreu.

Procedimento

1. Navegar até **IU da web de segurança de endpoint**.
2. Selecionar **Administrador** > **Configurações de triagem**.
3. Clicar **Configurações de carimbo de data/hora** guia em **Configurações de triagem automática** página.
4. Especifique o período de tempo antes e depois do carimbo de data/hora para o qual as informações são necessárias.
5. Insira o número de segundos antes do carimbo de data/hora especificado para o qual as informações são necessárias.
6. Insira o número de segundos após o carimbo de data/hora para o qual as informações são necessárias.
7. Clicar **Salvar**.

Nota:
Você pode mudar todos os valores da página de volta para as configurações padrão clicando em **Redefinir para Padrões**e clicando em Salvar.

- **Área do espaço de aquisição**: a página Aquisições mostra quanto espaço em disco resta para as aquisições.
- **Configuração de limites de utilização de disco para aquisições:**
  - Triagens, aquisições de arquivos e aquisições de dados podem se acumular ao longo do tempo e usar uma quantidade crescente de espaço em disco. Para controlar isso, você pode alocar uma quantidade definida de espaço em disco para eles. Dez por cento do espaço em disco especificado é reservado para aquisições de triagem automáticas. Quando o espaço total de aquisição alocado é excedido, as triagens automáticas mais antigas são excluídas.
  - Quando o tamanho total do disco de aquisições concluídas excede um limite especificado, o dispositivo Endpoint Security exclui as aquisições concluídas mais antigas até que espaço em disco suficiente seja liberado para colocar o total abaixo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

do limite especificado. As aquisições que ainda não foram concluídas não são afetadas.

- O dispositivo Endpoint Security excluirá automaticamente as aquisições se um Administrador, Analista ou Investigador usar a IU da Web do Endpoint Security para excluir manualmente o agente associado.

Para definir limites de utilização de disco para aquisições completas usando a IU da Web:

- Navegue até **Endpoint Security Web UI**.
- Selecionar **Limites de utilização de disco** do **Administrador** menu.
- No **Limite de espaço de aquisição** área, especifique a quantidade máxima de espaço em disco (em GB) que pode ser usada para armazenar triagem, arquivos e aquisições de dados. Os valores e padrões válidos variam de acordo com o modelo do dispositivo Endpoint Security. Os valores apropriados para o seu modelo são mostrados na página Limites de utilização de disco.
- Clicar **Salvar**.

Nota:
Todas as configurações mencionadas são respeitadas e, em caso de falhas ou erros, a Now Platform apenas retorna esses erros.

Instalar a aplicação e configurar uma origem para a integração

Instale e configure a aplicação da ServiceNow Store em sua instância da Now Platform.

Antes de Iniciar
Função necessária: administrador do NowPlatform (admin)

Nota:
Um MID Server ativo é obrigatório para configurar uma origem.

Baixe a aplicação Security Incident Response integration with FireEye HX na ServiceNow Store e instale.

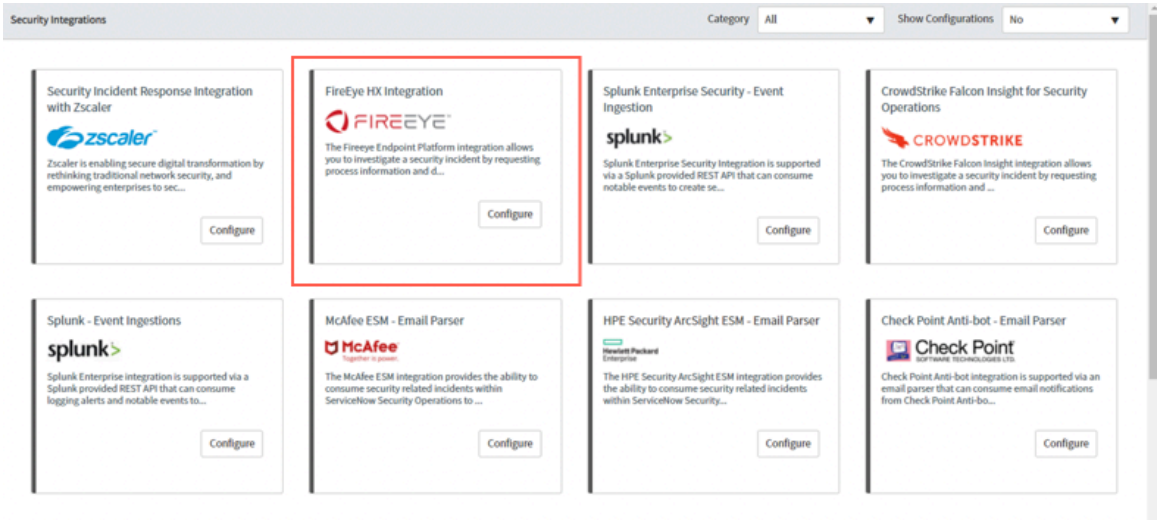
Depois de instalar a aplicação com êxito, siga as etapas abaixo para configurá-la:

Procedimento

1. Navegar até **Integrações** > **Configurações de Integração**.
2. Selecione o **Configurações de Integração** módulo para exibir as integrações disponíveis e localize o **FireEye** bloco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

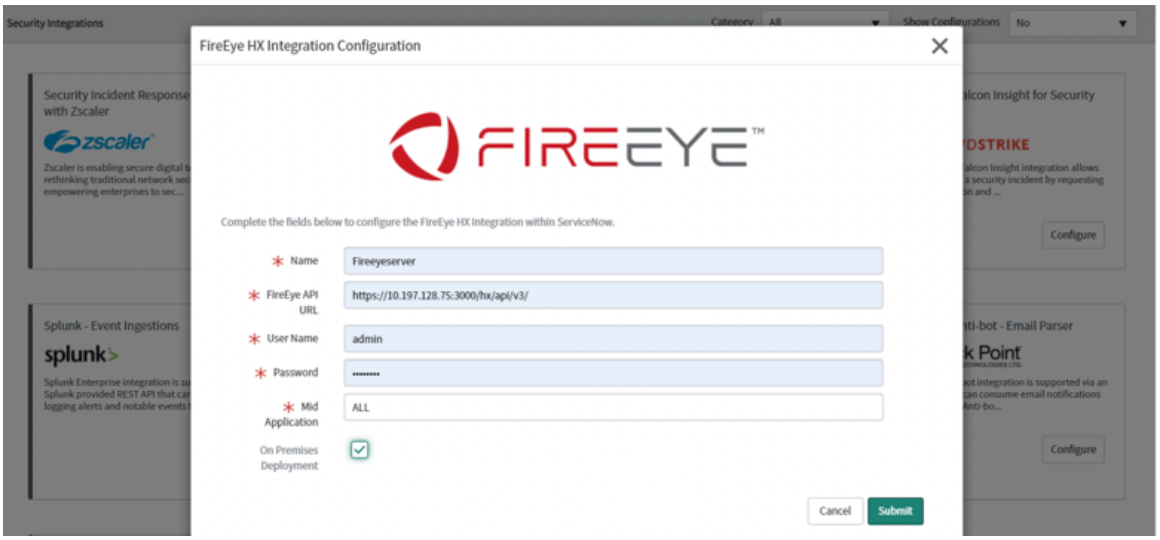


3. Clicar **Configurar** no bloco FireEye.
4. Forneça os seguintes detalhes para configurar a integração do FireEye:

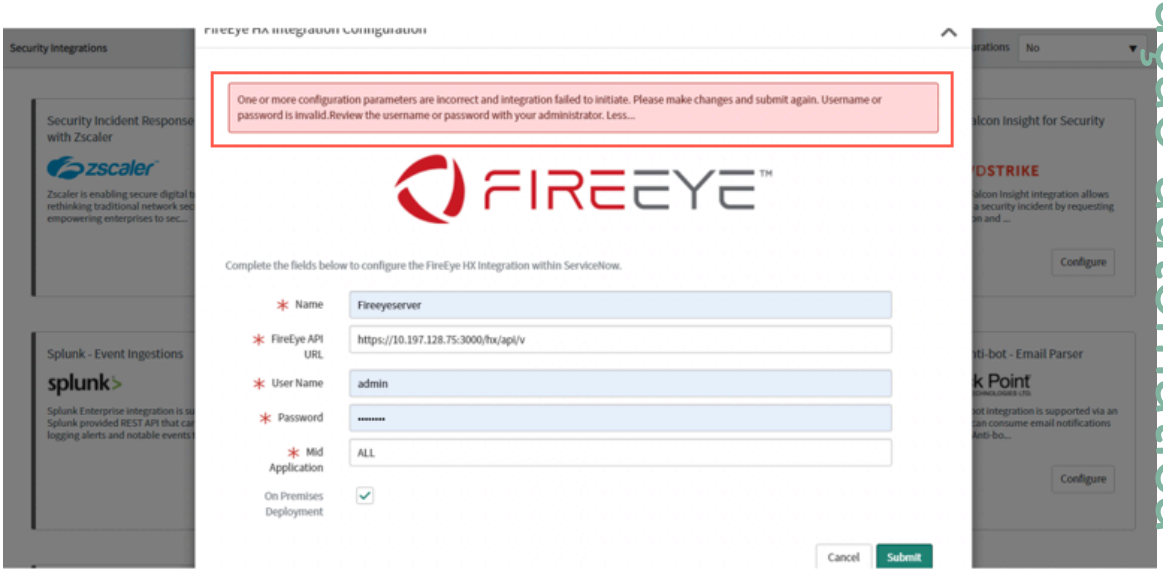
Campo	Descrição
Nome	Nome da configuração do FireEye. Este nome é usado para identificar a origem e as credenciais e configuração associadas. Este nome ajuda a distinguir as credenciais e contas e identifica cada origem para evitar conflitos com perfis.
URL da API	URL base que hospeda a API FireEye.
Nome de usuário	Insira o nome de usuário da conta do FireEye.
Senha	Insira a senha da conta do FireEye.
Aplicação de MID	Aplicação MID que está configurada em seu ambiente. O MID Server é necessário para processar arquivos zip para alguns dos recursos de aprimoramento. Por padrão, será TODOS. Os usuários devem fornecer um nome de aplicação válido manualmente.
Implantação no Local	O padrão é desabilitado. Se você estiver usando a versão baseada em nuvem do FireEye, verifique se a caixa de seleção está desmarcada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clicar **Enviar**.
   A lista Configurações do FireEye é exibida com seu novo registro de configuração. Você concluiu a configuração de um servidor FireEye. Se você não conseguir se conectar ao FireEye ou suas credenciais estiverem incorretas, uma mensagem de erro de validação será exibida, conforme mostrado na figura a seguir. Verifique se suas credenciais estão corretas e tente novamente.



Tradução automática

Configurações padrão do FireEye

A seguir estão as definições de configuração adicionais após a conclusão da instalação.

Depois de concluir a instalação, você pode encontrar o módulo Configurações padrão do FireEye na navegação à esquerda. Ele contém configurações padrão para diferentes funcionalidades do FireEye.

Configurações adicionais

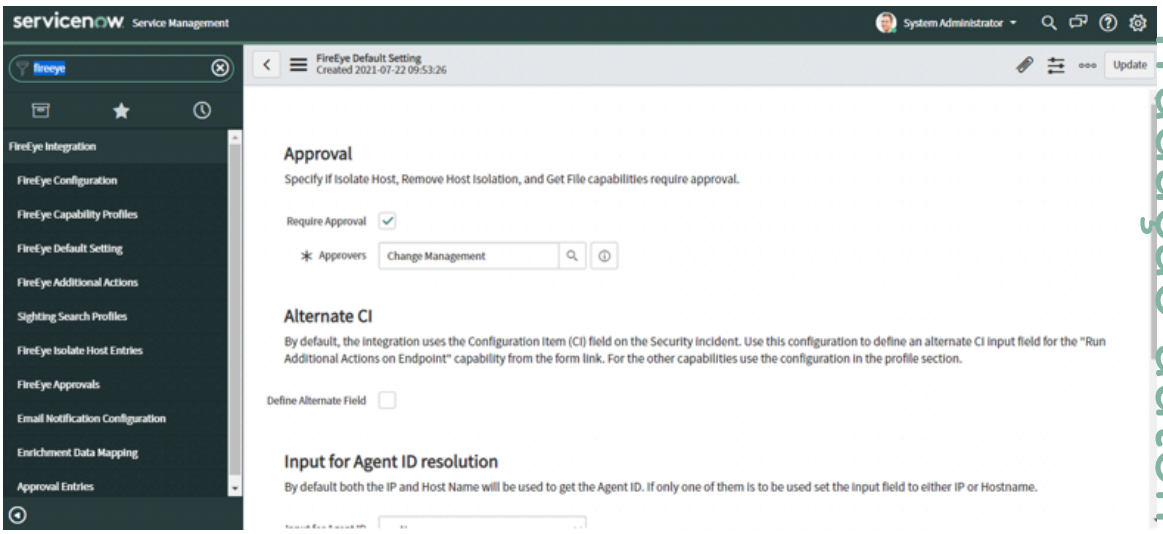
A seguir estão as definições de configuração adicionais:

1. **Aprovação**: Esta aprovação é especificamente para os recursos Isolar Host, Remover Isolamento de Host e Obter Arquivo quando eles são acionados diretamente da Lista relacionada e na ausência de perfis para eles. Se houver/(forem) perfil(is) existente(s) para esses recursos, a configuração de aprovação no perfil será respeitada.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Requer Aprovação:** Quando você habilita Exigir aprovação, o campo Aprovadores fica disponível no formulário.
- **Aprovadores**: Lista de grupos de aprovadores. Depois de enviar uma solicitação, a aprovação é necessária do grupo para concluir a solicitação.

2. **IC alternativo**: habilitar esta caixa de seleção fornecerá uma lista de campos disponíveis para passar um IC alternativo para a capacidade. Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança. Esta configuração é aplicável somente para a capacidade "Executar ações adicionais no endpoint". Portanto, use esta configuração para definir um campo de entrada de IC alternativo somente para a funcionalidade "Executar ações adicionais no endpoint". Para os outros recursos, use a configuração na seção de perfil. Se os perfis não definirem um IC alternativo, os recursos selecionarão o campo IC no formulário Incidente de segurança.
3. **Entrada para resolução de ID de agente**: por padrão, o IP e o nome do host serão usados para obter o ID do agente. Se apenas um deles for usado, defina o campo de entrada como IP ou Nome do host.

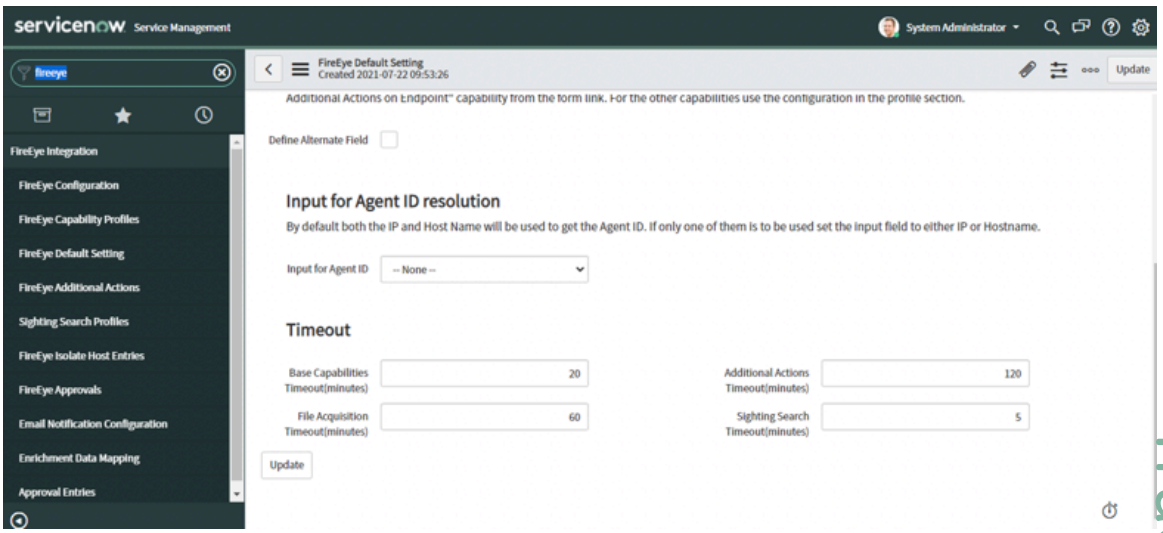


4. **Tempo limite**:
   - **Tempo limite das capacidades básicas (minutos):** Os recursos Aprimoramento, Isolar Host e Remover Isolamento de Host falharão se nenhuma resposta for renderizada no tempo definido.
   - **Tempo limite de ação adicional (minutos):** A execução de ações adicionais na capacidade do endpoint falhará se nenhuma resposta for renderizada no tempo definido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Tempo limite de aquisição de arquivos (minutos):** O recurso Obter arquivo falhará se nenhuma resposta for renderizada no tempo definido.
- **Tempo limite de pesquisa de detecções (minutos):** A pesquisa será interrompida após o tempo definido.



Criar um novo perfil de capacidade para a integração do endpoint do FireEye

Crie um perfil e selecione os recursos FireEye HX que você deseja que o perfil execute.

Antes de Iniciar
Função necessária: administrador de incidentes do NowPlatform Security (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa
Os perfis são criados para agrupar recursos e ajudariam os analistas a executar a investigação/correção com facilidade.

A seguir está a lista de capacidades que você pode adicionar ao(s) perfil(is):

1. Obter detalhes do host
2. Obter usuários conectados
3. Obter Estatísticas de Rede
4. Obter Processos em Execução
5. Obter serviços em execução
6. Obter arquivo
7. Isolar Host
8. Remover isolamento

Você não pode combinar as capacidades Obter arquivo, Isolar host e Remover isolamento de host com outras capacidades ao criar um perfil. Os perfis para eles devem ser criados individualmente. Por outro lado, Obter detalhes do sistema, Obter usuários conectados, Obter estatísticas de rede, Obter processos em execução e Obter serviços em execução podem ser combinados. Você pode criar perfis individualmente ou agrupando-os na íntegra ou em partes de acordo com sua necessidade. Depois que uma funcionalidade é incluída em um perfil, ela não pode ser incluída em outro perfil.

Para criar um novo perfil de capacidade, siga estas etapas:

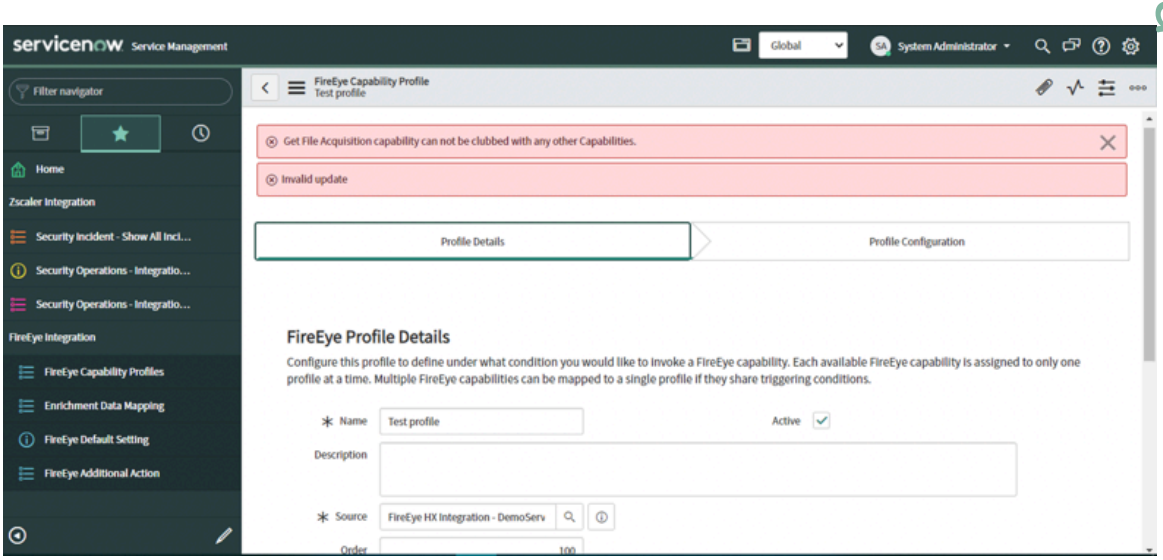
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Integração do FireEye** > **Perfis de capacidade do FireEye**.
   A lista de perfis de capacidade é exibida.
2. Clicar **Novo**.
3. No formulário, preencha os campos.

Nome	Nome do perfil de recurso FireEye HX. Este nome ajuda a identificar o tipo de perfil e a descrevê-lo.
Descrição	Informações adicionais sobre o perfil que descrevem melhor o perfil.
Origem	Nome da origem FireEye HX. Somente origens configuradas estão disponíveis na lista de seleção.
Capacidades do FireEye HX.	Recursos do perfil FireEye HX. Selecione os recursos desejados para este perfil na coluna Disponível e mova-os para a coluna Selecionado.
Ordem	Prioridade de fluxo. O padrão é 100. O valor deste campo indica a ordem em que os Fluxos são executados quando dois ou mais perfis compartilham condições de acionamento. O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300, 400.
Ativo	Isso indica que o perfil está ativo. Quando o perfil está ativo, ele é acionado automaticamente quando um incidente de segurança é criado que corresponde às condições de filtragem que você especificou na configuração.

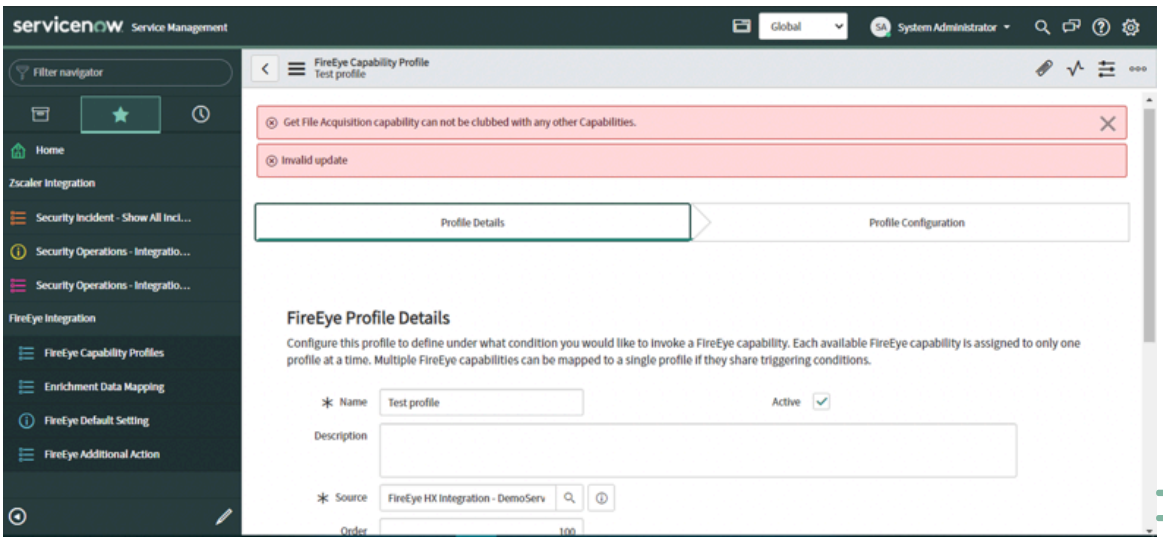


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A figura a seguir é um exemplo de um formulário preenchido para detalhes de perfil com o recurso Obter detalhes do host.

4. Clicar **Avançar** para continuar para Configuração de perfil.



Nota:
As capacidades Isolar Host, Remover Isolamento de Host e Obter Arquivo não podem ser combinadas com outras capacidades.

O que Fazer Depois

A próxima etapa é configurar seu perfil. Antes de definir as configurações do perfil, talvez você prefira revisar os conceitos de configuração de perfis e condições de gatilho. Para obter mais informações, consulte Entenda como as condições do gatilho funcionam com um item de configuração para um perfil.

Entenda como as condições do gatilho funcionam com um item de configuração

Depois de criar um perfil e selecionar os recursos do FireEye que você deseja que o perfil execute, defina as configurações do perfil para que ele seja executado somente quando um conjunto de condições específicas for atendido.

Você pode definir condições do gatilho para que o perfil seja executado automaticamente sempre que um incidente de segurança correspondente à condição do gatilho for criado. Se a condição do gatilho não estiver definida, esses perfis poderão ser executados manualmente, clicando no formulário "Executar perfil(is) de EDR" no incidente de segurança e selecionando o perfil.

Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança. Este valor é usado para corresponder os IDs dos seus ativos às informações armazenadas no CMDB da Now Platform. Quando um incidente de segurança é criado e um perfil é executado automaticamente ou manualmente, o CMDB é pesquisado para recuperar o nome do host e/ou o endereço IP com base no valor do campo IC. O nome do host e ou IP é usado para resolver o ID do agente em FireEye HX para identificar o endpoint.

Em um caso ideal, um valor correspondente é encontrado no banco de dados e os dados são coletados do console FireEye HX para o ativo correspondente. Os dados de vários recursos são inseridos em sua instância da Now Platform e exibidos nas listas relacionadas de incidentes de segurança. Quando o campo Item de configuração (IC) não estiver preenchido no incidente de segurança com um nome de host ou um endereço IP que corresponda ao banco de dados, você poderá selecionar um campo alternativo no incidente

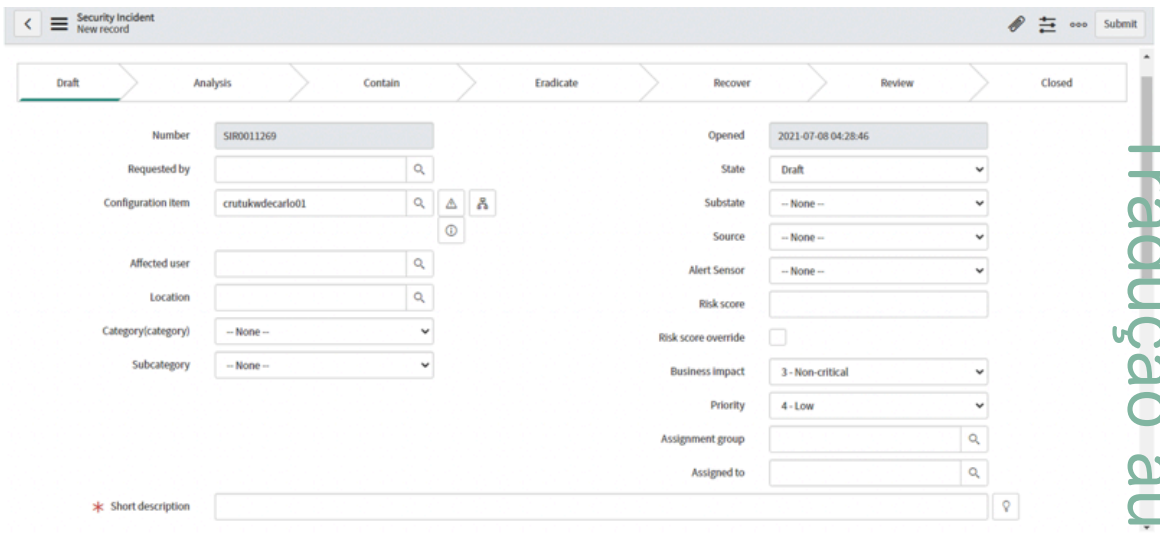
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de segurança que contenha o nome do host ou o IP a ser executado a resolução do ID do agente.

Durante a etapa de configuração da configuração do perfil, você pode selecionar um campo de IC alternativo para identificação do endpoint para garantir que você possa identificar o endpoint em FireEye HX. Você pode selecionar qualquer campo no incidente de segurança como um campo de gatilho de IC alternativo, incluindo campos personalizados que você cria. Ao selecionar este campo de IC alternativo como backup, você garante que seus perfis sejam executados mesmo se o campo de IC não estiver preenchido no incidente de segurança associado na criação do incidente.

Nota:
Os campos de IC alternativos são considerados somente para recursos que podem ser adicionados a um perfil. Para todas as ações adicionais, o IC alternativo é selecionado na página de configurações padrão.



Configurar perfis e incidentes de segurança para a integração FireEye HX

Depois de criar um perfil e selecionar os recursos FireEye HX que você deseja que o perfil execute, defina as configurações para que o perfil possa ser invocado somente sob as condições definidas.

Antes de Iniciar
Função necessária: sn_si.admin

Configure o perfil para que ele seja executado somente quando as condições especificadas forem atendidas. Selecione um campo de entrada alternativo para o campo Item de configuração (IC), se necessário, e defina as condições de filtragem para que o perfil possa ser acionado automaticamente quando um incidente de segurança que atende às condições do gatilho for criado.

Nota:
Você pode navegar até o **Configuração de perfil** página somente depois de inserir o **Detalhes do perfil**.

Procedimento

1. Navegar até **Integração do FireEye** > **Perfis de capacidade do FireEye**.
2. Clicar **Avançar** em **Detalhes do perfil** página depois de concluir a seção de detalhes do perfil.
3. Revise e configure as seguintes seções:

Tradução automática

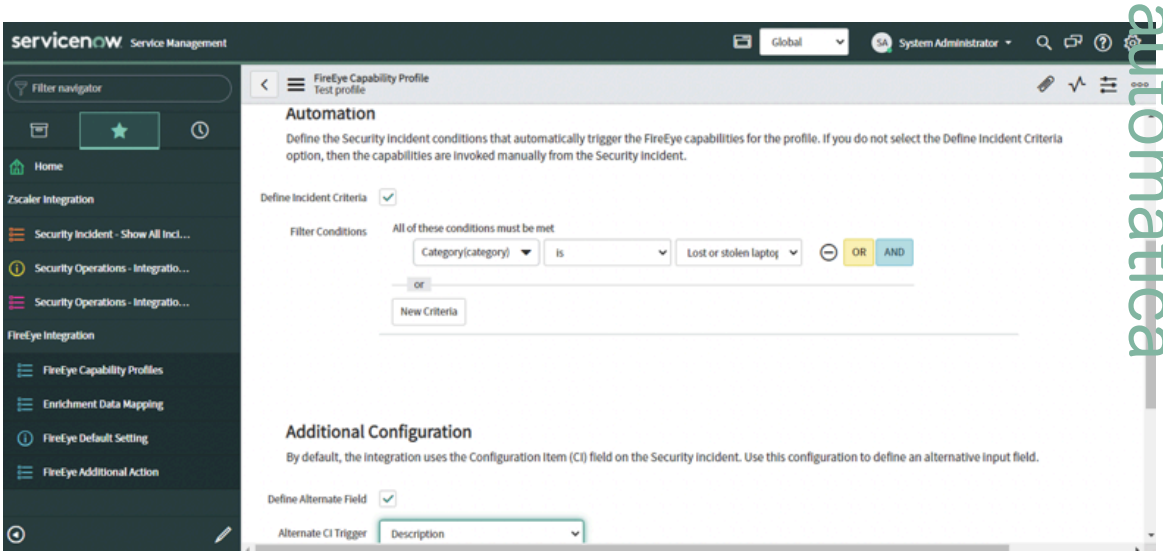
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Definir critérios de incidente (automação)**: define as condições de incidente de segurança que acionariam automaticamente os recursos FireEye HX para o perfil. Se você não selecionar o **Definir critério de incidente** Com a opção, o perfil e os recursos subjacentes podem ser invocados manualmente a partir do incidente de segurança.
  - Selecionar **Definir critério de incidente** Opção para acionar automaticamente FireEye HX recursos no perfil.
  - No **Condições do filtro**, selecione o campo obrigatório.
  - Você pode adicionar **Novos critérios** e também definem a condição OR ou AND.

  Nota:
  Isolar Host, Remover Isolamento de Host, Obter Arquivo não podem ser acionados automaticamente.

- **Configuração adicional**: quando o campo Item de configuração (IC) não estiver preenchido no incidente de segurança com um nome de host ou um endereço IP que corresponda ao banco de dados, você poderá selecionar um campo alternativo no incidente de segurança para consultar as FireEye HX APIs.
  - Selecione o **Definir campo alternativo** Opção para definir um campo de entrada alternativo.
  - Selecione o campo de entrada em **Campo de gatilho de IC alternativo**.

  Nota:
  Para obter mais informações, consulte Entenda como as condições do gatilho funcionam com um item de configuração.

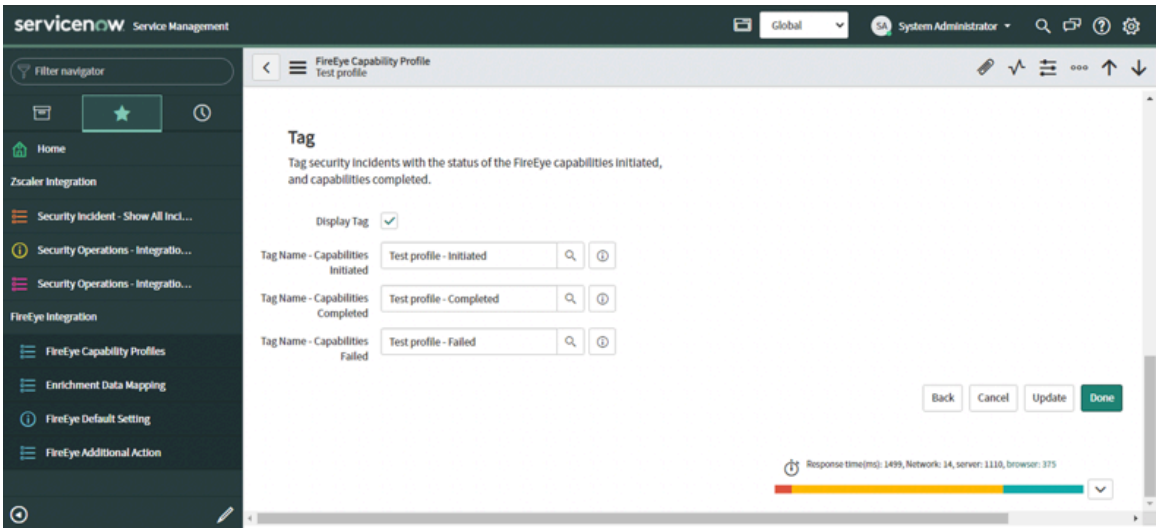


- **Marcadores**: opcionalmente, você pode marcar os incidentes de segurança com os marcadores de perfil iniciado FireEye HX, perfil concluído e perfil com falha.

  Selecione o **Marcador de exibição** caixa de seleção para habilitar a marcação de incidentes de segurança, o nome do perfil é prefixado ao habilitar a marcação. Por padrão, esta opção está desabilitada para todos os perfis.

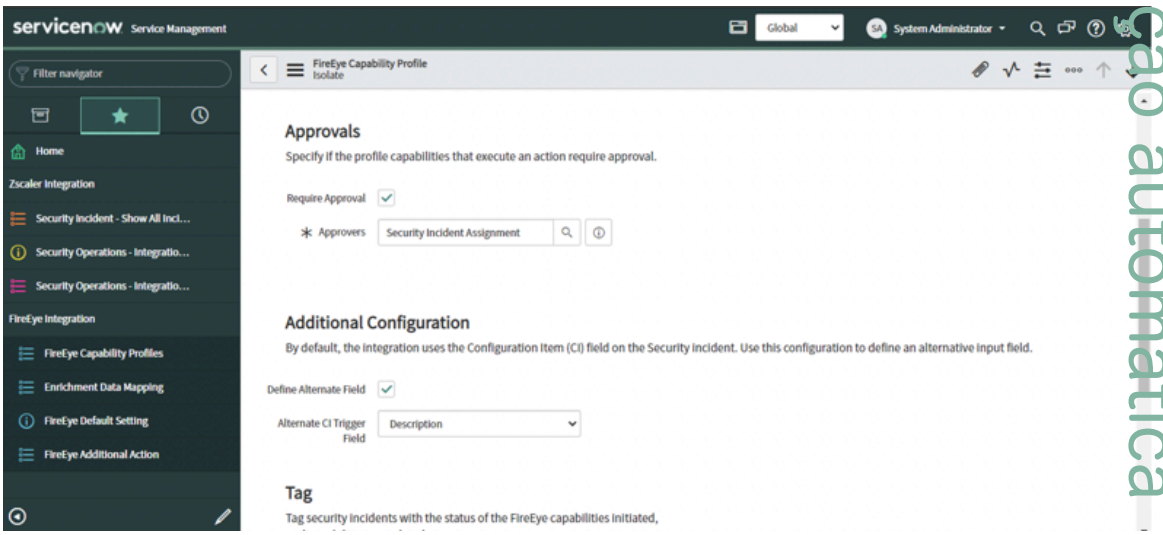
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- **Aprovações**: selecione o **Requer Aprovação** caixa de seleção para fornecer um nível extra de controle ao usar os recursos FireEye HX para isolar máquinas host, restaurá-las na rede e para obter os arquivos.

  A opção de aprovações na configuração do perfil aparece somente para os recursos Isolar Host, Remover Isolamento de Host e Obter Arquivo.



Tradução automática

4. Clique em **Concluído**.
5. Verifique as condições do gatilho FireEye HX.

Verificar os filtros de condição do gatilho

Teste o perfil e verifique se os filtros de condição do gatilho que você configurou estão funcionando conforme o esperado.

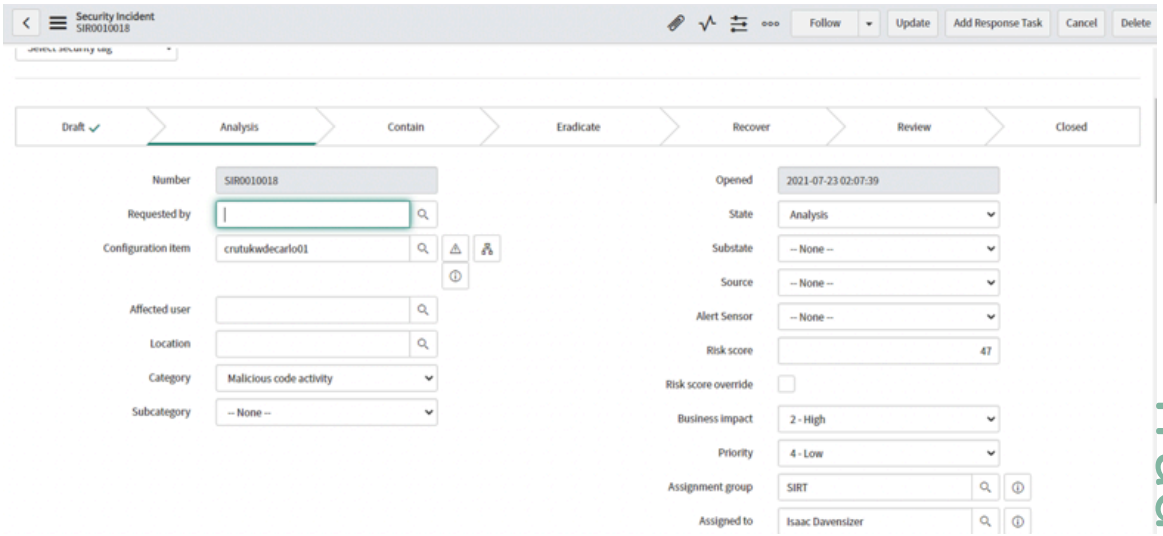
Antes de Iniciar
Função necessária: sn_si.admin ou sn_si.analyst

Depois de ativar o perfil, com base nas condições do gatilho configuradas, você pode exibir os resultados da consulta nos incidentes de segurança da Now Platform.

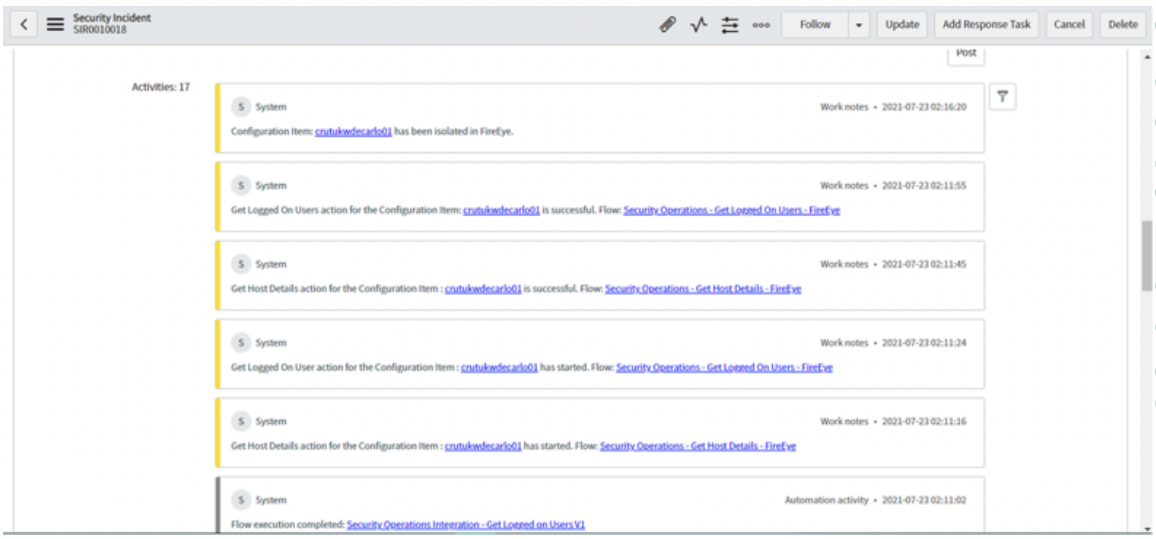
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecionar **Novo** para criar um novo incidente de segurança.
3. Forneça as condições de filtro conforme fornecidas no perfil de recurso para acionar o respectivo perfil.



4. Clicar **Salvar**.

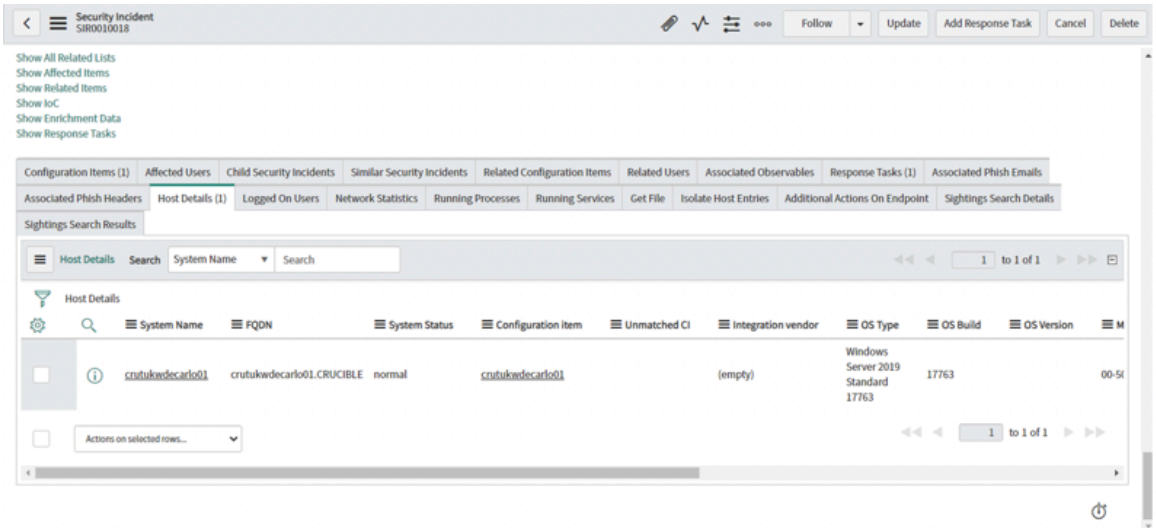


5. Revise as anotações de trabalho e a seção de atividades.
6. Exiba o perfil iniciado, o perfil concluído ou os marcadores com falha no perfil.
7. Clicar **Mostrar todas as Listas relacionadas**.
8. Clique em qualquer lista relacionada (guia).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por exemplo, Detalhes do host.



Acionar um perfil de capacidade do FireEye em Links relacionados

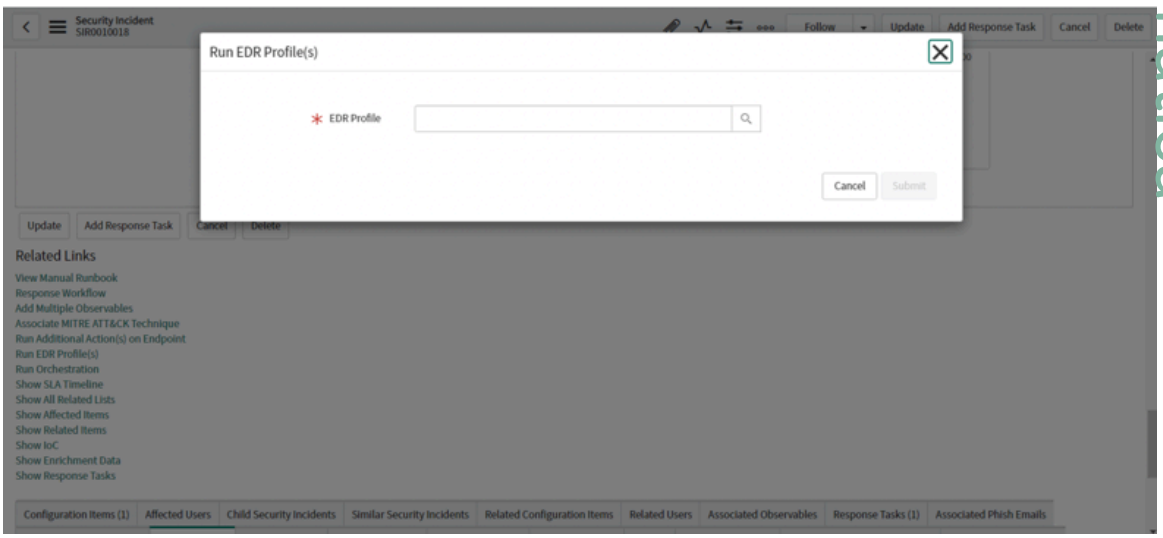
Acione um perfil de recurso manualmente depois de revisar um incidente de segurança de links relacionados.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Procedimento

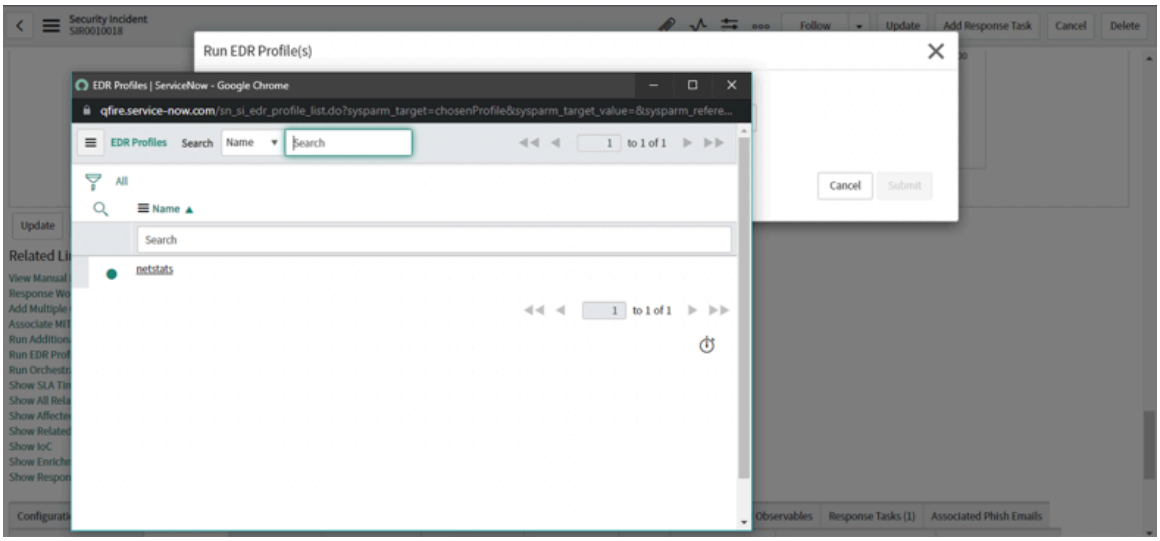
1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar.
3. Clicar **Executar perfil(is) de EDR**na seção de links relacionados.

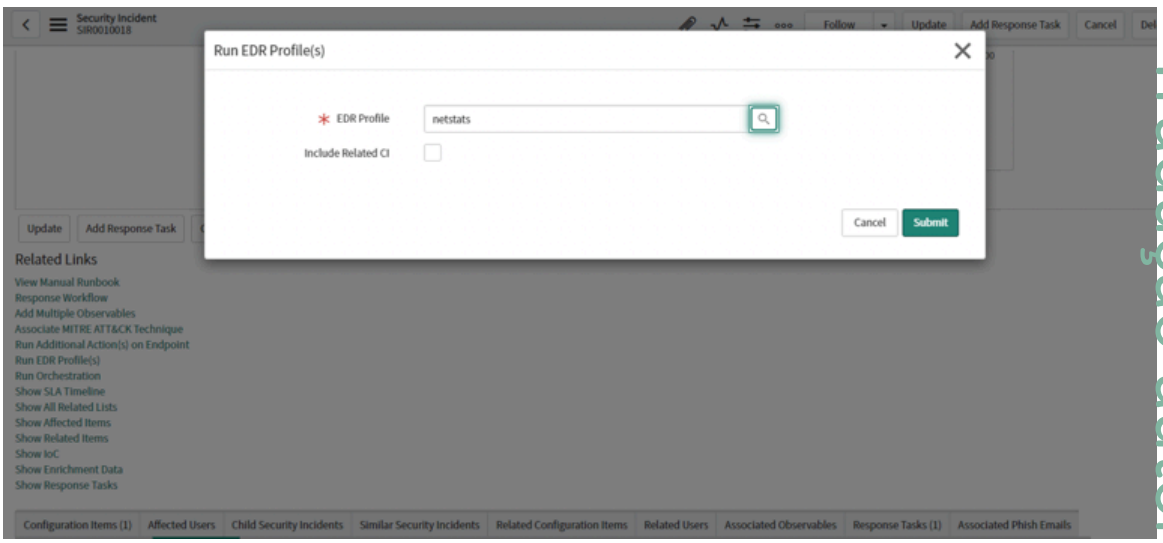


4. Pesquise e selecione um perfil na lista de perfis disponíveis e clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.





Tradução automática

5. O perfil selecionado é acionado manualmente.
6. Revise as anotações de trabalho e a seção de atividades.
7. Exiba os marcadores e verifique as listas relacionadas dos dados.

Nota:
Além de executar o perfil do IC ou o IC alternativo do incidente de segurança, você também pode executar o perfil dos valores de IC presentes na lista relacionada Item de configuração marcando a caixa de diálogo Incluir IC relacionado. Isso também buscará dados para os valores de IC presentes na lista relacionada. Como alternativa, você pode executar o perfil apenas para os valores de IC presentes na lista relacionada.

Acionar um perfil de capacidade do FireEye da lista relacionada de item de configuração

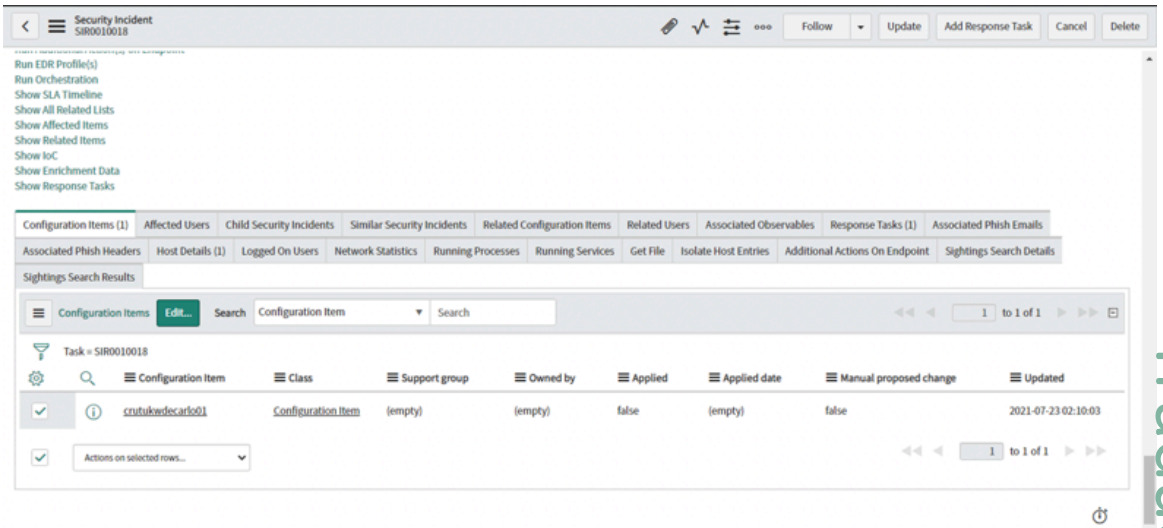
Acione um perfil de recurso manualmente a partir da lista relacionada do item de configuração.

Antes de Iniciar
Função necessária: sn_si.admin, sn_si.analyst

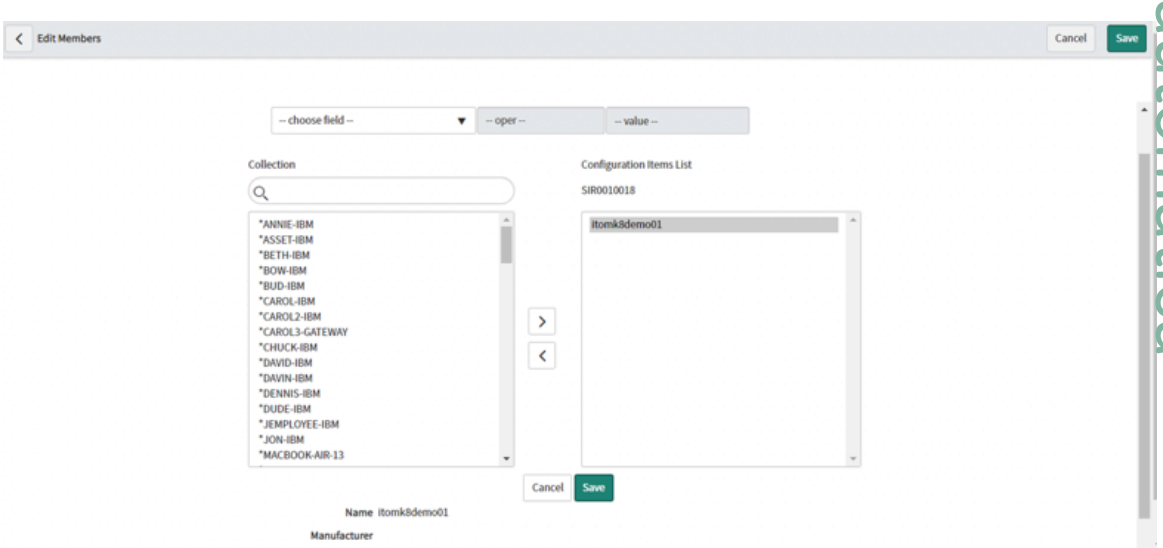
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações FireEye HX.
3. Clicar **Mostrar todas as listas relacionadas** na seção de listas relacionadas.
4. Clique no botão **Item de Configuração** lista relacionada.



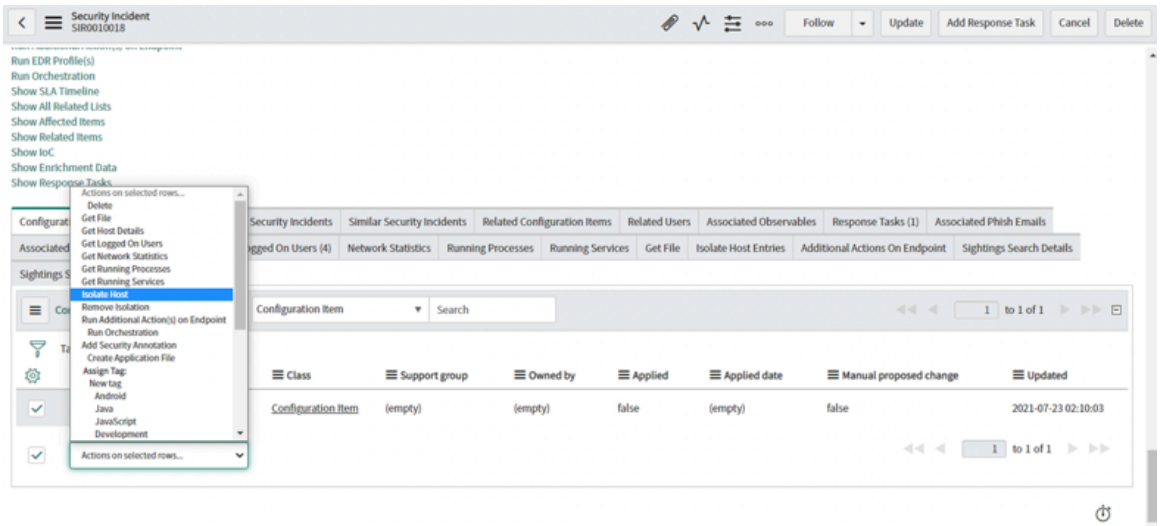
5. Clicar **Editar** para adicionar os itens de configuração disponíveis, se os valores ainda não estiverem presentes, e clique em **Salvar**.



6. Selecione o(s) item(ns) de configuração adicionado(s) e, em Ações nas linhas selecionadas, selecione um recurso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. A funcionalidade selecionada é acionada manualmente.
8. Revise as anotações de trabalho e a seção de atividades.
9. Exiba os marcadores e verifique os dados nas listas relacionadas.

Capacidade de obtenção de arquivo do FireEye

As solicitações de aquisição de arquivo instruem um Endpoint Security Agent a obter um arquivo do endpoint do host. As aquisições de arquivos são usadas para análise estática ou dinâmica de compromissos potenciais ou verificados, bem como para retenção de evidências durante investigações de ameaças internas. A capacidade Obter arquivo deve ser criada como um perfil separado.

Antes de Iniciar

Função necessária: administrador

Acionar Obter perfil de arquivo e criar um perfil de recurso FireEye HX com **Obter arquivo** capacidade.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar.
3. Clicar **Executar perfil(is) de EDR**na seção de links relacionados.
4. Procure e selecione Obter perfil de arquivo na lista de perfis disponíveis.
5. Forneça o **Nome de arquivo** e **Caminho do arquivo**.

> **Nota:**
> Insira o nome do arquivo para o qual você deseja adquirir. Especifique um nome de caminho preciso ou outra variável de ambiente do Windows baseada em caminho apropriada. Você deve especificar a letra da unidade ou os nomes do caminho. Endpoints diferentes podem ter mapeamentos de unidade diferentes. Se você especificar explicitamente um nome de pasta, poderá terminar o caminho com uma barra invertida. No entanto, a barra invertida final não é obrigatória.

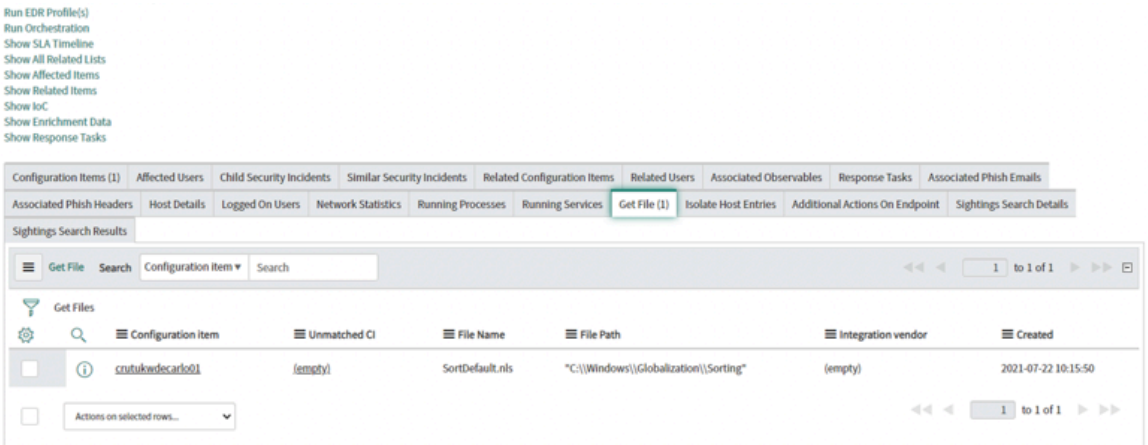
6. Clicar **Enviar**.
7. Revise as anotações de trabalho e a seção de atividades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Exiba os marcadores e verifique os resultados no **Obter arquivo** lista relacionada.

Nota:
O perfil Obter arquivo agora é acionado manualmente.



Para revisar uma aquisição de arquivo baixada:

- Abra o arquivo .zip de aquisição.
- Insira a senha necessária para abrir o arquivo. A senha pode ser exibida passando o mouse sobre o link de download no console FireEye HX. Siga as etapas abaixo para exibir a senha:
  - Faça login no console do FireEye HX.
  - Navegar até **Aquisições** e filtre por Tipo de aquisição - Arquivo.
  - Selecione o registro desejado.

    Nota:
    Você poderá ver os detalhes do arquivo adquirido na guia à direita.

  - Passe o mouse sobre **Baixar** link disponível na parte superior para obter a senha.

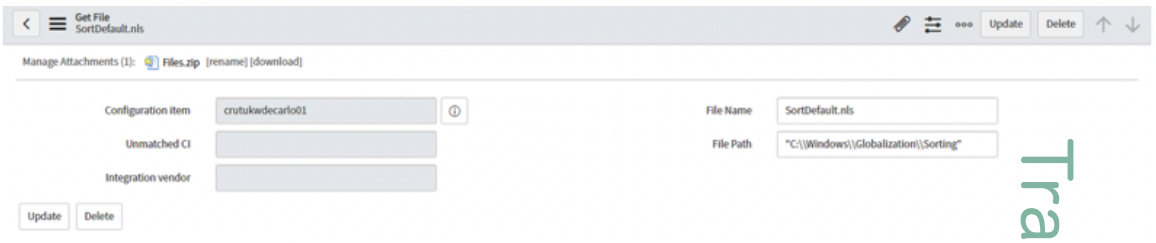
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

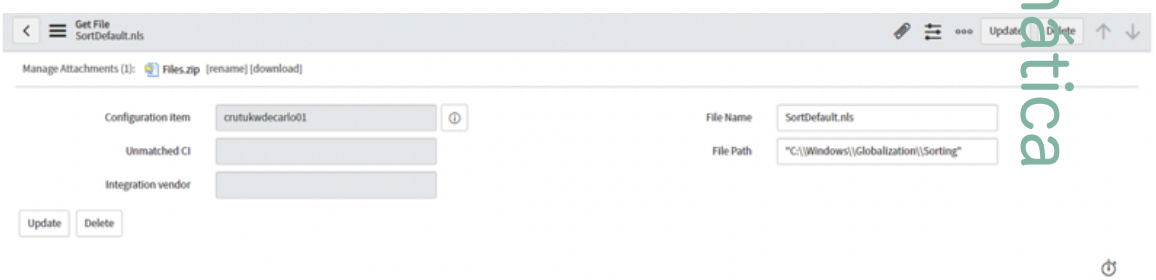
- Abra e revise os arquivos dentro do arquivo .zip usando qualquer editor de texto ou XML.

Nota:

- É recomendável que o arquivo recuperado seja adicionado como um observável manualmente, para que ele possa ser rastreado como uma evidência em relação ao incidente de segurança. Isso também ajudará a exibir os arquivos no futuro, quando a senha for esquecida ou alterada.
- O tamanho máximo de arquivo compatível com a ação Obter arquivo é de 1024 MB e esse valor pode ser configurado alterando **com.glide.attachment.max_size**e o tempo limite padrão é de 60 minutos, que pode ser configurado na página FireEye HX Configurações padrão.



- Obter arquivo também pode ser acionado na lista relacionada de itens de configuração.



Tradução automática

Ações adicionais do FireEye no endpoint

A integração do FireEye oferece suporte à execução de ações adicionais além das ações padrão-ouro.

Essas ações compreendem a aquisição de triagem e as aquisições de dados. Duas aquisições de dados prontas para uso são compatíveis:

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Script de detalhes investigativos abrangentes
- Script de detalhes de investigação padrão

Além disso, a Aquisição de triagem também é compatível imediatamente. Todos esses três são criados por padrão junto com a origem. Os clientes também podem criar suas próprias ações, ou seja, aquisições de dados do módulo de ações adicionais do FireEye. [1] O tamanho máximo de arquivo compatível com as ações adicionais do FireEye é 1024 e esse valor pode ser configurado alterando **com.glide.attachment.max_size**e o tempo limite padrão é de 120 minutos, que pode ser configurado na página de configuração padrão do FireEye.

Script de detalhes investigativos abrangentes

Permite a coleta de todos os artefatos forenses e de investigação do endpoint, mas é a opção mais proibitiva. Esta configuração é ideal para situações em que haverá apenas uma janela para coletar dados do endpoint em questão e a capacidade de adquirir mais dados não pode ser garantida posteriormente. Portanto, use esta ação com cuidado.

Script de detalhes de investigação padrão

Habilita as opções mais comuns para coletar artefatos forenses e de investigação de um endpoint. Deve ser a ferramenta de resposta primária quando você suspeita que um endpoint pode estar comprometido e precisa executar uma análise detalhada desse endpoint. Tem como objetivo encontrar um equilíbrio entre coletar os dados mais relevantes e valiosos, evitando as opções caras que podem ser coletadas posteriormente, quando uma investigação mais aprofundada se mostrar necessária.

Aquisição de triagem

As coleções de triagem contêm informações do cache de lookback, bem como informações adicionais de auditoria forense, como histórico de download de URL, histórico de download de arquivo, listagens de processos e portas e informações do sistema padrão. Você pode querer examinar essas informações quando um tráfego de rede anômalo for detectado e quiser mais visibilidade sobre as ações do endpoint.

Manutenção de scripts de aquisição de dados no FireEye

As solicitações de aquisição de dados (às vezes chamadas de solicitações de resposta em tempo real) permitem que você adquira todos os dados necessários de um único endpoint em execução. Usando a página Scripts de aquisição de dados no FireEye, você pode criar, editar, copiar e excluir os scripts de aquisição de dados usados para solicitações de aquisição de dados.

Como acessar a página de scripts de aquisição de dados no FireEye

Para acessar a página Scripts de aquisição de dados:

1. Navegue até Endpoint Security interface do usuário da web.
2. Selecione Scripts de aquisição de dados no menu Administrador.

Como criar um script no FireEye

Para criar um script de aquisição de dados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Selecionar **Scripts de aquisição de dados** > **Administrador** menu da interface do usuário da Web do Endpoint Security.
2. Clicar **Criar script**.
3. Insira um nome para o novo script no **Nome do script** campo.
4. Opcionalmente, insira uma descrição do script.
5. Selecione o sistema operacional ao qual o script se aplica. Você só pode selecionar um único sistema operacional na caixa de diálogo Criar script.
6. Clicar **Criar** para iniciar a definição do script.
7. Selecione um tipo de dados de aquisição no **Adicionar um tipo de aquisição**caixa suspensa e clique em **Adicionar**. As opções para o tipo de aquisição solicitado aparecem à direita da lista de scripts.
8. Forneça valores para as opções de tipo de aquisição ou use os valores padrão que já estão selecionados. A IU da Web não avisa ou remove guias, espaços ou caracteres indesejados (como \n) em suas especificações.
9. Repita as duas etapas anteriores para solicitar dados adicionais para o script de aquisição de dados. Alguns tipos de dados de aquisição estão disponíveis apenas uma vez para um script, enquanto outros podem ser especificados mais de uma vez. Depois de adicionar um tipo de aquisição a um script, a lista de tipos de aquisição disponíveis no **Adicionar um tipo de aquisição**A caixa suspensa se ajusta corretamente.
10. Para remover um tipo de dados de aquisição do script, clique no ícone x ( ) na guia de aquisição no lado esquerdo da página.

Nota:
Esta integração não é compatível com **Permitir edições antes de adquirir** opção ao criar scripts. Portanto, certifique-se de que a caixa de seleção esteja desmarcada.

Exportar um script do FireEye

Você pode exportar um script de aquisição de dados para um arquivo JSON. Para exportar um script de aquisição de dados:

1. Selecionar **Scripts de aquisição de dados** > **Administrador** da interface do usuário da Web do Endpoint Security.
2. Selecione Scripts de aquisição de dados no menu Administrador.
3. Selecione o script que você deseja exportar no lado esquerdo da página.
4. selecionar **Ação/ Comportamento** > **Exportar Script**.
5. Um arquivo JSON é baixado para o seu computador. O nome do arquivo JSON inclui o sistema operacional para que você possa determinar facilmente quais scripts são para qual sistema operacional.

Como criar uma nova ação de aquisição de dados na Now Platform

Para criar uma nova ação, siga estas etapas:

1. Navegar até **Integração do FireEye** > **Ações adicionais do FireEye**. A lista Ações adicionais do FireEye é exibida.
2. Clicar **Novo**. O formulário da nova ação é exibido.
3. Preencha o formulário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Ação	Nome da ação do FireEye realizada. Este nome ajuda a identificar o tipo de Ação e a descrevê-lo.
Aquisição	Uma aquisição obtém os dados para analisar. Este é um campo somente leitura e o padrão é Aquisição de dados.
Origem	Nome da origem do FireEye. Somente origens configuradas estão disponíveis na lista de seleção.
Capacidade	Este é um campo somente leitura e é preenchido com a capacidade Executar ações adicionais
Tipo de aquisição	Tipo de ação de aquisição que precisa ser obtida e analisada.
Ativo	Isso indica que a Ação está ativa.
Requer Aprovação	Quando você habilita a opção Requer aprovação, o campo Aprovadores fica disponível no formulário. Depois de enviar uma solicitação, a aprovação é necessária do grupo para concluir a solicitação.
Marcador de exibição	Tipo de sistema operacional, como Windows, Mac, Linux, para adicionar scripts. **Nota:** Somente um tipo de sistema operacional é compatível no momento. Você pode criar uma ação por sistema operacional. Para outros sistemas operacionais, crie novas ações conforme necessário.
Scripts	O script importado do FireEye precisa ser fornecido para o tipo de SO selecionado. Somente um script pode ser adicionado a cada tipo de SO.

4. Clicar **Enviar**.

Acionar aquisições de dados a partir de incidente de segurança

As ações adicionais criadas podem ser executadas por meio do link relacionado chamado **Executar ações adicionais no endpoint** sobre o incidente de segurança.

Nota:
Permitir edições antes de adquirir A funcionalidade FireEye não é compatível com as ações adicionais no endpoint.

Criar e configurar um perfil para pesquisa de vistas com a integração do FireEye

Configure o perfil de pesquisa de vistas usando o procedimento a seguir.

Antes de Iniciar
Função necessária: administrador de incidentes do NowPlatform Security (sn_si.admin)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sempre que uma origem for criada, as configurações de pesquisa de vistas individuais para cinco tipos (Arquivo, IPs (v4), MD5, SHA1 e SHA256) serão criadas e inativas por padrão. Você deve torná-lo ativo antes de usar a Pesquisa de detecções. Cada tipo de observável tem uma consulta de pesquisa diferente para recuperar vistas. Estaríamos iniciando uma pesquisa diferente para cada tipo de observável. A pesquisa de vários observáveis para uma pesquisa de vista não é possível no FireEye, pois ele executaria uma operação AND nos observáveis, e o resultado pode ser impreciso.

Nota:
Para a pesquisa de Vistas, somente cinco pesquisas ativas podem estar presentes de uma só vez. O restante será enfileirado e começará após a conclusão de qualquer uma das vistas em andamento.

Se você quiser criar um novo perfil de pesquisa de vistas, siga as etapas abaixo para criar um:

Procedimento

1. Navegar até **Integrações** > **Configuração de Pesquisa de Vistas**.
2. Clicar **Novo**.
3. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome do perfil de recurso.
Pesquisa salva	Isso executará uma pesquisa salva, ou seja, o campo de Nome deve corresponder ao nome da pesquisa salva.
Origem de pesquisa de vistas	Define a origem configurada para a integração.
Pesquisar	Adicione uma cadeia de caracteres de pesquisa nativa para formar uma consulta.
Ativo	A consulta será executada somente se estiver ativa.
Tipo de observável	Define o tipo de categoria de observável.
Máximo de observáveis por pesquisa	O número de observáveis antes da consulta de pesquisa é dividido em várias consultas. Defina este valor como 1 para esta integração.
Parâmetros de pesquisa de detecções	Use os parâmetros de pesquisa de detecções para definir consultas mais complexas que incluem lógica e outros operadores compatíveis com o armazenamento de log especificado.

4. Clicar **Enviar** para concluir a configuração.

Invocar pesquisa de detecções a partir de um incidente de segurança

Invoque a pesquisa de vistas de um incidente de segurança SIR seguindo o procedimento abaixo.

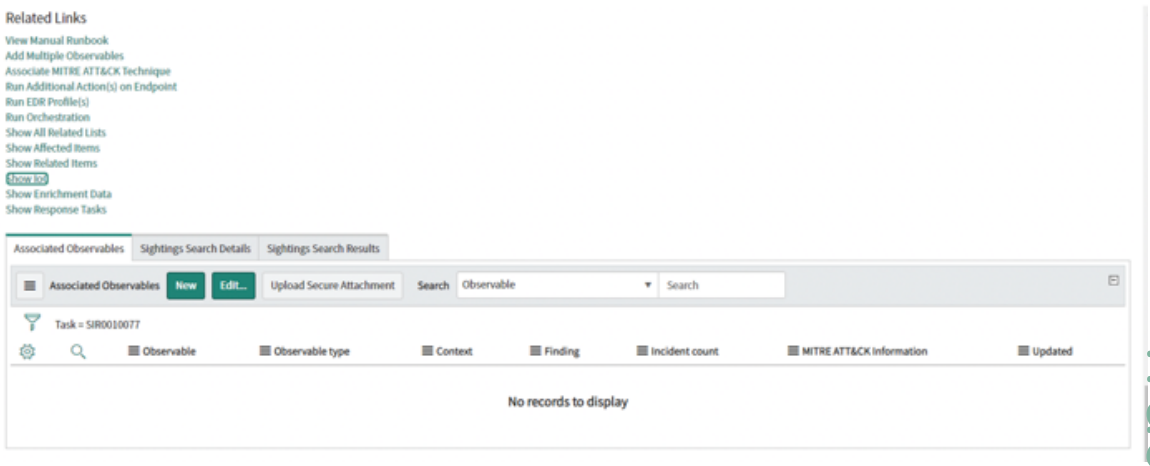
Antes de Iniciar
Função necessária: administrador da Now Platform (sn_si.admin)

Tradução automática

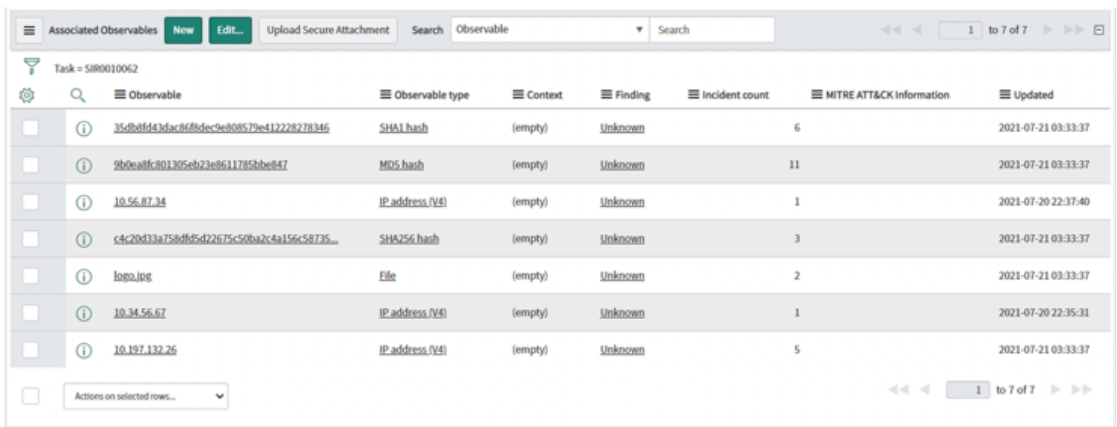
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até Incidentes de segurança.
2. Abra qualquer SIR existente ou crie um novo SIR.
3. Clique em Mostrar IoC em Links relacionados.
4. Clicar **Observáveis Associados** listas relacionadas.



5. Adicione observáveis existentes ou crie um novo observável.



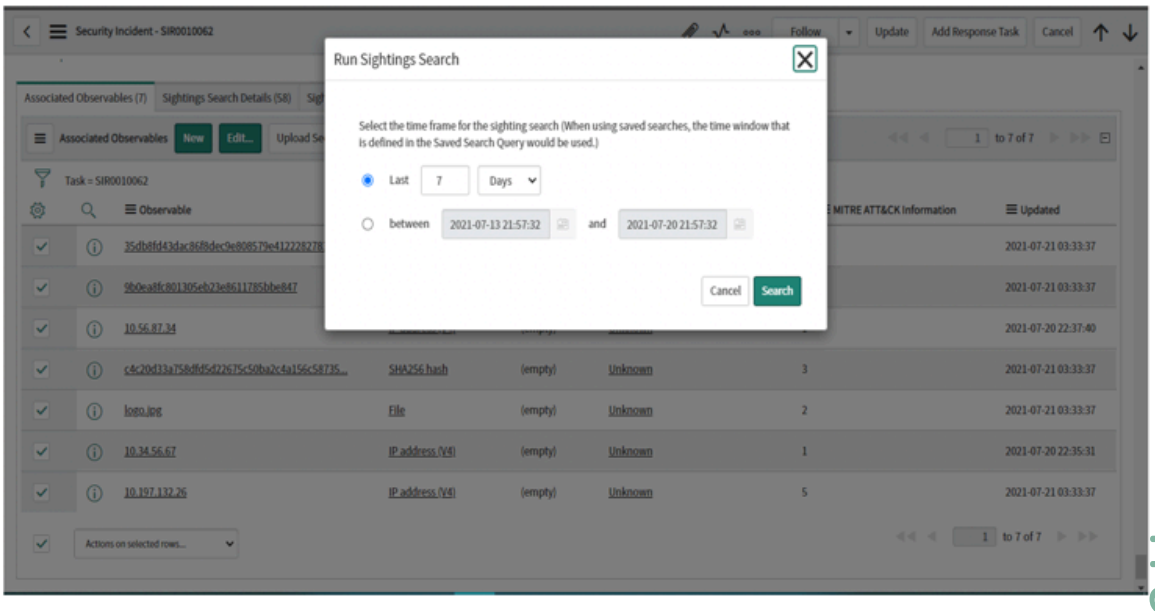
6. Selecione os observáveis e, em Ações nas linhas selecionadas, clique em **Executar pesquisa de vistas**.

7. Ignore as entradas na próxima caixa de diálogo que solicita dados de tempo.

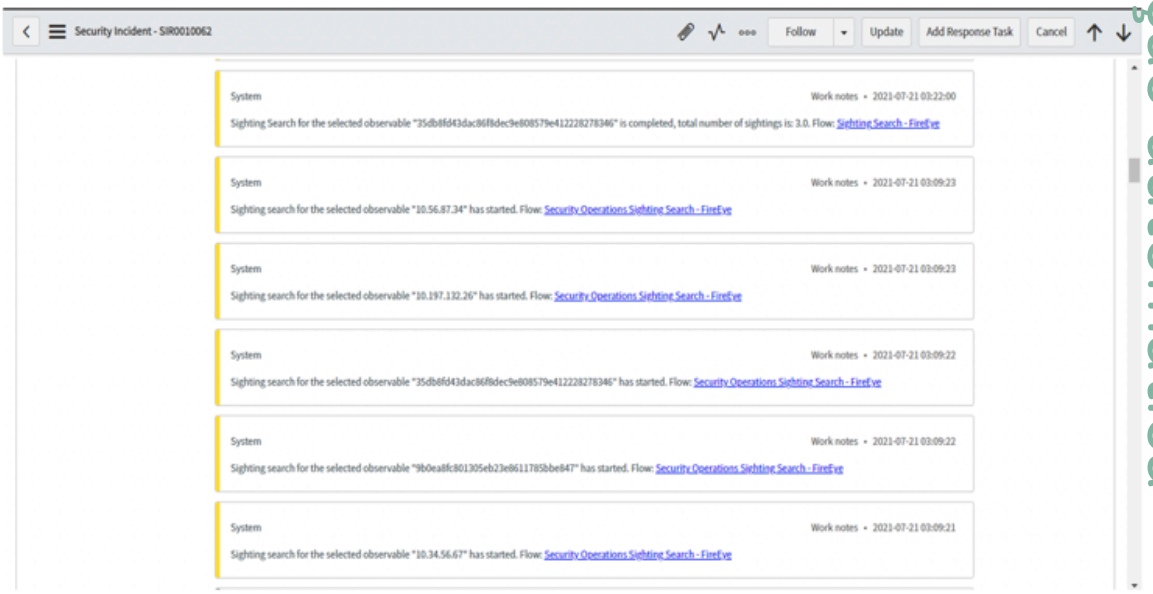
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Há valores padrão preenchidos. No entanto, a pesquisa é realizada em tempo real e os valores de tempo são ignorados para esta integração.



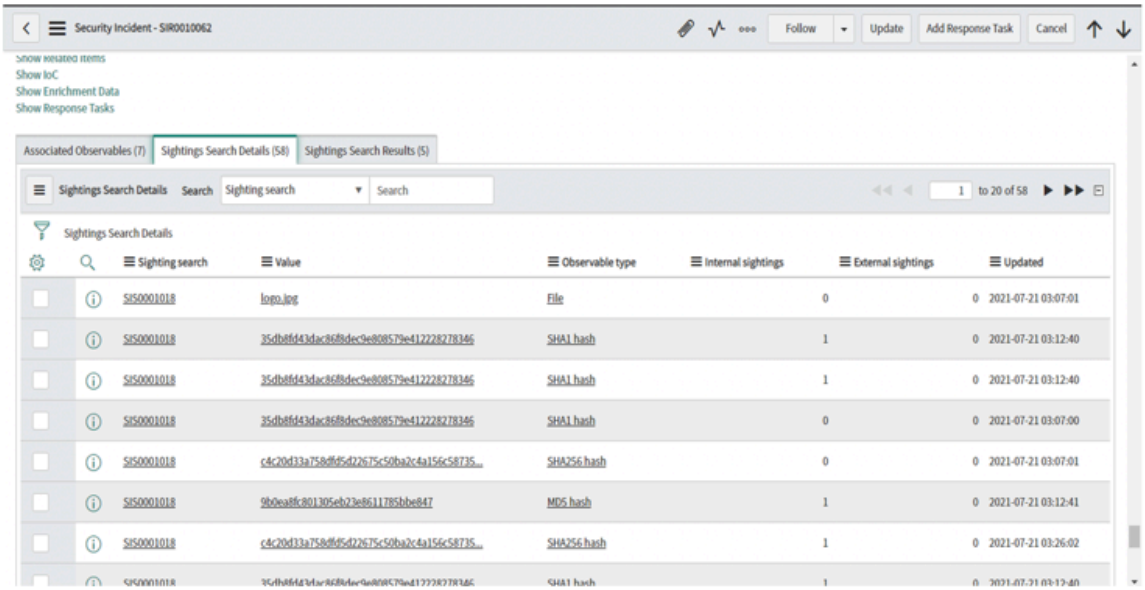
8. Verifique o status das anotações de trabalho.

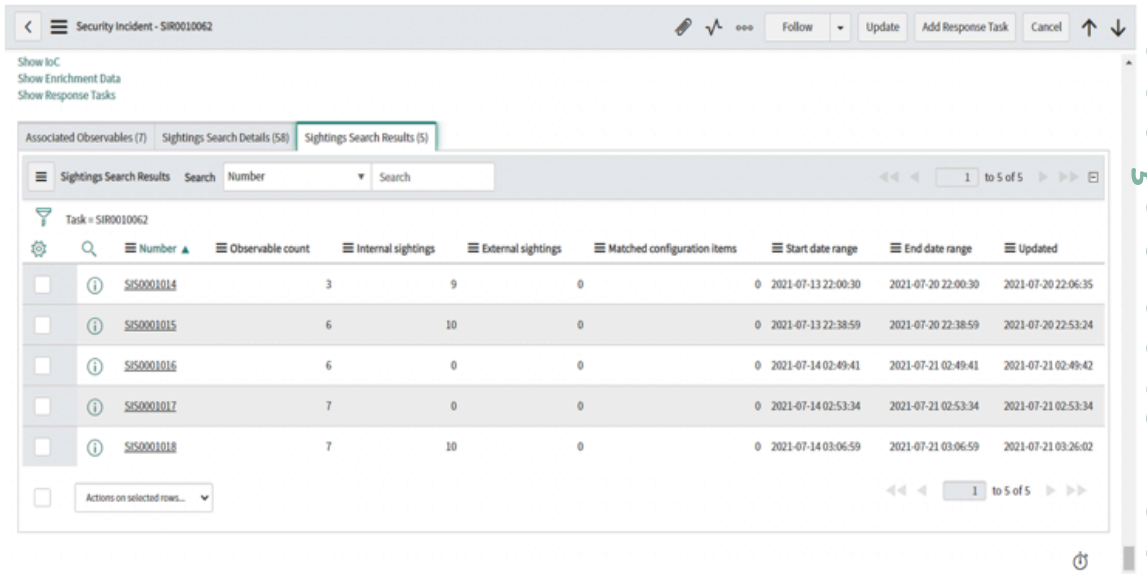


9. Ao concluir a pesquisa, verifique os resultados e os detalhes nas listas relacionadas.
10. Clique em **Detalhes de Pesquisa de detecções** guia para obter detalhes e **Resultados da pesquisa de detecções** Guia para resultados de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.





Tradução automática

Integração de Have I been pwned?

A integração Security Operations Have I been pwned? permite que você envie pesquisas em nomes de domínio e endereços de e-mail para determinar se os dados pessoais do usuário foram comprometidos por violações de dados.

Explorar Integrações do Security Incident Response	**Configurar** • Configuração da integração do Security Operations Have I been pwned? • Ativar a integração do Security Operations Have I been pwned?
Usar	**Desenvolver**

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Realizar pesquisas em observáveis Pesquisa de ameaças - Fluxo de trabalho Have I been pwned?	• ServiceNow Security Operations diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Faça ou responda perguntas na comunidade do Security Operations
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Configuração da integração do Security Operations Have I been pwned?

Have I been pwned? é um recurso gratuito usado para avaliar se alguém pode ter sido colocado em risco devido à violação de sua conta online ou à "pwned" em uma violação de dados. Ele se integra facilmente com Security Operations.

Antes de usar a integração Have I been pwned?, você deve ativar o plug-in. Se necessário, você também pode atualizar sua certificação SSL X509.

Os plug-ins Security Incident Response, Inteligência contra ameaçase Security Operations Have I been pwned? são necessários para implementar a integração Security Operations Have I been pwned?.

Ativar a integração do Security Operations Have I been pwned?

O recurso Configuração de integração permite que você ative e configure rapidamente integrações de segurança de terceiros, incluindo a integração Security Operations Have I been pwned?. Antes de usar a integração Have I been pwned?, você deve baixá-la do ServiceNow Store.

Antes de Iniciar

- O plug-in Inteligência contra ameaças deve ser instalado e ativado antes que você possa usar a integração Security Operations Have I been pwned?.

Função necessária: sn_si_admin

Procedimento

Baixe a integração do ServiceNow Store.
Esta integração oferece suporte a uma API aberta e não requer configuração adicional. Have I been pwned? agora pode ser selecionado para executar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Tópicos relacionados

Realizar pesquisas em observáveis

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atualize seu certificado X.509

Se você precisar de uma conexão SSL para a integração, há circunstâncias em que o certificado fornecido pelo fornecedor terceirizado ainda não é confiável em ServiceNow ou expirou. Esta tarefa é opcional.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um Certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

   a. Insira o URL do endpoint na barra de endereço do navegador.
   Por exemplo: `https://<3rdparty>/`.

   b. Clique no ícone de cadeado na linha de endereço.

   c. Clique em **Mais informações** e na guia **Segurança**.

   d. Clique em **Exibir certificado** e na guia **Detalhe**.

   e. Clique em **Exportar** para salvar o PEM em seu sistema de arquivos local.

   f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
   Ele deve começar com `-----BEGIN CERTIFICATE-----` e terminar com `-----END CERTIFICATE-----`.

2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e crie um novo registro para a integração.
4. Em **Certificado PEM**, cole o certificado que você baixou e copiou para a área de transferência anteriormente.
5. Adicione o certificado ao registro do provedor de identidade.
   a. Navegar até **SSO Multiprovedor** > **Provedores de Identidade**.
   b. Selecione o provedor de identidade padrão ativo para o qual você criou o novo certificado.
   c. Role para baixo até a lista relacionada de **certificados X.509** e clique em **Editar**.
   d. Mova o certificado recém-criado para a coluna **Selecionado**.
6. Clique em **Salvar**.
   Os outros campos no registro são gerados automaticamente.

Nota:
Se você tiver um certificado que expirou, será necessário removê-lo. Para obter informações sobre como remover o certificado expirado, consulte KB0691439 Substituir um certificado SAML expirando .

Tradução automática

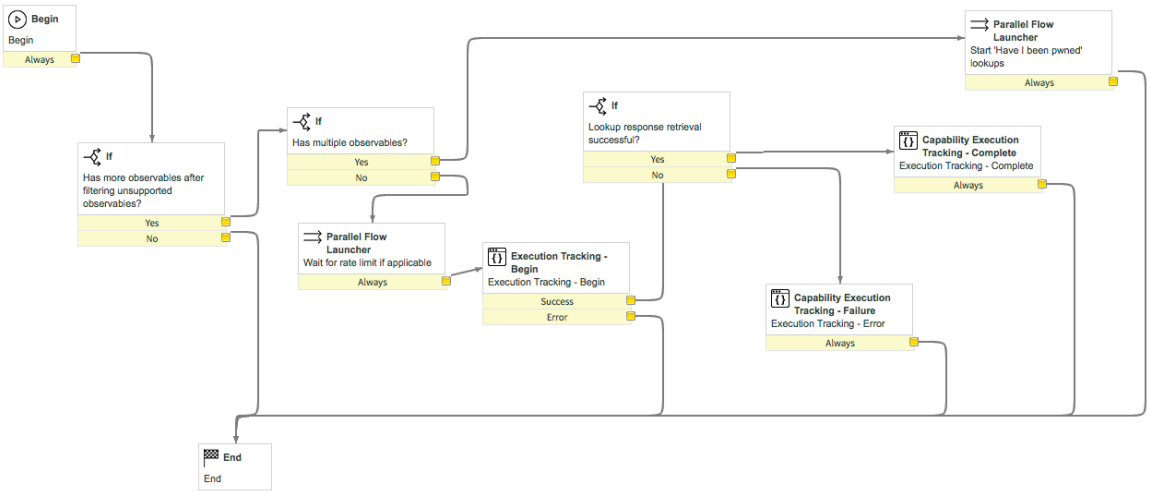
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de ameaças - Fluxo de trabalho Have I been pwned?

O fluxo de trabalho Pesquisa de ameaças - Have I been pwned? executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido por Have I been pwned?, eles serão verificados quanto a malware e os resultados serão retornados.

Antes de Iniciar
Função necessária: sn_si_admin

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado pelo Integração do Security Operations - Pesquisa de ameaças quando você executa uma pesquisa de ameaça em um ou mais observáveis e a implementação Have I been pwned? é selecionada. Para obter mais informações, consulte Realizar pesquisas em observáveis.



Para obter informações sobre as atividades usadas por este fluxo de trabalho, consulte Atividades de fluxo de trabalho de integração comuns.

HPE Security ArcSight ESM - Integração do analisador de e-mails

A integração do analisador de e-mail do HPE Security ArcSight ESM é compatível com o uso de um analisador de e-mail que consome notificações por e-mail do ESM para criar incidentes de segurança.

Configurar HPE Security ArcSight ESM - integração do analisador de e-mail

A integração do analisador de e-mail do HPE Security ArcSight ESM usa notificações por e-mail do ESM para gerar aprimoramentos e fluxos de trabalho de resposta.

Antes de Iniciar
Função necessária: sn_si_admin

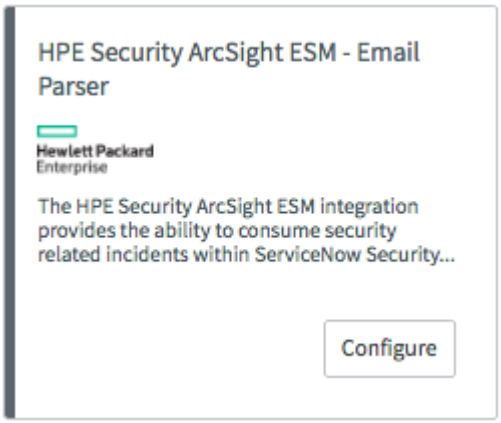
Por Que e Quando Desempenhar Esta Tarefa
Um modelo de analisador de e-mail do HPE Security ArcSight ESM é fornecido para uso na integração. Ele deve ser configurado e ativado antes que a integração ocorra. Atualizar o analisador o ativa.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. No cartão HPE Security ArcSight ESM - Analisador de e-mail, clique em **Configurar**.
3. Na caixa de diálogo **HPE Security ArcSight ESM - Configuração do analisador de e-mail**, clique no link **Configurar analisador de e-mail**.
4. Clique no link do **ESM do ArcSight** para editar as configurações no analisador de e-mail do modelo fornecido.
   Preencha pelo menos o campo O e-mail é de. Para criar seu próprio analisador de e-mail, consulte Criar analisadores de e-mail no Security Operations.
5. Marque a caixa **Ativa**.
6. Clique em **Atualizar** no formulário **Analisador de e-mail**.
   O analisador de e-mail está ativo. Você não precisa retornar para **Configurações de integração**.

HPE ArcSight Logger - Integração de Aprimoramento de incidente

A integração HPE ArcSight Logger - Incident Enrichment pesquisa seus logs e adiciona informações de vista relevantes aos seus incidentes de segurança.

Explorar Integrações do Security Incident Response	**Configurar** • Introdução ao HPE ArcSight Logger - Incident Enrichment integration • Criar registros de configuração de pesquisa de vistas
Usar • Executar uma pesquisa de vistas • Integração do Security Operations - Fluxo de trabalho de pesquisa de detecções • Security Operations - Fluxo de trabalho de pesquisa de detecções do agente de log do Arcsight • Exibir detalhes da pesquisa de detecções • Exibir Resultados da Pesquisa de Vistas	**Desenvolver** • ServiceNow Security Operations diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Solução de problemas de integração
- Faça ou responda perguntas na comunidade do Security Operations
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Introdução ao HPE ArcSight Logger - Incident Enrichment integration

HPE ArcSight Logger transmite dados em tempo real e os categoriza em logs específicos e se integra facilmente com Security Operations. Antes de usar a integração HPE ArcSight Logger - Incident Enrichment, você deve baixá-la do ServiceNow Store e adicionar a URL da API e as credenciais de login.

Antes de Iniciar

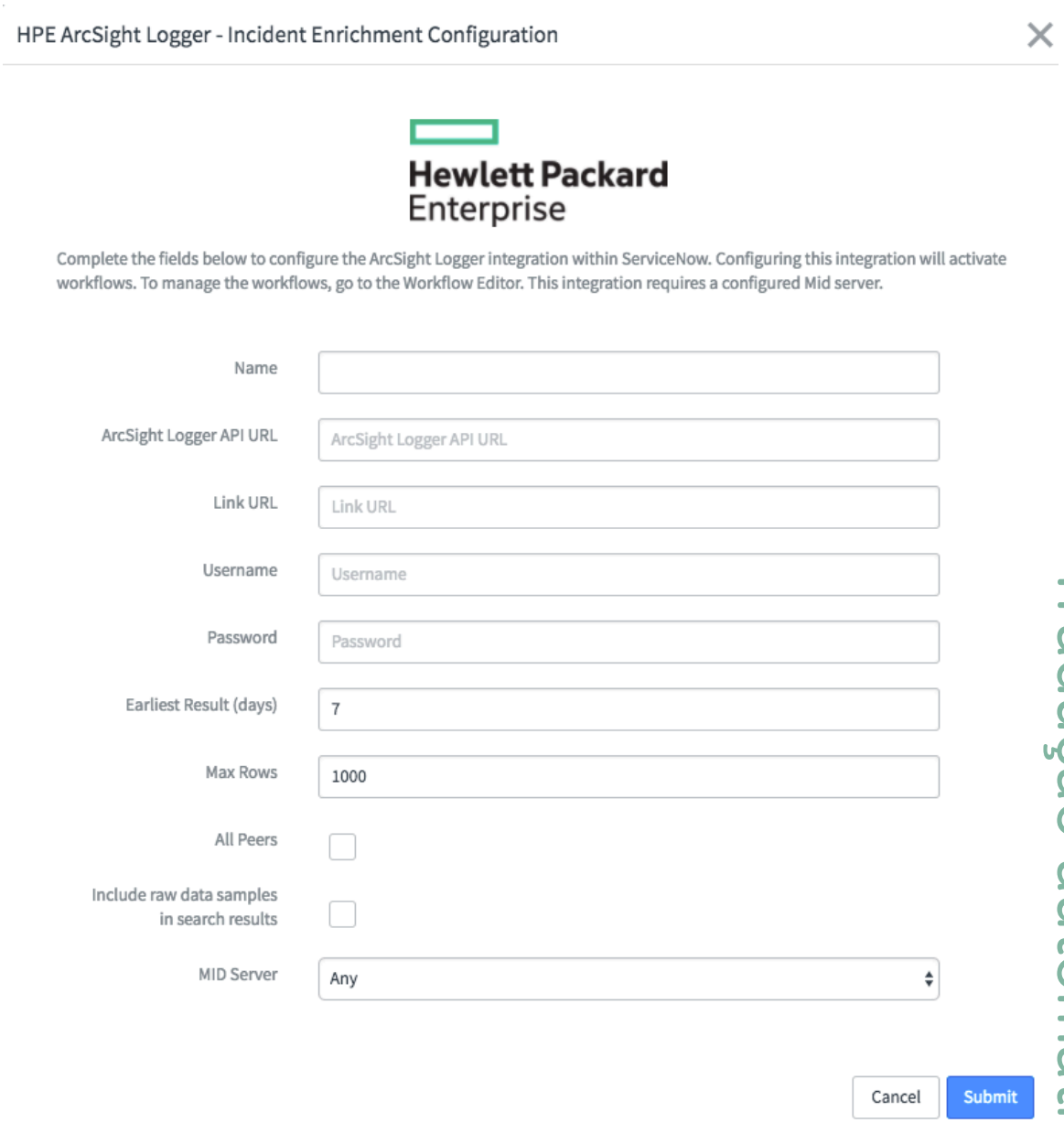
Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Security Operations** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão HPE ArcSight Logger - Aprimoramento de incidente, clique em **Novo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

4. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
URL base da API do agente de log do ArcSight	O URL base que você adquiriu no site do HPE Security ArcSight Logger.
URL do Link	[Opcional] A URL do link que vincula a uma instância do HPE Security ArcSight Logger, quando disponível.
Nome do usuário	Seu nome de usuário Intel HPE ArcSight Logger.
Senha	Sua senha Intel HPE ArcSight Logger.
Resultado Mais Antigo (dias)	Os resultados mais antigos que você deseja ver em número de dias.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Máx. de Linhas	O número máximo de linhas que você deseja pesquisar.
Todos os Pares	O padrão é desmarcado e pesquisa somente o agente de log local ao qual você está conectado. Quando marcado, ele pesquisa todos os agentes de log conectados entre si.
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados da pesquisa de detecções. A quantidade de dados retornados depende da configuração na propriedade do **número de linhas de dados brutos** nas propriedades do Security Incident Response.
MID Server	Selecione **Qualquer** para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota:
Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho.

5. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
6. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Integração de Hybrid Analysis

A aplicação Hybrid Analysis faz parte de uma comunidade online aberta na qual os usuários analisam arquivos e URLs em busca de ameaças. Você compartilha resultados e utiliza pesquisas da comunidade para obter respostas a incidentes mais eficazes. Quando integrada ao produto Now Platform Security Operations, a inteligência contra ameaças compartilhada fornece informações adicionais sobre a severidade de observáveis específicos.

A integração Hybrid Analysis executa pesquisas de ameaça nos seguintes observáveis:

- Hashes de arquivo
- Endereços IP
- URLs

O fluxo de trabalho verifica se há novos observáveis conforme eles chegam em incidentes de segurança. Se os observáveis forem de um tipo reconhecido pela integração da API, os observáveis serão avaliados. Os observáveis determinados como maliciosos são marcados.

Esta integração é compatível com as versões Kingston, London, Madrid e New York da Now Platform®.

Instalar e configurar Hybrid Analysis

Antes de executar a integração na sua instância, conclua as etapas de instalação e configuração para que a aplicação Hybrid Analysis se integre corretamente com Now Platform Security Operations.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform e Security Incident Response.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador (admin) instala o app e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração e verifica os resultados esperados. Esta função também tem acesso ao módulo Security Operations e atribui a função sn_si.analyst.
Obtenha uma chave de API.	Visite o site do Hybrid Analysis para obter informações sobre chaves de API e para criar uma conta: site do Hybrid Analysis . A configuração requer que você insira as chaves de API.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Para a versão Madrid e versões posteriores da família, o plug-in com.snc.si_dep é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Security Operations aplicações. As aplicações Security Operations a seguir devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative um aplicativo de cada vez na ordem listada abaixo para garantir uma instalação sem problemas: **1.** Security Integration Framework **2.** Security Support Common **3.** Orquestração de suporte de segurança **4.** Security Incident Response Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Execute as etapas a seguir para atualizar as propriedades do sistema e instalar e configurar a integração.

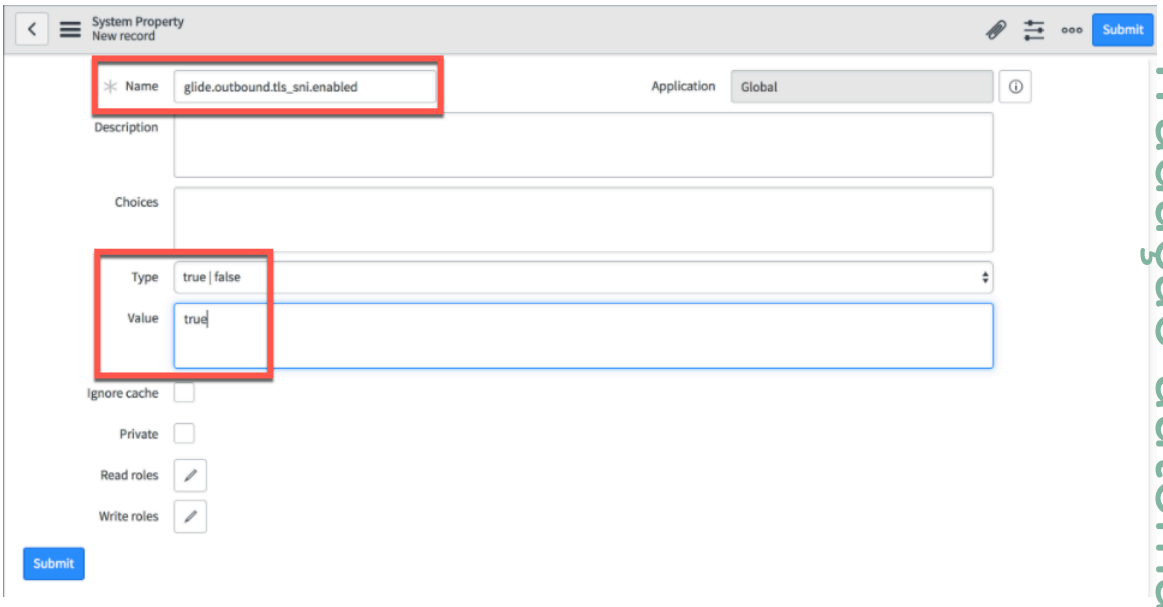
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. No filtro de navegação, insira `sys_properties.list` e pressione **Enter**.
   A lista **Propriedades do sistema** é exibida.
2. Clique em **Nova**.
   Um novo registro é exibido.
3. Preencha os campos ou selecione os valores listados na tabela a seguir e clique em **Enviar**.

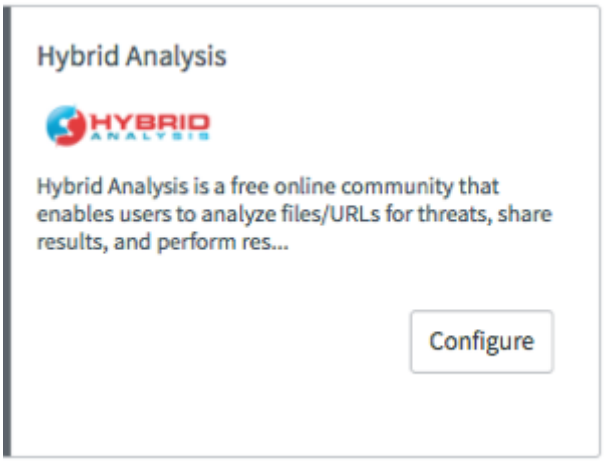
Nome do campo	Valor
Nome	glide.outbound.tls_sni.enabled
Tipo	Selecionar **verdadeiro l falso**
valor	verdadeiro



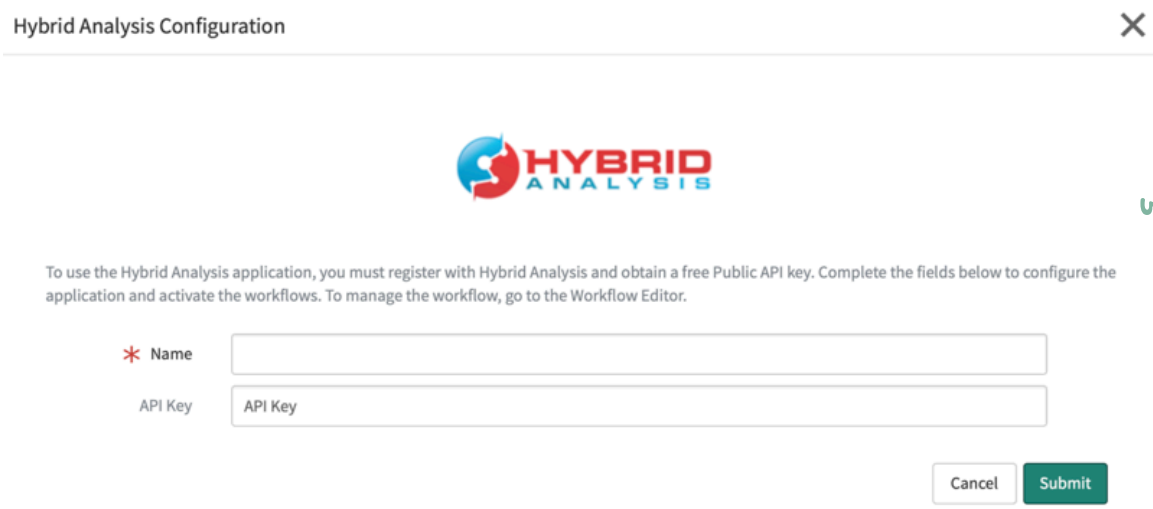
4. Se você não instalou a aplicação para a integração, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.
5. Após a conclusão da instalação, navegue até **Integrações** > **Configurações de integrações** e localize o bloco Hybrid Analysis.
6. Clique em **Configurar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Na caixa de diálogo **Configuração de análise híbrida**, insira a chave de API que você obteve no site Hybrid Analysis e clique em **Enviar**.



8. Verifique a configuração bem-sucedida.
   A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida.

   Trouble?

   Se uma mensagem de erro for exibida durante a configuração, a chave de API Hybrid Analysis pode ser inválida.

Verificar resultados esperados para Hybrid Analysis

Os observáveis são gerados automaticamente por um incidente de segurança e verificados pela aplicação. Localize os resultados da pesquisa no incidente de segurança para verificar se a pesquisa de ameaças foi executada com sucesso. Exiba também dados brutos e execute pesquisas de ameaça em observáveis secundários.

Antes de Iniciar

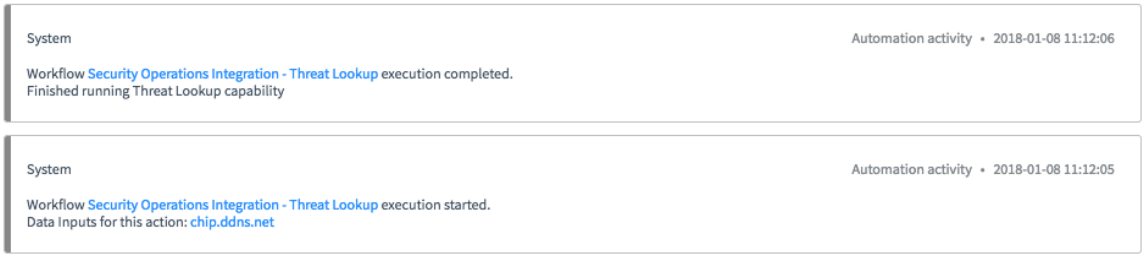
Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o registro de incidente de segurança com o qual você está trabalhando e verifique se a pesquisa foi executada com sucesso.

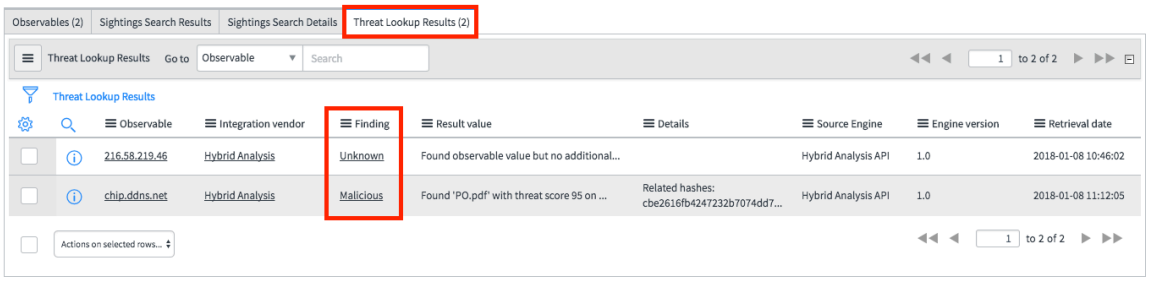


   Depois que a aplicação é configurada, o fluxo de trabalho é iniciado automaticamente após a criação do incidente. O status de execução e conclusão da pesquisa é exibido nas anotações de trabalho no incidente de segurança.

2. Revise as anotações de trabalho para obter mais informações sobre como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

3. Navegue até a parte inferior do registro do incidente de segurança e clique no link relacionado **Mostrar todas as listas** relacionadas para exibir os resultados.

   Nota:
   As imagens nas etapas a seguir são mostradas com a configuração **Formulários** com guia ativa nas Configurações do sistema. No canto superior direito do quadro da faixa, clique no ícone de engrenagem Configurações. Na caixa de diálogo **Configurações do sistema** exibida, clique em **Formulários** e verifique se **Formulários com guia** e **Com o formulário** estão selecionados.

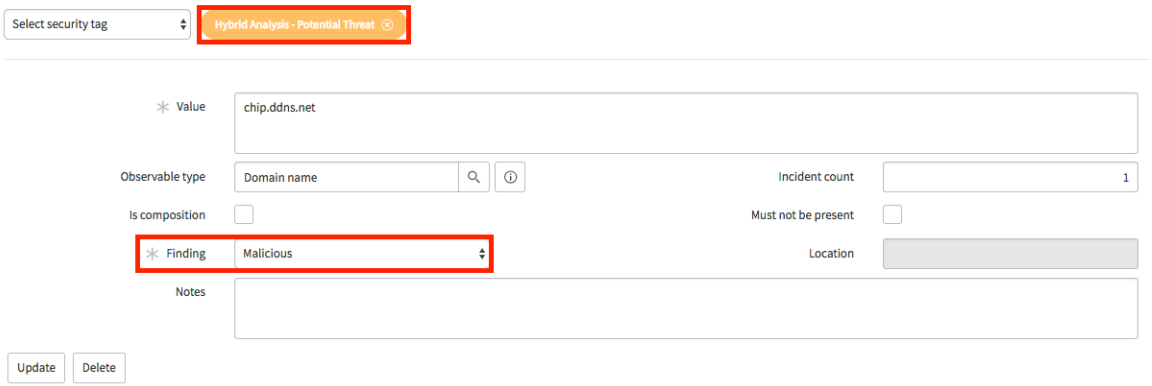


   A guia **Resultados da pesquisa de ameaças** exibe os resultados da pesquisa na parte inferior do registro do incidente de segurança. Observe que a coluna **Descoberta** exibe Desconhecido para registros não determinados como mal-intencionados. Para resultados correspondentes a mal-intencionados, a coluna **Descoberta** exibe Mal-intencionado.

4. Na coluna **Observável**, clique em um observável para abrir o registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

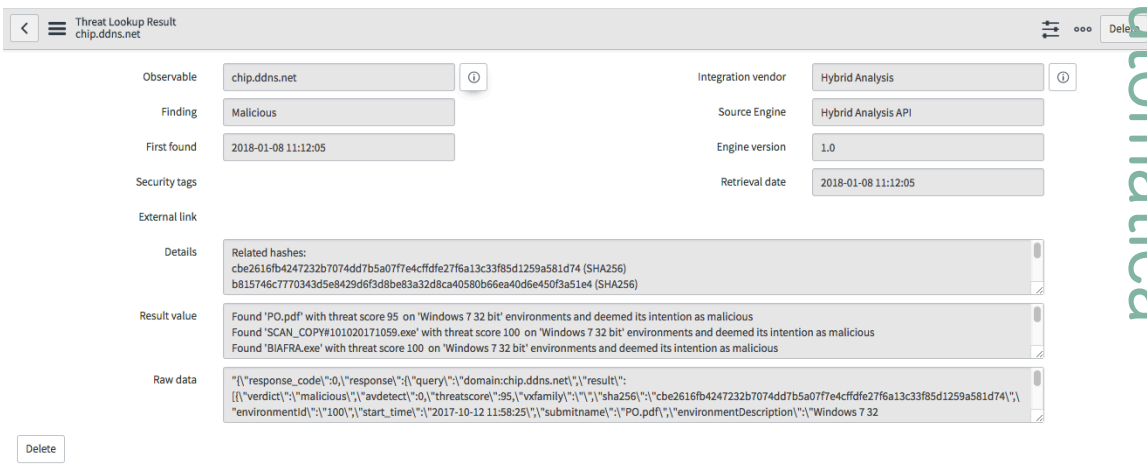


Para pesquisas correspondentes a mal-intencionadas, o campo **Descoberta** exibe Mal-intencionado e o observável é marcado com a origem Inteligência contra ameaças que o considerou mal-intencionado, neste caso, a integração Hybrid Analysis.

5. **Opcional:** Siga as etapas para exibir dados brutos, exibir uma lista de observáveis secundários e executar uma pesquisa de ameaça em observáveis secundários selecionados.

   a. Navegue de volta para o incidente de segurança e, na guia **Resultados da pesquisa de ameaças**, clique no ícone de informações azul ao lado de um observável.

   b. Na janela exibida, clique em **Abrir registro** para exibir os dados.
   A partir de qualquer observável visível nos dados brutos exibidos na pesquisa, a integração Hybrid Analysis também cria observáveis secundários ou relacionados.



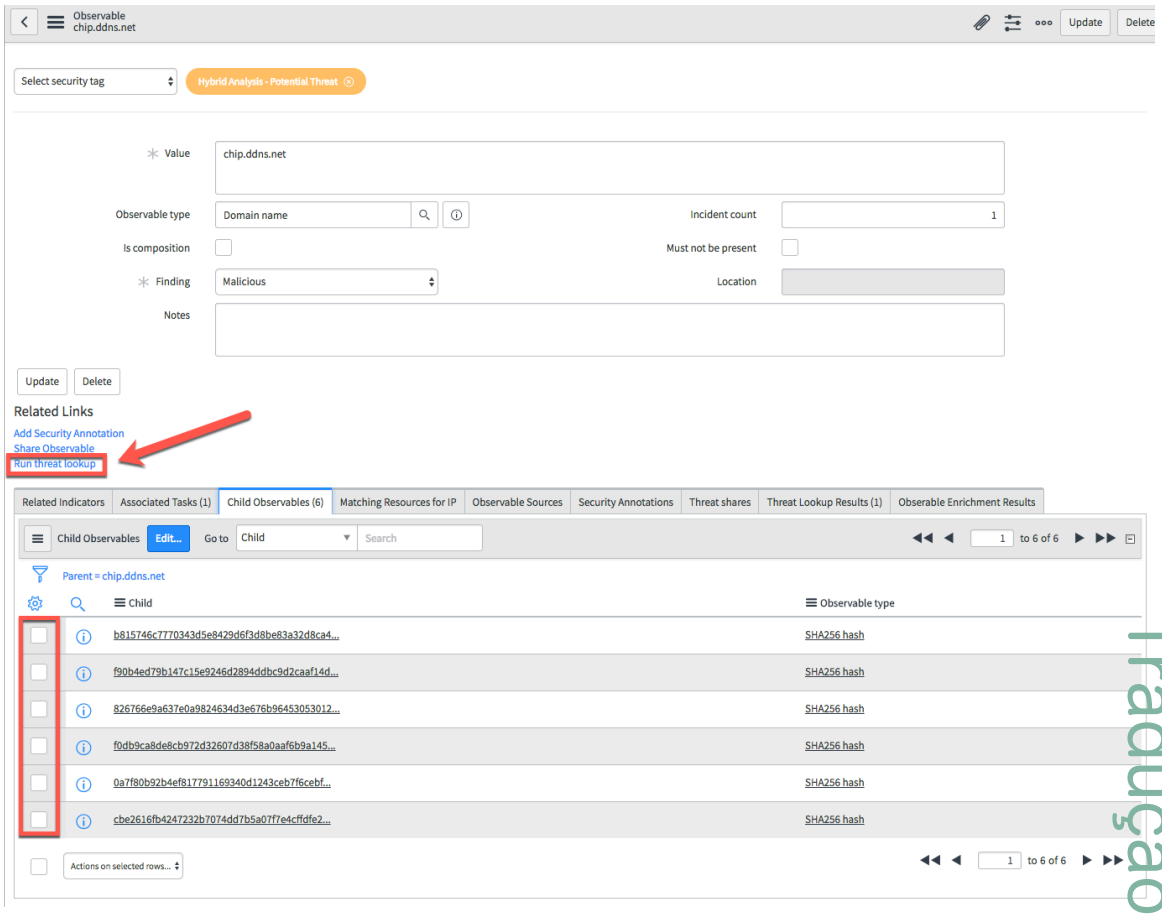
   O link criado pela API, os dados brutos e outras informações são exibidos.

   c. Navegue de volta para o incidente de segurança e clique no link relacionado **Mostrar IoC**.
   Os observáveis secundários são exibidos na guia **Observáveis secundários** no incidente de segurança, porque a pesquisa encontrou uma conexão existente entre esses observáveis relacionados e o observável enviado inicialmente.

   d. Clique no campo ao lado de um observável na coluna **Secundário** para selecioná-lo, seguido pelo link relacionado **Executar pesquisa de ameaça** para realizar uma pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



e. Na caixa de diálogo exibida, verifique se a integração Hybrid Analysis está selecionada e clique em **Enviar**.

f. Nas anotações de trabalho, verifique se a pesquisa foi executada com sucesso e, na guia **Resultados da pesquisa de ameaças** no incidente de segurança, localize os resultados da pesquisa para os observáveis secundários.

Trouble?

Se você não vir resultados na guia **Resultados da pesquisa de ameaças**, verifique se o observável é um tipo compatível para pesquisa pela integração.

(Opcional) Anexar manualmente um observável para Hybrid Analysis

Você pode anexar observáveis manualmente quando quiser executar pesquisas de ameaça em observáveis que não estão anexados a um incidente de segurança no gatilho de evento inicial. Além disso, você pode executar esta tarefa quando quiser mais informações sobre um observável relacionado.

Antes de Iniciar

Verifique se o observável é de um tipo compatível com a integração. A integração realiza pesquisas nos seguintes tipos de observáveis:

- Hashes de arquivo
- Endereços IP
- URLs

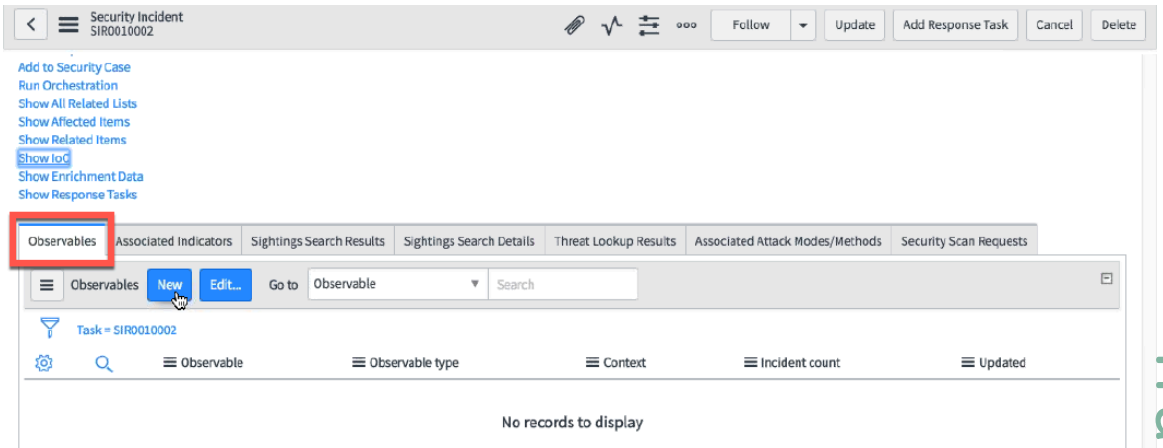
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_si.analyst

Procedimento

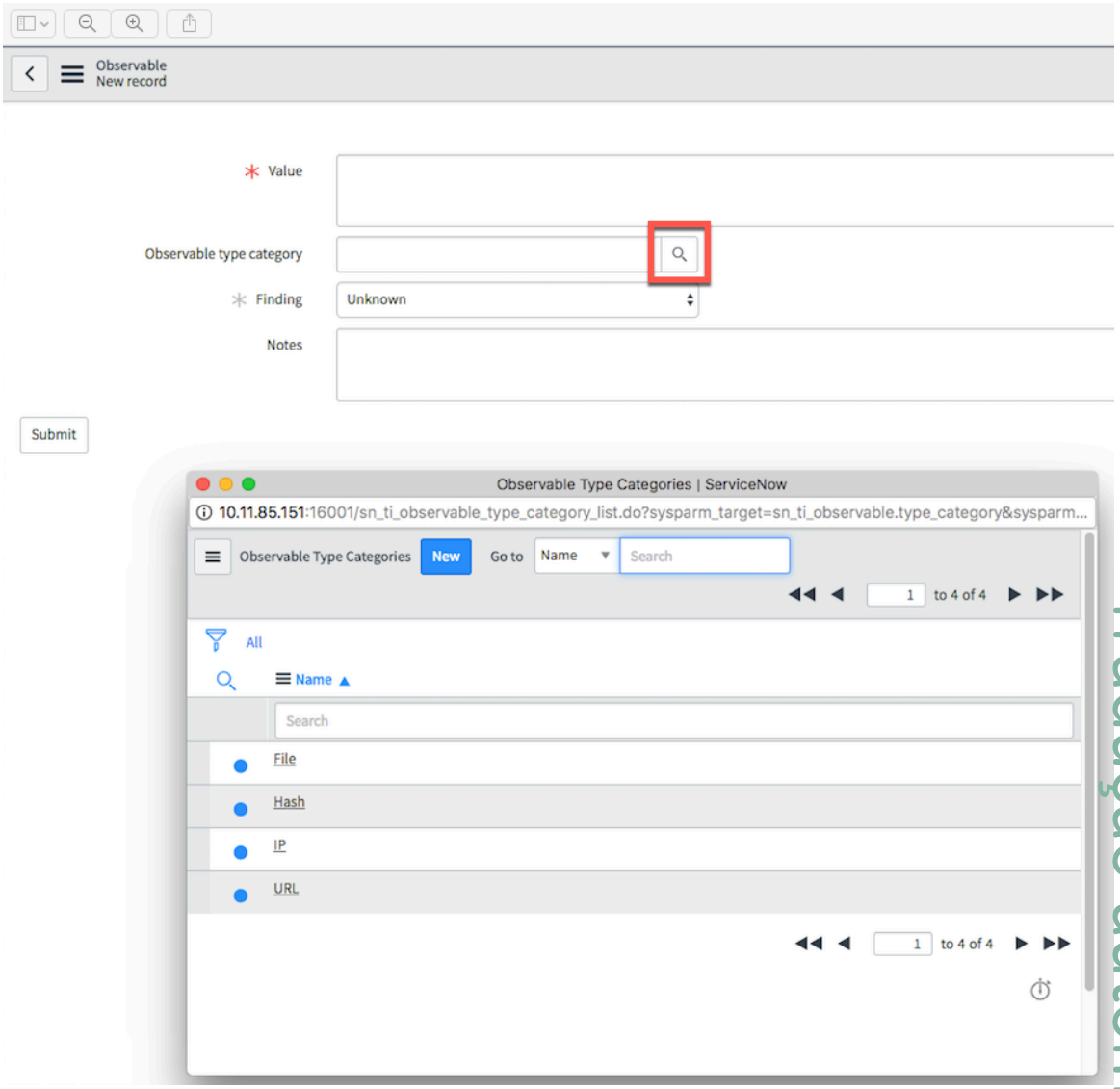
1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar Todos os Incidentes** e abra um incidente de segurança ao qual você deseja anexar o observável.
2. No incidente de segurança aberto, clique no link **Mostrar IoC**em **Links relacionados**.



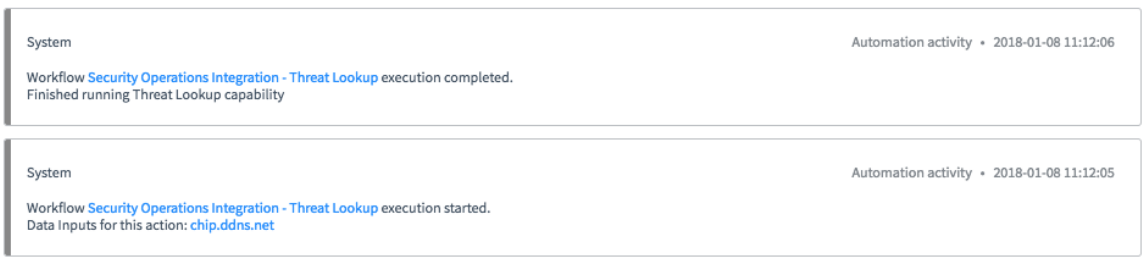
3. Na guia **Observáveis**, clique em **Novo**.
   O formulário Observável é exibido.
4. No campo **Valor**, insira um observável (hash de arquivo, endereços IP ou URL).
5. Clique no ícone de pesquisa e, na caixa de diálogo **Categorias de tipo de observável**, clique no tipo de observável desejado na lista para preencher o campo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



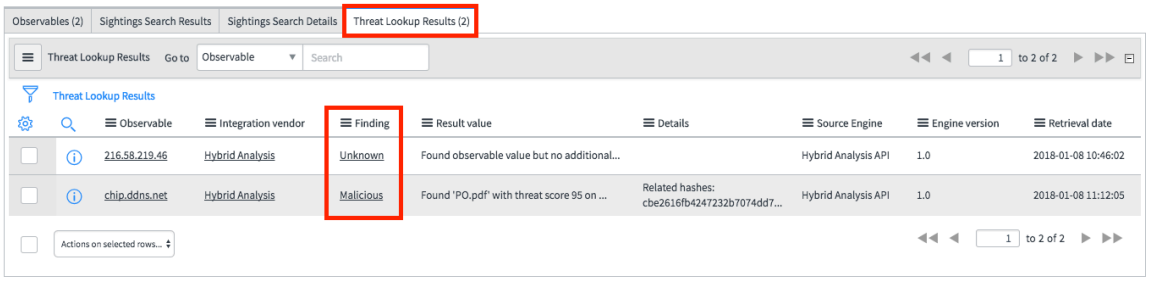
6. Clique em **Enviar**.
   O fluxo de trabalho é iniciado e verifica o novo observável. O status de execução e conclusão é exibido na seção de anotações de trabalho no registro do incidente de segurança.
7. Navegue até o seu incidente de segurança e revise as anotações de trabalho.



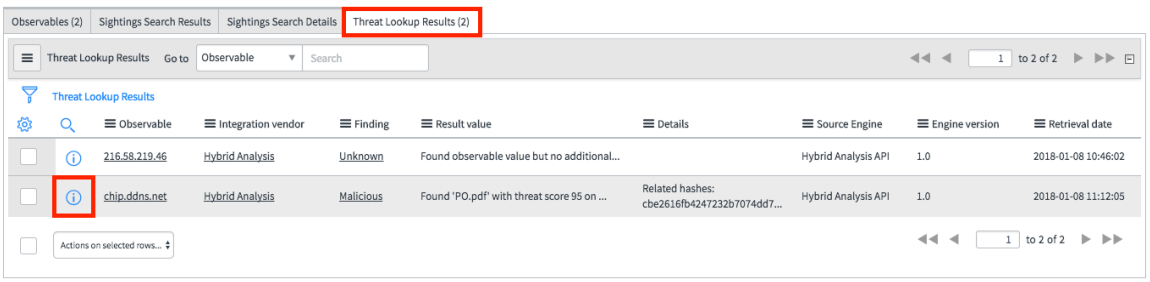
8. Na parte inferior do registro, clique no link relacionado **Mostrar todas as listas** relacionadas.
9. Clique na guia **Resultados da pesquisa de ameaças** para exibir os resultados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



10. Na coluna **Observável**, clique no ícone de informações azul ao lado de um determinado observável para obter mais informações e dados brutos.



11. Na caixa de diálogo exibida, clique em **Abrir registro** para exibir os dados brutos e mais detalhes.
Como alternativa, você também pode anexar um observável existente ao registro de incidente de segurança.
12. **Opcional:** Com a guia **Observáveis** selecionada, clique em **Editar**.
13. **Opcional:** No formulário **Editar membros** exibido, mova um observável existente da **Coleção** para a **Lista de observáveis** e clique em **Salvar**.
Você retornará ao incidente de segurança.
14. Na coluna da extrema esquerda, selecione os observáveis nos quais deseja executar a pesquisa e, na lista de seleção **Ações nas linhas selecionadas...**, selecione **Executar pesquisa de ameaça**.
Uma mensagem é exibida na parte superior do registro informando que a solicitação está sendo processada.
Verifique se a pesquisa foi executada com sucesso.

Trouble?
Revise as anotações de trabalho para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

IBM QRadar Offense Ingestion Integração

A integração IBM QRadar Offense Ingestion permite que você busque automaticamente IBM QRadar ofensas e as converta em incidentes de segurança e habilite ações de resposta automatizadas.

Esta integração é compatível com o seguinte:

- Descoberta de IBM QRadar infrações que são candidatas a incidentes de segurança.
- Buscando eventos ou fluxos recentes associados a uma infração.
- Rastreie atualizações de chave para ofensas periodicamente.
- Mapeamento de campos de ofensa, evento e fluxo para campos de incidente de segurança.
- Exibição preliminar dos campos mapeados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Configure ingestões programadas de infrações para criar incidentes de segurança periodicamente.
- Encerre as ofensas quando os incidentes de segurança forem encerrados.

Instalar e configurar a aplicação ServiceNow para a integração de ingestão de infração IBM QRadar

Antes de executar a integração na sua instância Now Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente aos produtos Security Incident Response e Security Operations na sua instância Now Platform.

Antes de Iniciar

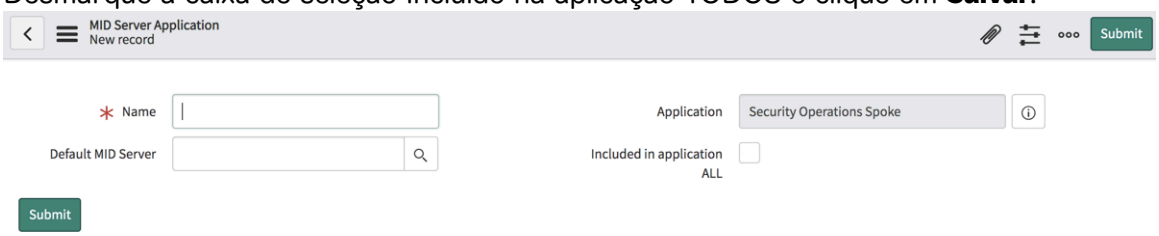
Função necessária: sn_si.admin

Procedimento

1. Se você não instalou a aplicação [IBM QRadar de ServiceNow Store para a integração, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.
2. Depois de instalar a aplicação com êxito, navegue até **Integrações** > **Configurações de integrações** e localize o bloco IBM QRadar.
3. Para configurar a aplicação, clique em **Novo**.
4. Como alternativa, se um botão **Configurar** for exibido em um bloco, clique nele para editar uma configuração existente.
5. Na caixa de diálogo **Configuração de ingestão** de infrações exibida, preencha os campos.

   Para criar uma nova aplicação do MID Server, siga estas etapas:

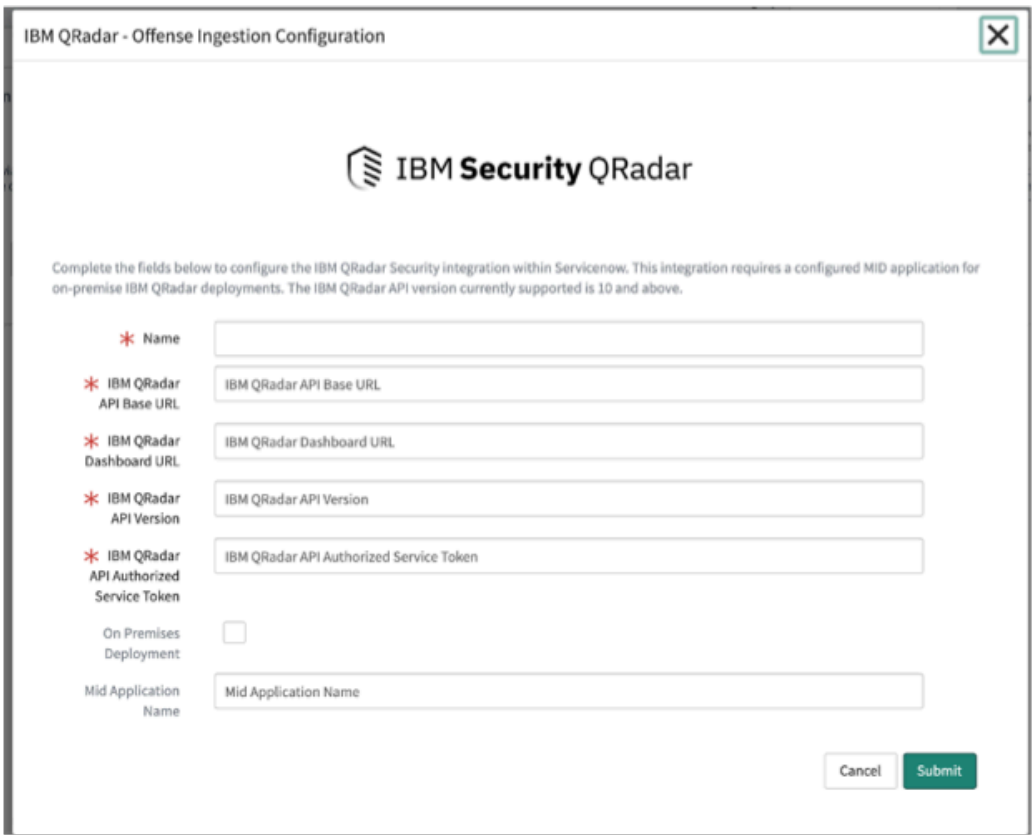
   - Navegar até **MID Server** > **Candidaturas** e clique em **Novo**.
   - Insira um nome para a aplicação do MID Server e selecione um MID Server a ser usado como padrão.
   - Desmarque a caixa de seleção Incluído na aplicação TODOS e clique em **Salvar**.



   - Clique em **Editar**. Na página **Editar Membros**, selecione todos os MID Servers disponíveis, mova-os para a Lista de MID Servers e clique em **Salvar**. Dependendo da disponibilidade, um dos MID Servers configurados com a aplicação MID Server será usado.
6. Insira os detalhes da configuração e especifique a aplicação do MID Server que você criou.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A origem que você configura no formulário de **configuração de ingestão de infração do IBM QRadar** pode ser reutilizada para vários perfis Now Platform, desde que cada perfil inclua infrações.

7. Clique em **Enviar**.
   Depois de validada e enviada com sucesso, cada configuração de servidor IBM QRadar é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista de seleção Mostrar configurações, clique em **Sim**.

Nota:
Se você encontrar alguns problemas com o recurso de segmentação de domínio IBM QRadar, entre em contato com o Suporte ao cliente IBM QRadar para obter assistência.

O que Fazer Depois
Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar o perfil.

Configure sua instância Now Platform® para a integração de ingestão de infração IBM QRadar

A seção a seguir lista as tarefas de configuração que você deve concluir em sua instância Now Platform® antes de instalar a aplicação do ServiceNow Store.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração sem problemas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform® e Security Incident Response (SIR) necessárias.	As funções a seguir são necessárias para a instalação, configuração e uso da integração na sua instância Now Platform®. • Um usuário com a função de administrador Now Platform® (admin) instala a aplicação a partir do ServiceNow Store e atribui a função de administrador de incidente de segurança (sn_si.admin). • Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no Now Platform®: ◦ Nomeia, cria e edita perfis de infração. ◦ Seleciona e mapeia IBM QRadar campos de dados de infração para os campos de incidente de segurança. ◦ Visualiza os detalhes do incidente de segurança para precisão antes de finalizar a configuração. ◦ Programa a ingestão de infração em andamento. ◦ Habilita atualizações de infração quando um incidente de SIR é criado e encerrado. ◦ Atribui a função de analista de incidente de segurança (sn_si.analyst). ◦ Usuários com o sn_si.analyst trabalham com incidentes de segurança. Para obter mais informações sobre funções e atribuição de funções a usuários, consulte Funções no site de documentação do produto da ServiceNow.
Verifique se você está usando as seguintes versões: • IBM QRadar versão 7.3.2 ou posterior. • IBM QRadar API versão 10 ou posterior. Versões anteriores não são compatíveis.	Se você tiver acesso ao console IBM QRadar, terá acesso à API necessária para esta integração. Não há nenhuma outra configuração especial necessária para a API.
Verifique se você instalou e configurou uma aplicação do MID Server.	Aplicação do MID Server configurada. Um MID Server em sua instância Now Platform® é necessário para se conectar ao serviço IBM QRadar se o servidor IBM QRadar for implantado em sua rede corporativa. Consulte o site de documentação do produto da ServiceNow para obter informações sobre MID Servers.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	Se você estiver usando o serviço em nuvem IBM QRadar, um MID Server não será necessário.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas. **1.** Security Incident Response **2.** Ingestão de eventos e alertas para Security Operations: esta aplicação requer: ○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub Runtime ○ com.glide.hub.action_step.rest => Etapa de ação do ServiceNow IntegrationHub - REST **Nota:** Os componentes do Integration Hub são instalados junto com o plug-in Event and Alert Ingestion. Se eles não estiverem instalados, entre em contato com o Suporte ao cliente para obter assistência. Para obter mais informações sobre como instalar as aplicações principais Security Operations, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

O que Fazer Depois

Você configurou com sucesso sua instância Now Platform® para a integração. A próxima etapa é instalar a aplicação [IBM QRadar de ServiceNow Store para a integração.

Criar um perfil para integração de ingestão de infração IBM QRadar

Como um usuário com a função sn_si.admin, você cria um perfil de infração em sua instância Now Platform e determina quais infrações criam incidentes de segurança. Antes que os incidentes de segurança Now Platform Security Incident Response (SIR) sejam criados a partir de infrações, os valores de campo das ofensas são exibidos em um layout de um incidente de segurança Now Platform para que você possa visualizar como o incidente de segurança real será criado.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

De uma perspectiva de integração usando APIs disponíveis, IBM QRadar ofensas são ingeridas automaticamente no ambiente Security Operations da sua instância Now Platform, dependendo do tipo de perfil definido. Os fluxos de trabalho de integração ingerem diferentes tipos de infrações, como tentativas de acesso não autorizadas e malware, por exemplo. Essas ofensas são ingeridas com base nos perfis que você configura no ambiente Security Operations da sua instância. Todas as ofensas são inicialmente ingeridas para um tipo de ofensa configurado em um perfil. As infrações ingeridas podem ser filtradas para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

especificar quais infrações criam incidentes de segurança. Por exemplo, você pode preferir filtros que criam incidentes de segurança somente para infrações identificadas como de alto risco. Antes de um perfil ser ativado e criar incidentes de segurança a partir de ofensas ingeridas, os valores de campo individuais nas ofensas são mapeados para campos correspondentes em um layout de incidente de segurança para uma visualização.

Os nomes dos perfis de infração na sua instância Now Platform devem ser exclusivos. Você pode criar várias configurações para várias origens e também vários perfis para uma única origem.

Criar perfis para ingestão de IBM QRadar infrações

Você pode configurar um perfil para ingerir ofensas.

Antes de Iniciar

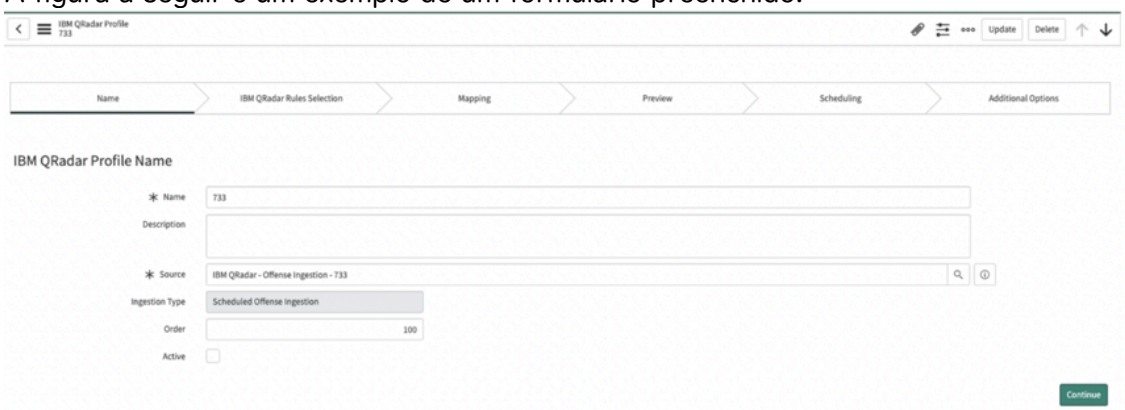
Função necessária: sn_si.admin

Procedimento

1. Para criar um perfil para uma ofensa em sua instância Now Platform, navegue até **Integração do IBM QRadar** > **Perfil do IBM QRadar**.
2. Clique em **Nova**.
3. Preencha os campos.

   Um exemplo de formulário preenchido segue a tabela.

   A figura a seguir é um exemplo de um formulário preenchido.



O que Fazer Depois

A próxima etapa é selecionar as infrações para ingestão.

Selecionar regras IBM QRadar

Com base na Origem IBM QRadar, selecione uma ou mais regras IBM QRadar para o perfil.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Exiba as regras IBM QRadar disponíveis em sua instância da Now Platform para saber quais regras IBM QRadar ativas para as quais você deseja ingerir e criar incidentes de segurança.

Em IBM QRadar, você pode identificar regras por sua origem como Regras do sistema, de substituição e de usuário. Por padrão, a origem de uma regra está vinculada a uma regra

Tradução automática

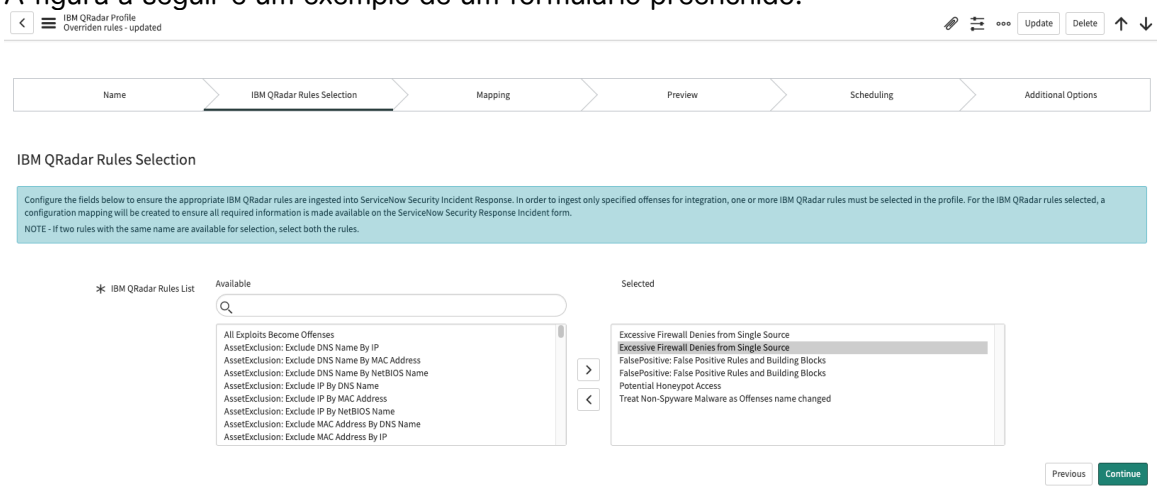
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

do sistema. Quando você modifica uma regra do sistema em IBM QRadar, sua origem é definida como Substituir.

Clique na lista no campo IBM QRadar Lista de regras. Uma lista de regras IBM QRadar ativas que estão presentes no console IBM QRadar é exibida. Selecione uma ou mais regras na lista e mova-as para a coluna **Selecionada**. As infrações acionadas por uma ou mais das IBM QRadar regras selecionadas são ingeridas neste perfil.

Regras com o mesmo nome: na instância Now Platform, uma lista de regras ativas ou habilitadas é exibida. Se você modificar uma regra do sistema ativa ou habilitada em IBM QRadar, uma nova regra de substituição será criada. Isso resulta em duas regras exibidas com o mesmo nome no Now Platform. Quando este cenário ocorrer, selecione as regras para ingerir e criar incidentes de segurança.

A figura a seguir é um exemplo de um formulário preenchido:



Clique em **Continuar** para prosseguir para a próxima etapa no assistente.

Mapeamento de campos de infração para a integração IBM QRadar

Depois de selecionar as regras, a próxima etapa é mapear campos de ofensa, evento ou fluxo para os campos no formulário de incidente de segurança.

Visão geral

Para a etapa de mapeamento, você deve primeiro ingerir amostras de infrações para uma ou mais regras IBM QRadar selecionadas. Em seguida, você deve garantir que todos os dados de campo de infração relevantes sejam mapeados para o local apropriado no formulário de incidente SIR e, em seguida, visualizar o incidente SIR na seção de visualização.

O mapeamento dos campos de infração de amostra envolve o seguinte:

- Buscando e preenchendo os dados de amostra: consulte Ingestão da amostra de IBM QRadar infrações.
- Mapeamento dos campos de infração para o incidente de segurança: consulte Mapeamento de campos de infração IBM QRadar para campos de resposta a incidente de segurança.

Ingestão da amostra de IBM QRadar infrações

Você pode ingerir exemplos de infrações para uma ou mais regras IBM QRadar selecionadas.

Tradução automática

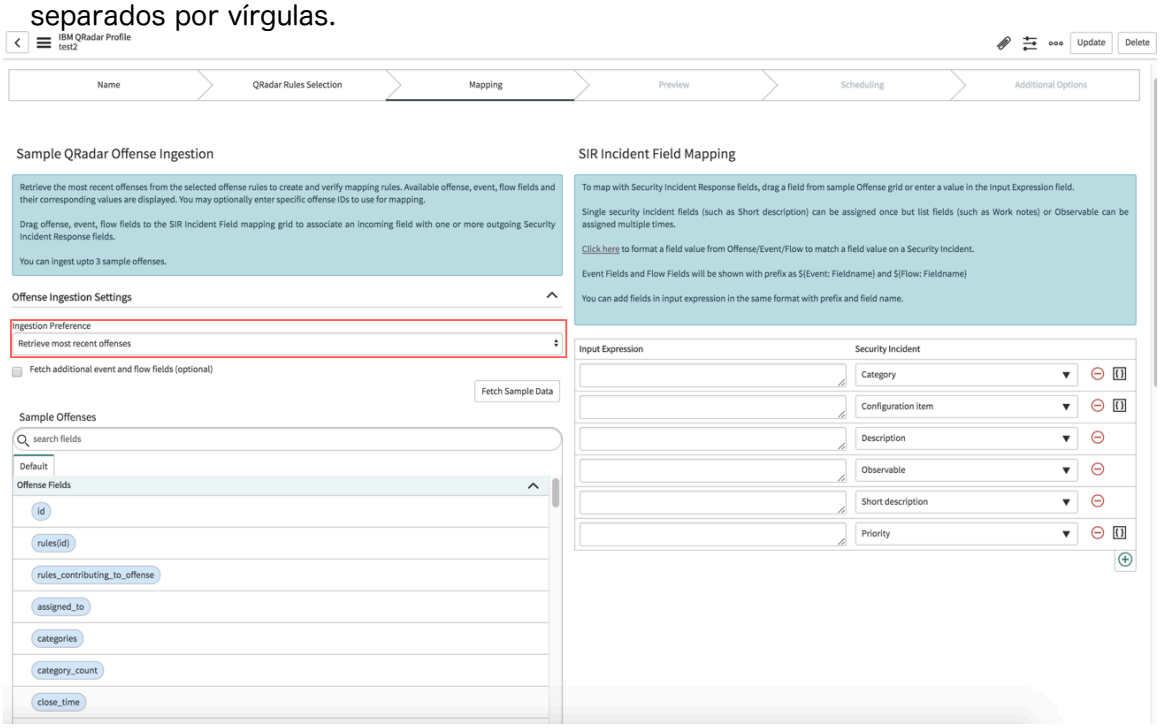
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Você pode extrair as três infrações de amostra mais recentes ou fornecer os IDs de ofensa exclusivos para as ofensas específicas que deseja usar para sua experiência de mapeamento.
   Na lista de seleção **Preferência de ingestão**, selecione uma das seguintes opções:
   - Recuperar infrações mais recentes: as três infrações mais recentes das regras selecionadas são recuperadas.
   - Selecionar infrações com base no ID de infrações: especifique o ID de infração para as infrações a serem recuperadas. Você pode especificar no máximo três IDs de ofensa separados por vírgulas.



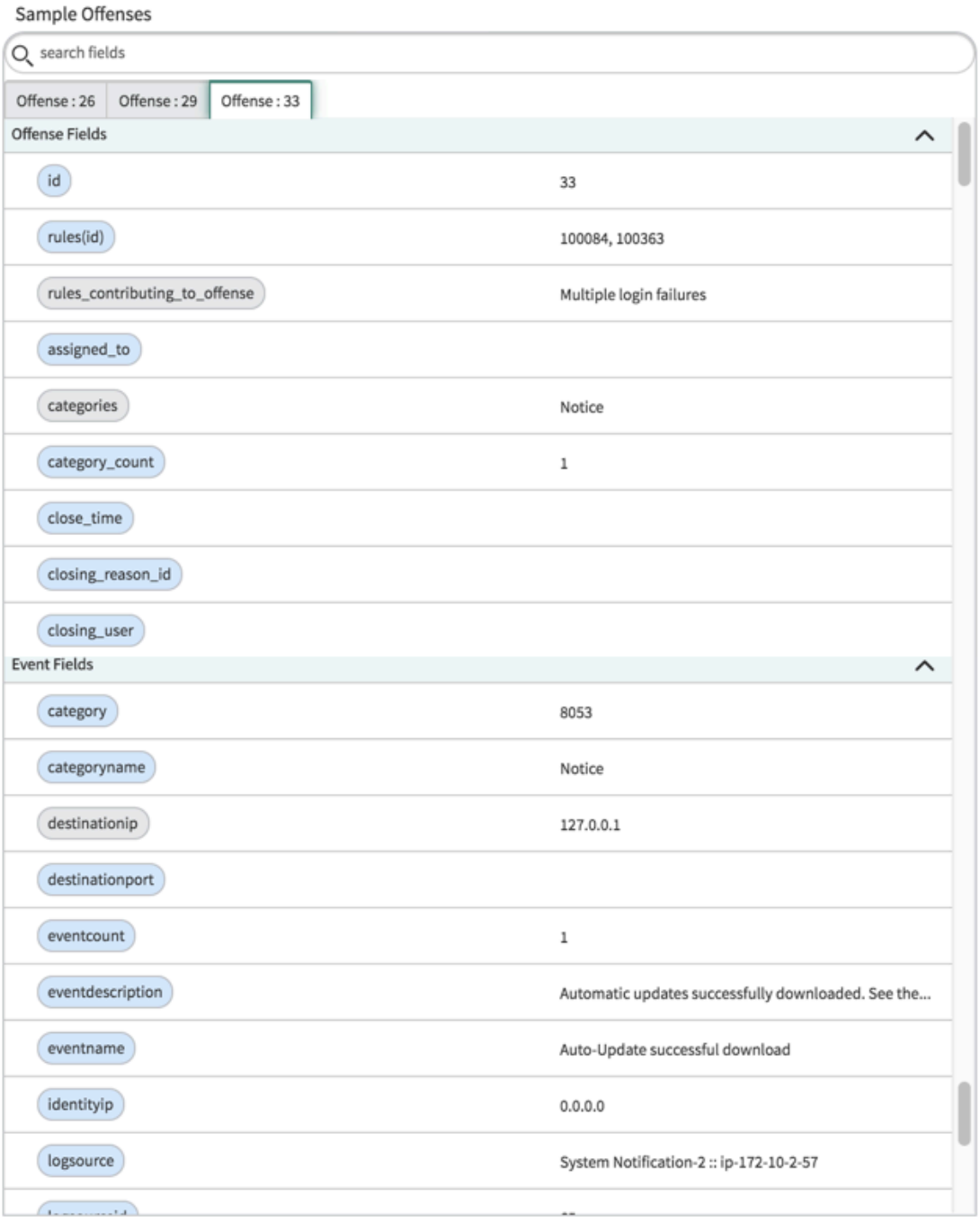
3. Clique em **Buscar dados de amostra** para extrair os dados de amostra mais recentes do console IBM QRadar para as regras de violação selecionadas.

   Os campos de infração e os resultados dos valores são exibidos como guias individuais. Uma ofensa pode ser acionada por três tipos de regras:
   - Evento: nesta regra, os logs de eventos são verificados e, se os critérios especificados forem atendidos, uma ofensa será criada.
   - Fluxo: os dados e o tráfego da rede são verificados e, se determinadas condições forem atendidas, uma ofensa será criada.
   - Comum: neste caso, você pode especificar condições para eventos ou fluxos e uma ou ambas as condições forem atendidas, uma ofensa será criada.

   A extração de exemplos de infrações pode demorar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela. Dependendo da regra ou das regras que acionaram a infração, junto com os campos de infração, os campos de evento ou fluxo são preenchidos conforme mostrado na figura abaixo:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

Nota:
Os campos de evento ou fluxo exibidos pertencem ao primeiro evento ou campo de fluxo que acionou a infração com base no evento ou regra de fluxo correspondente.

4. A seguir estão os campos de infração personalizados criados para esta integração.
   Os campos de infrações padrão, além desses campos personalizados, estão disponíveis para mapeamento.
   - rules_contributing_to_offense: IBM QRadar regras que contribuíram para a ofensa com base no ID da regra.
   - users: nomes de usuário para a ofensa

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- remote_destination_ip: os IPs de destino remotos da infração.

  Com base nos IDs de destino local da infração, os seguintes campos de endereço de destino local personalizados estão disponíveis:

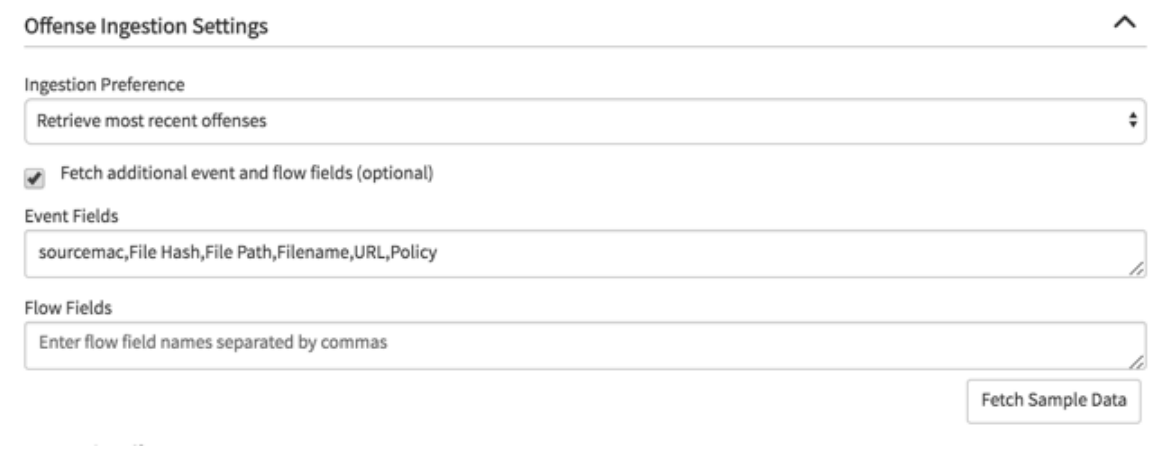
  - local_destination_address (domain_id)
  - local_destination_address (event_flow_count)
  - local_destination_address (first_event_flow_seen)
  - local_destination_address (id)
  - local_destination_address (last_event_flow_seen)
  - local_destination_address (local_destination_address_ids)
  - local_destination_address (magnitude)
  - local_destination_address (rede)
  - local_destination_address (offense_ids)
  - local_destination_address (local_destination_ip)

- Os seguintes endereços de origem estão disponíveis com base nos IDs de origem da infração:
  - source_addresses (domain_id)
  - source_addresses (event_flow_count)
  - source_addresses (first_event_flow_seen)
  - source_addresses (id)
  - source_addresses (last_event_flow_seen)
  - source_addresses (source_address_ids)
  - source_addresses (magnitude)
  - source_addresses (rede)
  - source_addresses (offense_ids)
  - source_addresses (source_ip)

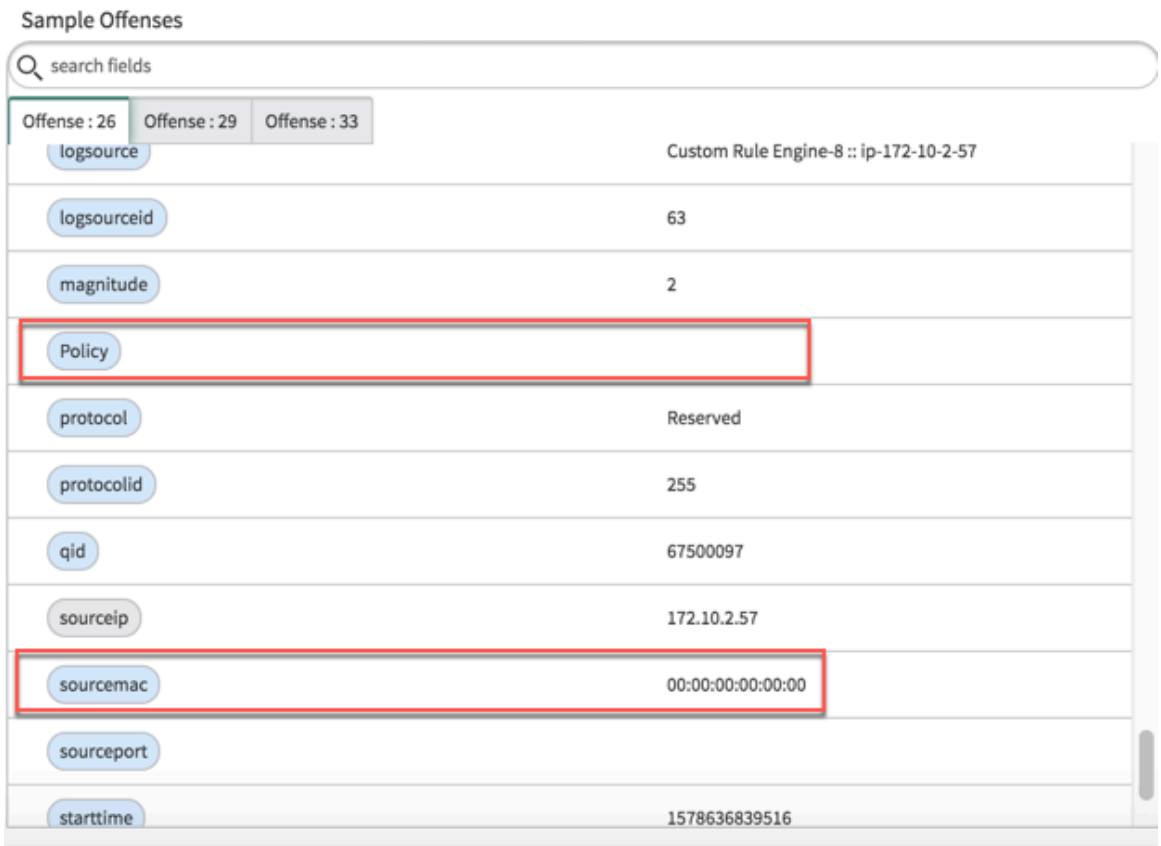
Marque a caixa de seleção **Buscar eventos adicionais e campos de fluxo (opcional)**. Você pode buscar eventos de amostra e dados de fluxo de qualquer evento personalizado válido e campos de fluxo. Especifique os campos personalizados separados por vírgulas, conforme mostrado abaixo:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



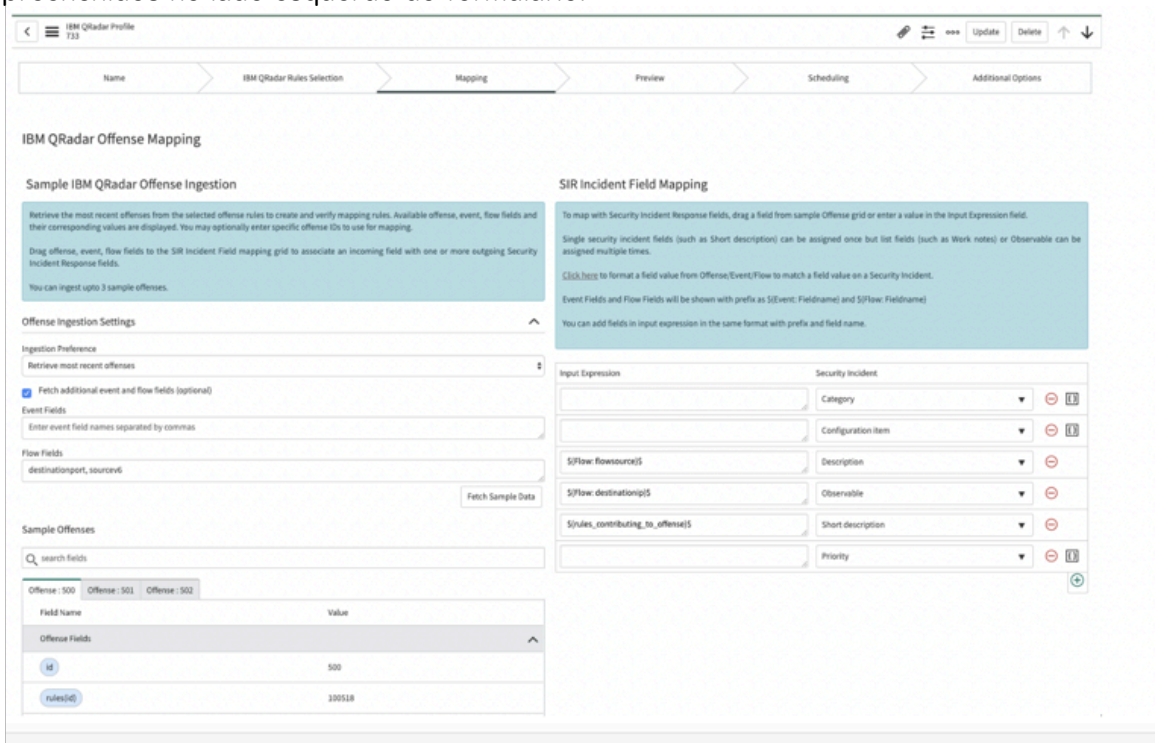
Clique **em Buscar dados de amostra**. Os campos de evento ou fluxo especificados junto com seus valores (se disponíveis) são anexados à seção Evento ou Fluxo, conforme mostrado abaixo:



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de buscar os dados de amostra, os valores correspondentes a esses campos são preenchidos no lado esquerdo do formulário.



O que Fazer Depois

Depois de buscar os dados de amostra, a próxima etapa é mapear os campos de infração para o incidente de segurança.

Mapeamento de campos de infração IBM QRadar para campos de resposta a incidente de segurança

Mapeie campos de ofensa, evento e fluxo individuais para campos em um incidente de segurança Now Platform SIR.

Mapeamento de campo de infração

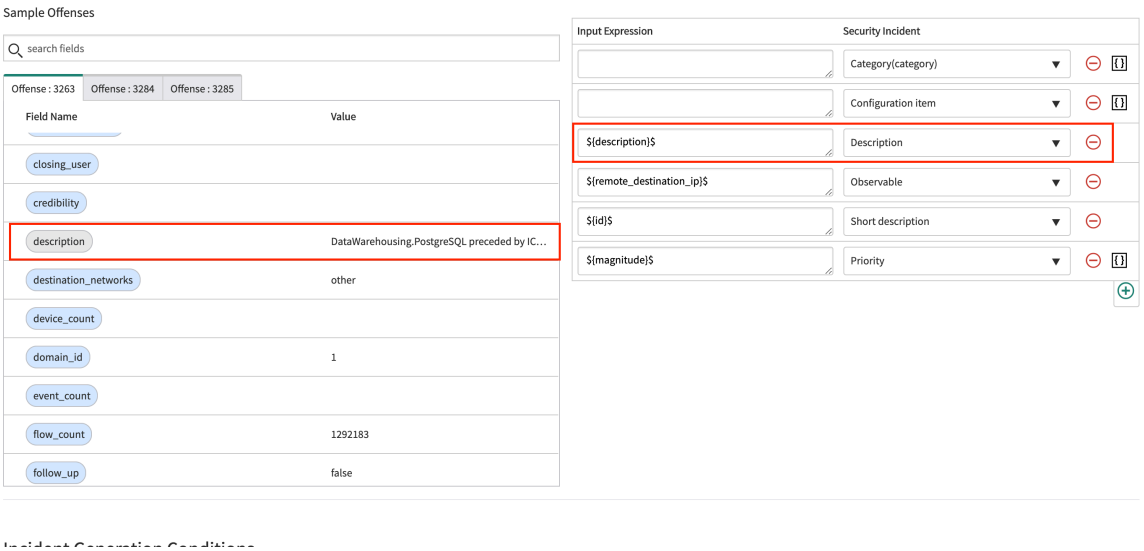
Como um usuário com a função sn_si.admin, use os campos da seção Infrações de amostra à esquerda e mapeie-os para os campos de incidente de segurança na coluna Mapeamento de campo de incidente SIR. Edite a configuração de mapeamento arrastando os campos de ofensa, evento ou fluxo do lado esquerdo e soltando-os na seção de mapeamento de incidente ServiceNow SIR à direita. O mapeamento à direita associa o campo de infração de entrada a um campo de incidente de segurança de saída.

1. Depois de buscar os dados de amostra, a próxima etapa é mapear os campos de infração, evento ou fluxo para o incidente de segurança. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e mantenha pressionado um nome de campo azul no lado esquerdo do formulário.
2. Arraste o nome do campo, por exemplo, descriçãoe solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.

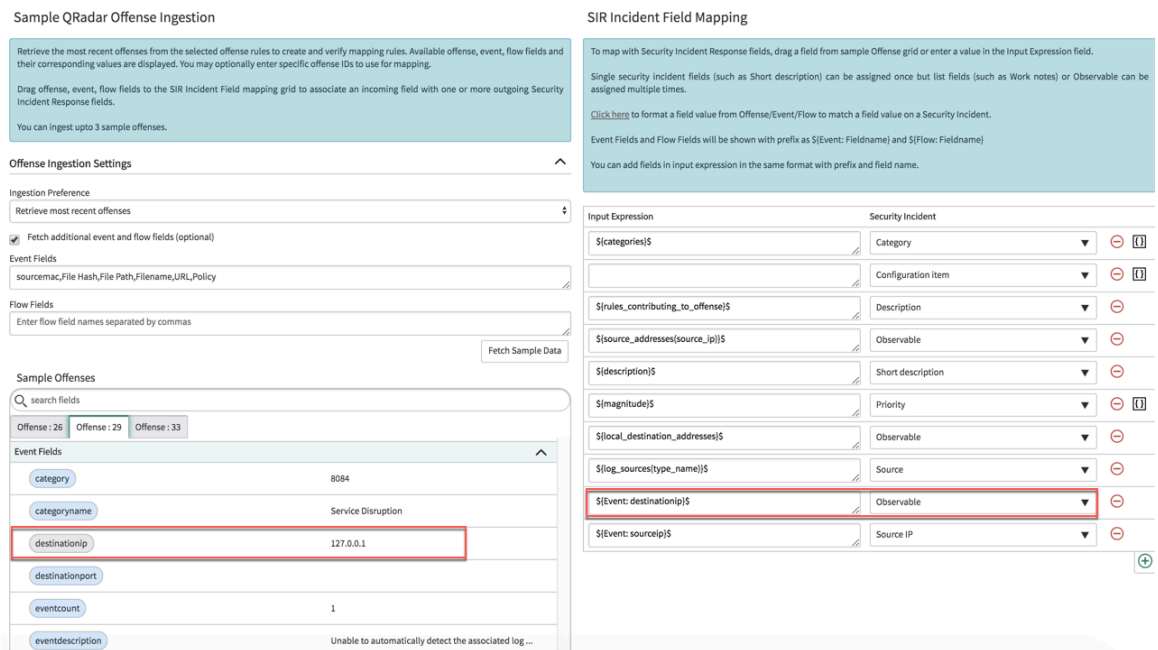
   O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, a descrição é mapeada para o campo Descrição no incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:
Se você inserir o nome do campo de evento ou fluxo manualmente na seção Expressão de entrada, deverá adicionar um prefixo como `${Event:eventfield}$` ou `${Flow:flowfield}$` antes do nome do campo que está sendo mapeado.



Para ajudar a garantir que nenhum campo de ofensa, evento ou fluxo seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. A codificação por cores dos campos de infração ajuda a rastrear os valores de infração que você já mapeou conforme eles se tornam esmaecidos, enquanto todos os campos não mapeados restantes aparecem em azul. Isso ajuda a visualizar melhor quais valores de campo foram adicionados ao incidente de segurança e se alguma informação de infração importante restante permanece não mapeada.

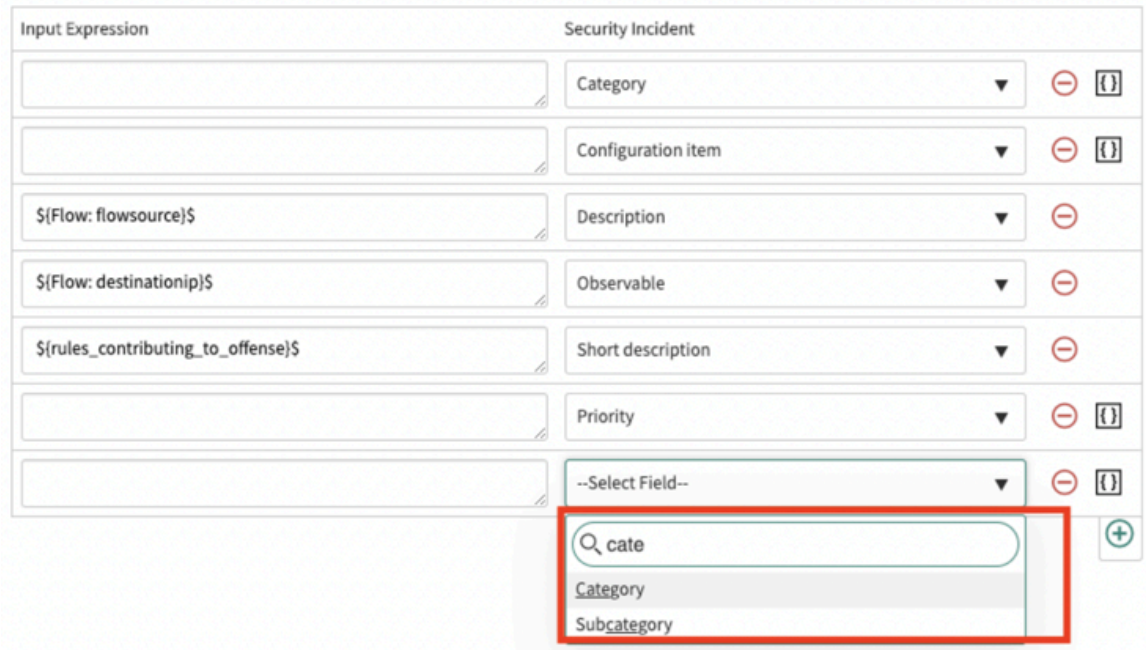
Os campos azul claro à esquerda indicam que um campo de infração ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar uma ofensa, um evento ou um campo de fluxo de entrada a mais de um campo em um incidente de segurança. Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação de cores ajuda a rastrear o mapeamento.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

3. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas:
   a. À direita do formulário na seção Mapeamento de campo de incidente de SIR, na parte inferior da grade, clique no ícone de adição (+). Um novo campo é exibido.
   b. Na coluna Incidente de segurança, expanda a lista de seleção exibida e selecione um campo.

      Na lista de seleção expandida para o novo campo, alguns campos estão sombreados. Na figura a seguir, Categoria tem um plano de fundo cinza porque foi mapeada no incidente de segurança. Semelhante à codificação de cores dos campos de infração no lado esquerdo do formulário, essa codificação de cores para os campos de incidente de segurança à direita ajuda a rastrear os campos de incidente de SIR já mapeados.



Nota:
Como vários observáveis podem ser exibidos no mesmo incidente de segurança, o campo Observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho oferecem suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, será exibida uma mensagem de erro informando que não há nenhum valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista de seleção na qual você pode escolher várias opções e você tentar mapear uma opção para esse campo que não é exibido na lista de seleção, o campo não será preenchido no incidente de segurança.

   c. Como alternativa, digite um valor no campo Pesquisar da nova linha.
   d. No lado esquerdo do formulário, selecione o campo de infração e arraste e solte-o em um campo de incidente de segurança apropriado à direita.
4. Remova campos usando o ícone - ao lado do nome do campo na seção de mapeamento de campo de incidente SIR.
5. Continue mapeando adicionando ou removendo valores de campo para o mapeamento.

Campos de infração com vários valores

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Os campos de incidente de segurança, como os campos **Categoria** e **Usuário** (por exemplo, Usuário afetado, Atribuído a) disponíveis com o produto base não oferecem suporte a vários valores.
- Os seguintes campos IBM QRadar oferecem suporte a vários valores:
  - *categorias*
  - *destino_redes*
  - *source_address_ids*
  - *local_destination_address_ids*
  - *remote_destination_ips*
  - *rules_contributing_to_offense*
  - *usuários*

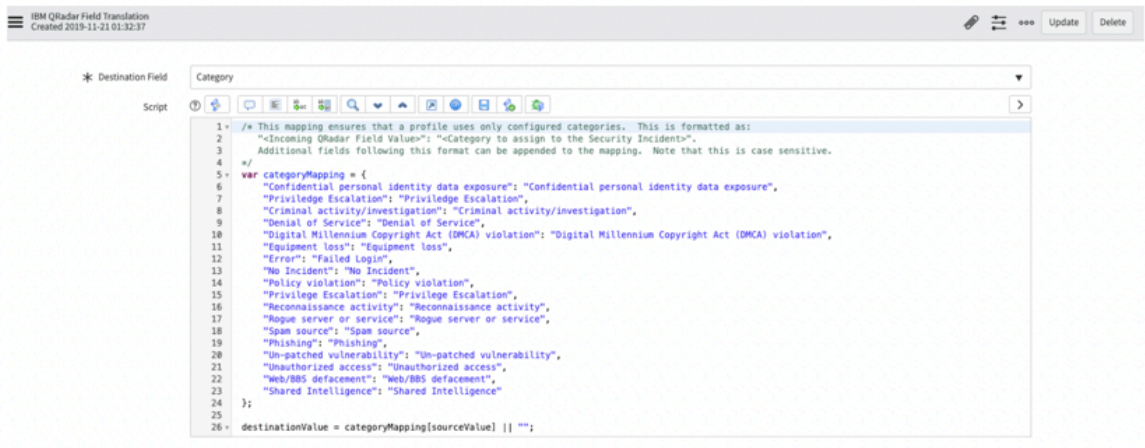
  Se você precisar mapear os campos acima para qualquer campo Security Incident Response além dos campos do tipo IC e Observável, deverá criar novos campos Security Incident Response do tipo **Lista** e usá-los para mapeamento.

Nota:
Por padrão, somente os campos do tipo **Lista** sem referência são compatíveis.

Formatar tradução de campo

Em determinados casos, os valores de campo de infração em IBM QRadar podem não ser traduzidos diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de script se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de script, um valor de categoria de Alerta de malware e Infecção de vírus pode ter valores de campo diferentes para a categoria de origem, mas ambos os valores podem ser convertidos em uma Atividade de código malicioso comum no campo Categoria no incidente de segurança SIR usando o formato Funcionalidade de tradução de campo.

Para usar o editor de script, clique no {0}. O editor de script é exibido.



Insira as mudanças no script e clique em **Atualizar** para salvar as mudanças e retornar à página Mapeamento.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condições de geração de incidentes

Depois que a seção de mapeamento estiver concluída, você poderá definir condições de filtro para especificar quais infrações devem criar incidentes de segurança e quais devem ser filtradas, por exemplo, infrações de baixa prioridade. Você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que uma ofensa de entrada deve satisfazer para criar um incidente de segurança. Para definir condições de geração de incidentes, siga estas etapas.

1. Role até a seção **Condições de geração de incidente** no formulário e marque a caixa de seleção **Filtrar com base nas condições** para habilitar a opção.

   O construtor de Condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

   As opções nas listas de seleção para o primeiro campo no construtor de Condições de filtro correspondem aos campos que são exibidos na seção Ingestão de infração do QRadar de amostra para as infrações que você ingeriu. Esses campos são dinâmicos e mudam dependendo das ofensas que você ingere. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas e devem corresponder exatamente aos valores da ofensa IBM QRadar. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao console IBM QRadar e revisar suas infrações para as palavras-chave.

   Nota:
   As `categorias`, `target_networks`, `source_address_ids`, `local_destination_address_ids`,`remote_destination_ips`, `rules_contributing_to_offense`e os campos de infração de `usuários` podem ter vários valores (já que os valores são armazenados em matrizes). Como a condição do filtro pode recuperar somente cadeias de caracteres, você deve usar a condição do filtro " `contém` " para esses campos para garantir que os dados sejam filtrados corretamente.

2. Usando as listas de seleção e os campos do construtor de condições, defina filtros para a primeira linha.
3. Para adicionar mais condições, à direita dos campos, clique em **E** ou **OU**.
   - Se **AND** for selecionado, todas as condições deverão ser correspondidas.
   - Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida.
4. (Opcional) Na segunda linha, defina uma segunda condição de filtro.

   A imagem a seguir é um exemplo com duas condições que devem ser correspondidas antes que os incidentes de segurança sejam criados.

   Você definiu as condições de geração de incidentes para que os incidentes de segurança sejam criados somente quando ambas as condições de filtragem inseridas forem correspondidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esse tipo de filtragem de condição de geração de incidente ajuda a restringir as ofensas e limita o número de incidentes de segurança desnecessários que você cria sem modificar a regra subjacente ou os filtros em IBM QRadar. Se critérios de filtragem adicionais forem definidos, somente as infrações que corresponderem a todos os critérios serão mapeadas para incidentes.

Nota:
Se algum dos nomes de campo de infração tiver caracteres especiais, como aspas (“), hifens ('), sublinhados (-) ou e comercial (@), talvez esses caracteres precisem ser substituídos para fins de filtragem, mas um sufixo numérico será anexado a diferencie campos com nomes de infração duplicados. Por exemplo, se o primeiro campo de violação for `alerts.alert` e o segundo campo de violação for `alerts@alerts`, esses campos não poderão ser identificados exclusivamente, pois os caracteres de texto padrão restantes são os mesmos. Nesse caso, um sufixo é adicionado ao segundo campo de infração e o campo é renomeado para `alerts@alert(1)` quando exibido na lista Condições do filtro.

Critérios de agregação de infração para lidar com infrações semelhantes e evitar incidentes duplicados

Defina critérios de agregação de infração adicionais que agregam uma infração de entrada a um incidente de segurança SIR existente em vez de criar incidentes semelhantes, potencialmente duplicados. Usando critérios de valor de correspondência de campo para cada perfil, essa capacidade de agregação adicional pode reduzir o número de incidentes de segurança ativos e sobrepostos, colocando todos os dados de infração relacionados em um único incidente de segurança. Para definir os critérios, siga estas etapas abaixo:

1. Role até a seção Critérios de agregação de infração no formulário e marque a caixa de seleção **Condições de agregação** para habilitar esta opção.

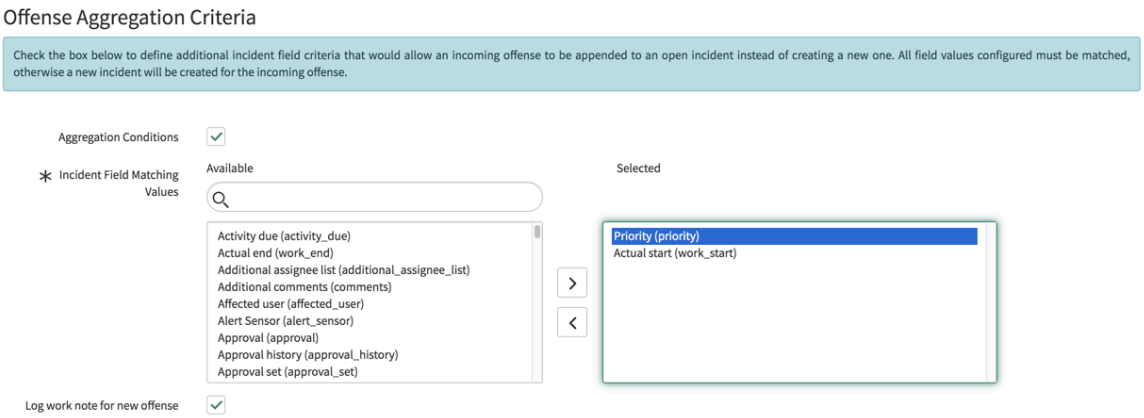
   As colunas Valores correspondentes do campo de incidente são exibidas. Esses nomes de campo são os campos no incidente de segurança que incluem todos os campos personalizados que estão configurados no incidente de segurança SIR.

2. Na lista Disponível, selecione os valores de campo que você deseja corresponder aos incidentes de segurança existentes no seu Now Platform e mova-os para a lista Selecionado.

   Todos os valores de campo selecionados devem ser correspondidos para anexar este alerta de entrada a um incidente de segurança existente. Isso inclui campos, como observáveis e itens de configuração, que podem ter vários valores de campo de ofensa mapeados para eles. Todos os valores devem corresponder. Se apenas um subconjunto dos valores for correspondido, as condições de agregação de infração não serão atendidas e um novo incidente de segurança será criado. Veja a captura de tela abaixo para mapeamento de campo de vários valores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se uma nova infração corresponder a todos os valores selecionados nas condições de campo de agregação na etapa de mapeamento, a nova infração será adicionada automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todas as ofensas agregadas adicionadas em uma lista relacionada em um incidente de segurança. Esta lista detalha os carimbos de data/hora associados e os valores de campos agregados. Essas informações ajudam a entender por que essas infrações estão sendo agregadas a incidentes de segurança existentes. Se esta guia não for exibida, role até o lado esquerdo do registro em Links relacionados e clique no link **Mostrar todas as listas** relacionadas.

3. (Opcional) Para registrar uma anotação de trabalho para uma nova ofensa que foi adicionada recentemente ao incidente de segurança, marque a caixa de seleção para habilitar esta opção. A anotação de trabalho registra que uma nova infração foi adicionada junto com um link para os detalhes da infração e quaisquer outros detalhes que possam ter sido adicionados ao campo de anotação de trabalho na seção de mapeamento.

   Você mapeou com sucesso valores de uma ofensa IBM QRadar para campos em um incidente de segurança. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem de geração de incidentes. Você também anexou infrações a incidentes de segurança existentes quando os valores do campo de infração correspondem aos critérios de agregação configurados.

4. Clique em **Continuar** para prosseguir com a configuração do perfil. A próxima etapa é visualizar os campos mapeados em um incidente de segurança SIR

Visualizar o incidente de segurança para a integração IBM QRadar

Depois de concluir a etapa de mapeamento, visualize os valores que você mapeou em um incidente de segurança SIR. Esta etapa de visualização permite que você verifique se mapeou todos os campos de infração que deseja exibir no incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.admin

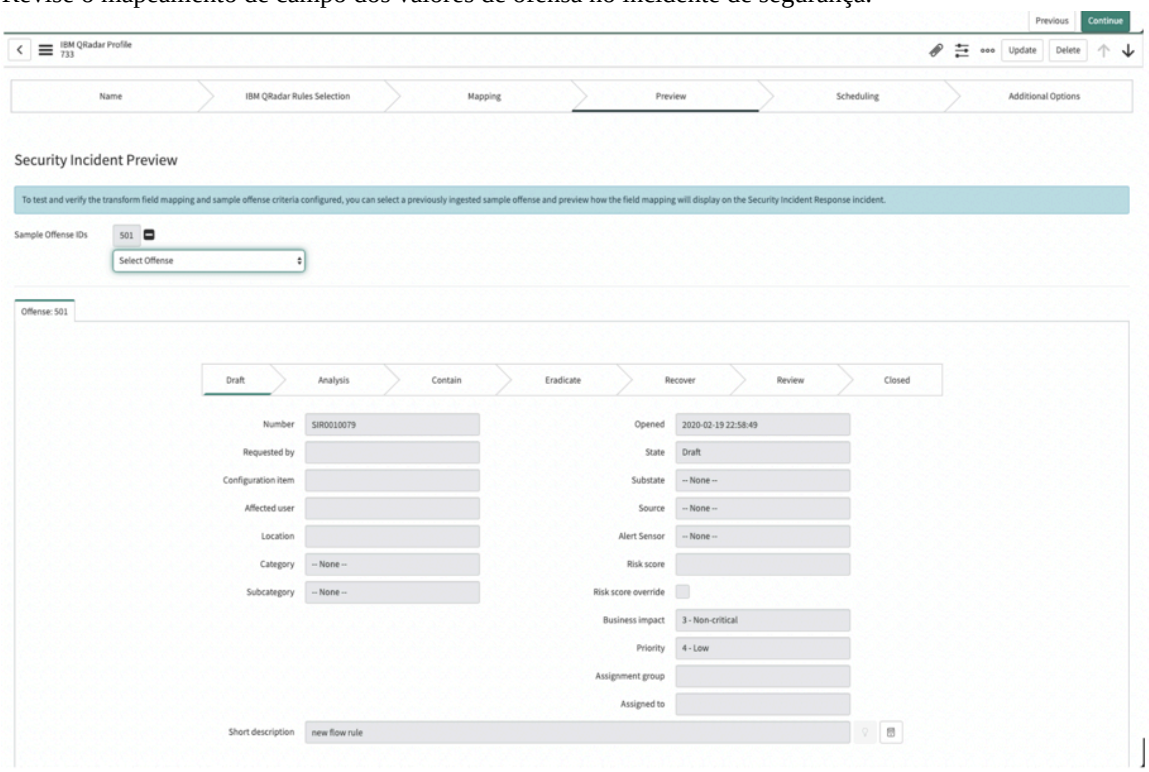
Por Que e Quando Desempenhar Esta Tarefa
Como um usuário com a função sn_si.admin, visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou para preencher quaisquer dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. As visualizações de SIR incidentes de segurança não são salvas como incidentes reais no produto Security Incident Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualizar** na barra de andamento.
2. Na lista de seleção IDs de infração de amostra, selecione um item.
   O incidente de segurança é exibido. Esta exibição é somente leitura e um registro deste incidente de segurança não é salvo.
3. Revise o mapeamento de campo dos valores de ofensa no incidente de segurança.



A imagem anterior é um exemplo de uma visualização com um erro de mapeamento das amostras que foram ingeridas.

4. Para resolver esse erro, clique em **Mapeamento** na barra de andamento.
5. Edite o mapeamento para corrigir valores incorretos ou preencha os dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir os erros descritos nas mensagens de erro.

O que Fazer Depois

Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campo no incidente de segurança, a próxima etapa é definir a programação.

Definir programação para a integração IBM QRadar

Você pode definir a programação para a ingestão de infração. Durante esta etapa, você pode verificar as configurações padrão para a recuperação da ofensa ou modificar a programação conforme necessário. Esta etapa também permite que você recupere o histórico de infrações usando um intervalo de datas.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você pode escolher se deseja ingerir alguma ofensa histórica durante a etapa de Programação. Você também escolhe com que frequência pesquisará novas infrações futuras e infrações atualizadas que correspondam à configuração do perfil.

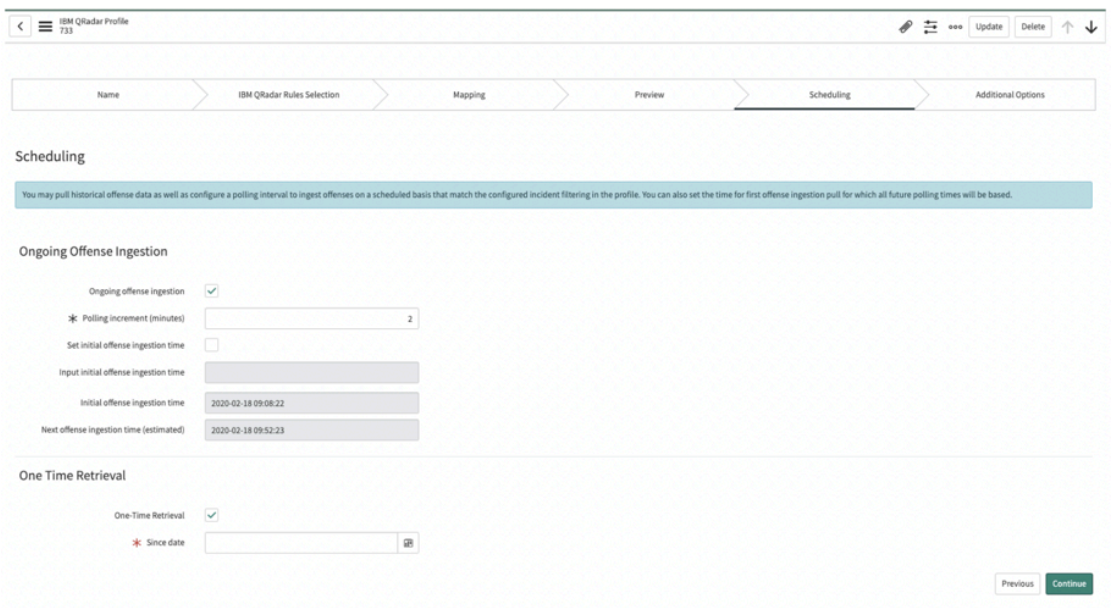
Como um usuário com a função sn_si.admin, você configura esses intervalos de pesquisa por perfil. O desempenho da integração de ingestão de infração IBM QRadar pode ser afetado pelos diferentes intervalos de pesquisa. Ao programar, talvez você prefira equilibrar a redução da sobrecarga de pesquisa no servidor IBM QRadar com o desejo de ser notificado o mais rápido possível quando uma ofensa for criada ou atualizada. Um valor padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração para um minuto, se necessário.

Extraindo ofensas novas e atualizadas

Quando a programação de pesquisa é definida, o trabalho programado extrai ofensas novas e atualizadas que foram extraídas anteriormente, mas não atenderam aos critérios de filtragem de incidentes. Isso fornece a flexibilidade para criar incidentes com base em critérios que podem não estar presentes quando uma ofensa é criada pela primeira vez, mas se tornam disponíveis após uma atualização, por exemplo, durante a fase de investigação. Depois que um incidente é criado para uma ofensa específica, suas atualizações subsequentes são ignoradas, pois é esperado que a ofensa agora seja tratada como um incidente de segurança ativo ServiceNow. No entanto, todas as outras ofensas que foram ingeridas anteriormente, mas não atenderam aos critérios de geração de incidentes, continuarão a ser extraídas e verificadas em relação aos critérios de geração de incidentes até que se tornem parte de um incidente ativo.

Procedimento

1. Se a página Programação na barra de andamento não for exibida, selecione **Programação**.
2. Escolha um para programar como e quando as ofensas são extraídas do console IBM QRadar.



3. Clique em **Continuar** para navegar até a página Opções adicionais.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Automatizar atualizações e fechamento de infração com base no status do incidente no SIR

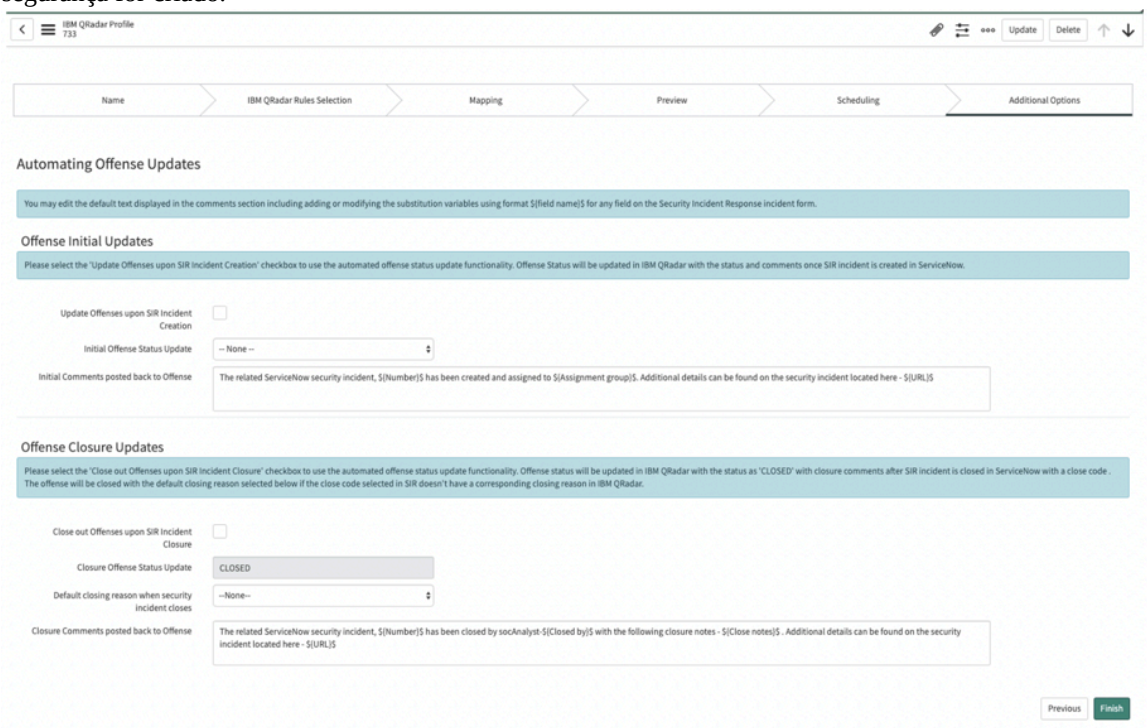
A integração IBM QRadar tem uma interface bidirecional que permite que ambas as infrações criem incidentes de segurança, bem como a capacidade de atualizar as infrações depois que o incidente de segurança é criado e/ou encerrado com detalhes relevantes do incidente, como número do incidente de segurança, atribuição grupo, URL do incidente de segurança e assim por diante.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais**.
2. Siga as instruções abaixo para concluir a configuração para atualizar as infrações quando o incidente de segurança for criado.



3. Clique em **Concluir** para concluir a configuração e mover o perfil para o estado **Aguardando**.
   Uma caixa de diálogo de confirmação é exibida. Você concluiu com êxito a instalação e a configuração da integração. Ative este perfil para extrair ofensas do console IBM QRadar com base em sua programação.

IBM QRadar definições de configuração de integração

Use esta opção para modificar as propriedades do sistema padrão de integração de ingestão IBM QRadar.

Para modificar as propriedades do sistema, faça login como um usuário com a função *sn_si.admin* e navegue até **Integração do IBM QRadar** > **Configurações de integração do IBM QRadar**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de integração do IBM QRadar

Nome da Propriedade	Descrição
Imponha um limite no número de incidentes de segurança que podem ser criados em um período de 24 horas. sn_sec_qradar.max_si_per_day	Especifica o número máximo de incidentes de segurança que podem ser criados em 24 horas. • Tipo: inteiro • Valor padrão: 1000
Imponha um limite no número de infrações que podem ser agregadas a um único incidente. sn_sec_qradar.max_aggregation_per_si	O limite de agregação de infração para um incidente de segurança. Por exemplo, se houver 102 infrações, as primeiras 100 infrações serão agregadas ao security incident_1 e as 2 restantes ao security incident_2. • Tipo: inteiro • Valor padrão: 100
Esta propriedade define o período de tempo do AQL para buscar eventos/fluxos recentes para uma ofensa específica. sn_sec_qradar.on_demand_recent_days_limit	Especifica o número de dias para buscar eventos ou fluxos recentes para uma infração específica. • Tipo: inteiro • Valor padrão: 7
Esta propriedade limita o número de eventos recentes obtidos para uma infração específica. sn_sec_qradar.on_demand_event_limit	Especifica o número de eventos recuperados para uma ofensa. Os eventos mais recentes são recuperados primeiro com base no carimbo de data/hora do evento. • Tipo: inteiro • Valor padrão: 100
Esta propriedade limita o número de fluxos recentes obtidos para uma infração específica. sn_sec_qradar.on_demand_flow_limit	Especifica o número de fluxos que são recuperados para uma ofensa. Os fluxos mais recentes são recuperados primeiro com base no carimbo de data/hora do fluxo. • Tipo: inteiro • Valor padrão: 100
Esta propriedade define o valor de tempo limite (segundos) para o AQL que busca fluxos/eventos recentes para uma ofensa específica. sn_sec_qradar.on_demand_timeout	• Tipo: inteiro • Valor padrão: 300
Tempo limite de IDs de pesquisa (segundos) para registros na fila para pesquisa de AQLs de uma infração.	O tempo limite do AQL para uma ofensa na fila antes de criar um incidente de segurança. Por exemplo, se houver 90

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de integração do IBM QRadar

Nome da Propriedade	Descrição
sn_sec_qradar.sid_ttl	infrações, as primeiras 50 infrações serão processadas para dados AQL no primeiro lote e as 40 infrações restantes no lote subsequente no mesmo intervalo de pesquisa. • Tipo: inteiro • Valor padrão: 300
Limite para controlar o número de pesquisas que podem ser executadas em IBM QRadar em um momento que é acionado pela integração programada trabalho.sn_sec_qradar.records_threshold_in_queue_for_aql	Especifica o número de infrações que você busca em um único lote em um intervalo de pesquisa. • Tipo: inteiro • Valor padrão: 50
Este é o número de dias para limpeza das tabelas de integração. sn_sec_qradar.queue_item_expire	A seguir estão as tabelas de integração: • sn_sec_qradar_events — Eventos do IBM QRadar • sn_sec_qradar_flows — Fluxos do IBM QRadar • sn_sec_qradar_offense_updates — Atualizações de infração do IBM QRadar • sn_sec_qradar_offense_to_task — IBM QRadar infração para tarefa • Tipo: inteiro • Valor padrão: 30
Limite de infração por execução de trabalho programado por perfil na recuperação única ou na ingestão contínua. sn_sec_qradar.max_offense_limit_per_run	Especifica o número de infrações que você busca na Now Platform em uma única recuperação. • Tipo: inteiro • Valor padrão: 1000
Defina esta propriedade para ativar o recurso Atualizações de infração. sn_sec_qradar.get_offense_updates	**Nota:** Habilitar esta configuração pode causar um atraso na criação de um incidente de segurança. • Tipo: verdadeiro| falso • Valor padrão: falso

Todas as configurações de integração modificadas serão aplicadas durante o próximo intervalo de pesquisa, conforme definido no perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opcional: copiar um perfil IBM QRadar

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, convém copiar os perfis para economizar tempo.

Antes de Iniciar

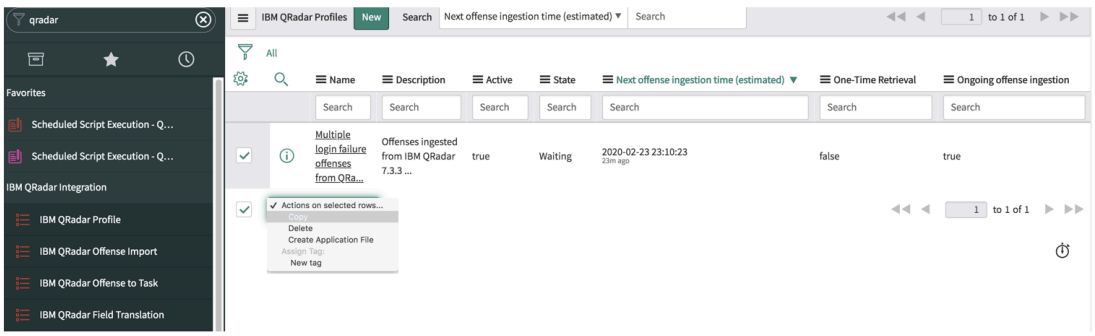
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Como um usuário com a função sn_si.admin, se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado está desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

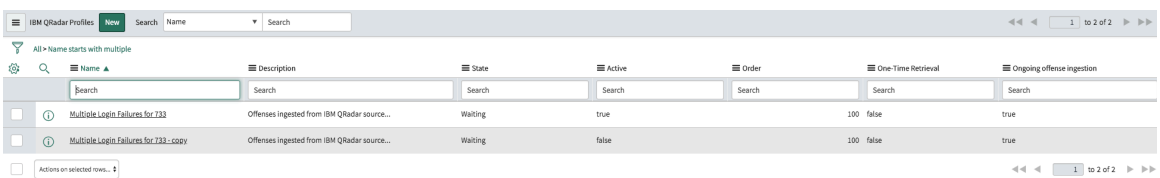
Procedimento

1. Navegar até **Todos** > **Integração do IBM QRadar** > **Perfil do IBM QRadar**.
2. Na lista Perfis do IBM QRadar exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Copiar**.



O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo o mapeamento e a configuração de programação. O nome do perfil contém cópia. Embora o perfil original esteja habilitado (verdadeiro), a cópia está desabilitada neste ponto (falso). Você pode editar os valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil, conforme necessário.

Nota:
Se você selecionar uma origem diferente para o perfil, deverá selecionar novas regras (Selecionar regras IBM QRadar) para o perfil. Mas se você usar a mesma origem e selecionar novas regras, as amostras de infrações serão apagadas.



Você copiou com sucesso as configurações de um perfil existente para um novo perfil. Observe que o status da coluna **Ativa** está definido como falso, pois o perfil precisa ser ativado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Você será solicitado a ativar (habilitar) o novo perfil depois de concluir as etapas de configuração.

Separação de domínio e ingestão de infração IBM QRadar

A separação de domínio é compatível com a ingestão de ofensa IBM QRadar. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Básico

- Lógica de negócios: confirme se os dados vão para o domínio adequado para os casos de uso do provedor de serviço de aplicativo.
- O aplicativo oferece suporte à separação de domínio em tempo de execução. O Domain Separation inclui separação de domínio de interface do usuário, chaves de cache, relatórios, acúmulos e agregações.
- O proprietário da instância deve configurar o aplicativo para funcionar em vários locatários.

Exemplo de caso de uso: quando um SP (service provider, provedor de serviço) usa o bate-papo para responder à mensagem de um locatário-cliente, o cliente deve conseguir ver a resposta do SP.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como a separação de domínio funciona na ingestão de infração IBM QRadar

Siga estas etapas para obter a separação de domínio:

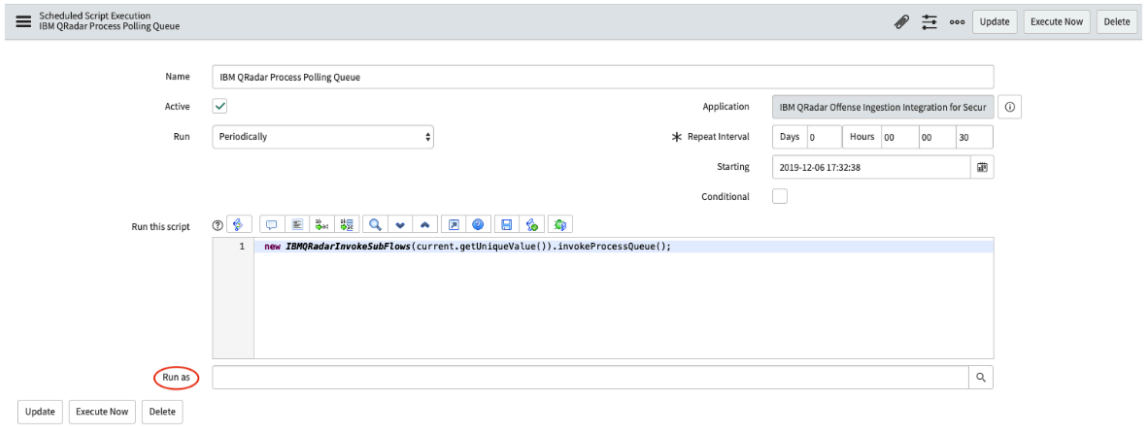
- Crie um usuário com a função *sn_si.admin* no respectivo domínio.

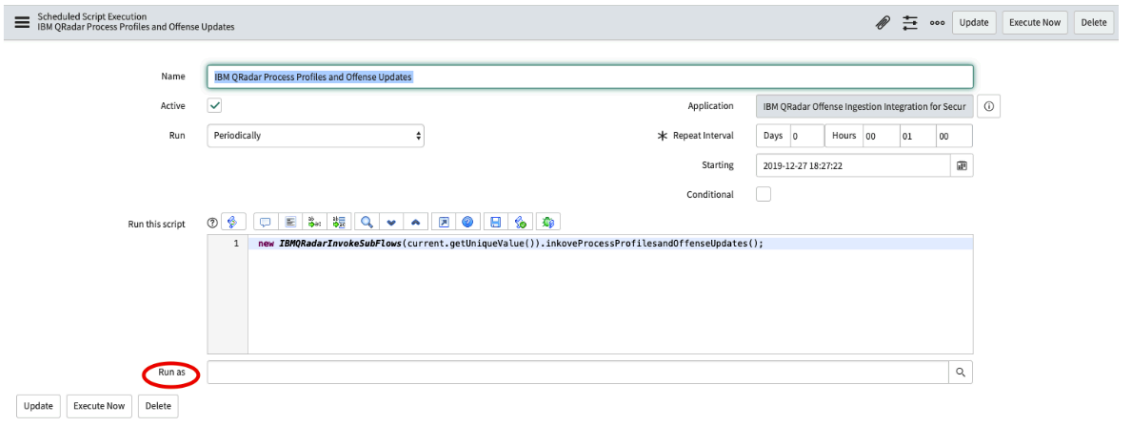
  Nota:
  Ao criar o perfil, use o seletor de domínio para selecionar o domínio específico. Não crie o usuário no domínio primário e, posteriormente, altere o domínio do perfil. Você deve ter um usuário específico para cada domínio do seu perfil com a função *sn_si.admin*. Use este usuário para criar ou modificar configurações no perfil.

- Desabilite os trabalhos programados existentes.
- Replique a IBM QRadar Fila de pesquisa de processo, os IBM QRadar Perfis de processo e os trabalhos programados de Atualizações de infração para cada domínio.
- Altere **Executar como** do usuário do sistema para o usuário com a função *sn_si.admin* no respectivo domínio e execute o trabalho programado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.





Tópicos relacionados

Domain Separation para provedores de serviço

Formulário do Security Incident Response após ingestão de infração

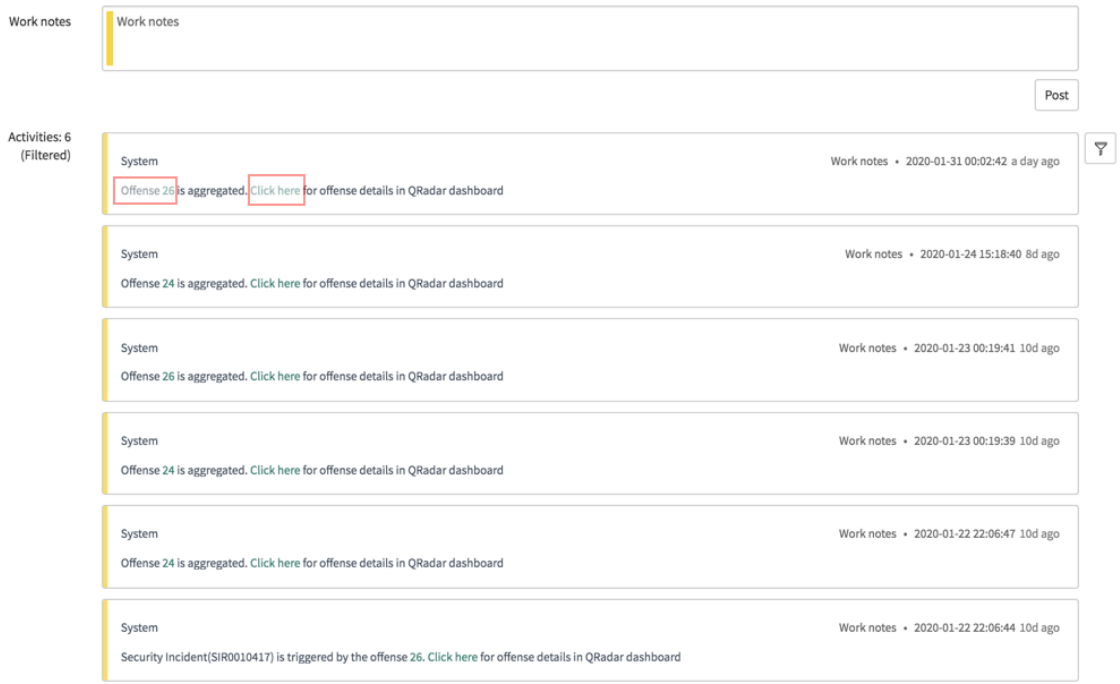
Depois que uma ofensa IBM QRadar foi ingerida, um incidente de segurança é criado e as atualizações correspondentes são feitas no registro do incidente de segurança.

Anotações de trabalho

Uma anotação de trabalho é publicada com detalhes da ofensa que acionou o incidente de segurança.

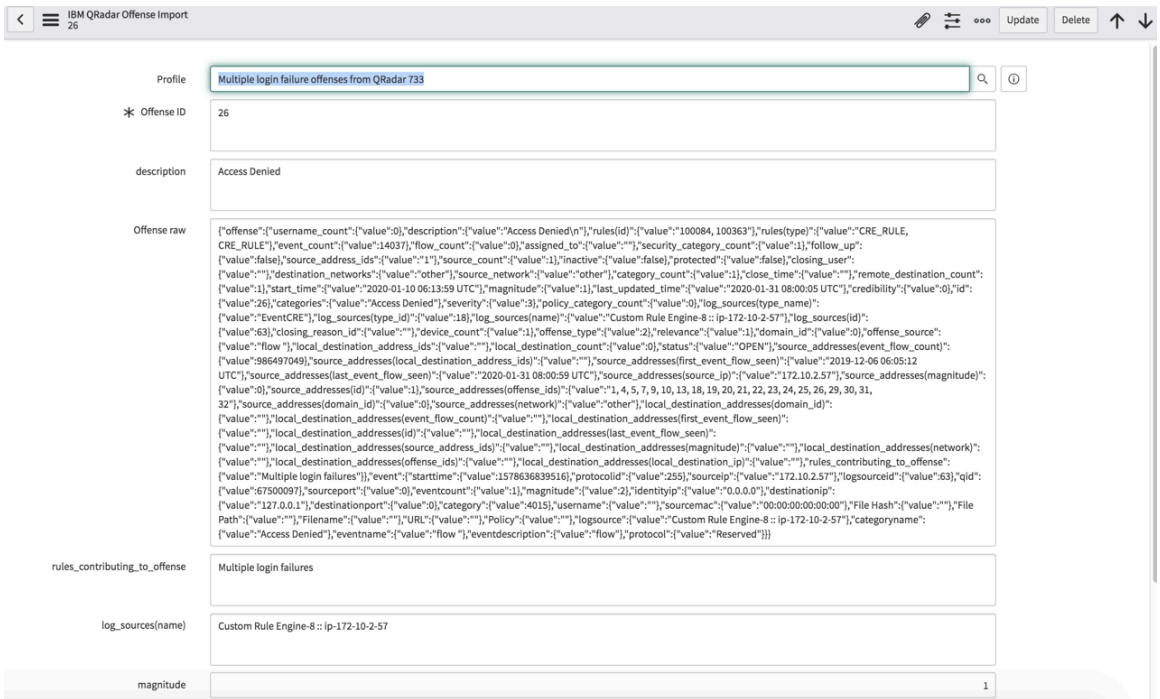
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Clique no link da ofensa para navegar até o registro do incidente de segurança interno. O hiperlink **Clique aqui** leva você para o painel IBM QRadar, onde você pode exibir os detalhes da infração.

Se você tiver selecionado a opção **Registrar anotação de trabalho em log para nova infração** nos Critérios de agregação de infração conforme descrito em Mapeamento de campos de infração IBM QRadar para campos de resposta a incidente de segurança, uma anotação de trabalho será publicada quando a infração for agregada.

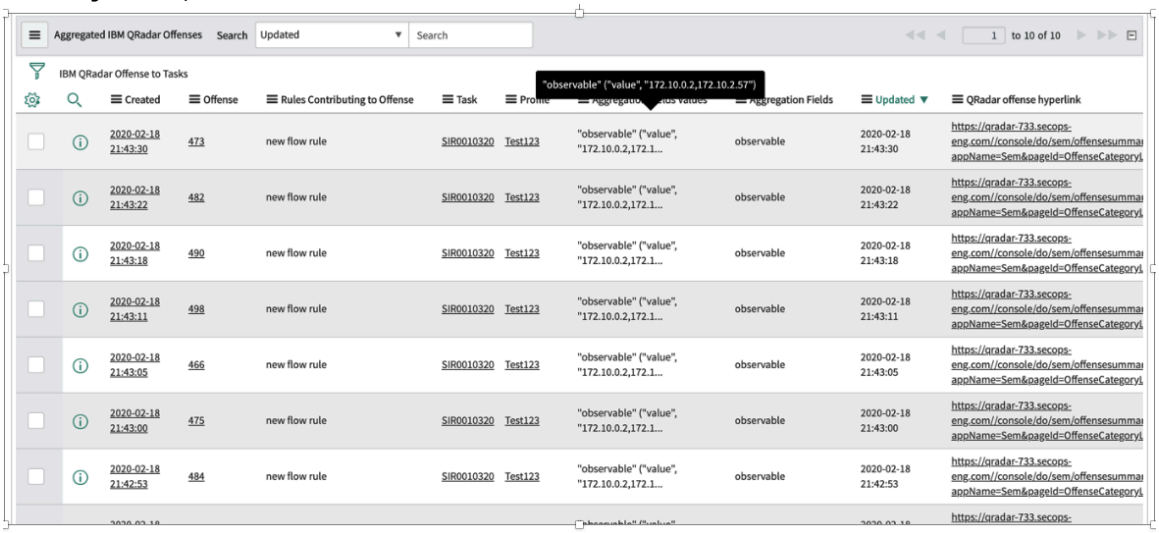


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

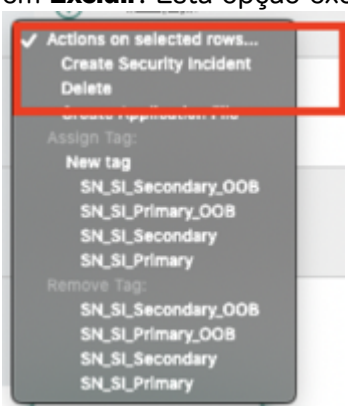
Infrações agregadas

Clicar **Listas relacionadas** > **Infrações agregadas do IBM QRadar** para exibir as infrações agregadas ao incidente de segurança. Clique no hiperlink de infração do QRadar para exibir a infração no painel IBM QRadar.



Criar incidente de segurança: selecione uma infração na lista, clique no menu **Ações** e clique em **Criar incidente de segurança**. Esta opção cria um incidente de segurança para a ofensa e essa ofensa é desagregada do incidente de segurança primário.

Excluir registro de infração: selecione uma infração na lista, clique no menu **Ações** e clique em **Excluir**. Esta opção exclui o registro de infração.



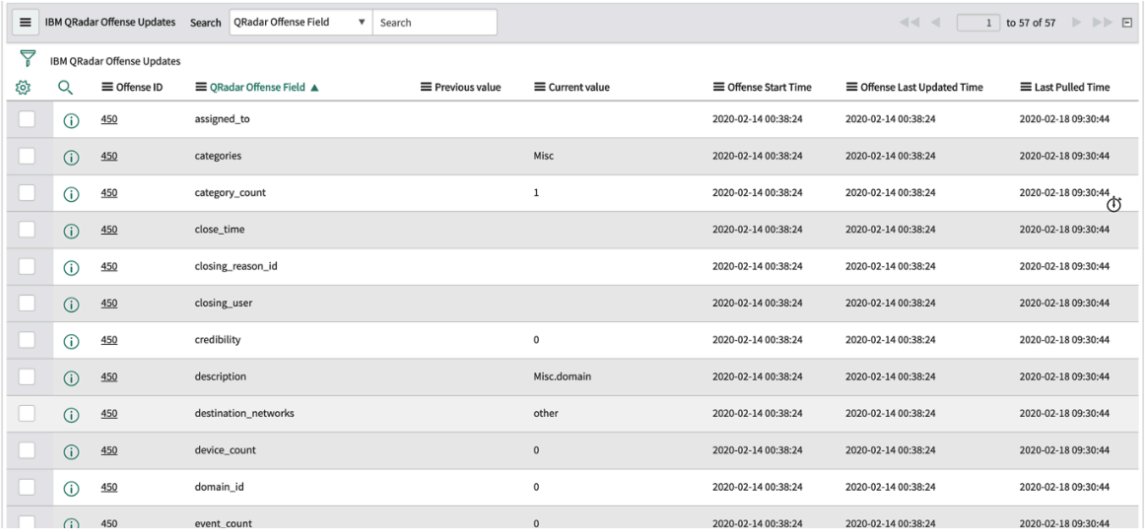
Atualizações de infração do IBM QRadar

Isso mostra os campos de infração padrão e personalizados e rastreia as mudanças na infração durante cada intervalo de pesquisa. Isso é útil, pois você pode exibir todas as atualizações de infração diretamente sem navegar até o painel IBM QRadar. Todas as mudanças nos valores são exibidas nos campos Valor anterior e Valor atual.

Para habilitar o recurso de atualizações de infração, navegue até **Integração do IBM QRadar** > **Configurações de integração do IBM QRadar** e habilitar **Defina esta propriedade para ativar o recurso Atualizações de infração**. Por padrão, essa configuração está desabilitada.

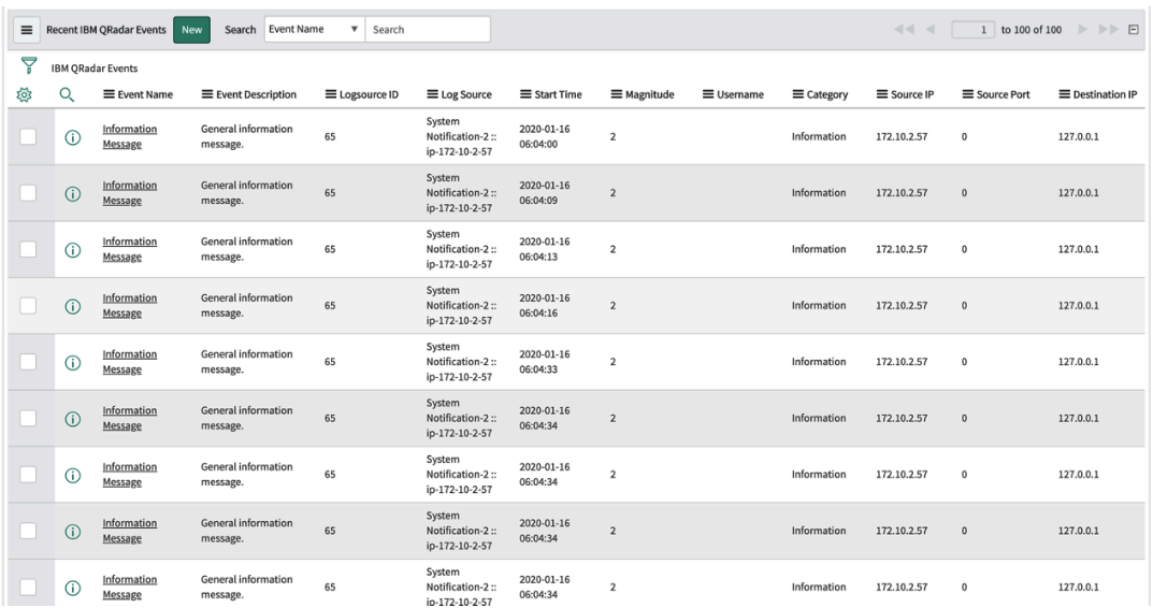
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Eventos recentes do IBM QRadar

Clique na opção **Buscar eventos recentes do IBM QRadar** nos **Links relacionados** para exibir os eventos IBM QRadar mais recentes.



Por padrão, um número máximo de 100 eventos é exibido. Você pode modificar esta configuração padrão no IBM QRadar definições de configuração de integração.

Nota:
A imagem acima mostra os campos de evento padrão associados à ofensa. Se você configurou e mapeou algum campo de evento personalizado (consulte Mapeamento de campos de infração IBM QRadar para campos de resposta a incidente de segurança), poderá exibi-lo na Exibição de lista clicando no link Nome do evento.

Tradução automática

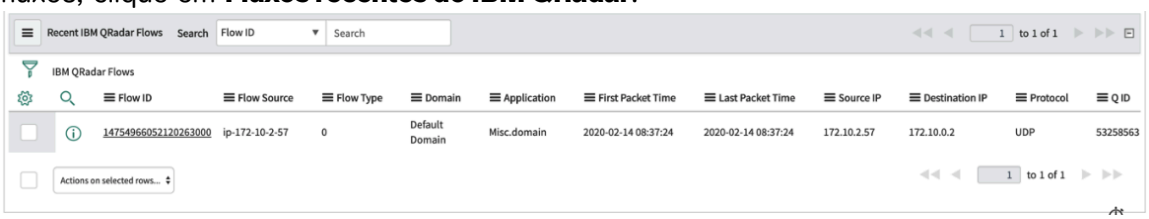
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

IBM QRadar Events
Disk Sentry Disk Usage Exceeded Warn Thr

Event Field Name	Value
File Hash	
File Path	
Filename	
Policy	
URL	
Category	8084
Categoryname	Service Disruption
Destinationip	127.0.0.1
Destinationport	0
Eventcount	1
Eventdescription	Disk Sentry: Disk Usage Exceeded Warning Threshold
Eventname	Disk Sentry Disk Usage Exceeded Warn Threshold
Identityip	0.0.0.0
Logsource	System Notification-2 :: ip-172-10-2-57
Logsourceid	65
Magnitude	2
Protocol	Reserved
Protocolid	255
Qid	38750076
Sourceip	172.10.2.57
Sourcemac	00:00:00:00:00:00
Sourceport	0
Starttime	2020-01-07 12:02:03
Username	

Fluxos recentes do IBM QRadar

Usando o Integration Hub e o Flow Designer, vários fluxos, subfluxos e ações estão disponíveis com a integração IBM QRadar. Ao clicar na opção **Buscar fluxos recentes do IBM QRadar** em Links relacionados, os fluxos mais recentes são recuperados. Para exibir esses fluxos, clique em **Fluxos recentes do IBM QRadar**.



Por padrão, um número máximo de 100 fluxos é exibido. Você pode modificar esta configuração padrão no IBM QRadar definições de configuração de integração.

Nota:
A imagem acima mostra os campos de fluxo padrão associados à ofensa. Se você configurou e mapeou algum campo de fluxo personalizado (consulte Mapeamento de campos de infração IBM QRadar para campos de resposta a incidente de segurança), poderá exibi-lo na Exibição de lista clicando no link do ID de fluxo.

Uso do Flow Designer e do Hub de integração com a integração de ingestão de infração do IBM QRadar

Usando a funcionalidade Flow Designer e Hub de integração, vários subfluxos e ações foram criados como parte da integração de ingestão de infração IBM QRadar.

Os seguintes subfluxos IBM QRadar estão disponíveis:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Validação de conexão e credencial: usado no bloco de configuração para validar o host e as credenciais na configuração inicial.
- Recuperação de regras do IBM QRadar: isso é usado na seção Regras da configuração do perfil para recuperar todas as regras ativas em IBM QRadar. Este subfluxo é acionado de forma assíncrona.
- Buscar dados de infrações de amostra do IBM QRadar: isso é usado na seção Mapeamento da configuração do perfil para buscar dados de amostra. Este subfluxo é acionado de forma assíncrona.
- Atualizações de status de infração do IBM QRadar: é acionado por um trabalho programado a cada minuto e atualiza a infração em IBM QRadar quando o incidente de segurança é criado ou encerrado.
- Processar perfis de trabalho programado e infrações de fila: isso é acionado por um trabalho programado a cada minuto para extrair infrações por perfil com base no intervalo de pesquisa. Isso extrai as infrações e as enfileira na tabela de pesquisa para processamento posterior.
- Processar fila de pesquisa e pesquisa em lotes: isso é acionado por um trabalho programado a cada 30 segundos para processar a Fila da tabela de pesquisa.
- Buscar fluxos recentes do IBM QRadar: isso é acionado a partir do link do formulário de incidente de segurança para obter os fluxos de infração mais recentes.
- Buscar eventos recentes do IBM QRadar: isso é acionado a partir do link do formulário de incidente de segurança para obter os eventos de infração mais recentes.

Para exibir esses subfluxos, faça login como um usuário com a função *sn_si.admin* e navegue até **Flow Designer** > **Designer**. Clique no link Nome de qualquer um dos subfluxos listados acima para exibir o subfluxo em detalhes.

Solução de problemas de IBM QRadar integração de ingestão de infração

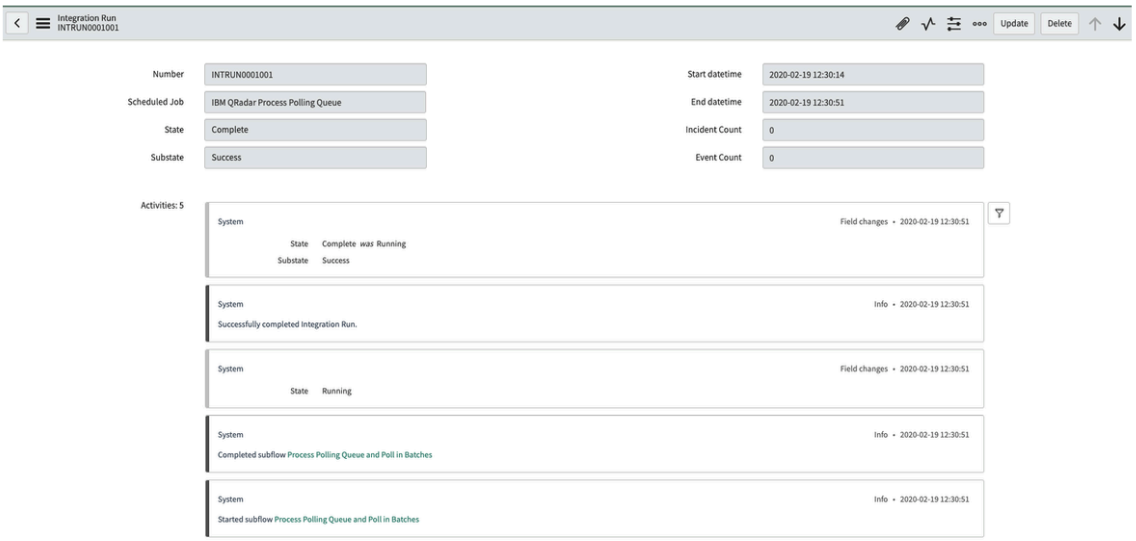
Esta seção aborda dicas importantes de solução de problemas e perguntas frequentes relacionadas à IBM QRadar ingestão de infração.

- Execução de integração: quando um trabalho programado começa a ser executado, um registro de execução de integração com logs, erros e avisos é exibido. O número de infrações extraídas e o número de incidentes criados em uma execução de trabalho programada também são exibidos. Usuários com a função sn_si.analyst podem ver se houve falha na extração de erros/perfis durante a execução da integração.

  As anotações de trabalho na execução de integração fornecem links para os subfluxos executados. Usuários com a função sn_si.analyst podem verificar a tabela sn_event_ingestion_integration_run em busca de erros ocorridos. Para solucionar problemas de integração, você deve primeiro verificar a execução da integração. Os erros são registrados como anotações de trabalho nos registros de execução de integração para cada execução de trabalho programada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- Problemas de SSL: ao se conectar a IBM QRadar instâncias de nuvem, certifique-se de que a instância tenha um certificado de CA válido que não tenha expirado. Você pode importar o RSA ou seus próprios certificados para a plataforma e garantir que o nome comum do certificado corresponda ao nome do host. Consulte https://support.servicenow.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D55ecefd61bf3774cada243f6fe4bcb44 para mais detalhes.
- Perfil incompleto: ao configurar o perfil, na seção Opções adicionais (Automatizar atualizações e fechamento de infração com base no status do incidente no SIR), você deve clicar no botão **Concluir** para garantir que o perfil seja movido para o estado Aguardando, indicando que está aguardando a ingestão.
- Validar perfil: para validar se a integração está funcionando corretamente, verifique os estados do perfil, a data da última extração do perfil, a tabela de importação de infração, a infração para os registros da tabela de tarefas.
- Configuração do MID Server: se você estiver instalando a aplicação IBM QRadar no local, depois de configurar o MID Server, deverá criar uma aplicação do MID Server. O nome da aplicação do MID Server deve ser usado no bloco de configurações de integração em vez do nome do MID Server.

Nota:
O tempo limite padrão do MID Server é de 30 segundos. Para ver instruções sobre como desabilitar o período de tempo limite, consulte <link>. Observe que esta é uma mudança em todo o sistema e pode afetar outras integrações.

- Atualizações de infração: se você habilitou a propriedade `sn_sec_qradar.get_offense_updates` e notou um atraso na criação de incidentes de segurança, desabilite a propriedade. Não habilite esta propriedade quando o intervalo de pesquisa for baixo e a carga de infrações no QRadar for alta, pois isso aumenta a carga da fila.
- Evento, dados de fluxo, remote_ip ou dados de usuários ausentes em um incidente de segurança: se você observar que os dados de evento, dados de fluxo, remote_ip ou usuários estão ausentes em um incidente de segurança, aumente o tempo limite (segundos) do parâmetro `sn_sec_qradar.sid_ttl`. Aumentar a duração atrasa a criação do incidente de segurança até que os AQLs concluam a análise de cada infração.
- Tempos limites: se você exibir erros de tempo limite nos logs da aplicação, revise e modifique as seguintes ações do Flow Designer:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ações do Flow Designer

Parâmetros	Ação
Buscar exemplos de infrações var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 60000);	Revise e atualize a duração em milissegundos.
Buscar exemplos de infrações var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs);	Adicione um parâmetro para `executeAction` e insira a duração em milissegundos.
Buscar infrações para registros de perfil e fila na tabela de pesquisa var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 180000);	Revise e atualize a duração em milissegundos.
Wrapper para testar conexão REST var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.test_connection_rest', rest_inputs);	Adicione um parâmetro para `executeAction` e insira a duração em milissegundos.
Wrapper para validar credenciais de API REST var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.validate_credentials_rest', rest_inputs);	Adicione um parâmetro para `executeAction` e insira a duração em milissegundos.
Etapa REST para atualizações do IBM QRadar Offense var result = sn_fd.FlowAPI.executeAction('sn_sec_qradar.'+restStep, inputs,60000);	Revise e atualize a duração em milissegundos.

IBM QRadar - Integração de aprimoramento de incidente

A integração IBM QRadar - Incident Enrichment pesquisa seus logs e adiciona informações de vista relevantes aos seus incidentes de segurança.

Explorar	Configurar
Integrações do Security Incident Response	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Introdução ao IBM QRadar - Incident Enrichment integration
- Criar registros de configuração de pesquisa de vistas

Usar

- Executar uma pesquisa de vistas
- Integração do Security Operations - Fluxo de trabalho de pesquisa de detecções
- Security Operations - Fluxo de trabalho de pesquisa de detecções do QRadar
- Exibir detalhes da pesquisa de detecções
- Exibir Resultados da Pesquisa de Vistas

Desenvolver

- ServiceNow Security Operations diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Faça ou responda perguntas na comunidade do Security Operations
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Introdução ao IBM QRadar - Incident Enrichment integration

IBM QRadar é um produto de gestão de eventos e informações de segurança empresarial (SIEM) que se integra facilmente com Security Operations. Antes de usar a integração IBM QRadar - Incident Enrichment, você deve baixá-la do ServiceNow Store e adicionar o URL Base de API e a Chave de API apropriados.

Antes de Iniciar

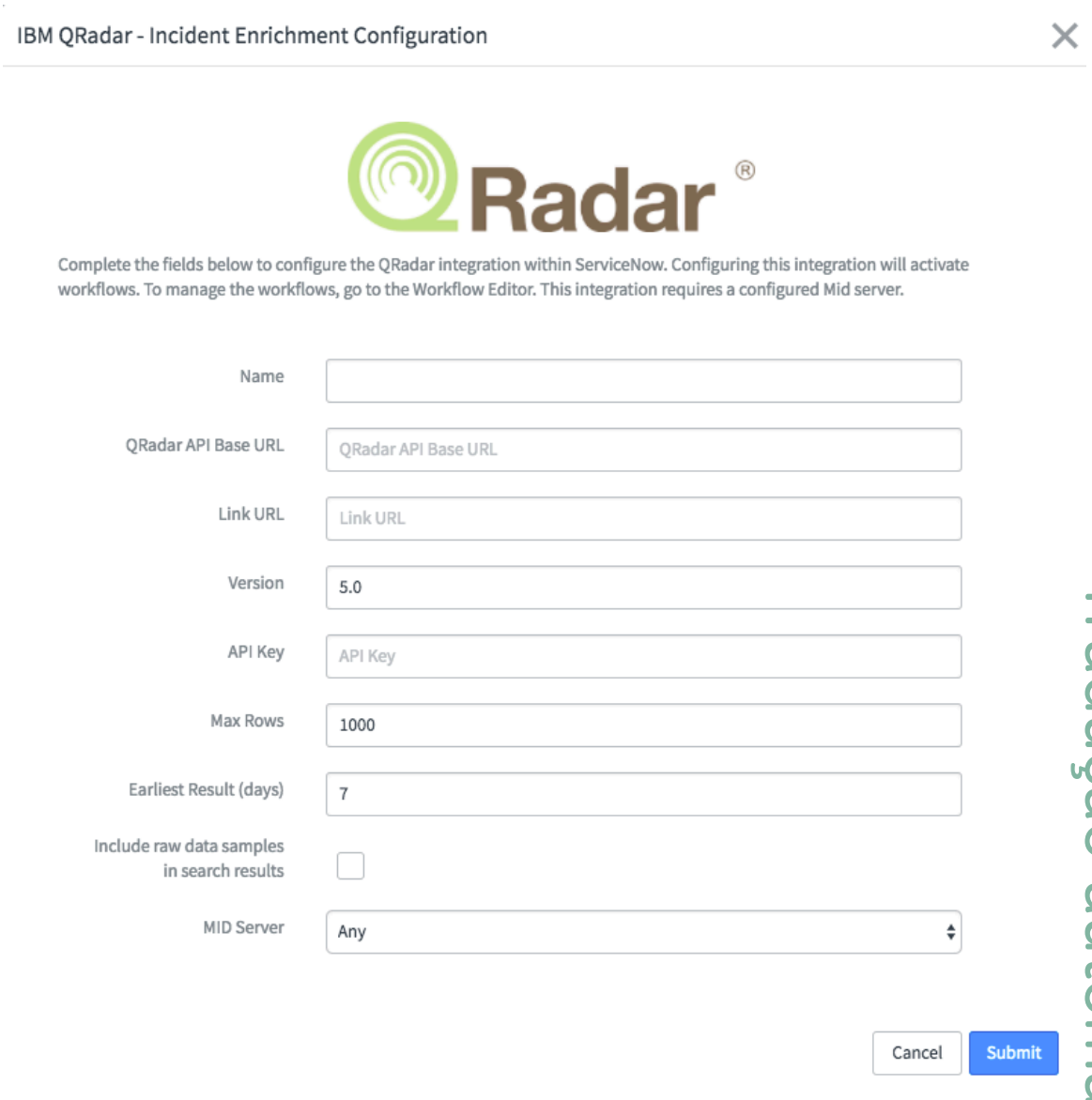
Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse IBM QRadar e obtenha o URL Base da API e a Chave de API no seu perfil IBM QRadar.
3. Em sua instância, navegue até **Security Operations** > **Integrações** > **Configurações de Integração**. As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão IBM QRadar - Aprimoramento de incidente, clique em **Novo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
URL de Base de API do QRadar	O URL base que você adquiriu no site IBM QRadar.
URL do Link	[Opcional] A URL do link que vincula a uma instância IBM QRadar, quando disponível.
Versão	A versão IBM QRadar ; 5.0 é o padrão.
Chave de API	A chave de API que você obteve do site IBM QRadar.
Máx. de Linhas	O número máximo de linhas que você deseja pesquisar.
Resultado Mais Antigo (dias)	Os resultados mais antigos que você deseja ver em número de dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados da pesquisa de detecções. A quantidade de dados retornados depende da configuração na propriedade do **número de linhas de dados brutos** nas propriedades do Security Incident Response.
MID Server	Selecione **Qualquer** para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota:
Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho.

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
8. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Visão geral do LogRhythm

A flexibilidade de mapeamento desta integração fornece a um analista visibilidade de eventos e dados de alarme relacionados que podem ser integrados a Now Platform incidentes de segurança para investigação e correção adicionais.

Perfis de alarme são criados em sua instância Now Platform para personalizar como diferentes LogRhythm campos de alarme são exibidos em um incidente de segurança Now Platform. É fornecido um mapeamento padrão de campos de alarme, que pode ser editado para atender às necessidades específicas do cliente.

A figura a seguir é um exemplo de um ambiente de cliente. Quando um evento aciona a criação de um incidente de segurança na instância Now Platform®, uma solicitação é enviada da instância Now Platform® para extrair alarmes do console do cliente LogRhythm por meio de um MID Server ou mesmo sem ele.

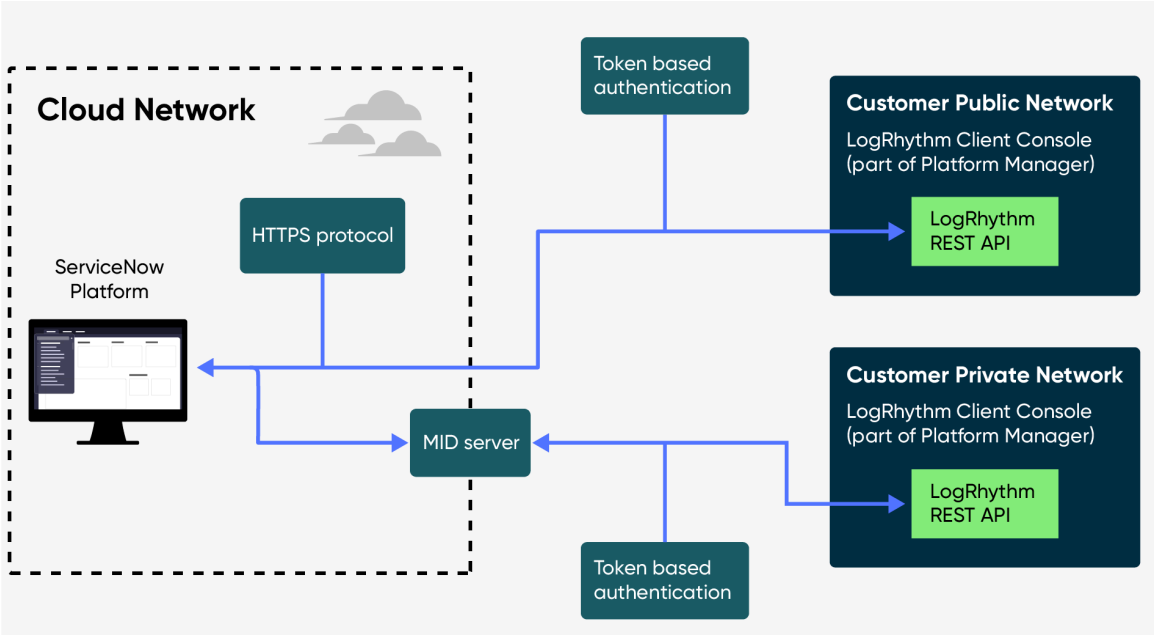
A chave de REST API é usada pelo Now Platform® para autenticar com o LogRhythm Console do cliente. Esta conexão permite que sua instância Now Platform extraia alarmes LogRhythm individuais com base em perfis configurados.

A REST API é usada para coletar detalhes da mensagem não acessados pela REST API.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

LogRhythm integration



Principais recursos

Esta integração inclui os seguintes recursos principais:

- Flexibilidade para criar vários perfis de alarme para diferentes tipos de alarme, como Phishing e Malware.
- Mapeamento de arrastar e soltar de valores de campo de alarme LogRhythm] para campos de incidente de segurança SIR associados.
- Uma visualização do layout de incidente de segurança SIR com base em LogRhythm alarmes de amostra.
- Inclua alarmes históricos, bem como alarmes futuros em andamento em intervalos configuráveis.
- Automatizado LogRhythm fechamento do alarme após SIR fechamento do incidente. Um URL para o incidente SIR, bem como um ID de incidente, é fornecido para fácil referência.

Versões compatíveis do Now Platform

Esta integração é compatível com o Quebec ou versões posteriores do Now Platform®.

Versões compatíveis de LogRhythm

Esta integração é compatível com LogRhythm 7.8 ou posterior. As versões anteriores não são compatíveis devido a limitações de API.

Nota:
Os tópicos a seguir são numerados. Para uma instalação sem problemas e para ajudá-lo a verificar os resultados esperados, siga os tópicos na ordem em que são apresentados.

Configurar a REST API para LogRhythm

Você usa a chave de REST API LogRhythm para coletar detalhes adicionais do evento para campos de alarme individuais. A chave de API fornece detalhes que não estão disponíveis usando a REST API LogRhythm.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

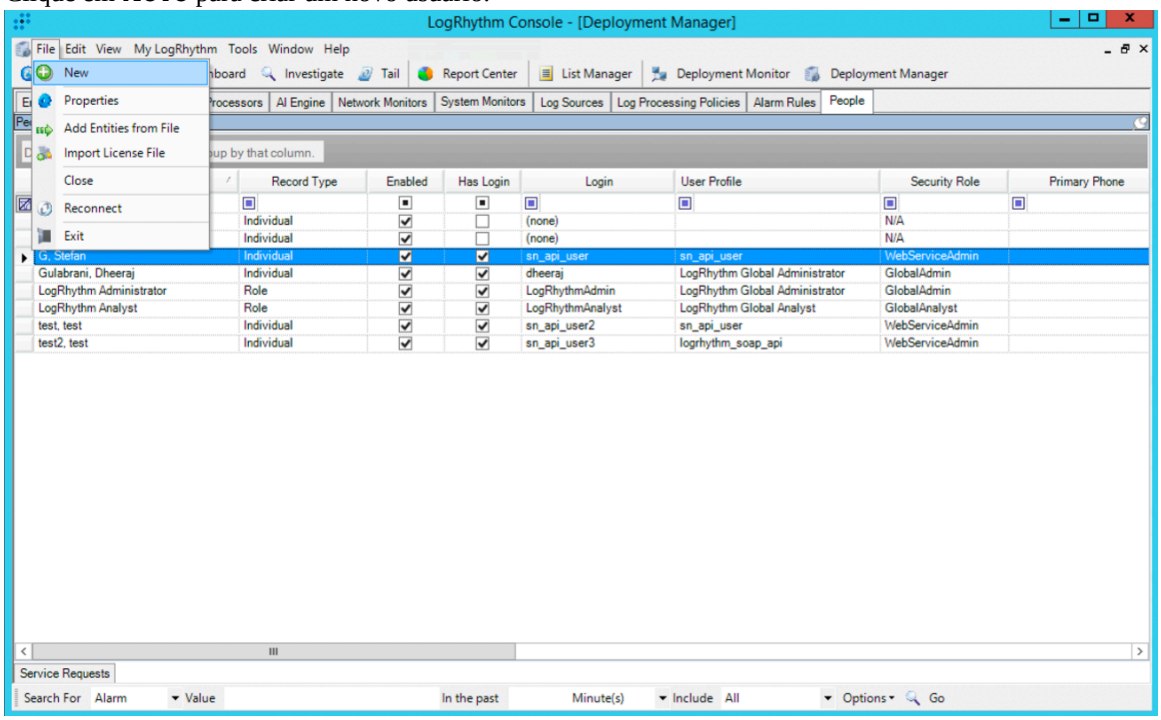
Função necessária: LogRhythm Administrador do Console de cliente/Gerenciador de plataforma

Por Que e Quando Desempenhar Esta Tarefa

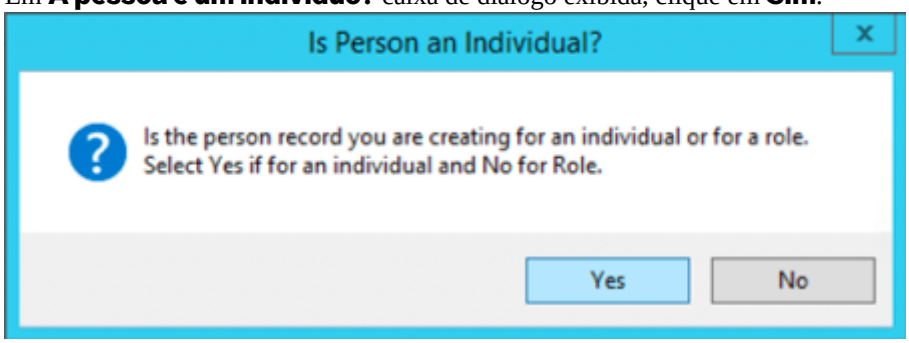
Esta tarefa é realizada no LogRhythm Console do cliente. Configure a LogRhythm REST API antes de instalar o plug-in do ServiceNow Store.

Procedimento

1. Navegue até o LogRhythm Console do cliente e selecione o menu **Arquivo**.
2. Clique em **Novo** para criar um novo usuário.



3. Em **A pessoa é um indivíduo?** caixa de diálogo exibida, clique em **Sim**.

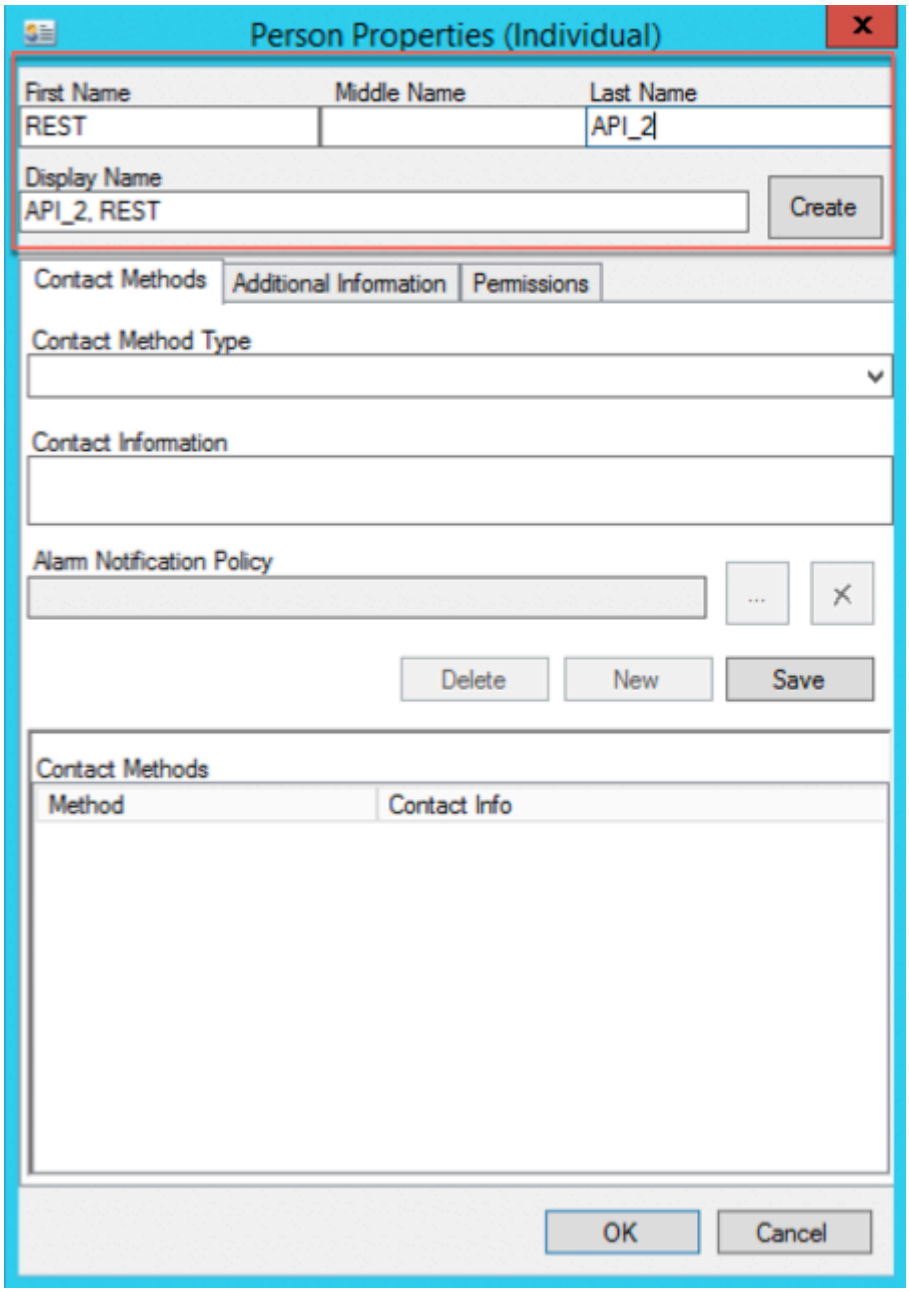


4. Na caixa de diálogo Propriedades da pessoa exibida, preencha os campos Nome.

   Use um nome diferente para a LogRhythm REST API do que você usou para criar a REST API, por exemplo, REST API_2.

Tradução automática

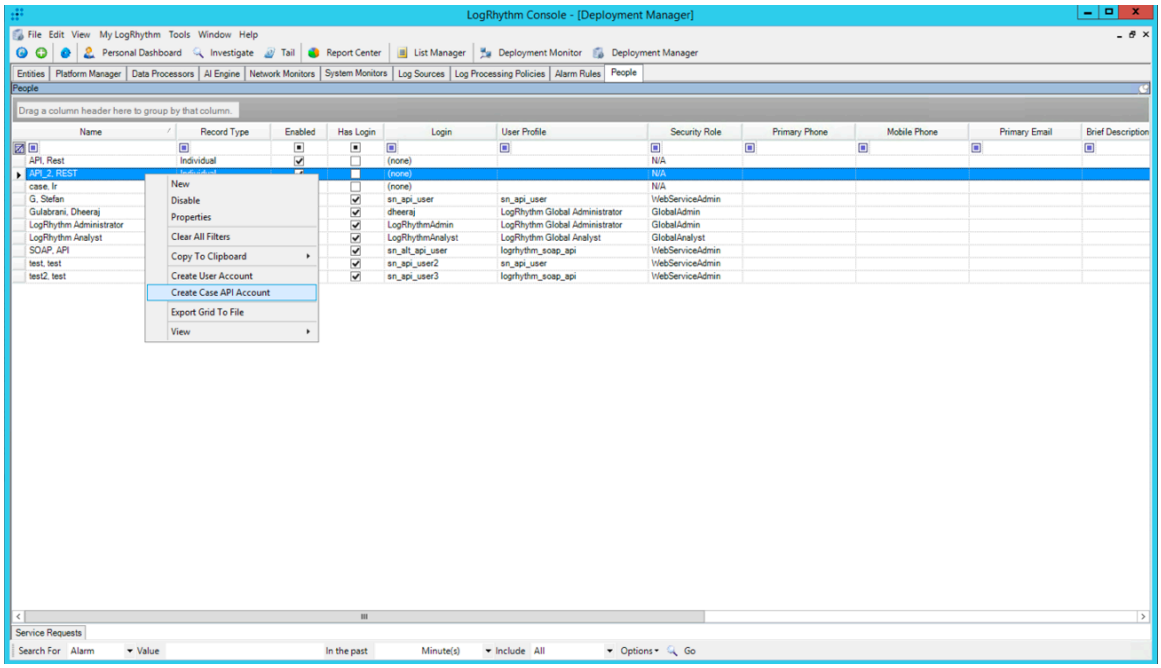
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **OK**.
6. Clique com o botão direito do mouse na nova listagem na coluna Nome (**API_2_REST**) e, na lista de seleção, selecione **Criar conta de API do caso**.

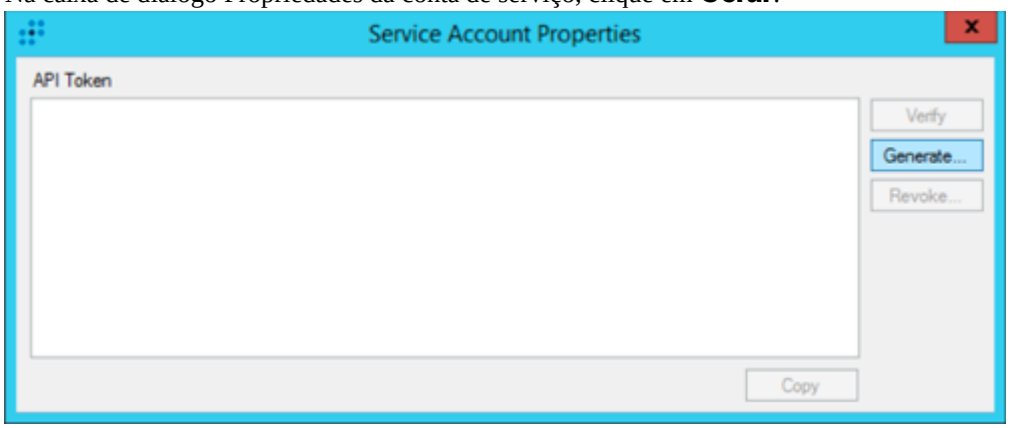
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

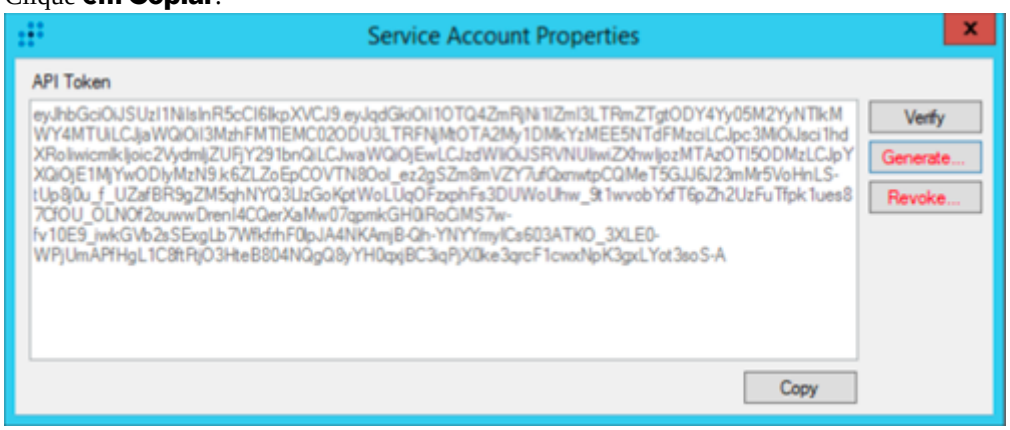


Nota:
A API do caso não é usada, mas as credenciais para a Conta da API do caso e a REST API LogRhythm são as mesmas.

7. Na caixa de diálogo Propriedades da conta de serviço, clique em **Gerar**.



8. Clique **em Copiar**.



Você configurou a REST API LogRhythm. Cole a cadeia de caracteres copiada na etapa anterior na instância Now Platform no campo LogRhythm Token de REST API durante as etapas de configuração listadas em Instalar o plug-in e configurar LogRhythm.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Agora você está pronto para Instalar o plug-in e configurar LogRhythm.

Instalar o plug-in e configurar LogRhythm

Antes de executar a integração na sua instância, conclua as etapas de instalação e configuração para que a aplicação se integre corretamente com Security Operations no Now Platform®.

Antes de Iniciar

Função necessária: administrador

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas. A versão LogRhythm mais recente é 7.8 ou posterior.

Nota:
Seus perfis de alarme existentes não serão mais compatíveis com a versão LogRhythm mais recente, portanto, você precisa criar novos perfis de alarme e executar as configurações necessárias.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform® e Security Incident Response (SIR) necessárias.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador do sistema (admin) instala o plug-in da aplicação e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O (sn_si.admin) supervisiona as seguintes tarefas: ◦ Nomeia, cria e edita perfis de alarme. ◦ Mapeia e filtra alarmes: identifica alarmes LogRhythm específicos que criam incidentes de segurança e configura como esses campos de alarme são mapeados para um incidente de segurança Now Platform®. ◦ Visualiza os detalhes do incidente de segurança para precisão antes de finalizar a configuração. ◦ Ingere alarmes históricos e programa alarmes extraídos. ◦ Atribui a função de analista de incidente de segurança (sn_si.analyst). ◦ Esta função também tem acesso ao módulo Security Operations. • O analista de incidentes de segurança (sn_si.analyst) responde a incidentes de segurança que são criados com base nas configurações de perfil de alarme.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
Obtenha um nome de usuário e senha da API LogRhythm e verifique se você está usando a versão LogRhythm 7.8 ou posterior.	Visite o site do produto para obter informações sobre chaves de API e para criar uma conta: Site do LogRhythm Enterprise . As contas de usuário, credenciais e certificados devem ser configuradas corretamente antes de instalar a aplicação. A integração requer LogRhythm versão 7.8 ou posterior e as LogRhythm REST APIs. Consulte Configurar a REST API para LogRhythm.
Verifique se você instalou e configurou um MID Server.	Um MID Server é necessário em seu ambiente Now Platform. Consulte o site de documentação do produto da ServiceNow para obter informações sobre como instalar e configurar MID Servers.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Para a versão Rome e versões posteriores da família, o plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras aplicações Security Operations necessárias para a integração. Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Orquestração de suporte de segurança Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

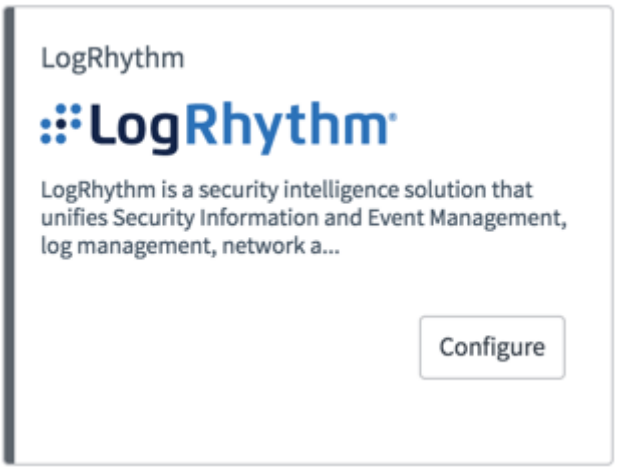
Importante:
Se você tiver problemas de conectividade com o console do cliente LogRhythm, consulte o Verificar conectividade para LogRhythm.

Tradução automática

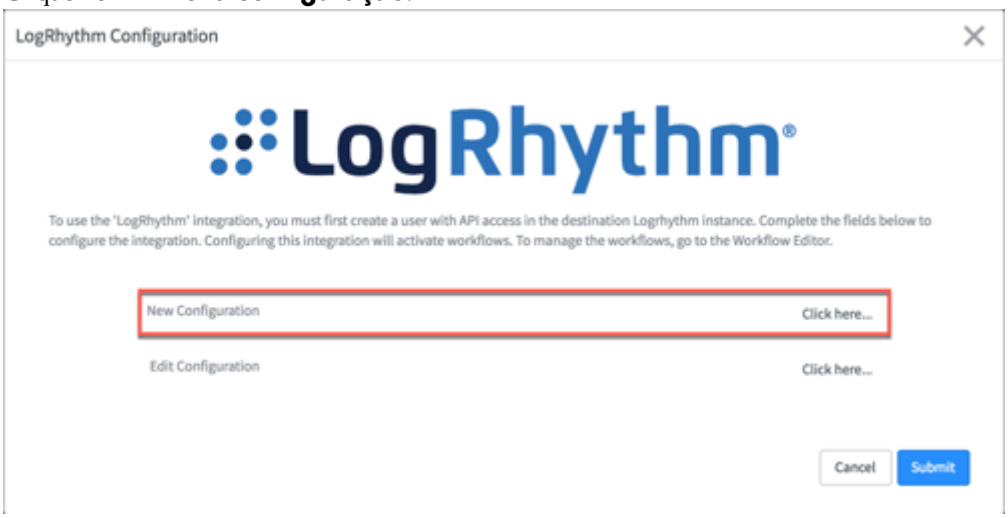
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se você não instalou a aplicação para a integração, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.
2. Quando a instalação for concluída, navegue até **Integrações** > **Configurações de integrações** e localize o bloco LogRhythm.
3. Clique em **Configurar**.



4. Clique no link **Nova configuração**.



5. No formulário, preencha os campos:

Configuração do LogRhythm

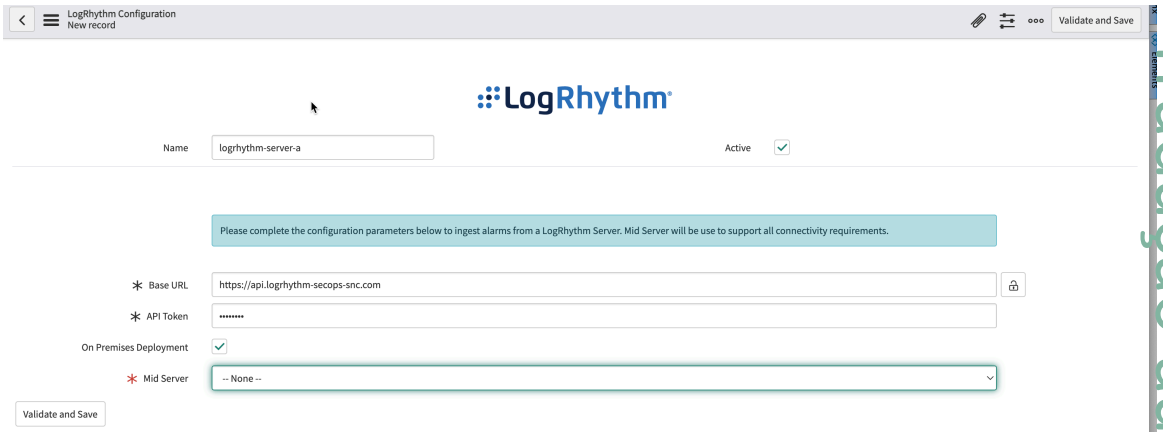
Campo	Descrição
Nome	LogRhythm nome do servidor, por exemplo, logrhythm-server-a.
URL base	URL base que hospeda a REST API LogRhythm. O MID Server permite o acesso à rede onde o console do cliente LogRhythm está hospedado. Este URL é onde o servidor LogRhythm está hospedado nessa rede. Clique no ícone de cadeado na extremidade

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	direita para editar o campo e inserir o texto de um URL, por exemplo, https://logrhythm.secops-eng.com:8501/.
Token de API	Insira o token que está associado à REST API que você criou no LogRhythm Console do cliente.
Implantação no local	Opção para selecionar se for uma implantação no local LogRhythm.
MID Server	MID Server específico que está configurado em seu ambiente. Somente os MID Servers que estão ativos e foram validados estão disponíveis nesta lista de seleção.

A figura a seguir é um exemplo de um formulário preenchido.



6. Clique **em Validar e salvar**.
   Depois que a validação for concluída com sucesso, uma mensagem será exibida e a página Configurações LogRhythm será recarregada. A próxima etapa é criar um perfil de alarme.

O que Fazer Depois

Depois de concluir com sucesso a validação, a próxima etapa é Como criar um perfil de alarme para LogRhythm.

Como criar um perfil de alarme para LogRhythm

Em um perfil de alarme que você cria e nomeia, você especifica quais alarmes deseja extrair do LogRhythm Console do cliente. Você também define como eles são mapeados para campos em um incidente de segurança Now Platform.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Com base no perfil de alarme configurado, um perfil de alarme pode ingerir todos os tipos de alarmes prontos para uso, mas você pode usar critérios de filtro para ingerir tipos específicos de alarmes. Usando esta integração Now Platform, todas as regras de alarme configuradas ou específicas com base no perfil criado são ingeridas. Regras de alarme, como somente alarmes de nível de alto risco, podem ser filtradas para especificar quais alarmes devem criar incidentes de segurança. Antes que os incidentes de segurança sejam criados, os valores de campos individuais nos alarmes filtrados são mapeados para os

Tradução automática

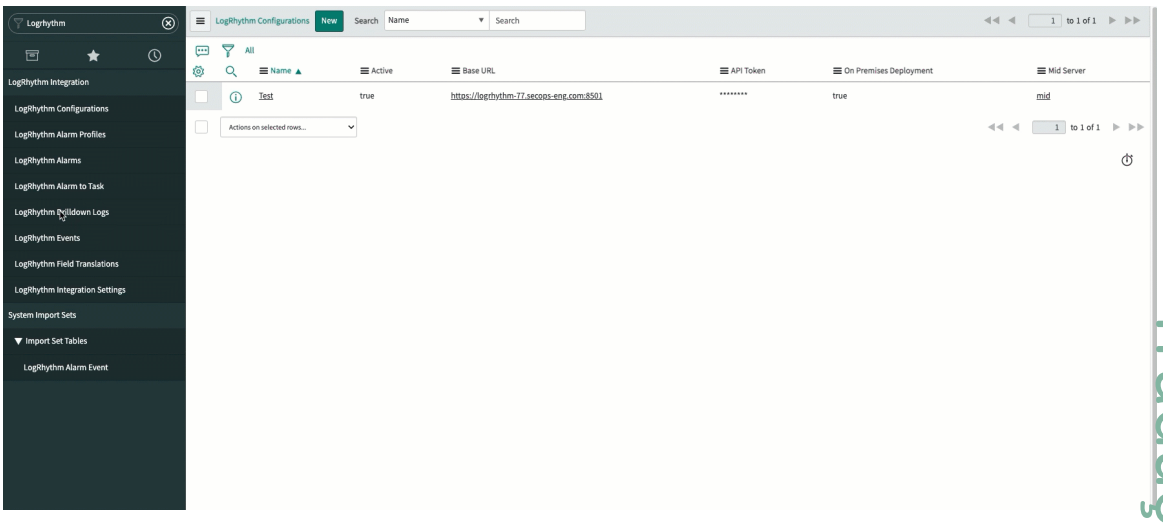
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

campos correspondentes no incidente de segurança Now Platform. Esta configuração é feita por meio de um perfil de alarme na sua instância Now Platform.

Procedimento

1. Navegar até **Todos** > **LogRhythm Integration**.
2. Selecione o módulo **Perfis de alarme do LogRhythm** para exibir a lista de **Perfis de alarme**.

Perfil do Alarme



3. Para criar um novo perfil de alarme, clique em **Novo**.
   Um novo formulário de perfil de alarme é exibido. Na parte superior da página, na barra de andamento, a opção **Nome** está selecionada. Essa barra rastreia seu andamento durante a configuração.
4. No formulário, preencha os campos.

Perfil do Alarme

Campo	Descrição
Nome	Nome do perfil de alarme. Este nome ajuda a identificar os tipos de alarme, como *acesso não autorizado* (*VPN*), *malware*ou *phishing*.
Descrição resumida	Texto curto para informações adicionais sobre o perfil de alarme, que pode incluir o tipo de alarmes ou uma categoria de alarme. Uma descrição de exemplo: todos os alarmes associados a tentativas de acesso não autorizadas ao PowerShell e Sudo.
Origem	Servidor de origem na lista de seleção. A lista consiste em LogRhythm configurações que você já definiu, por exemplo, logrhythm-server-a. Consulte Instalar o plug-in e configurar LogRhythm.
Ordem	Prioridade de perfil de alarme. Este campo indica a ordem na qual os perfis de alarme são executados quando dois ou mais perfis de alarme compartilham as condições de acionamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Por padrão, esta opção não está selecionada. Depois de concluir todas as etapas de configuração do perfil de alarme e clicar em **Concluir**, você será solicitado a marcar esta caixa de seleção para ativar o perfil de alarme. Quando o perfil de alarme está ativo, ele extrai alarmes do LogRhythm Console do cliente automaticamente.

5. Clique em **Continuar** para salvar seus dados e prosseguir para o formulário de mapeamento.

   Se a validação for bem-sucedida, a página será recarregada e o formulário de **mapeamento** será exibido. Você não pode prosseguir com a configuração até ter validado com sucesso sua conexão e credenciais.

Tópicos relacionados

Mapeamento de LogRhythm alarmes para o incidente de segurança

Mapeamento de LogRhythm alarmes para o incidente de segurança

Depois de selecionar a origem LogRhythm que você deseja ingerir, é necessário mapear campos de alarme LogRhythm individuais para os campos de incidente de segurança Now Platform.

O mapeamento de alarmes inclui as seguintes tarefas:

- Mapear LogRhythm alarmes. Para esta tarefa, você lista e ingere (Pull) alarmes de amostra usando os IDs de alarme ou os alarmes mais recentes do console do cliente LogRhythm.
- Os campos de Alarme de amostra são categorizados em três grupos:
  - Campos dealarme: os campos de alarme disponíveis e seus valores correspondentes são exibidos.
  - Campos de evento: os campos de evento disponíveis e seus valores correspondentes são exibidos.
  - Campos DrillDownLog: os campos de log de detalhamento que estão disponíveis e seus valores correspondentes são exibidos.
- Cada ID de alarme que você extraiu é exibido como uma guia. Nas guias ID do alarme, verifique se todos os campos de alarme críticos da seção Ingestão de amostra de alarme à esquerda do formulário estão mapeados para a seção Mapeamento de campo de incidente SIR à direita do formulário.
- Depois de mapear os alarmes para o campo Mapeamento de campo de incidente SIR, você pode ver a categoria de alarme também sendo exibida no campo Expressão de entrada. Por exemplo, `${Alarm: alarmid}$`.
- Você pode modificar a configuração adicionando ou removendo campos no incidente de segurança. Rastreie campos ignorados ou duplicados com a codificação de cores fornecida.
- Você pode filtrar alarmes para especificar quais alarmes são incluídos na aplicação SIR. Você pode filtrar os alarmes diretamente ou usar as categorias de alarme para expandir sua pesquisa com base em Alarmes, Eventos ou DrillDownLogs.
- Use o editor de script se quiser formatar valores para os campos Prioridade e Categoria no incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O próximo passo é Mapear campos de alarme LogRhythm para campos de incidente de segurança.

Tópicos relacionados

- Mapear campos de alarme LogRhythm para campos de incidente de segurança
- Use o editor de script para formatar valores LogRhythm
- Filtrar alarmes para LogRhythm

Mapear campos de alarme LogRhythm para campos de incidente de segurança

Você mapeia campos de alarme individuais para os campos de incidente de segurança. O mapeamento pré-configurado pode ser editado e a codificação de cores fornecida para os campos ajuda a monitorar os alarmes já mapeados. Esta etapa ajuda a visualizar como suas edições afetam os campos no incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Se você não estiver familiarizado com os alarmes LogRhythm, navegue até o Console do cliente LogRhythm e revise alguns exemplos de IDs de alarme. Para o exemplo a seguir, os alarmes LogRhythm9468 e 9474 foram usados para mapear os alarmes para o incidente de segurança.

Por Que e Quando Desempenhar Esta Tarefa

Usando este formulário, você mapeia as regras de alarme LogRhythm à esquerda para os campos de incidente de segurança à direita.

A figura a seguir mostra o mapeamento padrão de alarmes pré-configurados para cada perfil de alarme. Este mapeamento padrão pode ser editado e, com este formulário, você personaliza os campos que preenchem o incidente de segurança. Depois de concluir este mapeamento, você poderá ver como a adição ou a remoção de campos de alarme pode afetar os valores de campo no incidente de segurança.

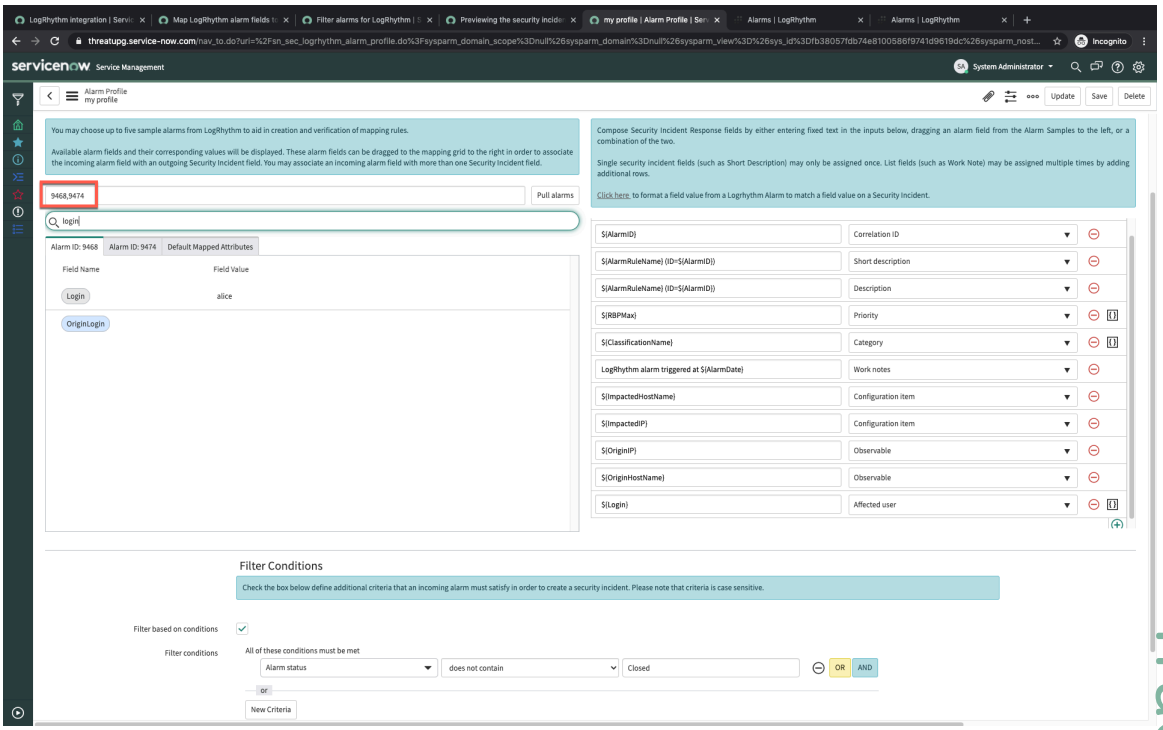
No lado esquerdo deste formulário na figura a seguir, as regras de alarme LogRhythm estão descritas. Os valores dessas regras de alarme são mapeados para os campos de incidente de segurança no lado direito do formulário.

Procedimento

1. Depois de criar um perfil de alarme para o LogRhythm, clique em **Mapeamento** na barra de andamento.
2. No campo **Ingestão de amostra de alarme**, insira até cinco amostras de IDs de alarme LogRhythm separadas por vírgulas (9468,9474).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Ao lado do campo de alarme, clique em **Extrair alarmes**.

   A extração de alarmes de amostra pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela.

   Depois que os IDs de alarme de amostra são enviados e extraídos com sucesso do servidor LogRhythm, os campos de alarme e seus valores correspondentes são exibidos em guias.

   Nota:
   Depois que um ID de alarme é extraído com sucesso, o Now Platform pode retornar a seguinte mensagem: Os seguintes novos campos estarão disponíveis para filtragem em breve. Recarregue este perfil em alguns minutos se a filtragem com base nesses campos for necessária. itenspacotesem, itenspacotesfora.

   Esta mensagem ocorre quando o único alarme que foi extraído contém nomes de campo não processados anteriormente pelo Now Platform. Esses campos estão disponíveis para mapeamento, no entanto, se esta mensagem for exibida, recarregue o formulário para que esses campos sejam exibidos e disponíveis nas listas de seleção de filtro do construtor de condições quando estiver pronto para definir condições de filtragem.

A ingestão desses alarmes de amostra na configuração do perfil de alarme ajuda a impedir o mapeamento de campos de alarme para o incidente de segurança que não contêm valores. Ele também alinha os campos de alarme com valores para os campos apropriados no incidente de segurança. Esta etapa garante que todos os campos de alarme críticos sejam mapeados e que não haja valores de campo ausentes no incidente de segurança.

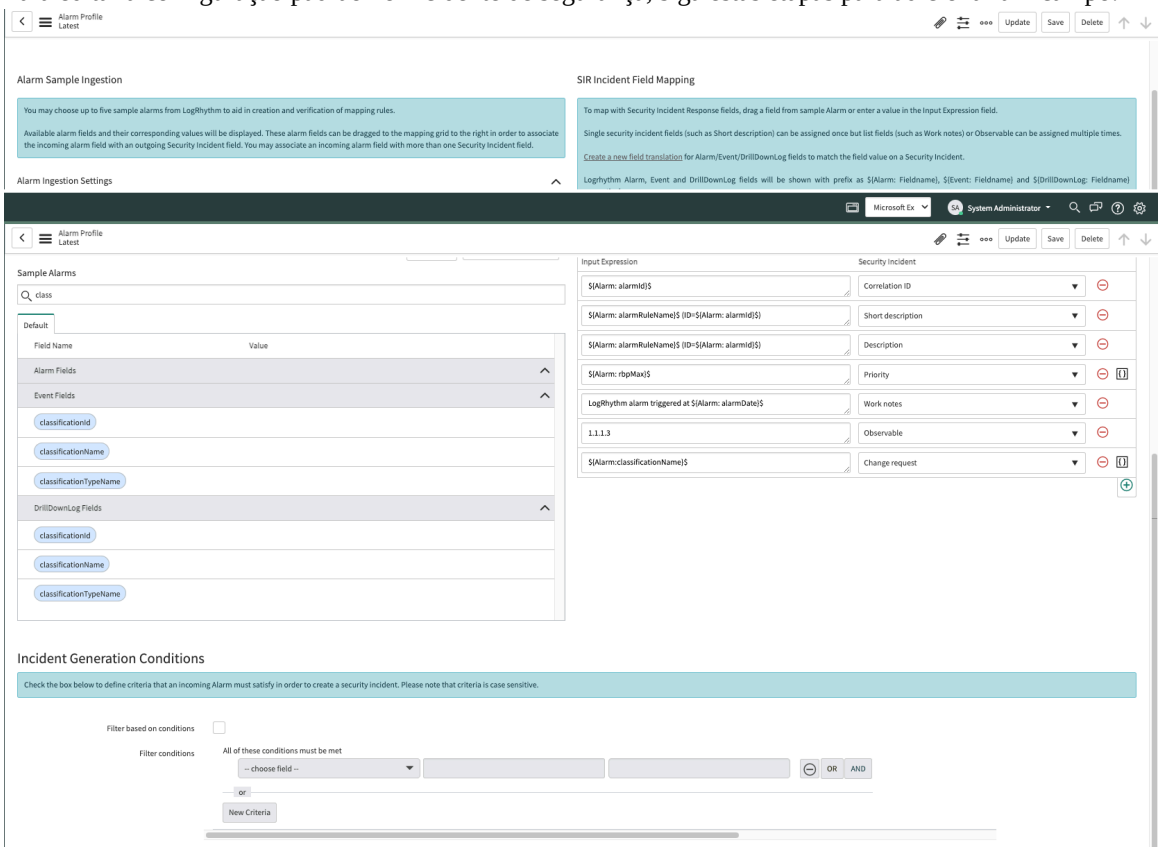
Para ajudar a garantir que nenhum alarme seja ignorado ou duplicado no processo de mapeamento, os campos de alarme são codificados por cores. Um campo de alarme azul claro (Account, AlarmRuleID, AlarmStatusetc.) indica que um campo ainda não foi selecionado para mapeamento para um incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um campo cinza (AlarmDate, AlarmIDe AlarmRuleName) indica que um campo já foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação de cores ajuda a rastrear o mapeamento porque, em determinados casos, um campo de alarme pode ser mapeado para mais de um campo em um incidente de segurança. Por exemplo, os campos Observáveis e Anotação de trabalho podem ter mais de um valor.

4. Para limpar os dados de alarme de amostra, clique em **Limpar dados de alarme de amostra**.
5. Para editar a configuração padrão no incidente de segurança, siga estas etapas para adicionar um campo:



a. No canto inferior direito do formulário, clique no ícone de adição.
Um novo campo é exibido.

b. Na coluna Incidente de segurança, selecione um campo disponível na lista de seleção.

Na lista de seleção expandida, alguns dos campos estão sombreados. Por exemplo, a Categoria tem um plano de fundo cinza, o que indica que ela foi mapeada no incidente de segurança. Semelhante à codificação de cores dos campos de alarme LogRhythm, essa codificação de cores dos campos de incidente de segurança garante que os valores dos campos de alarme não sejam mapeados inadvertidamente para o mesmo campo de incidente de segurança.

Na ilustração acima, a regra de alarme ${Alarm:classificationName}$ já está mapeada para o campo Categoria no incidente de segurança neste perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
O campo Observável pode ser mapeado para mais de campo no mesmo incidente de segurança para que vários observáveis possam ser exibidos. Da mesma forma, os campos Item de configuração e Anotações de trabalho podem ser mapeados para exibir vários valores.

No lado de Ingestão de amostra do alarme do formulário, o azul indica que um campo de regra de alarme não foi mapeado. Cinza indica que foi mapeado. Na lista de seleção no lado Mapeamento de campo de incidente SIR do formulário, branco indica que um campo não foi mapeado. Cinza indica que um campo foi mapeado. Use esta codificação de cores para ajudá-lo a rastrear o mapeamento de campo.

Na ilustração acima, Usuário afetado foi selecionado na lista de seleção como um novo campo no incidente de segurança.

c. Na seção Ingestão de amostra de alarme no lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar o ID do alarme desejado no campo Expressão de entrada.

Na ilustração acima, Login foi selecionado.

d. Arraste-o para o campo limpo e solte-o.
Na coluna esquerda da seção Mapeamento de campo de incidente de SIR, o novo valor do campo Usuário afetado é exibido. Nesse caso, o valor de Login do alarme LogRhythm é exibido no campo Usuário afetado no incidente de segurança.

6. Como alternativa, para inserir manualmente um valor para campos na coluna Expressão de entrada, coloque o cursor no campo de expressão de entrada e insira um valor de alarme desejado.

Por exemplo, na ilustração acima, outro campo foi adicionado (Grupo de atribuição) ao formulário de incidente de segurança, e a atribuição de incidente de segurança foi inserida manualmente no campo.

7. Continue editando o mapeamento pré-configurado conforme necessário.
Se você precisar traduzir valores de campos de alarme LogRhythm para valores compatíveis com os campos no incidente de segurança, poderá usar o editor de script. Consulte Use o editor de script para formatar valores LogRhythm.

O que Fazer Depois
Depois de concluir o mapeamento de campo, a próxima etapa é Filtrar alarmes para LogRhythm.

Filtrar alarmes para LogRhythm

Definir critérios de filtragem para alarmes depois de mapear os campos ajuda a determinar quais alarmes devem ser incluídos na aplicação SIR. Filtrar alarmes ajuda a reduzir significativamente o número de alarmes que você ingere quando o perfil de alarme é ativado.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Use as condições de filtragem na parte inferior do formulário de mapeamento para filtrar alarmes específicos ou limitar a ingestão somente para alarmes que atendam a determinados critérios no nível de campo. A filtragem reduz significativamente o número de alarmes que você ingere depois que o perfil de alarme é ativado. Use a filtragem para incluir uma quantidade gerenciável de alarmes que sua equipe do Security Operations Center (SOC) pode oferecer.

Tradução automática

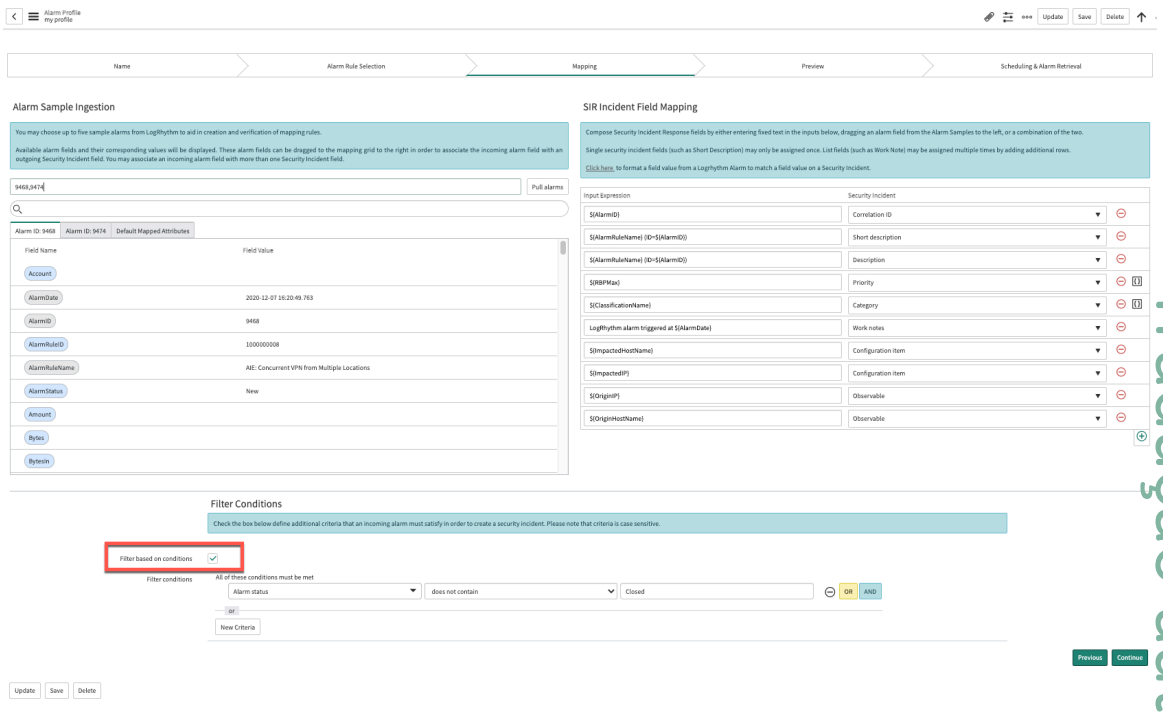
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

O exemplo a seguir mostra uma configuração de filtro padrão na qual Status-does-not-contain-Closed do alarme é a configuração padrão. Este filtro extrai somente alarmes ativos e essa configuração reduz o número de alarmes extraídos. As etapas a seguir ilustram como adicionar outro filtro útil que inclui somente alarmes com os valores de severidade ou prioridade mais altos.

Procedimento

1. Para editar os critérios de filtragem, marque a caixa de seleção **Filtrar com base nas condições**.

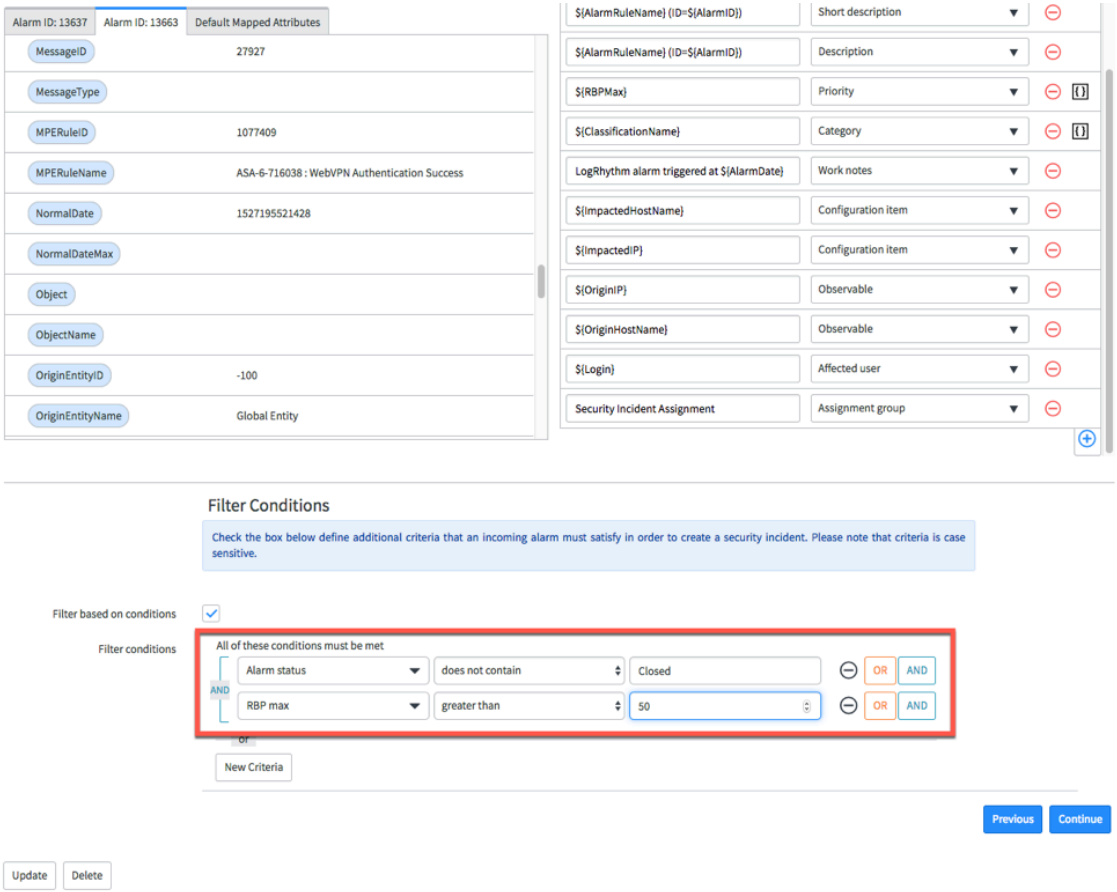


2. À direita do campo **Condições do filtro**, clique em **OU** ou **E.**
3. Na nova linha exibida, selecione as condições de filtragem nas listas de seleção.

   A imagem a seguir mostra um filtro adicional adicionado aos critérios nos quais a prioridade baseada em risco (RBP máx) é maior que 50. Com esta configuração de filtro, somente LogRhythm alarmes com um valor de prioridade baseado em risco maior que 50 são extraídos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Depois de verificar se todos os campos de alarme críticos LogRhythm estão mapeados para o incidente de segurança Now Platform e de definir critérios de filtragem para limitar a ingestão de alarmes, escolha um para continuar a configuração.

O que Fazer Depois

A próxima etapa é visualizar os campos mapeados no incidente de segurança. Consulte Visualizando o incidente de segurança com valores de alarme mapeados LogRhythm.

Visualizando o incidente de segurança com valores de alarme mapeados LogRhythm

Depois de concluir a etapa de mapeamento, visualize os valores que você mapeou para os campos no incidente de segurança. Esta etapa de visualização permite que você verifique se mapeou todos os campos de alarme críticos LogRhythm que deseja exibir no incidente de segurança.

Função necessária: sn_si.admin.

Incidente de segurança

Se a visualização do incidente de segurança não for exibida, clique em **Visualizar** na barra de andamento.

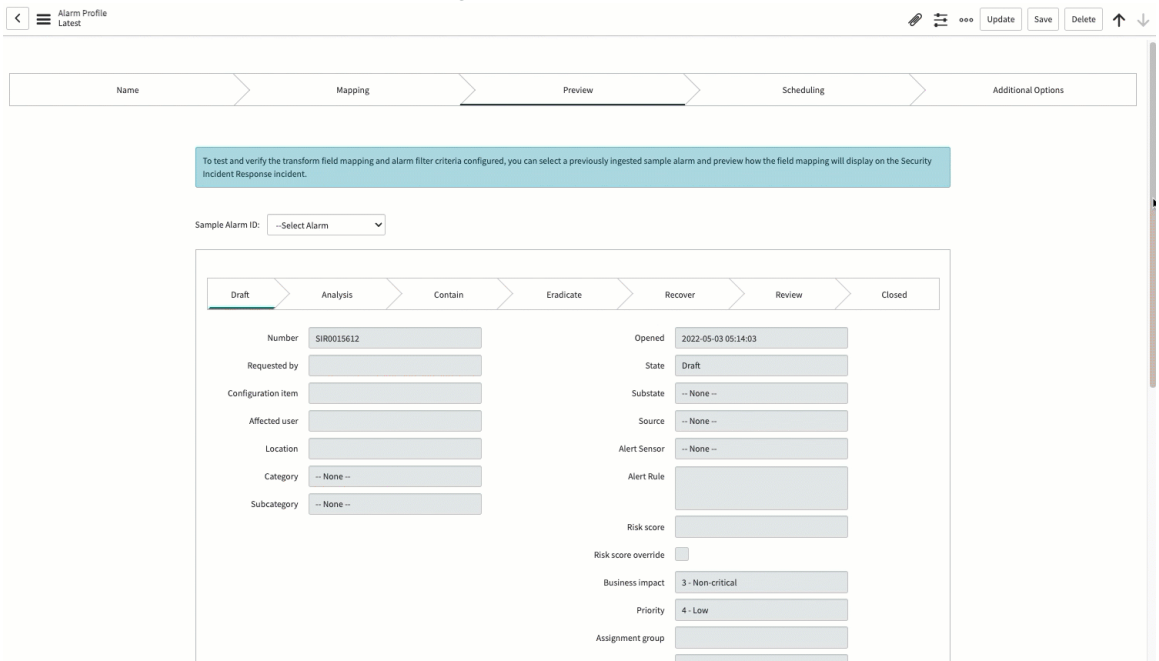
Um exemplo da visualização de todo o incidente de segurança Now Platform é exibido nas duas imagens a seguir. Este exemplo da visualização do incidente de segurança é preenchido com os campos de alarmes LogRhythm mapeados do alarme de amostra 13663.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na figura a seguir, os campos Item de configuração, Usuário afetado, Prioridade, Grupo de atribuiçãoe Descrição resumida do incidente de segurança são preenchidos.

Metade superior do incidente de segurança



Na metade inferior do formulário de incidente de segurança, o campo Descrição é preenchido. Na seção Itens relacionados, os campos Item de configuração, Observável e Anotação de trabalho são preenchidos com valores. Se vários valores para esses campos forem mapeados, cada valor será exibido no incidente de segurança, porque cada um desses campos pode aceitar mais de um valor.

Condições de erro na visualização

As mensagens de aviso a seguir podem ser exibidas ao visualizar o incidente de segurança. Se um alarme de amostra não for aprovado nos critérios de filtragem, o incidente de segurança inteiro não será preenchido.

Valor de entrada não encontrado

Se o ID do alarme estiver incluído nas condições de filtragem, uma mensagem de aviso ainda poderá ser exibida se não forem encontrados valores de entrada específicos para determinados campos mapeados. Para o exemplo a seguir, na visualização do registro, suponha que não haja nenhum valor no campo Atribuído a, embora ele tenha sido mapeado.

Para este tipo de mensagem, no registro de mapeamento, verifique se o valor de entrada está correto. Nesse caso, a pessoa no campo Atribuído a no incidente de segurança está incorreta na instância Now Platform. Quando este alarme é ingerido e cria um incidente de segurança com esta condição, os campos com este valor de entrada (Abel Tuter) são deixados em branco no incidente de segurança.

As mensagens restantes em azul são informativas e indicam que esses campos não têm valor para exibir na visualização. Esta visualização permite que o administrador de incidentes de segurança configure o perfil de alarme para verificar se esses campos não devem ter valor na fase inicial de criação porque, em determinados casos, os campos de incidentes de segurança podem ser preenchidos automaticamente mais tarde. Outros erros de mapeamento também são exibidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando estiver satisfeito com o mapeamento e a visualização do incidente de segurança, escolha um para continuar a configuração.

Opção	Descrição
Clique em **Continuar** ou **Programação** na barra de andamento.	Avance para o formulário **Programação e recuperação de alarme**. **Programação e recuperação de alarme** é selecionado na barra de andamento. A próxima etapa é programar a recuperação do alarme.
Clique **em Anterior**.	Retorne ao perfil de alarme e continue o mapeamento.
Insira outro ID de alarme na lista de seleção **ID de alarme de amostra** na parte superior do formulário de visualização.	A lista de seleção de **ID de alarme de amostra** é exibida para cada ID de alarme inserido. Você pode selecionar até cinco alarmes. Esta opção permite visualizar outro ID de alarme LogRhythm em um incidente de segurança.

Depois de visualizar o incidente de segurança e ficar satisfeito com os resultados, a próxima etapa é Programar e recuperar LogRhythm alarmes.

Programar e recuperar LogRhythm alarmes

Depois de visualizar o incidente de segurança com os alarmes LogRhythm que você selecionou e mapeou, você está pronto para programar a recuperação do alarme. Depois de concluir esta etapa, o perfil de alarme está pronto para ser ativado.

Antes de Iniciar
Função necessária: sn_si.admin

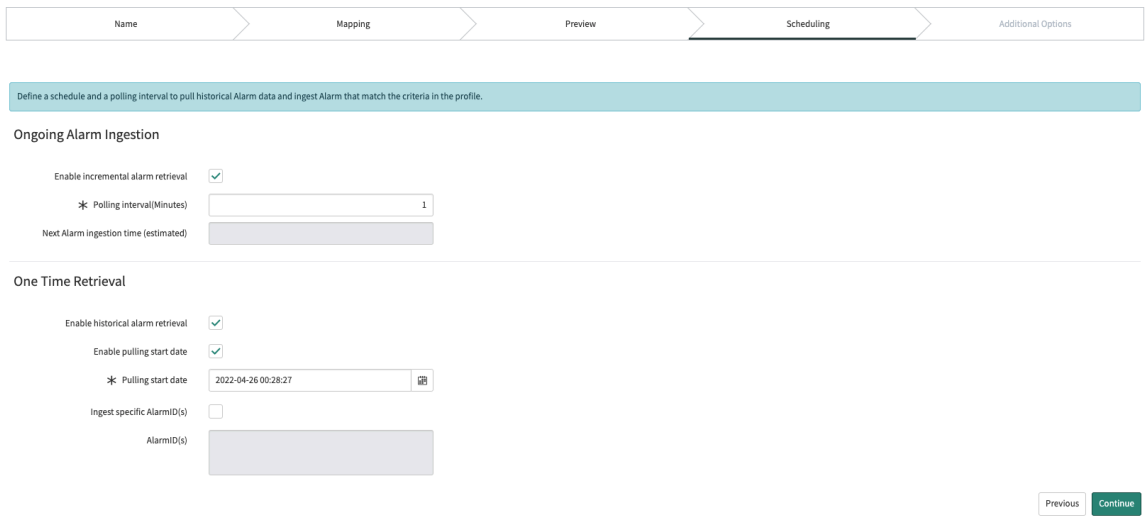
Por Que e Quando Desempenhar Esta Tarefa
A programação permite modificar a programação e os tipos de alarmes selecionados para recuperação. Você filtra os alarmes ingeridos com base em um intervalo de datas ou em IDs de alarme específicos. Com esta etapa, você determina se deseja ingerir alarmes históricos e com que frequência pesquisa alarmes futuros que correspondam à configuração do perfil do alarme.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Clique na etapa **Programação** na barra de andamento.

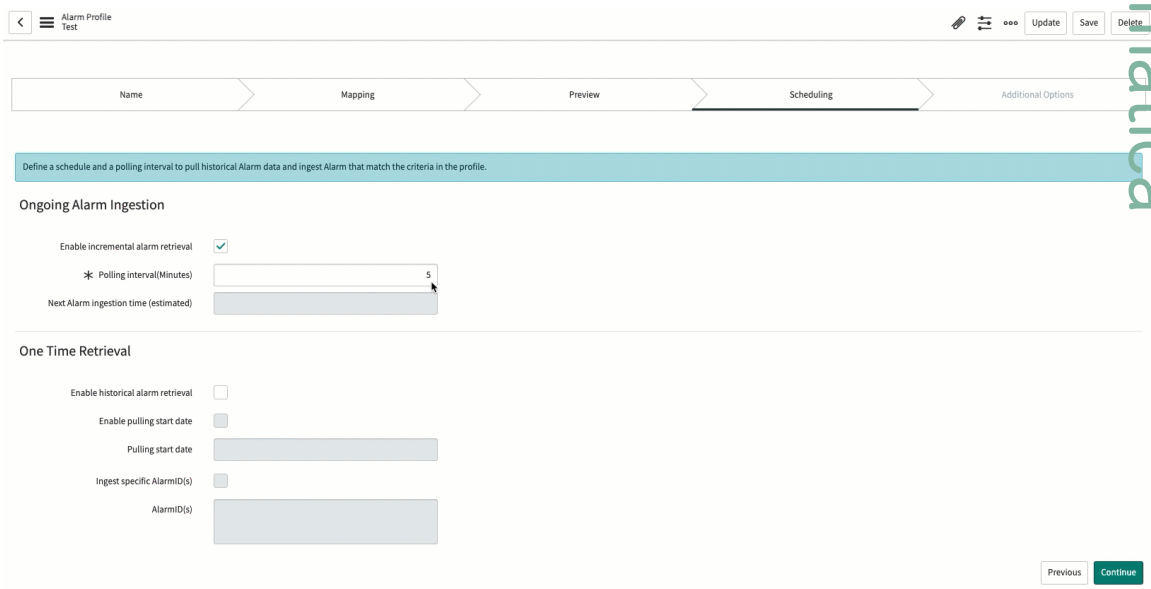


2. Escolha uma das opções a seguir para configurar a recuperação do alarme.

3. Para editar a recuperação de alarmes históricos, siga estas etapas para inserir uma data para a recuperação do alarme ou um ID de alarme específico.

   a. Selecione **Habilitar data**de **início da extração e selecione Data de início da extração**.

   b. No campo **Data de início da extração**, clique no calendário exibido, selecione a data seguida da marca de seleção verde para salvar sua entrada.



   A data é exibida.

   c. Como alternativa, selecione a opção **Ingerir ID(s) de alarme específico(s)** e, no campo **ID(s)** de alarme, insira os IDs de alarme específicos dos dados históricos para recuperar IDs de alarme específicos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode inserir até cinco alarmes separados por vírgulas.

d. Clique em **Atualizar**.

4. Escolha uma das opções a seguir para continuar editando ou concluir a configuração.

O que Fazer Depois
Depois de configurar os detalhes de Ingestão de alarme contínuo e Recuperação única, a próxima etapa é Opções adicionais para LogRhythm alarmes.

Opções adicionais para LogRhythm alarmes

A integração LogRhythm Enterprise fornece a capacidade de atualizar ou fechar automaticamente os alarmes LogRhythm com base nos incidentes de segurança.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Quando você habilita a opção Atualizações iniciais do alarme, os alarmes são atualizados automaticamente nos comentários do LogRhythm com as atualizações do alarme inicial. Da mesma forma, quando você habilita a opção Atualizações de fechamento do alarme, os alarmes são fechados automaticamente no LogRhythm junto com o Código de fechamento SIR e os comentários de fechamento.

O ID do alarme LogRhythm está conectado ao ID do incidente de segurança Now Platform ao longo do ciclo de vida do incidente. Essa correlação permite que ocorra um fechamento simultâneo e automatizado de incidente/alarme de segurança. Quando o registro de incidente de segurança Security Incident Response (SIR) é fechado, há um comentário publicado no alarme no console da Web LogRhythm. Este comentário indica que o alarme foi encerrado com base no fechamento do Now Platform incidente de segurança. O número do incidente e um URL que leva de volta ao incidente de segurança para referência também estão incluídos na seção de comentários no alarme LogRhythm.

Procedimento

1. Clique na etapa **Opções adicionais** na barra de andamento.

2. Para usar a atualização de alarme automatizada para a criação de incidente de SIR, escolha uma das opções a seguir para configurar a recuperação do alarme.

3. Para usar a atualização de alarme automatizada para o fechamento do incidente de SIR, escolha uma das opções a seguir para configurar a recuperação do alarme.

4. Clique em **Concluir** para salvar o perfil de alarme.

Trouble?
Se você não vir anotações indicando que o alarme foi encerrado com sucesso no incidente de segurança, revise as anotações de trabalho para obter mais informações sobre como prosseguir para corrigir o problema. Além disso, verifique a conexão do servidor. Se você confirmar que o incidente de segurança Now Platform foi encerrado e o servidor não expirou, talvez seja necessário fechar manualmente o alarme no LogRhythm Console da web.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações adicionais para a integração LogRhythm

Use as LogRhythm Configurações de integração para modificar o sistema predefinido e as propriedades de solução de problemas de acordo com seus requisitos.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **LogRhythm Integration** > **Configurações do LogRhythm Integration**.
2. Configure as propriedades do sistema de acordo com seus requisitos.
3. No formulário, preencha os campos.

LogRhythm Propriedades do sistema de integração

Campo	Descrição
Isso aplicará o filtro antes que os dados sejam salvos nas tabelas da ServiceNow.	Opção para determinar se você deseja aplicar o filtro antes que os dados sejam armazenados nas tabelas da ServiceNow. Por padrão, o valor é definido como Sim.
O número máximo de incidentes de segurança que pode ser criado em um dia	Opção para definir o número máximo de incidentes de segurança que podem ser criados em um dia. Por padrão, o valor é definido como 2000.
LogRhythm a ingestão periódica pode ter mais de 1.000 alarmes, portanto, a paginação é usada para ingerir os alarmes. Limite por página permitido para buscar o número de alarmes por página.	Opção para definir o número máximo de alarmes a serem recuperados em uma única página. Por padrão, o valor é definido como 100.
Exclua os registros da tabela "Origem para tarefa" mais antigos do que o número especificado de dias.	Opção para excluir registros da tabela Origem para Tarefa quando o número especificado de dias for violado. Por padrão, o valor é definido como 30.

4. Configure as propriedades de solução de problemas de acordo com seus requisitos.
5. No formulário, preencha os campos.

Propriedades de solução de problemas de integração do LogRhythm

Campo	Descrição
Depurar ingestão programada: habilita os logs do sistema no nível de depuração para a ingestão feita pelo trabalho programado. Isso registrará em log todas as mensagens/exceções geradas pela ingestão programada ao extrair alarmes/logs de detalhamento/ eventos de LogRhythm.	Opção para habilitar logs do sistema no nível de depuração para ingestão realizada pelo trabalho programado. Por padrão, o valor é definido como Não.
Depurar mapa de transformação: habilita os logs do sistema no nível de depuração para o mapa de transformação. Isso registrará em log todas as	Opção para habilitar logs do sistema no nível de depuração para o mapa de transformação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
mensagens geradas pelos mapas de transformação ao criar o incidente de segurança da importação de alarme. Isso também habilitou a ação de IU na tabela de importação de alarme para executar novamente o mapa de transformação.	Por padrão, o valor é definido como Não.
Depurar ingestão de amostra no perfil de alarme: isso habilita os logs do sistema no nível de depuração para a ingestão de amostra. Isso registrará em log todas as mensagens geradas enquanto as amostras são ingeridas.	Opção para habilitar logs do sistema no nível de depuração para ingestão de amostra. Por padrão, o valor é definido como Não.
Visualização de depuração no perfil de alarme: isso habilita os logs do sistema no nível de depuração para a visualização de perfil de alarme. Isso registrará em log todas as mensagens geradas enquanto a visualização é renderizada para o alarme de amostra.	Opção para habilitar logs do sistema no nível de depuração para visualização de perfil de alarme. Por padrão, o valor é definido como Não.
Depurar chamadas REST de saída: habilitar esta propriedade permitirá o registro em log de nível de depuração na tabela Logs do sistema para todas as chamadas REST (solicitação e resposta) com ou sem MID Server de LogRhythm.	Opção para habilitar o registro em log de nível de depuração na tabela Logs do sistema para todas as chamadas REST com ou sem MID Server de LogRhythm. Por padrão, o valor é definido como Não.

6. Clique em **Salvar**.

Use o editor de script para formatar valores LogRhythm

Além dos campos mapeados diretamente dos valores de alarme extraídos e dos valores de alarme inseridos manualmente, você pode usar o editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento que é opcional.

Antes de Iniciar

Função necessária: sn_si.admin

O editor de script muda os valores de um alarme LogRhythm para que os valores mapeados para os campos Prioridade e Categoria no incidente de segurança sejam compatíveis.

Por Que e Quando Desempenhar Esta Tarefa

Em determinados casos, se os valores de alarme LogRhythm forem mapeados para os campos Prioridade e Categoria no incidente de segurança, convém editar os valores mapeados. Se você quiser traduzir o valor de um alarme LogRhythm para um valor que seja compatível com os campos Prioridade ou Categoria no incidente de segurança, use o editor de script.

Procedimento

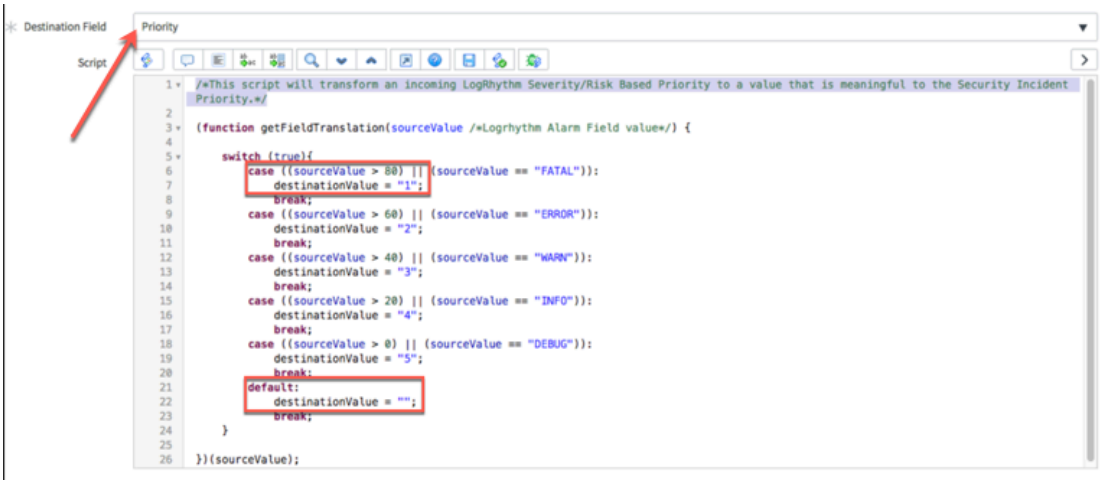
1. Com o formulário de mapeamento exibido, na seção Mapeamento de campo de incidente de SIR, clique no ícone de colchete [{}] para abrir o editor de script.

Os valores padrão são incluídos para os campos Prioridade e Categoria no incidente de segurança. Você pode editar esses valores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para este exemplo, no editor aberto, verifique se **Prioridade** é exibido na lista de seleção **Campo de destino**, conforme mostrado na figura a seguir. Observe que este campo é a *prioridade*do incidente de segurança , não a LogRhythm*prioridade*baseada em risco.



Em determinadas instâncias, uma inclusão de script pode ser apropriada para o campo Prioridade. Para um alarme LogRhythm, por exemplo, uma pontuação de prioridade baseada em risco é atribuída a um valor entre 0 e 100. No entanto, no Now Platform, o campo de prioridade em um incidente de segurança oferece suporte a valores entre 1 e 5. Conforme ilustrado na figura anterior, uma inclusão de script traduz os valores do campo de alarme LogRhythm para os valores apropriados compatíveis com o campo no incidente de segurança no Now Platform.

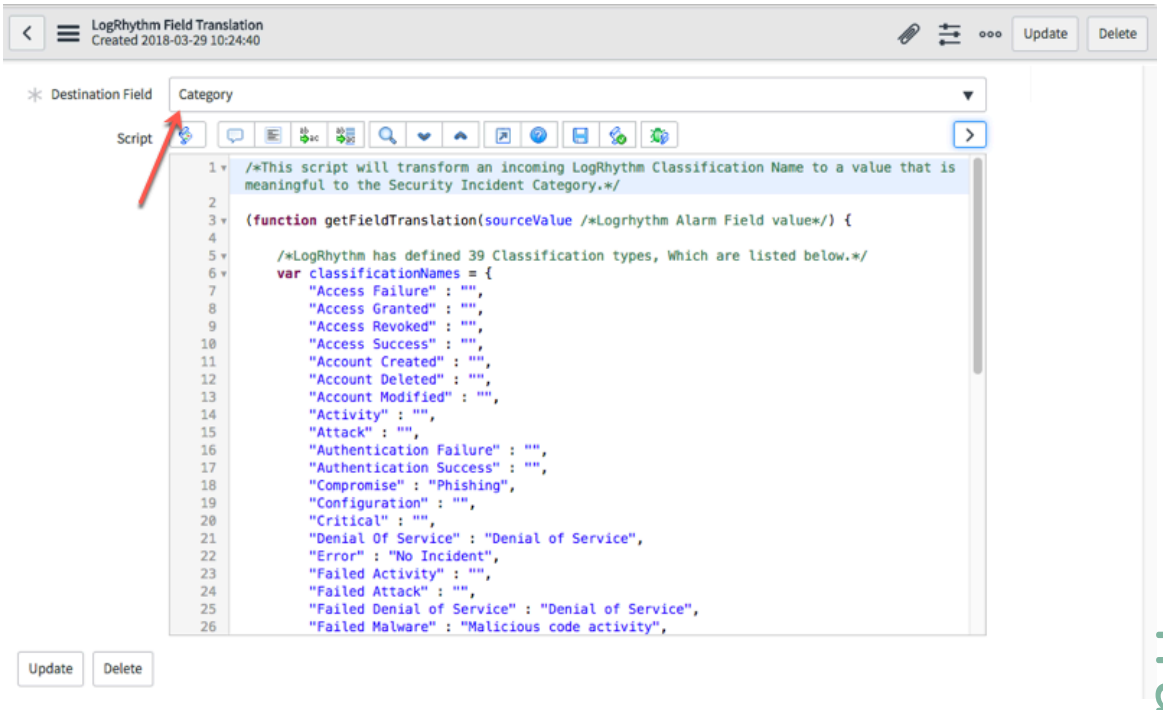
Neste exemplo para o campo Prioridade, se o valor do alarme LogRhythm for 80 ou mais, 1 será exibido no campo de incidente de segurança (Prioridade). Este valor se traduz em uma prioridade Crítica no incidente de segurança. Se não houver valor para o alarme, o campo no incidente de segurança será definido como nulo.

2. Insira as mudanças e clique em **Atualizar** para salvar as mudanças.
   A tabela LogRhythm Traduções de campo é exibida.
3. Feche a tabela para retornar ao formulário de mapeamento.

A figura a seguir mostra o editor de script com a Categoria selecionada na lista de seleção Campo de destino.

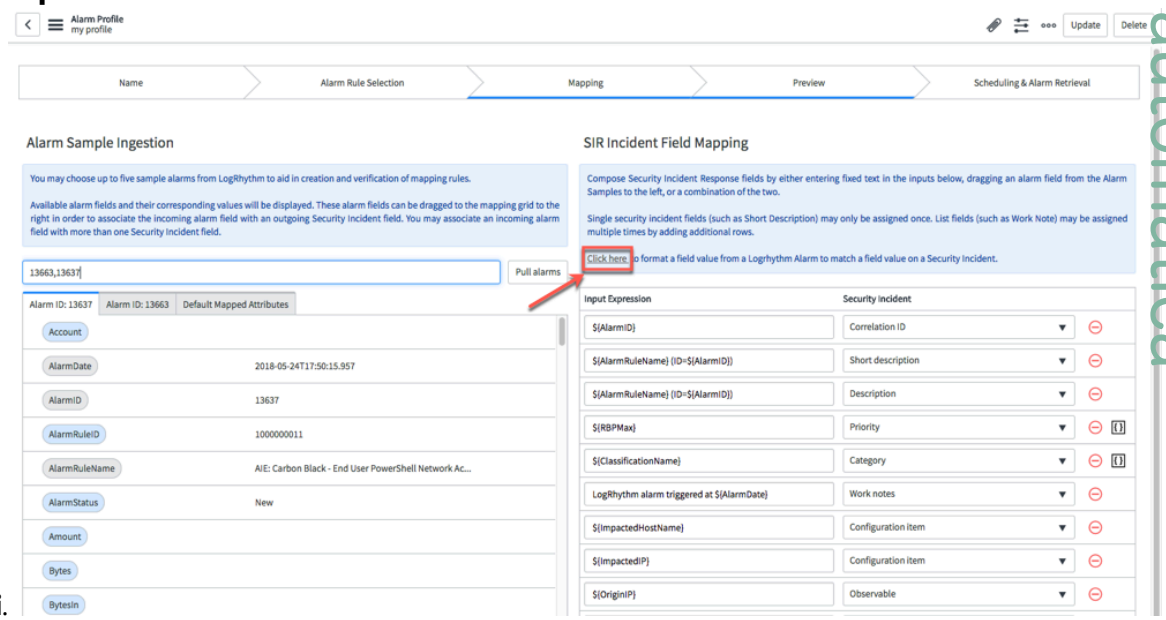
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Se você quiser adicionar um novo campo à lista Traduções de campo, siga estas etapas para adicionar um novo registro.

a. Com o formulário de mapeamento exibido, na seção Mapeamento de campo de incidente de SIR, clique no link **Clique aqui**.

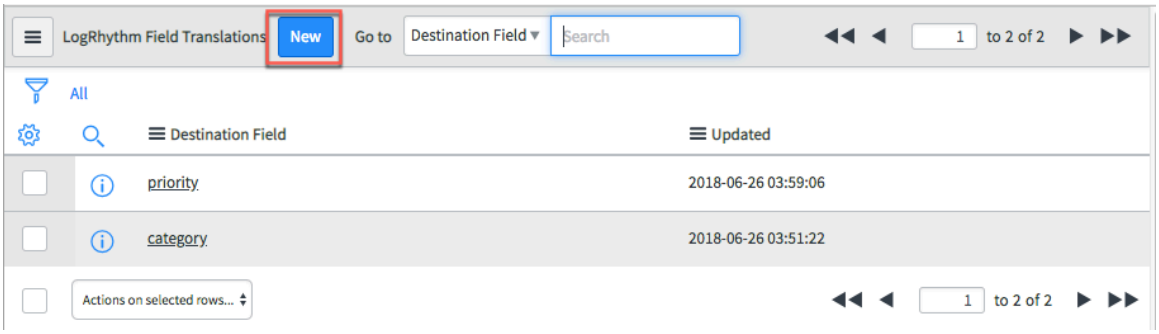


A lista LogRhythm de tradução de campo com os campos de destino de prioridade e categoria é exibida.

b. Clique em Novo.

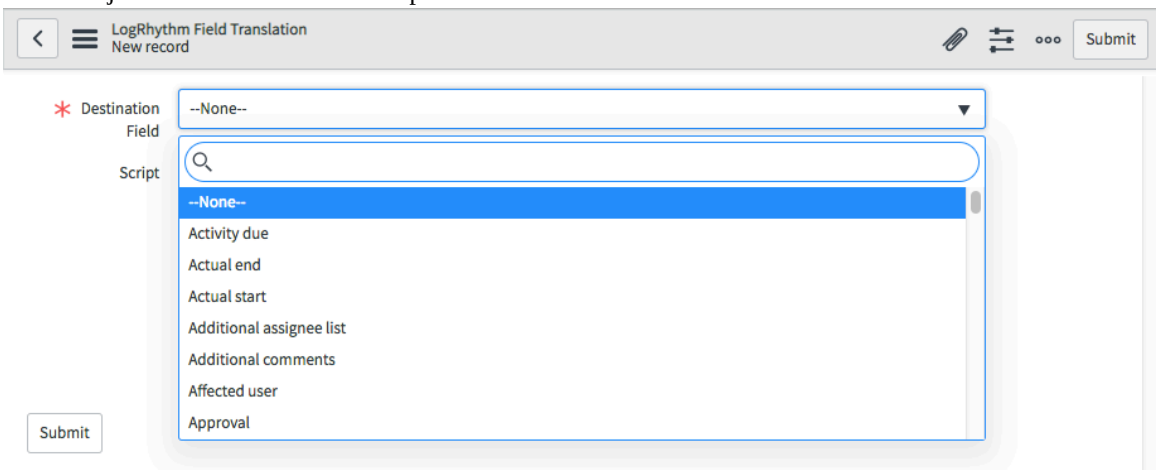
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Um novo registro é exibido.

c. Na lista de seleção Campo de destino, selecione um campo de destino no incidente de segurança no qual você deseja exibir seus valores de script.



d. Clique em **Enviar**.
O editor de script é exibido.

e. Insira as mudanças no editor e clique em **Enviar** para salvar as mudanças.
A tabela LogRhythm Traduções de campo com seu novo registro será exibida.

5. Feche a tabela para retornar ao formulário de mapeamento.

Copiar um perfil de alarme para LogRhythm

Copie um perfil existente e suas configurações associadas em vez de criar um novo perfil de alarme. Se você estiver criando vários perfis de alarme para diferentes tipos de alarmes e quiser reutilizar as configurações de um perfil existente, poderá copiar os perfis de alarme para economizar tempo. Este processo é opcional.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado é definido como inativo para que não seja ativado acidentalmente antes de concluir a configuração.

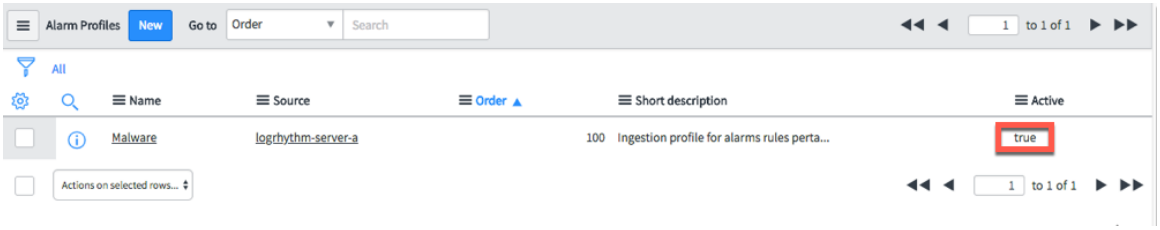
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

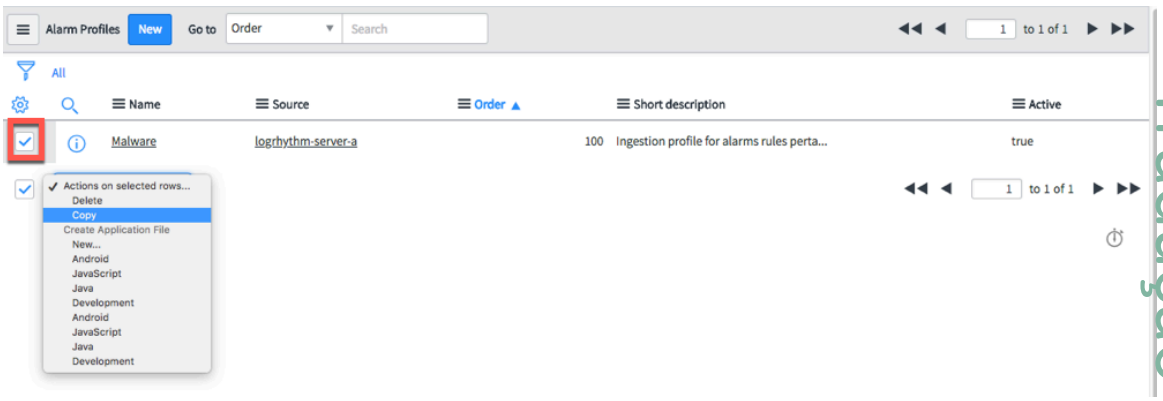
Procedimento

1. Navegar até **Todos** > **LogRhythm Integration** > **Perfis de alarme LogRhythm**.

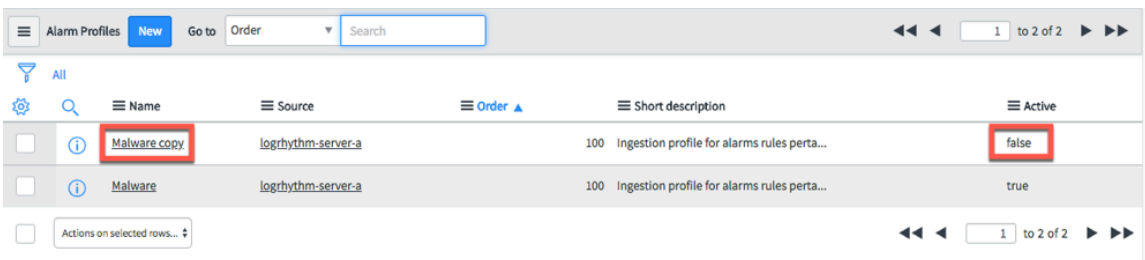
   Na lista exibida, observe que a coluna Ativo indica se o perfil está ativo (verdadeiro).



2. No campo à esquerda da coluna **Nome**, selecione o nome do registro.
3. Na lista de seleção **Ações nas linhas selecionadas**, selecione **Copiar**.



Na lista **Perfis de alarme**, a cópia e o perfil original são exibidos. Embora o registro original esteja ativo, a cópia está inativa neste ponto (falso). Depois de configurá-lo, você ativa este perfil copiado.



Você pode editar valores do perfil copiado e renomeá-lo para que as regras de alarme extraídas se apliquem ao novo perfil. Você será solicitado a ativar o novo perfil depois que as etapas de configuração forem concluídas.

Desabilitar fechamento de alarme automatizado para LogRhythm

Desabilite o recurso de fechamento de alarme automatizado se você não quiser mais exibir as informações de fechamento do incidente de segurança no LogRhythm Console da Web. Depois de desabilitado, o Now Platform não fecha mais os alarmes no console da Web LogRhythm. Este processo é opcional.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

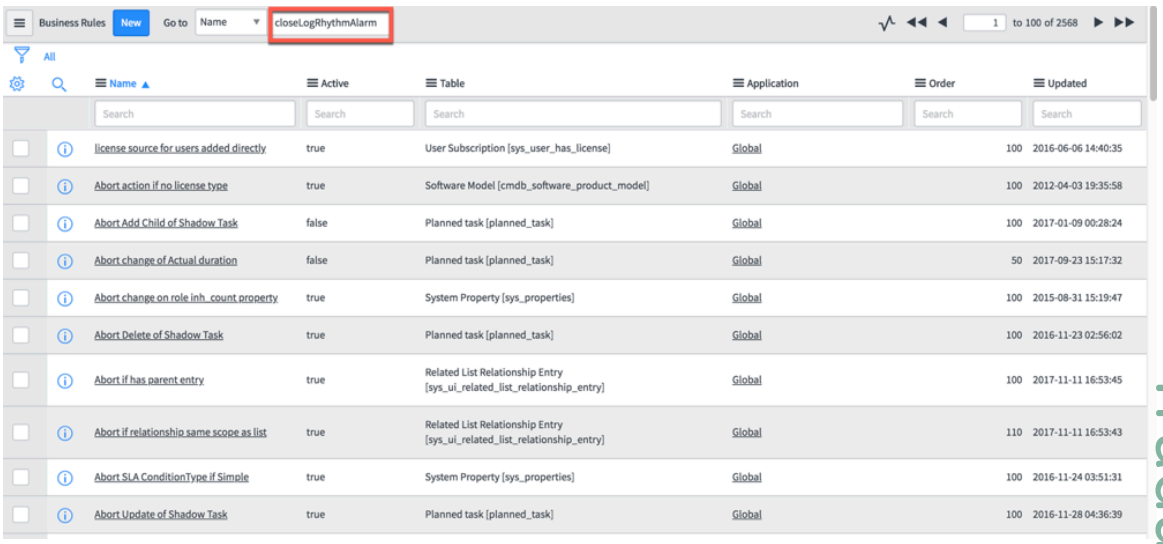
Depois de desabilitadas, as anotações de status e outras informações de fechamento no incidente de segurança não são mais exibidas no LogRhythm Console da Web.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Definição do sistema** > **Regras de negócios** e selecione o módulo **Regras de negócio**.
2. Se não for exibido na lista **Regras de negócios**, insira **LogRhythm Close Alarm On SI Closure** no campo de pesquisa e pressione **Enter**.



3. Na coluna **Nome**, clique no **link LogRhythm Close Alarm On SI Closure** para abrir o registro.
4. No registro exibido, desmarque a caixa de seleção **Ativo**.
5. Clique em **Atualizar**.
   O recurso de fechamento de alarme automatizado agora está desabilitado.

Exibir LogRhythm eventos de detalhamento

Exiba os eventos brutos ou básicos relacionados a um alarme LogRhythm no incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Como analista de segurança, você pode exibir os eventos brutos ou de base relacionados a um alarme LogRhythm sem precisar voltar para o console LogRhythm. Você pode fazer isso acessando uma lista relacionada que contém todos os eventos de detalhamento no incidente SIR.

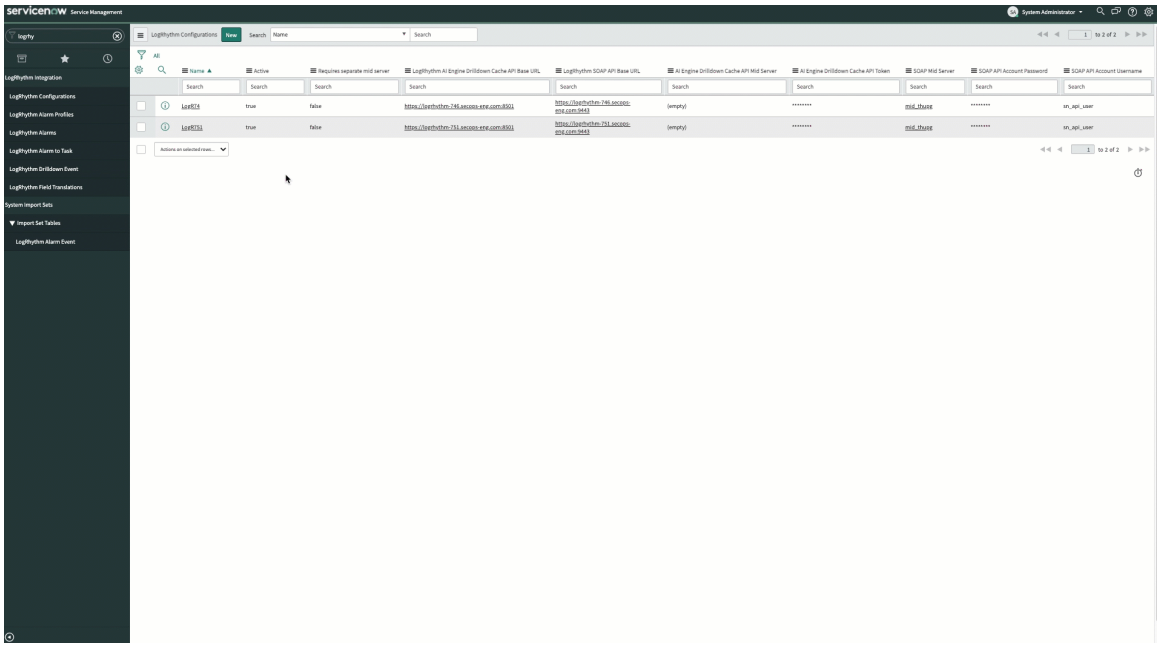
Procedimento

Navegar até **Todos** > **LogRhythm Integration** > **Eventos de detalhamento da LogRhythm**.

A ilustração a seguir mostra como navegar até o módulo **Eventos de detalhamento do LogRhythm**, classificar a lista de eventos por **Agrupar por ID de alarme**e clicar no incidente de segurança associado. No incidente de segurança, você pode encontrar a guia **Eventos de detalhamento do LogRhythm** nos links relacionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Solução de problemas da integração do LogRhythm

Solucione problemas de conectividade e ingestão de alarmes.

Consulte os seguintes tópicos para solução de problemas:

- Verificar conectividade para LogRhythm
- Execução de script e log do sistema para LogRhythm

Verificar conectividade para LogRhythm

Verifique sua conexão com o LogRhythm Client Console enviando solicitações de curl para testar a LogRhythm REST API. O processo de verificação é opcional.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Para verificar se a conexão com o LogRhythm Client Console está funcionando corretamente depois de configurar as LogRhythm REST APIs, envie duas solicitações de curl do computador que hospeda o MID Server que você configurou em Instalar o plug-in e configurar LogRhythm.

A REST API LogRhythm usa WSSE para autenticação, o que requer algum script externo para funcionar com Curl e Postman.

A REST API LogRhythm usa um token para autenticação, portanto, você pode fazer a chamada de validação real que a integração usa. O "0" no final do URL é um LogRhythm ID de alarme. A REST API LogRhythm com uma configuração padrão requer a porta 8501. Este número de porta deve ser incluído no URL que você planeja usar para o teste.

Procedimento

Atualizar a URL<LogRhythm REST url> e token<api token> na solicitação de curl a seguir e envie-a para validar a LogRhythm REST API: **curl -k -i -v --trace-time -o /dev/null -H "Content-Type: text/json" -H "Authorization: Portador** " "https://<cache drilldown url> /lr-drilldown-cache-api/drilldown/0"
Para uma conexão bem-sucedida com a LogRhythm REST API, você deve receber um HTTP 404, mas o corpo da resposta contém o ID do alarme: 0 não encontrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Execução de script e log do sistema para LogRhythm

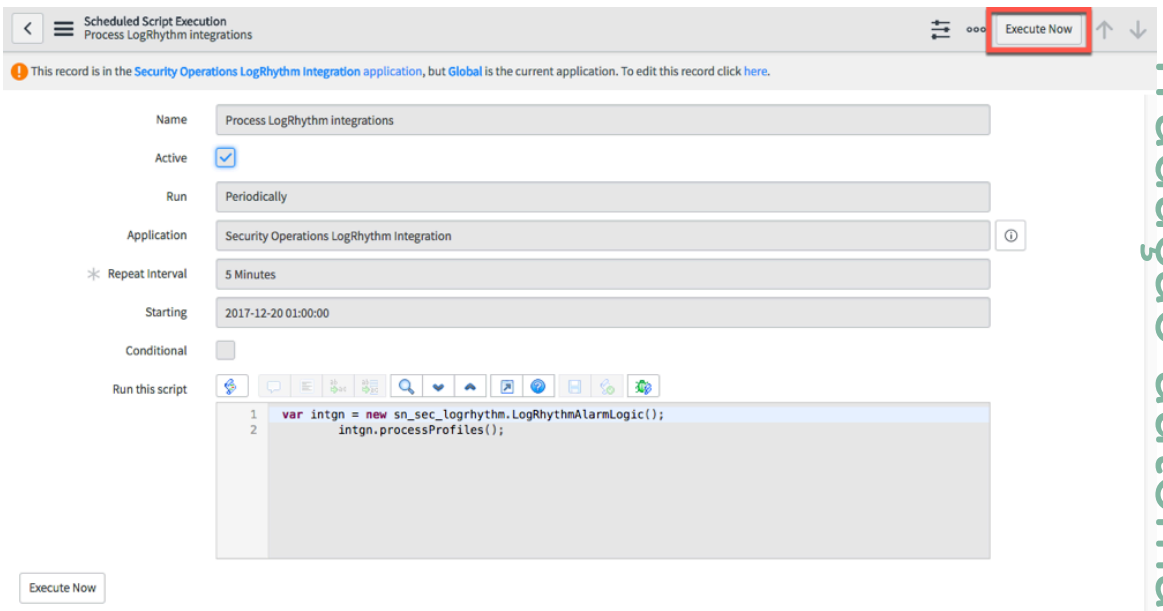
Se você estiver solucionando um problema de ingestão de alarme, poderá substituir o intervalo de pesquisa padrão de cinco minutos para exibir os resultados imediatamente. Neste cenário, chame a execução do script manualmente para executar a pesquisa. Esta execução é opcional.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Trabalho programado** > **Trabalhos programados** e selecione o módulo **Trabalhos programados**.
2. Clique no registro de trabalho de integrações do processo LogRhythm.
3. No registro Execução programada de script exibido, clique em **Executar agora**.



Se você precisar de mais ajuda na solução de problemas, poderá acessar o log do sistema para as consultas LogRhythm.

4. Para outros problemas gerais de solução de problemas, siga estas etapas para acessar os logs do sistema.

   a. Navegar até **Log do sistema** > **Todos** e selecione **Todos**.

   b. Defina o filtro (lr para) como **Origem** e insira `sn_sec_logrhythm`.

   c. Pressione **Enter**.
   Todas as mensagens geradas pela integração são exibidas nesta tabela. As mensagens listadas podem fornecer informações sobre os processos em execução da integração e podem ajudá-lo na solução de problemas.

Integração de McAfee ePO

A capacidade de detecção e resposta de endpoint de integração McAfee ePO que ajuda os analistas do Security Operations Center (SOC) a identificar ameaças cibernéticas e reparar os danos causados por arquivos mal-intencionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

Há dois conjuntos de recursos McAfee ePO usados nesta integração, os recursos que invocam ações, como isolar um host e iniciar uma verificação de malware, e os recursos que executam consultas para coletar detalhes do sistema e eventos de ameaça. Ambos os tipos de recursos, as ações e as consultas, são invocados de sua instância Now Platform®. Você pode agrupar esses recursos para que eles sejam executados automaticamente quando ocorrer um tipo específico de evento de segurança ou invocá-los manualmente a partir de um incidente de segurança Now Platform®.

Os seguintes recursos McAfee ePO estão disponíveis para esta integração.

Obter detalhes do sistema

Reúna detalhes do sistema que incluem detalhes do sistema operacional.

Iniciar verificação de malware

Com base na configuração e na programação da verificação, inicie uma verificação de um endpoint afetado.

Isolar/desassociar host

Remova um sistema do acesso à rede para investigação e restaure o acesso à rede.

Listar eventos de ameaça

Reúna o status de conformidade e os eventos de ameaça mais recentes.

Principais recursos

Esta integração inclui os seguintes recursos principais.

- Oferece suporte ao acionamento automatizado de McAfee ePO consultas baseadas em condições de incidente.
- Oferece suporte à inicialização de McAfee ePO recursos manualmente de Now Platform® Security Incident Response (SIR) incidentes de segurança que executam ações sob demanda.
- A flexibilidade para criar vários perfis para acionar diferentes tipos de recursos McAfee ePO e Now Platform® Security Operations. Esses perfis coletam informações de eventos de ameaça ou executam ações com base nas condições de categorias de incidentes específicas, como malware.
- Valide a configuração do seu perfil com uma visualização dos resultados de SIRMcAfee ePO em incidentes de segurança [].
- Se a marcação estiver habilitada, os marcadores de segurança identificarão quais McAfee ePO recursos são iniciados inicialmente por um fluxo de trabalho e quando as consultas ou ações são concluídas com sucesso.
- Uma trilha de auditoria completa das McAfee ePO consultas e ações é publicada nas anotações de trabalho em SIR incidentes de segurança e os comandos do Now Platform® são registrados no console McAfee ePO.
- Oferece suporte a vários consoles McAfee ePO.

ServiceNow Plug-ins

O plug-in com.snc.si_dep é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Security Operations aplicações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As aplicações Security Operations a seguir devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative um aplicativo de cada vez na ordem listada abaixo para garantir uma instalação sem problemas:

1. Security Integration Framework
2. Security Support Common
3. Orquestração de suporte de segurança
4. Security Incident Response
5. Espaço de resposta a incidentes de segurança

Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte Configure sua instância Now Platform para a integração McAfee ePO.

O plug-in de extensão ServiceNow

O plug-in ServiceNow Security Operations Extension for McAfee ePO# é necessário para esta integração. Você instala este plug-in ServiceNowMcAfee ePO no console []. Para obter mais informações, consulte Configure sua instância Now Platform para a integração McAfee ePO.

MID Server

Esta integração requer um MID Server instalado e configurado em sua instância Now Platform® para se conectar ao servidor McAfee ePO (console). Consulte o site de documentação do produto da ServiceNow para obter mais informações sobre MID Servers.

Versões compatíveis do McAfee

A integração é compatível com as versões 5.9.1 e 5.10 de McAfee ePO. Ele oferece suporte ao McAfee Agent: MA 5.5.1.388. Para obter mais informações sobre os produtos da McAfee e o ePolicy Orchestrator, consulte o site do produto da McAfee .

A integração é compatível com a versão 10.5 do produto McAfee Endpoint Security Threat Prevention. Se você não estiver executando a versão 10.5, consulte o administrador McAfee ePO para ver se sua versão pode oferecer suporte a verificações sob demanda por meio de ações de marcador.

McAfee ePO marcadores de segurança são usados nesta integração. Você deve criar esses marcadores no console McAfee ePO. Para obter mais informações sobre esses marcadores, consulte Configure seu console McAfee ePO para integrar com Security Incident Response (SIR).

Referências

Referência	Identificador de documento	Título do Documento
1	Site do produto da McAfee	Site do produto da McAfee
2	Documentação de produto de negócios da McAfee para ePolicy Orchestrator Cloud	Documentação de produto da McAfee
3	ServiceNow Site da documentação do produto	Site de documentação do produto da ServiceNow

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter uma check-list para rastrear seu andamento com a configuração, instalação e verificação dos resultados da integração, consulte Check-list para a integração McAfee ePO.

Para uma instalação sem problemas do aplicativo e para ajudá-lo a verificar os resultados esperados, siga os tópicos na ordem em que são apresentados.

Tópicos relacionados

Arquitetura de integração para McAfee ePO

Arquitetura de integração para McAfee ePO

O tópico a seguir é uma visão geral da arquitetura do sistema e lista os principais recursos da integração. Esta seção também fornece informações sobre as etapas de configuração que você precisa concluir na instância Now Platform e no console do McAfee ePolicy Orchestrator (McAfee ePO) antes de instalar a aplicação do ServiceNow Store.

Termos-chave para a integração McAfee ePO

Os termos a seguir são usados em toda a documentação de instalação e configuração da integração.

Now Platform

Um produto empresarial ServiceNow. O Now Platform é a base sobre a qual componentes individuais, como Security Incident Response (SIR), IT Service Management (ITSM) e outros produtos são criados.

Security Incident Response (SIR)

Uma aplicação Now Platform que rastreia o andamento dos incidentes de segurança desde a descoberta e a análise inicial, passando pela contenção, erradicação e recuperação, até a revisão e fechamento pós-incidente finais.

Plug-in

Plug-ins são componentes de software que fornecem recursos e funcionalidades específicos em sua instância Now Platform. Para obter mais informações sobre a instalação e configuração dos plug-ins de integração, consulte Instalar a aplicação e configurar um servidor para a integração McAfee ePO.

ePolicy Orchestrator (McAfee ePO)

O console do usuário em que você gerencia os serviços, produtos e configurações da McAfee.

Plug-in de extensão da McAfee

Este plug-in de extensão ServiceNow é necessário para esta integração. Este plug-in reside no console McAfee ePO e conecta o console McAfee ePO à sua instância Now Platform.

Capacidade

Uma atividade automática iniciada em sua instância Now Platform que é executada no console McAfee ePO para conduzir consultas de aprimoramento e executar ações em seus ativos.

Perfil

Configurações para capacidades McAfee ePO que você configura para especificar quando e sob quais condições as capacidades conduzem consultas de aprimoramento e executam ações em seus ativos.

MID server

Uma aplicação que facilita a comunicação e a movimentação de dados entre Now Platform e aplicações externas, fontes de dados e serviços.

ServiceNow administrador (admin)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um usuário com esta função baixa e instala os plug-ins SIR e McAfee ePO na sua instância Now Platform. Um usuário com esta função também atribui a função de administrador de incidente de segurança conforme necessário.

ServiceNow Administrador de incidentes de segurança (sn_si.admin)

Um usuário com esta função executa a configuração da integração McAfee ePO com o produto Security Incident Response (SIR) em sua instância Now Platform conforme necessário. Um usuário com esta função também atribui a função de analista de incidente de segurança conforme necessário.

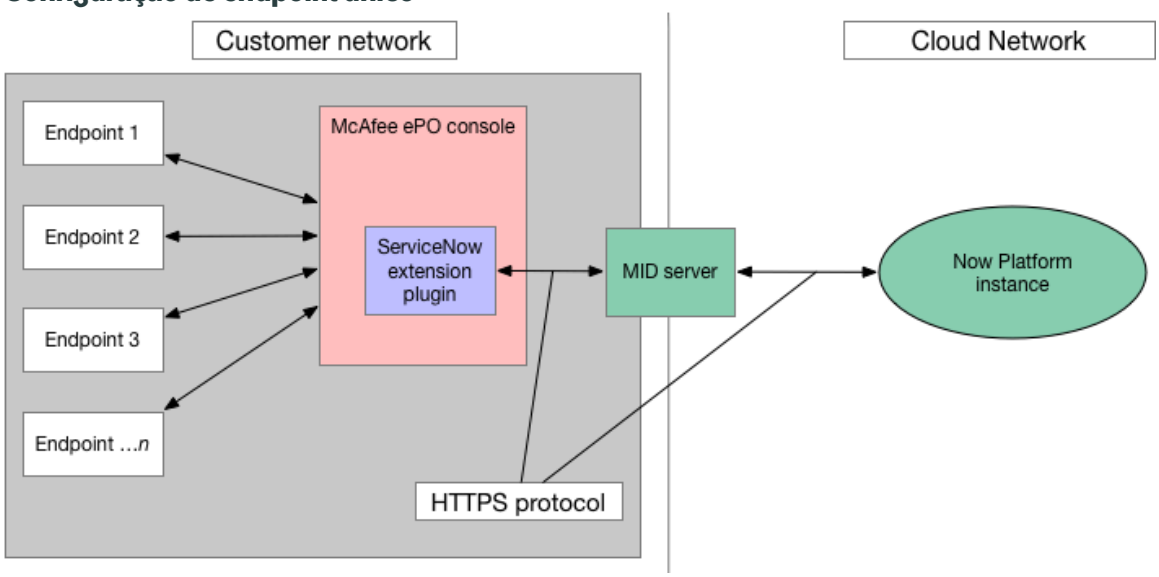
ServiceNow analista de incidente de segurança (sn_si.analyst)

Um usuário com esta função interage e analisa os incidentes de segurança no produto SIR.

Conexão do sistema e fluxo de dados

A figura a seguir é um exemplo de um ambiente de cliente. Um MID Server Now Platform é necessário para que sua instância Now Platform possa se conectar a um servidor McAfee ePO (console) por meio de um plug-in de extensão ServiceNow. Depois de conectado, você invoca recursos do seu Now Platform para iniciar verificações de malware, isolar máquinas host e restaurá-las para sua rede, recuperar resultados da última verificação e coletar detalhes do sistema em seus ativos. Quando esses recursos retornam resultados de seus ativos que correspondem aos seus critérios de pesquisa, os dados são extraídos por meio do MID Server para sua instância Now Platform. Os dados são exibidos nas listas relacionadas de um incidente de segurança Now Platform Security Incident Response (SIR). A figura a seguir ilustra o fluxo de dados para um grupo de endpoints gerenciados por um console McAfee ePO.

Configuração de endpoint único

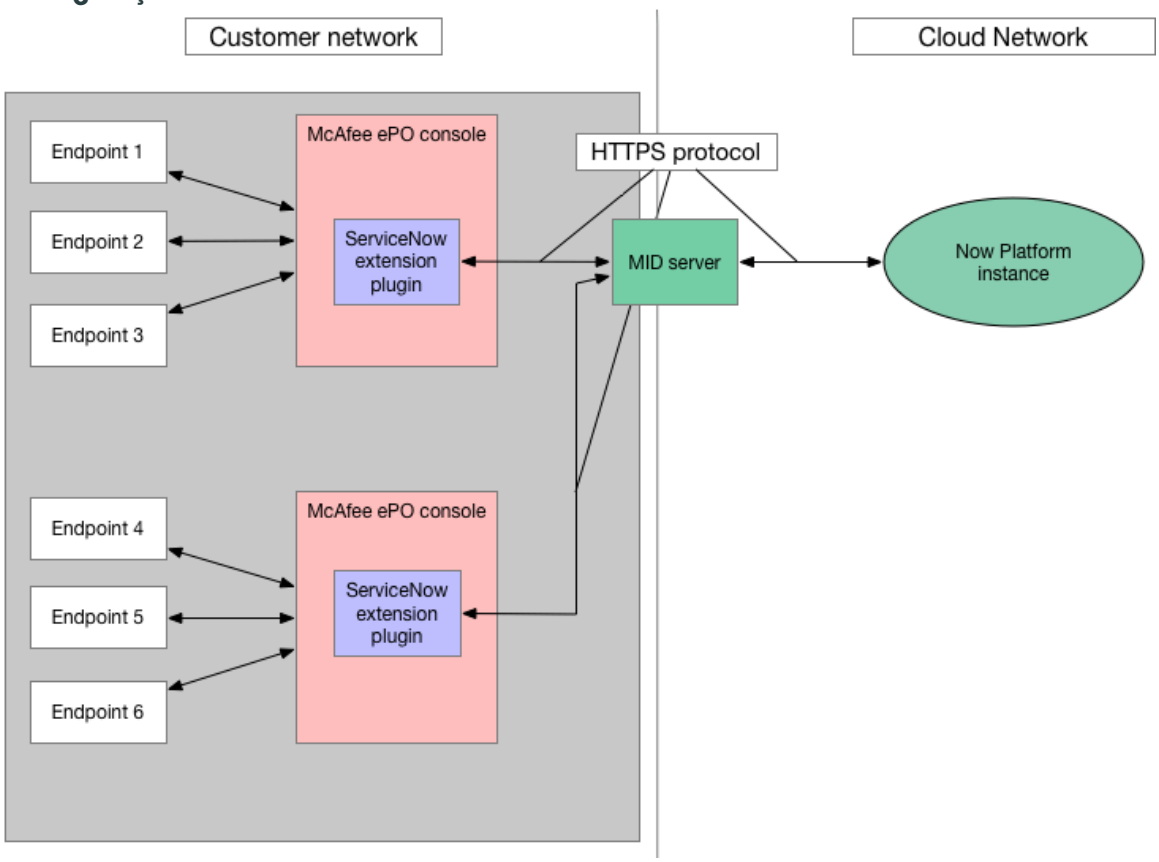


Conforme mostrado na figura a seguir, esta integração pode oferecer suporte a mais de um console McAfee ePO. Você pode ter um grupo de endpoints gerenciados por um console McAfee ePO e outro grupo de endpoints gerenciados por outro console McAfee ePO. Os dados de vários consoles McAfee ePO são extraídos por meio de um único MID Server. No entanto, você também pode configurar vários MID Servers, se exigido pela sua organização.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de MID servers



Fluxos de trabalho para a integração McAfee ePO

Esta integração inclui os seguintes fluxos de trabalho. Esses fluxos de trabalho são pré-configurados e projetados especificamente para esta integração. Você pode editar esses fluxos de trabalho para atender às necessidades da sua organização, conforme necessário. Para obter mais informações gerais sobre fluxos de trabalho e como usar o editor de fluxo de trabalho, consulte Introdução a fluxos de trabalho.

- Integração do McAfee EPO com o Security Operations - Obter detalhes do host
- Integração do Security Operations com o McAfee EPO - Iniciar verificação de malware
- Integração do Security Operations McAfee EPO - Isolar host
- Integração do Security Operations McAfee EPO - Listar eventos de ameaça
- Security Operations McAfee EPO integration - Remove Isolation

Conexão de sistemas externos

A integração requer que o MID Server se comunique via conexão de protocolo HTTPS com o console McAfee ePO.

Check-list para a integração McAfee ePO

Use esta check-list para orientar você em todas as tarefas da integração. A check-list a seguir inclui tarefas de configuração e instalação e exemplos de casos de uso que incluem os resultados esperados para a integração.

Antes de Iniciar
Função necessária: as funções são listadas para cada etapa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Acompanhe seu progresso com a instalação e configuração da integração com a tabela a seguir. Conclua todas as tarefas de uma etapa antes de passar para a próxima. Cada linha da tabela lista as tarefas e identifica as funções necessárias para executar as tarefas. Tópicos numerados do guia de instalação e configuração também são referenciados.

Procedimento

Siga as etapas na tabela na ordem em que são apresentadas.

Check-list

Item	Descrição
☐	Como um usuário com a função de administrador Now Platform®, configure sua instância Now Platform®. **a.** Atribua as funções Now Platform® e Security Incident Response. **b.** Verifique se todos os ServiceNow Security Incident Response e outros plug-ins compatíveis com a integração estão instalados e ativados para a versão do Now Platform. **c.** Instale e configure um MID Server em sua instância Now Platform®. **d.** Crie um grupo de aprovação se quiser processar solicitações enviadas pelo analista de incidentes de segurança para o host isolado e iniciar ações de verificação de malware. Para obter mais informações, consulte Configure sua instância Now Platform para a integração McAfee ePO.
☐	Como administrador McAfee ePO, configure o console McAfee ePO. **a.** Verifique se você está usando a versão 5.9 do McAfee ePO. **b.** Instale o plug-in de extensão ServiceNowMcAfee ePO no console []. **c.** Verifique se você criou marcadores de segurança no console McAfee ePO para o host isolado e inicie as ações de verificação de malware. Para obter mais informações, consulte Configure seu console McAfee ePO para integrar com Security Incident Response (SIR). Para obter mais informações e obter o arquivo do plug-in de extensão, na sua instância Now Platform, navegue até **Conhecimento** > **Artigos** > **Todos** e, no campo Pesquisar, insira Security Operations Extension da ServiceNow para McAfee ePO.
☐	Como um usuário com a função de administrador Now Platform, instale a aplicação McAfee ePO do ServiceNow Store, configure um servidor e conecte-se ao console McAfee ePO. Para obter mais informações, consulte Instalar a aplicação e configurar um servidor para a integração McAfee ePO.
☐	Como um usuário com a função de administrador de incidente de segurança Now Platform, edite os nomes dos marcadores de segurança em sua instância Now Platform® para que eles correspondam aos nomes de marcador que você criou no console McAfee ePO.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	Para obter mais informações, consulte Editar marcadores de segurança no Now Platform para a integração McAfee ePO.
☐	Como um usuário com a função de administrador de incidentes de segurança, crie um perfil para as capacidades McAfee ePO. Para obter informações sobre perfis, consulte McAfee ePO perfis de capacidade de integração. Para obter as etapas necessárias para criar um perfil, consulte Criar um perfil de capacidade para a integração McAfee ePO.
☐	Como um usuário com a função de administrador de incidentes de segurança, configure um perfil e teste os incidentes de segurança. **a.** Revise as informações sobre condições e configurações de gatilho. **b.** Configure um perfil. **c.** Teste e visualize incidentes de segurança. **d.** Localize os resultados da pesquisa e outros detalhes nas listas relacionadas ao incidente de segurança. **e.** Crie e configure diferentes tipos de perfis e teste incidentes de segurança para cada tipo. Para obter informações sobre condições de gatilho e o campo de IC alternativo, consulte Definir condições de gatilho com um campo Item de configuração (IC) para um perfil McAfee ePO. Para obter as etapas necessárias para configurar um perfil, testar e visualizar incidentes de segurança e exemplos de tipos de perfil, consulte os exemplos a seguir Configurando perfis para a integração McAfee ePO.
☐	Como um usuário com a função de analista de incidente de segurança Now Platform, envie solicitações adicionais para verificações de malware e Listar eventos de ameaça. Para obter mais informações, consulte Acionar perfil McAfee ePO manualmente a partir de um incidente de segurança No Now Platform, como um usuário com uma função de aprovação ou, como um membro de um grupo de aprovação, aprove as solicitações para isolar o isolamento de host e remover o isolamento. Para obter mais informações sobre como processar solicitações de aprovação, consulte Criar um grupo de aprovação.

Você concluiu com êxito as etapas de configuração, instalou e configurou a aplicação e verificou os resultados esperados para a integração.

Configure sua instância Now Platform® para a integração McAfee ePO

A seção a seguir lista as tarefas de configuração que você deve concluir na sua instância Now Platform® antes de instalar a aplicação para a integração McAfee ePO.

Configurar requisitos

Função necessária: Now Platform administrador (admin). Revise as informações a seguir antes de sua instância Now Platform® para a integração McAfee ePO.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A tabela a seguir é uma lista de requisitos de configuração para a aplicação. Verifique se você concluiu essas tarefas antes de instalar a aplicação para a integração de ServiceNow Store.

Configurar tarefa	Descrição
Verifique se você atribuiu as funções Now Platform® e Security Incident Response (SIR) necessárias.	As seguintes funções são necessárias: • Um usuário com a função de administrador do sistema (admin) para instalar a aplicação. • Um usuário com a função de administrador de incidentes de segurança (sn_si.admin) configura a aplicação e cria, ativa e remove perfis. • Um usuário com a função de analista de incidente de segurança (sn_si.analyst) trabalha com incidentes de segurança. As tarefas incluem a inicialização manual de perfis de incidentes de segurança. Se a opção de aprovação for selecionada em um perfil durante a etapa de configuração, os usuários com essa função também enviarão solicitações para isolar hosts e devolvê-los à rede.
Verifique se você está usando a versão 5.9 do McAfee ePO.	A integração é compatível com a versão 10.4.3 do McAfee ePolicy Orchestrator.
Verifique se você instalou o plug-in de extensão ServiceNowMcAfee ePO no console [].	Instale o plug-in McAfee ePOServiceNow no console []. Para obter mais informações e obter o arquivo do plug-in, na sua instância Now Platform, navegue até **Conhecimento** > **Artigos** > **Todos** e, no campo Pesquisar, insira Security Operations Extension da ServiceNow para McAfee ePO .
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	O plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras aplicações Security Operations necessárias para a integração. Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar tarefa	Descrição
	1. Security Incident Response **2.** Espaço de resposta a incidentes de segurança **3.** Security Integration Framework **4.** Security Support Common **5.** Orquestração de suporte de segurança Para obter mais informações sobre como instalar as aplicações principais do Security Operations, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.
Verifique se você instalou e configurou um MID Server.	Um MID Server instalado e configurado é necessário na sua instância Now Platform®. Consulte o site de documentação do produto da ServiceNow para obter mais informações sobre MID Servers.
Se você quiser habilitar o processo de aprovação para perfis, verifique se você criou um grupo de aprovação para processar solicitações.	Há um processo de aprovação opcional disponível para isolar máquinas host e restaurá-las na rede. Se esta opção estiver habilitada, a aprovação prévia será necessária antes que as máquinas host sejam isoladas e restauradas para sua rede. Se sua organização deseja um nível extra de controle sobre essas ações, habilite a opção **Requer aprovação** durante a etapa de configuração de um perfil. Por padrão, a autoridade de aprovação é atribuída ao administrador de incidentes de segurança Now Platform® (sn_si.admin). Esta autoridade pode ser reatribuída a um grupo de aprovação. No grupo, qualquer membro tem permissão para aprovar ou rejeitar solicitações. Você seleciona um grupo de aprovação ativo durante a etapa de configuração do seu perfil. Para obter mais informações, consulte Criar um grupo de aprovação.

Configure seu console McAfee ePO para integrar com Security Incident Response (SIR)

A seção a seguir lista as etapas de configuração que você deve concluir no console McAfee ePO antes de instalar a aplicação do ServiceNow Store para a integração.

Antes de Iniciar

Função necessária: McAfee ePO administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como um usuário com a permissão de administrador McAfee ePO, verifique se você instalou o plug-in de extensão Servicenow.zip no console McAfee ePO. Este plug-in de extensão é necessário para a integração. Para obter mais informações e obter o plug-in, na sua instância Now Platform, navegue até **Conhecimento** > **Artigos** > **Todos**. No campo Pesquisar, insira ServiceNow Security Operations Extension for McAfee ePO.

Por Que e Quando Desempenhar Esta Tarefa

O plug-in de extensão ServiceNow conecta sua instância Now Platform ao seu console McAfee ePO. Esta conexão permite que você faça referência aos marcadores de segurança que você cria no console McAfee ePO para o host isolado e inicie ações de verificação de malware para os perfis de recurso na sua instância Now Platform.

Os marcadores de segurança no console McAfee ePO devem corresponder aos marcadores de segurança nos registros de recurso na sua instância Now Platform.

As etapas a seguir mostram como instalar o plug-in de extensão, criar um marcador de segurança no console McAfee ePO e atribuir uma ação ao marcador. Para obter mais informações sobre os marcadores de segurança no console McAfee ePO, consulte o site de documentação do produto da McAfee .

Nota:
Os números na seção a seguir são do console McAfee ePO.

Procedimento

1. Se você não instalou o plug-in de extensão ServiceNowMcAfee ePO no console [], siga estas etapas para instalá-lo.

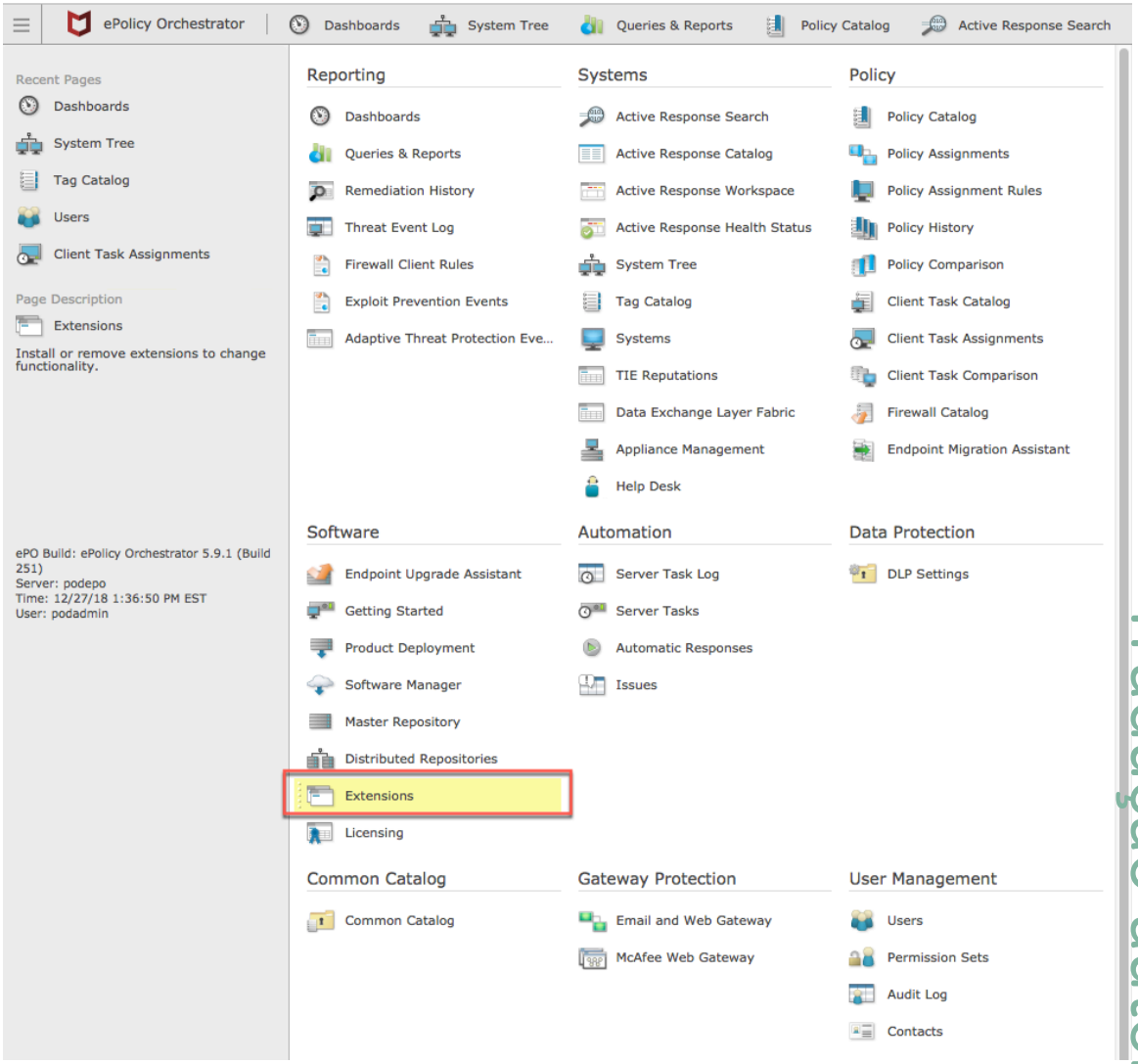
   a. Faça login no console McAfee ePO com seu nome de usuário e senha da McAfee.

2. Se a página mostrada na figura a seguir não for exibida, na parte superior esquerda da faixa da página inicial, clique no ícone de menu para exibi-la.

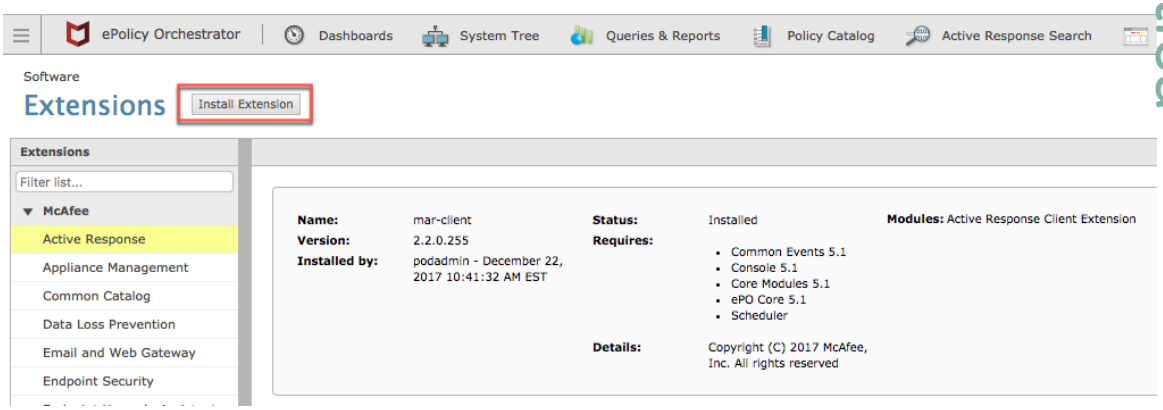
3. Na seção Software, clique no link **Extensões**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



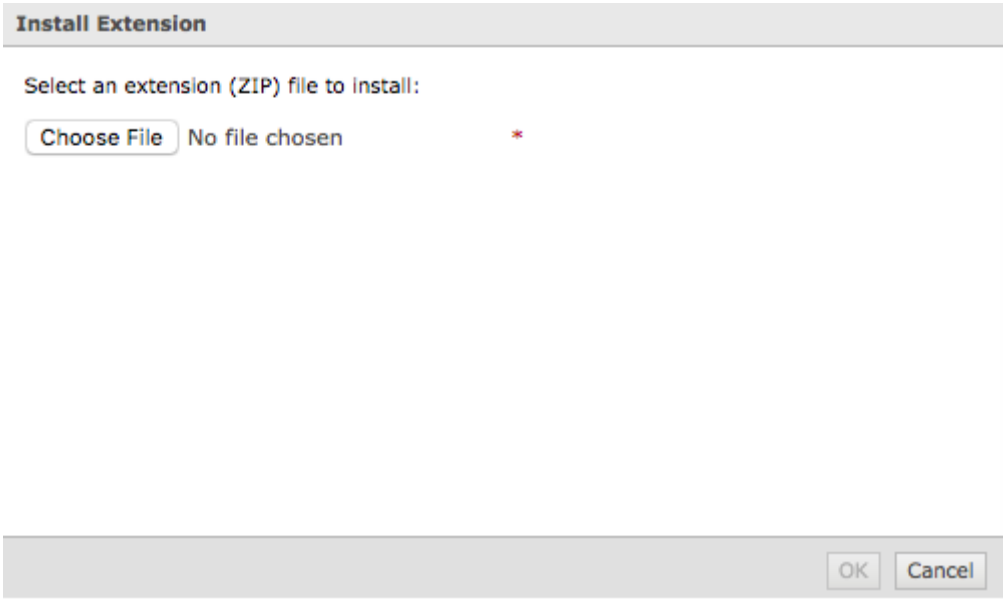
4. Na página Extensões exibida, clique em **Instalar extensão**.



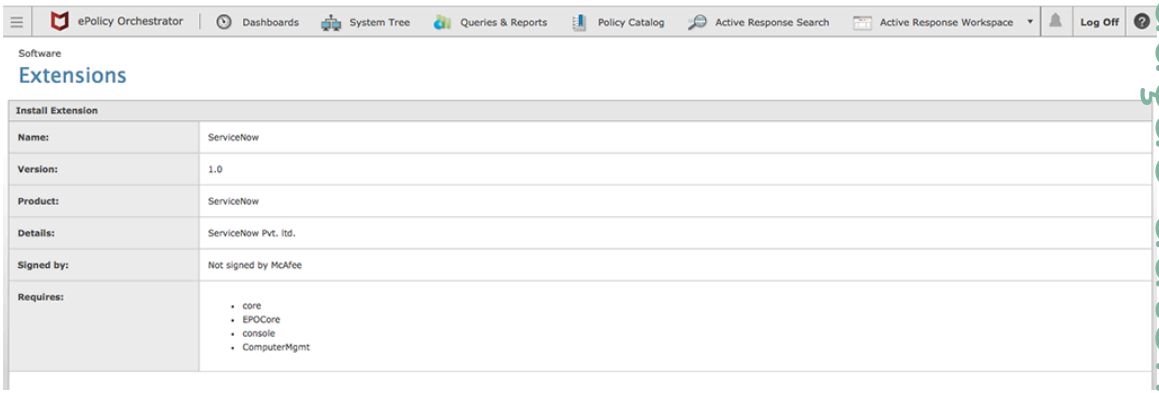
5. Na caixa de diálogo Instalar extensão, clique em **Escolher arquivo**, navegue até o arquivo Servicenow.zip no seu sistema e clique em **OK** para baixá-lo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Após a conclusão do download, a página Extensões de software será exibida com o plug-in de extensão ServiceNow listado.



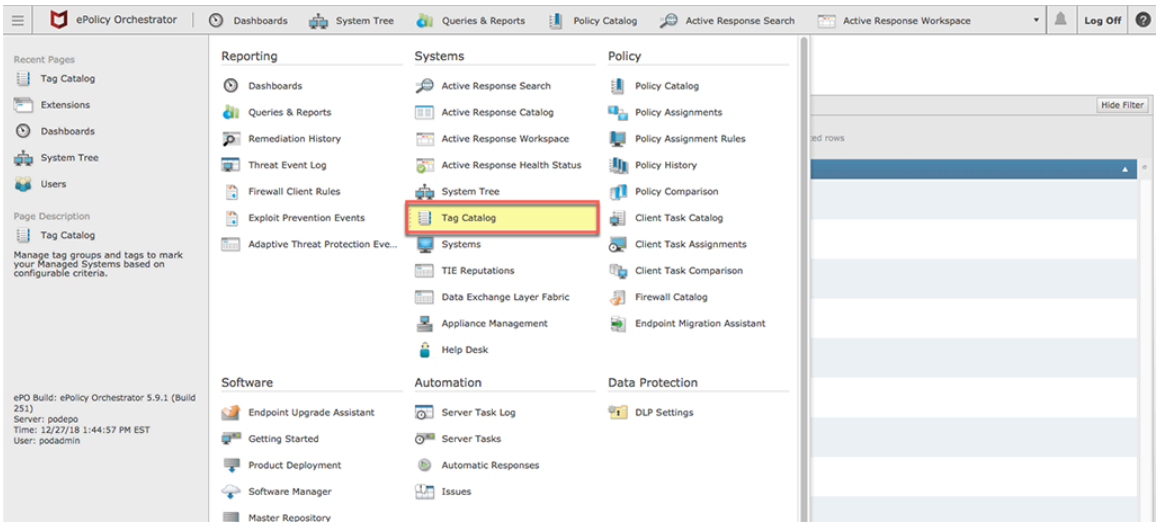
Você instalou com sucesso a extensão do plug-in ServiceNowMcAfee ePO no console [].

6. Se você não criou marcadores de segurança no console McAfee ePO para iniciar a verificação de malware e isolar as ações do host, siga estas etapas.

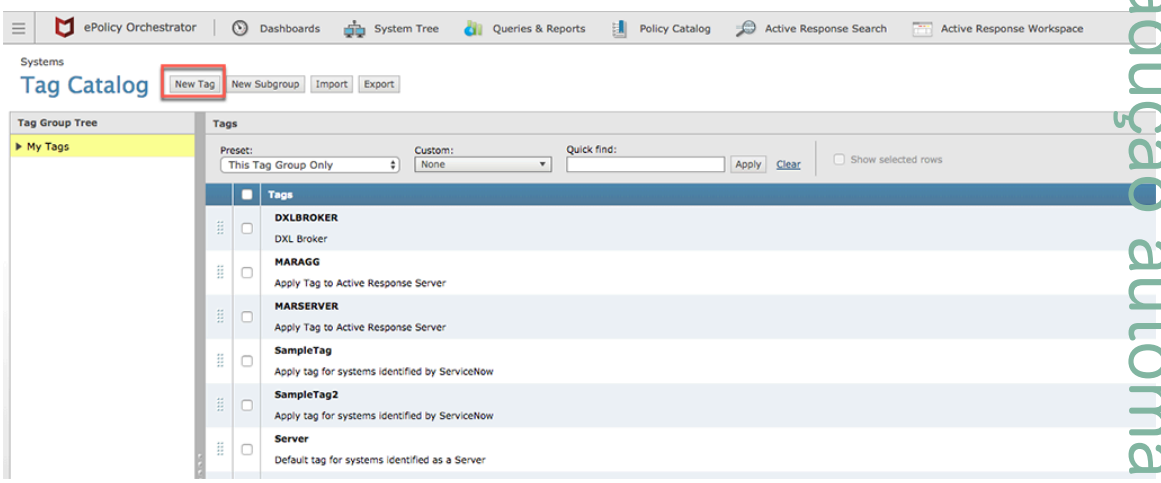
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegue até a página inicial e clique no link **Catálogo** de marcadores.

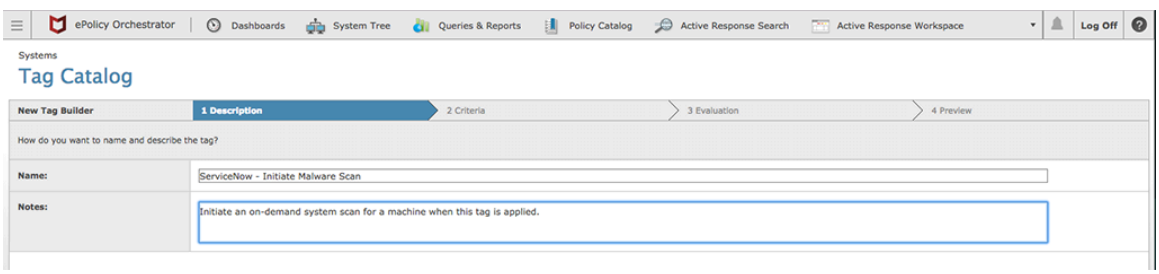


b. Na página Catálogo de marcadores exibida, clique em **Novo marcador**.



c. Com a etapa Descrição selecionada na barra de andamento exibida, insira um nome e uma descrição para o marcador.

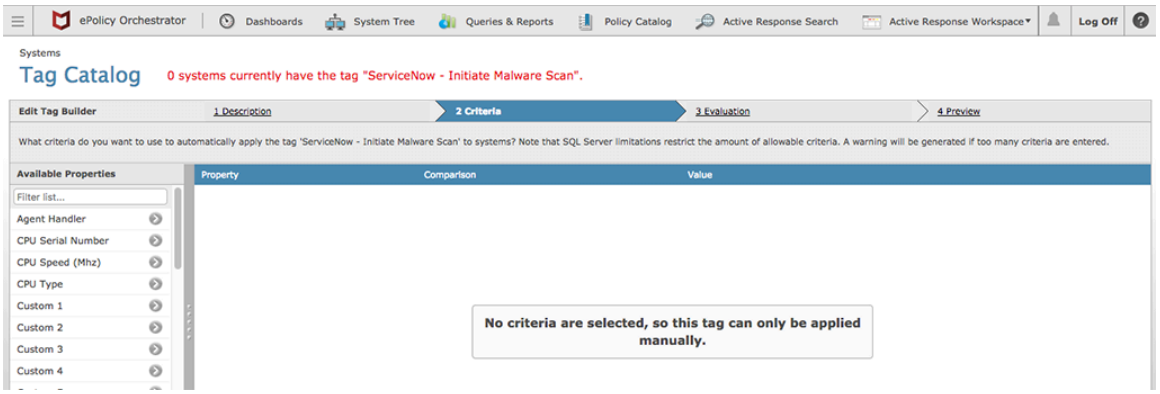
Para este exemplo, um marcador com um nome e uma descrição para o recurso Iniciar verificação de malware é exibido. Este nome de marcador é o que é correspondido e referenciado na sua instância Now Platform.



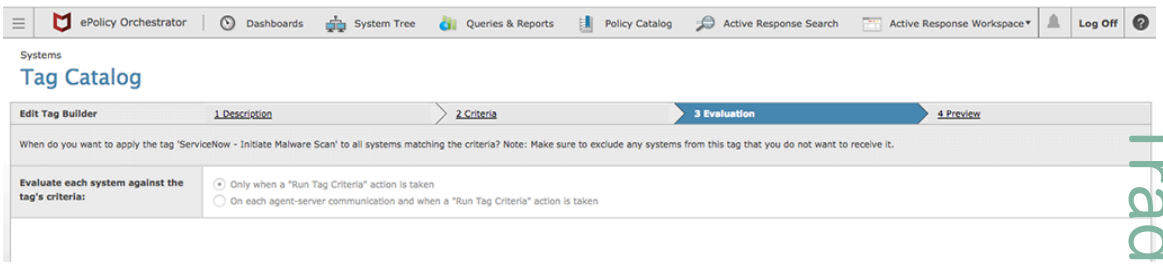
d. Para avançar para a etapa Critérios, clique em **Critérios** na barra de andamento.
As mensagens exibidas indicam que nenhuma ação está atribuída a este marcador e que o marcador só pode ser aplicado manualmente.

Tradução automática

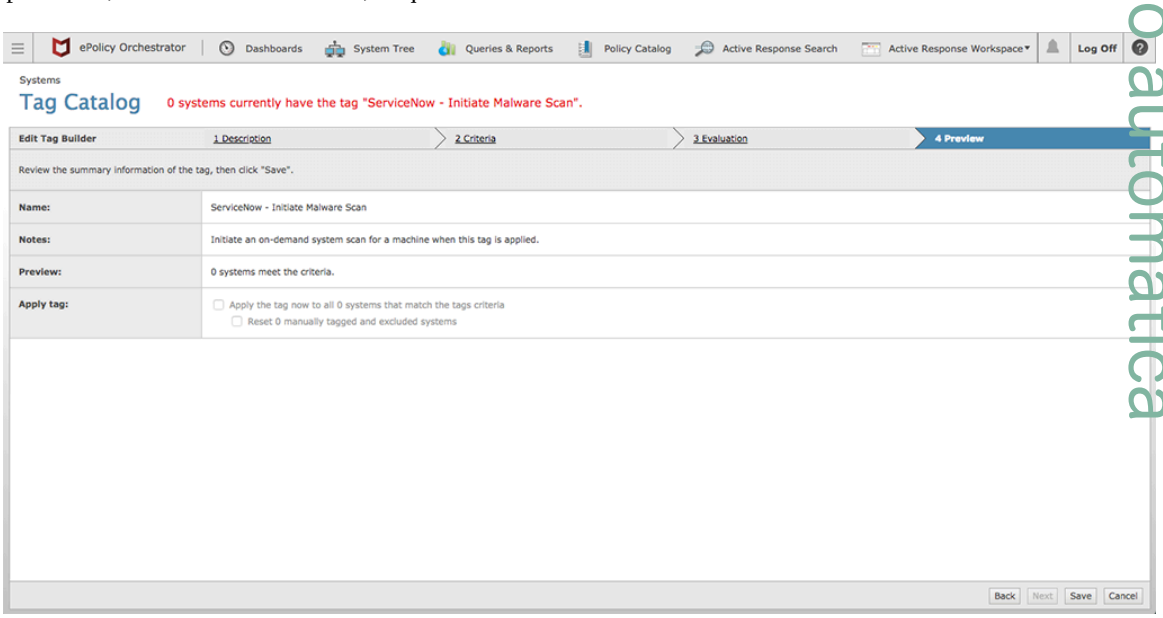
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



e. Clique em **Avaliação** na barra de andamento para continuar.



f. Com a página Catálogo de marcadores da etapa Avaliação exibida, deixe as configurações nesta página com os padrões e, na barra de andamento, clique em **Visualizar**.

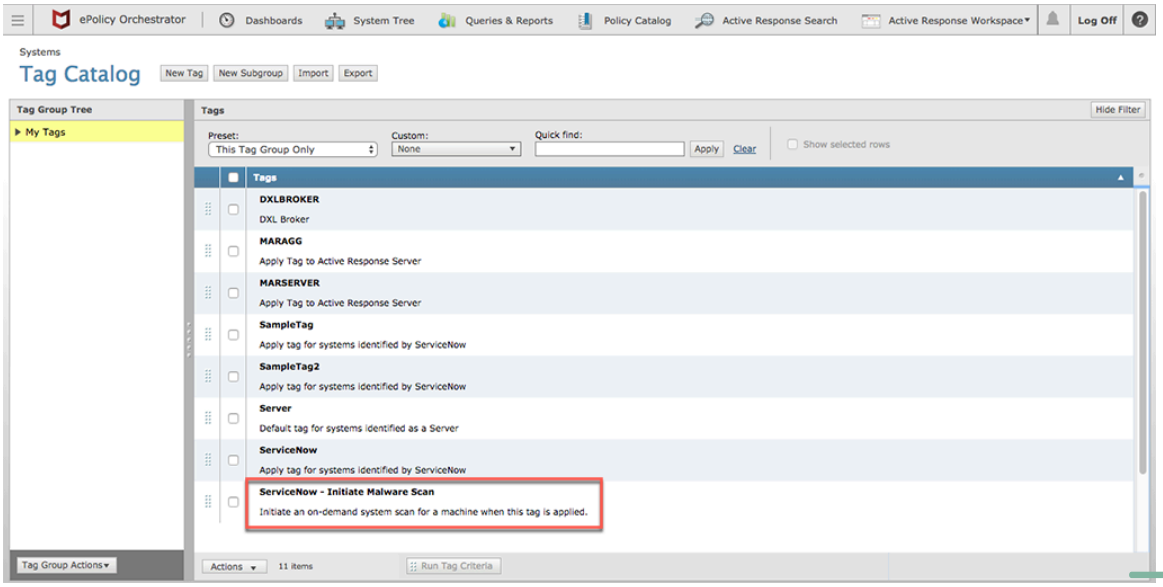


g. Com a página Visualização exibida, no canto inferior direito da página, clique em **Salvar** para salvar o registro.

Tradução automática

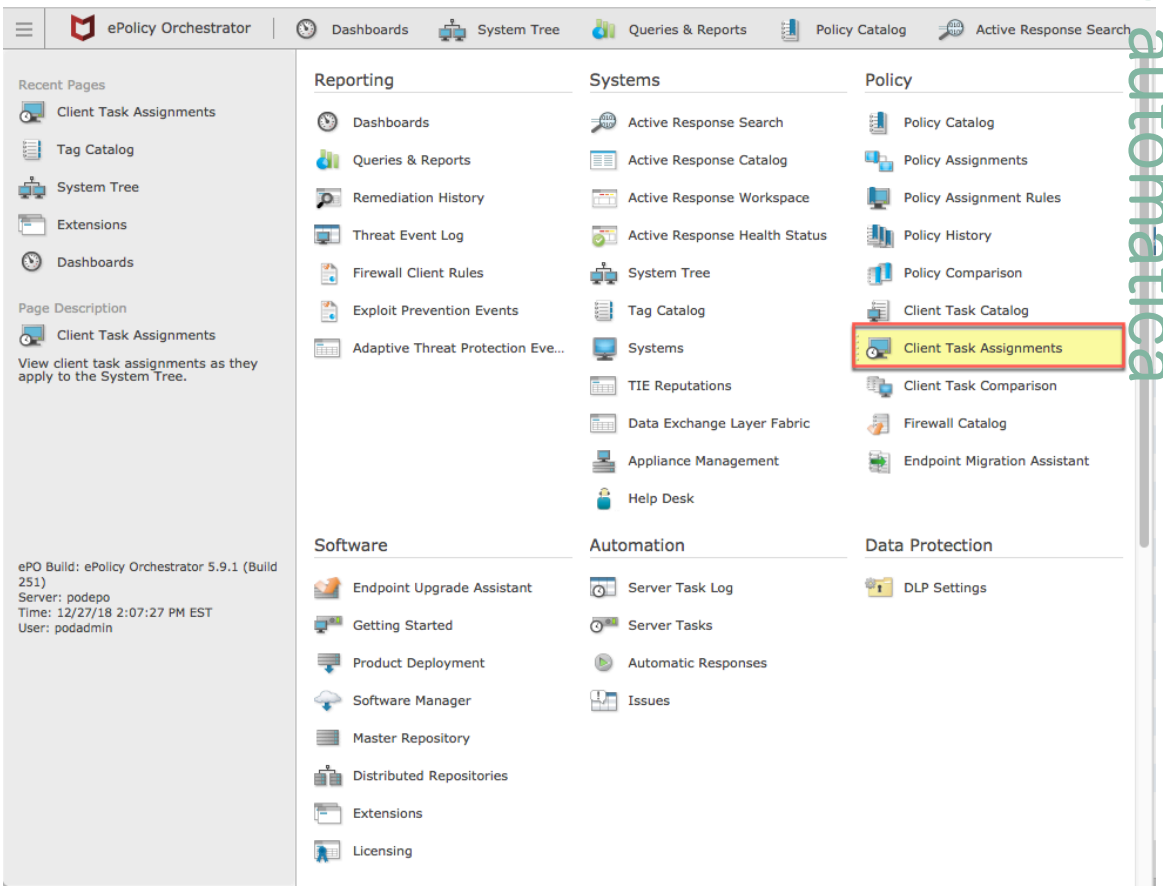
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O novo marcador é exibido no Catálogo de marcadores, conforme mostrado na figura a seguir.



7. Crie um marcador de segurança para a ação de isolamento de host repetindo as etapas anteriores. Depois de criar os dois marcadores, você está pronto para atribuir ações aos novos marcadores.
8. Para adicionar uma ação ao seu novo marcador, siga estas etapas.

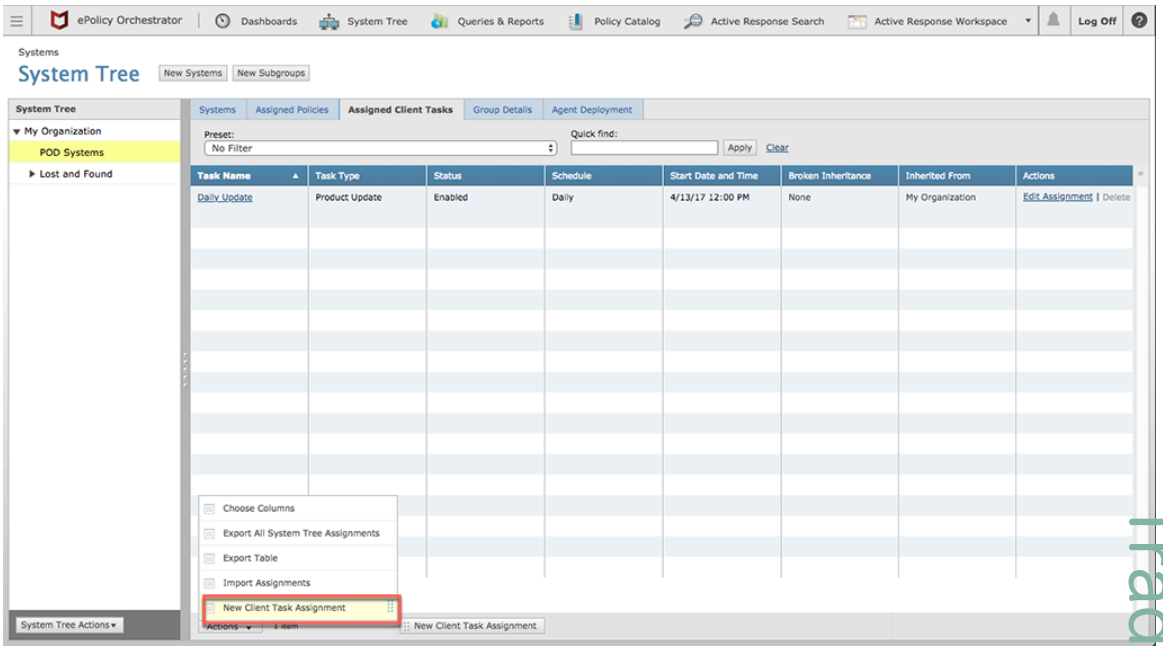
   a. Navegue até a página inicial e, na seção Política, clique no link **Atribuições de tarefa do cliente**.



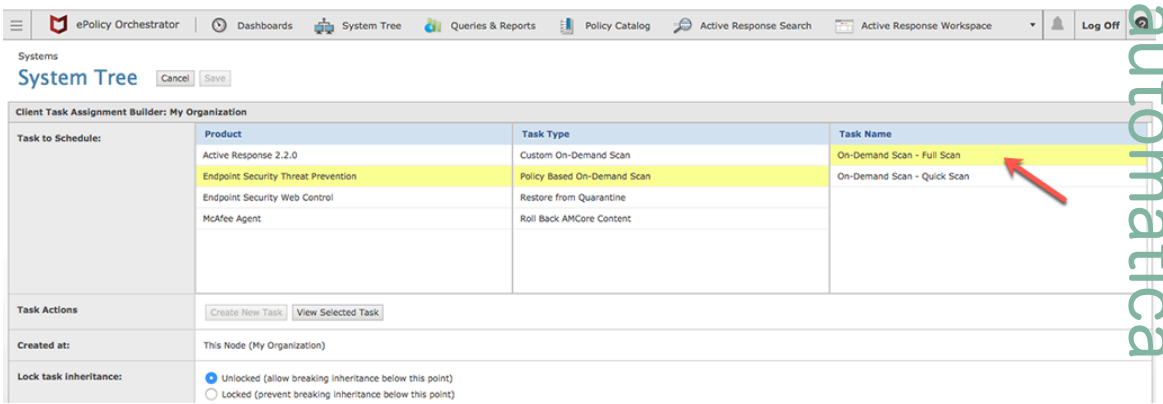
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

b. Na página Árvore do sistema exibida, na parte inferior da página, expanda o menu **Ações** e selecione **Nova atribuição de tarefa de cliente**.



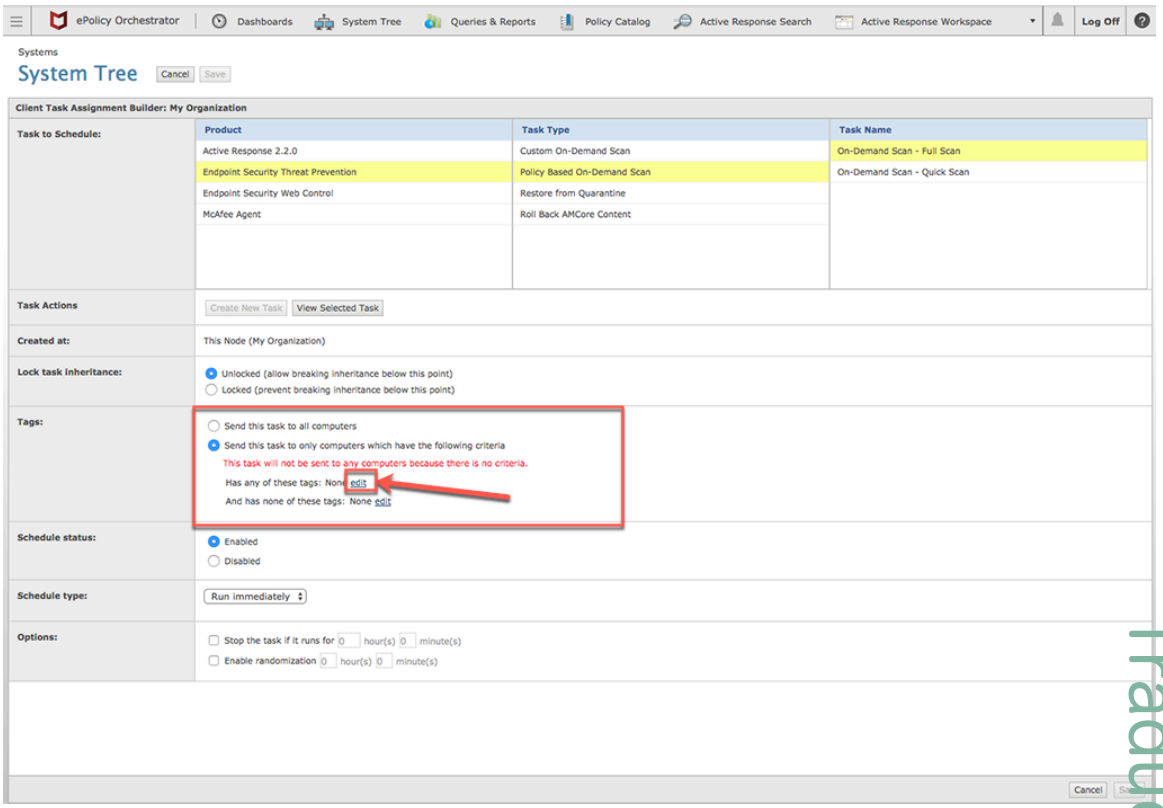
c. Na página exibida, navegue até **Prevenção de ameaças de segurança de endpoint** > **Varredura sob demanda baseada em política** > **Verificação sob demanda - Verificação completa** selecionando o caminho conforme mostrado na figura a seguir.



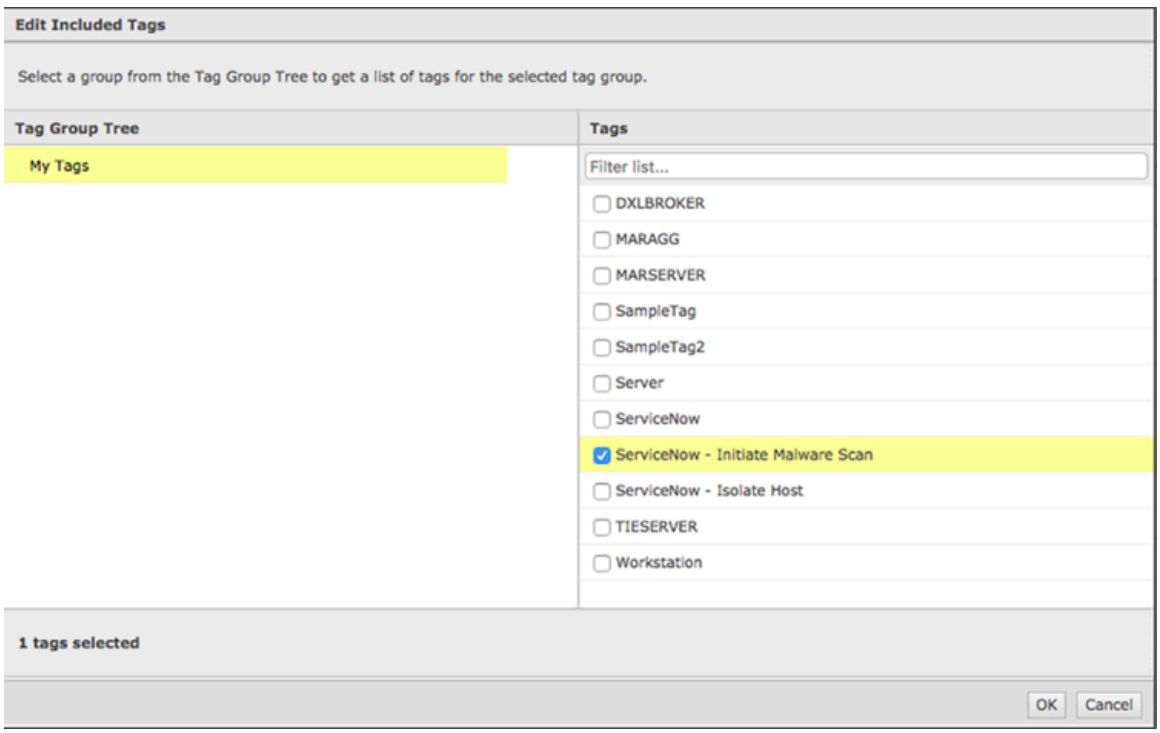
d. Na seção Marcadores, abaixo do botão de opção e ao lado de Tem um destes marcadores:, clique no link **editar** para editar os critérios do marcador.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



e. Na caixa de diálogo exibida, selecione o marcador Iniciar verificação de malware ServiceNow que você criou nas etapas anteriores e clique em **OK**.



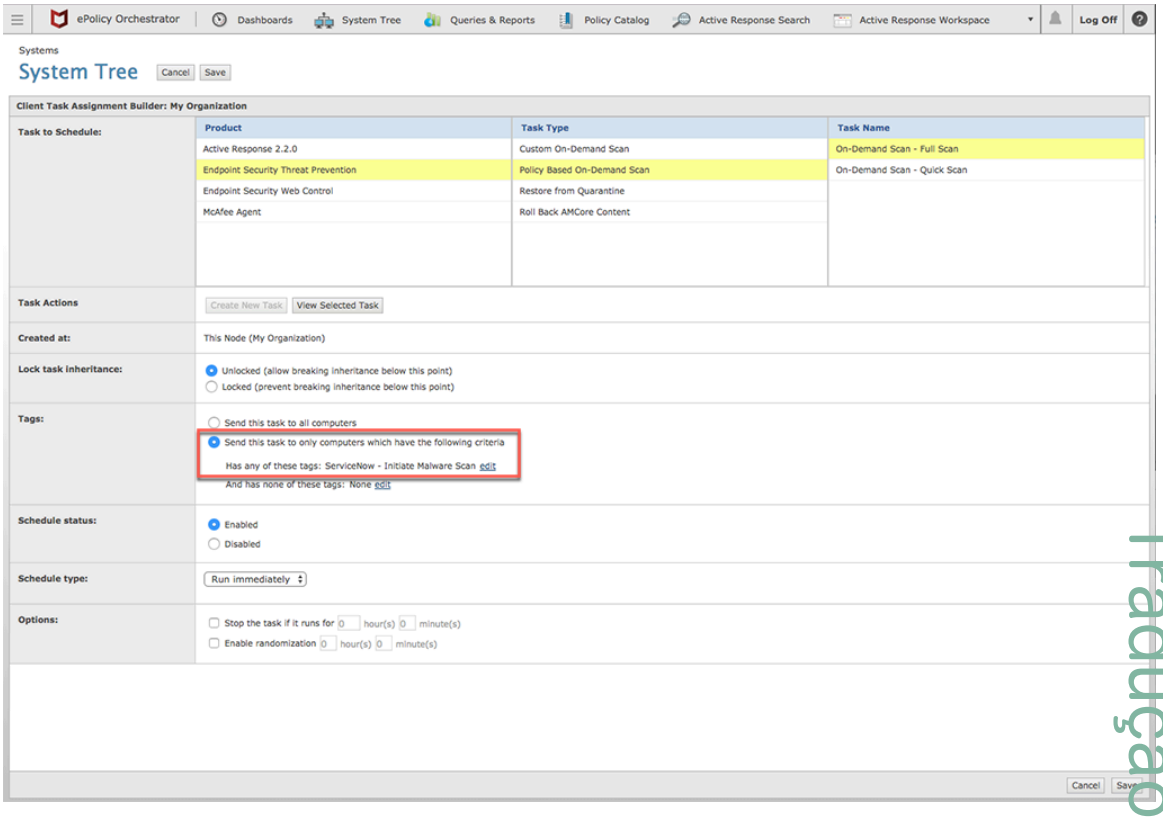
O marcador Iniciar verificação de malware da ServiceNow que você criou é atribuído à ação de verificação sob demanda.

f. Clique em **OK**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

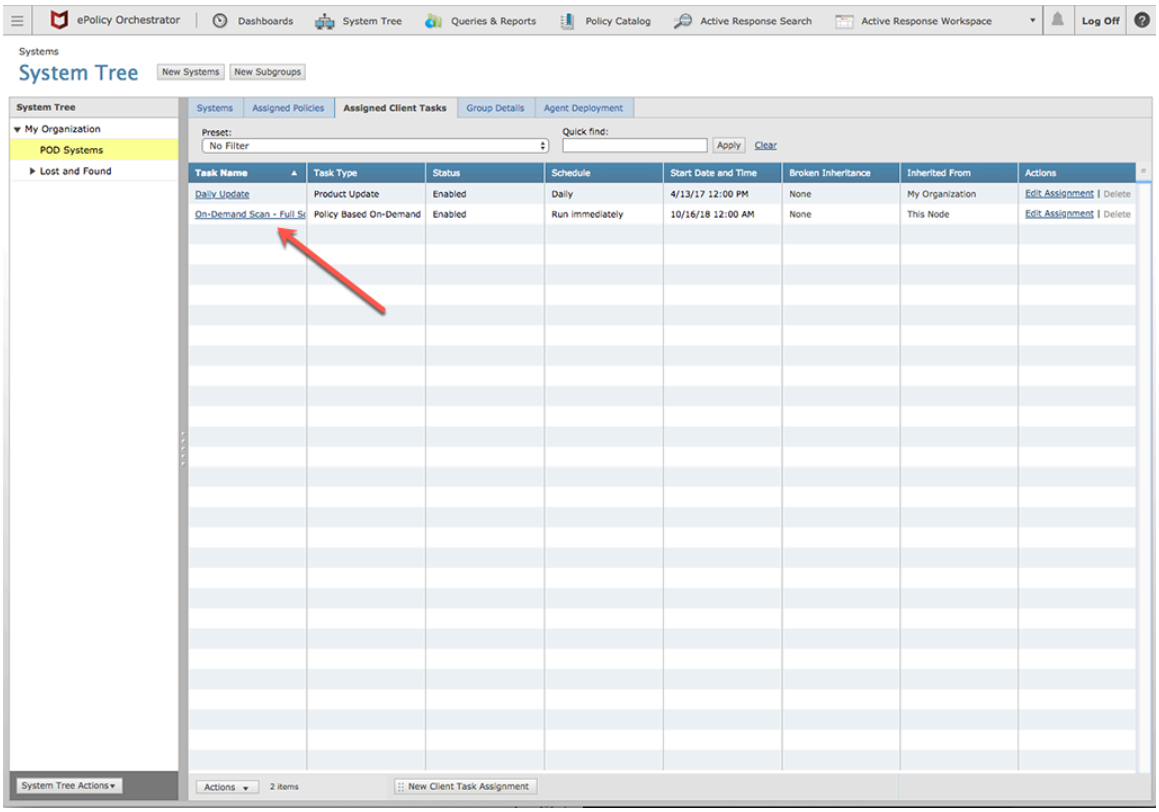
Na seção Marcadores, abaixo do botão de opção e ao lado de Tem um destes marcadores:, o marcador Iniciar verificação de malware é exibido.



g. Clique em **Salvar**.
Na página Árvore do sistema, a tarefa é exibida na lista Tarefas de cliente atribuídas (guia).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



h. Se você não atribuiu uma ação à ação Isolar Host, repita as etapas anteriores para atribuí-la.

Você instalou com sucesso o plug-in de extensão, criou marcadores de segurança e atribuiu tarefas aos seus marcadores. Você concluiu a configuração da integração no console do McAfee ePO. A próxima etapa é configurar um servidor na sua instância Now Platform.

Instalar a aplicação e configurar um servidor para a integração McAfee ePO

Antes de invocar os fluxos de trabalho para a integração, instale e configure a aplicação McAfee ePO do ServiceNow Store na sua instância Now Platform. A configuração é necessária para se conectar ao console McAfee ePO.

Antes de Iniciar

Função necessária: Now Platform administrador (admin)

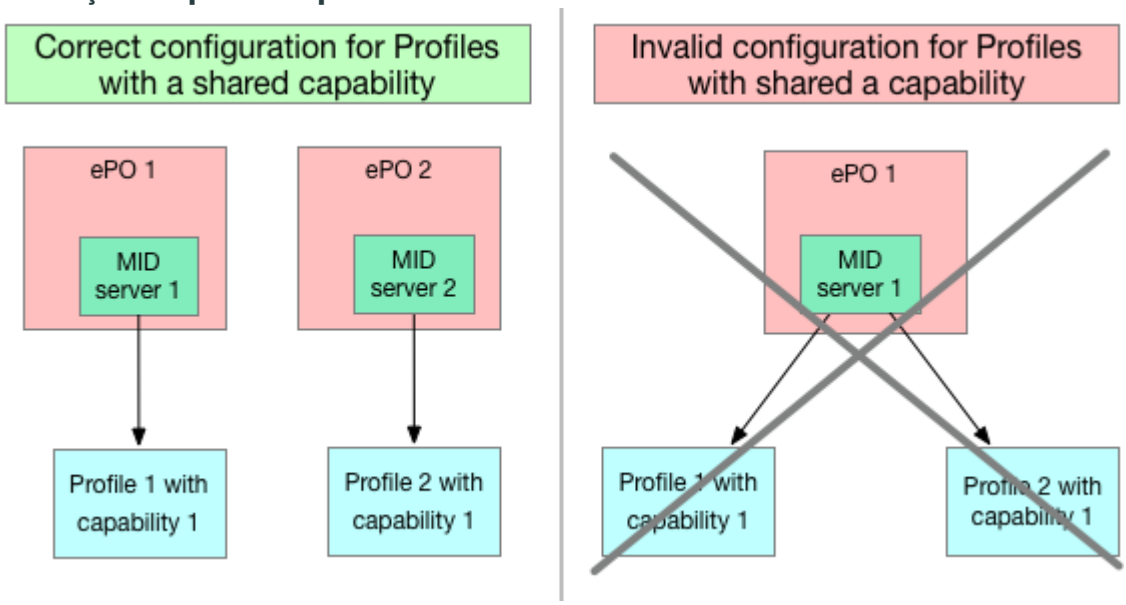
Por Que e Quando Desempenhar Esta Tarefa

A integração oferece suporte a vários servidores. No entanto, para evitar conflitos em perfis que compartilham as mesmas condições de gatilho, você não pode compartilhar um recurso McAfee ePO com vários perfis que usam o mesmo servidor McAfee ePO. Por exemplo, conforme mostrado na figura a seguir, você pode ter a capacidade 1 em mais de um perfil, desde que cada servidor McAfee ePO seja mapeado para um perfil exclusivo que tenha a capacidade 1.

Tradução automática

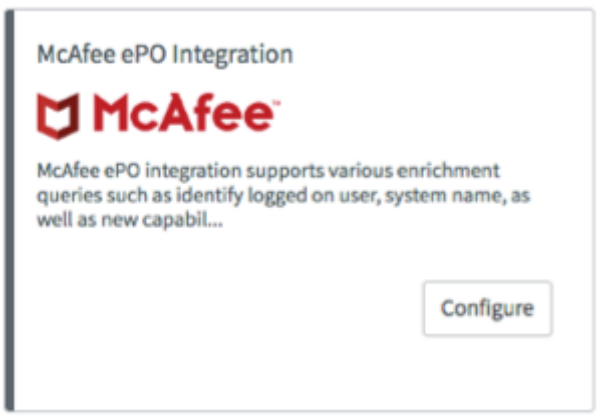
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Limitações do perfil compartilhado da McAfee



Procedimento

1. Baixe o McAfee ePO para Security Operations do ServiceNow Store e instale-o.
2. Navegar até **Security Operations** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco de integração McAfee ePO para Security Operations e clique em **Configurar**.



4. No formulário, preencha os campos.

Configuração de integração do McAfee ePO

Campo	Descrição
Nome	Nome da integração, por exemplo, `demo-1`.
Nome do Servidor do ePO	Nome do servidor McAfee ePO. Se você usar um servidor, um exemplo é o `McAfee HQ` (sede do McAfee). Este nome é como o servidor e as credenciais relacionadas são reconhecidos.

Tradução automática

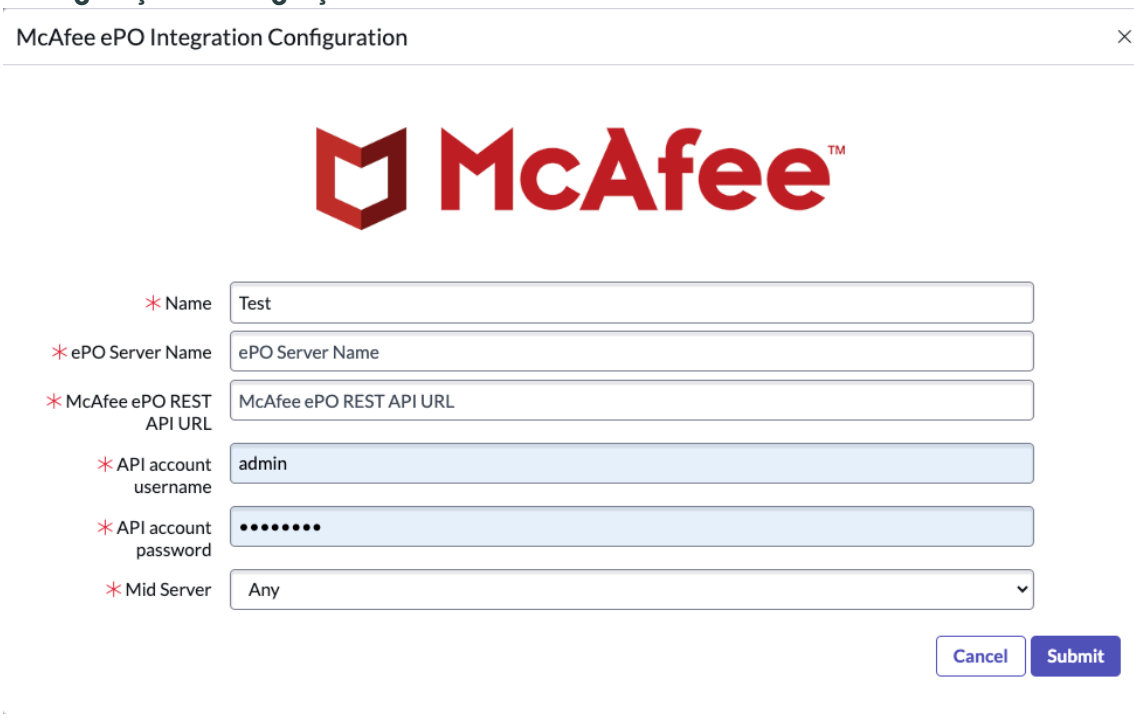
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Se sua organização requer suporte para vários servidores, insira o nome de cada servidor e repita o processo.
URL da REST API do McAfee ePO	URL base que hospeda a REST API McAfee ePO. Insira o URL com o protocolo https://, por exemplo, `https://corp.epo_server:8443`.
Nome de usuário da conta da API	Nome de usuário exclusivo da conta, por exemplo, `API da ServiceNow`.
Senha da conta da API	Senha exclusiva para a conta da API.
MID Server	Selecione o nome do MID Server que você configurou durante a configuração da sua instância Now Platform. Você pode selecionar um MID Server específico na lista ou selecionar **Qualquer** para habilitar a seleção automática de um MID Server válido na lista para esta integração. **Nota:** ○ O MID Server selecionado durante este tempo de configuração se aplica a esta integração. ○ Somente os MID Servers que estão ativos e validados são exibidos nesta lista. Por padrão, o valor é definido como **Qualquer**. Um nome de exemplo é, `secops_local_midserver`.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de integração do McAfee ePO



5. Clique em **Enviar**.
   A lista de Configurações do McAfee ePO é exibida com seu novo registro de configuração. Você concluiu com sucesso a configuração de um servidor McAfee ePO.

> **Nota:**
> Se sua organização requer suporte para vários servidores, repita as etapas.

Editar marcadores de segurança no Now Platform para a integração McAfee ePO

Como parte da configuração da integração, edite os nomes dos marcadores de segurança que você criou no console Now PlatformMcAfee ePO na instância []. Edite os nomes de marcador na instância Now Platform para que eles correspondam aos nomes dos marcadores no console McAfee ePO.

Antes de Iniciar

Função necessária: Now Platform administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

Os nomes dos marcadores de segurança no console McAfee ePO para iniciar a verificação de malware e isolar as ações de host devem corresponder aos nomes dos marcadores de segurança nos registros desses recursos da sua instância Now Platform.

Antes de criar um perfil de recurso para executar seus recursos, exiba a lista de recursos McAfee ePO disponíveis e edite os marcadores de segurança em sua instância Now Platform para que eles correspondam aos nomes de marcador de segurança no console McAfee ePO.

Para obter mais informações sobre como criar os nomes dos marcadores de segurança no console do McAfee ePO, consulte Configure seu console McAfee ePO para integrar com Security Incident Response (SIR).

Tradução automática

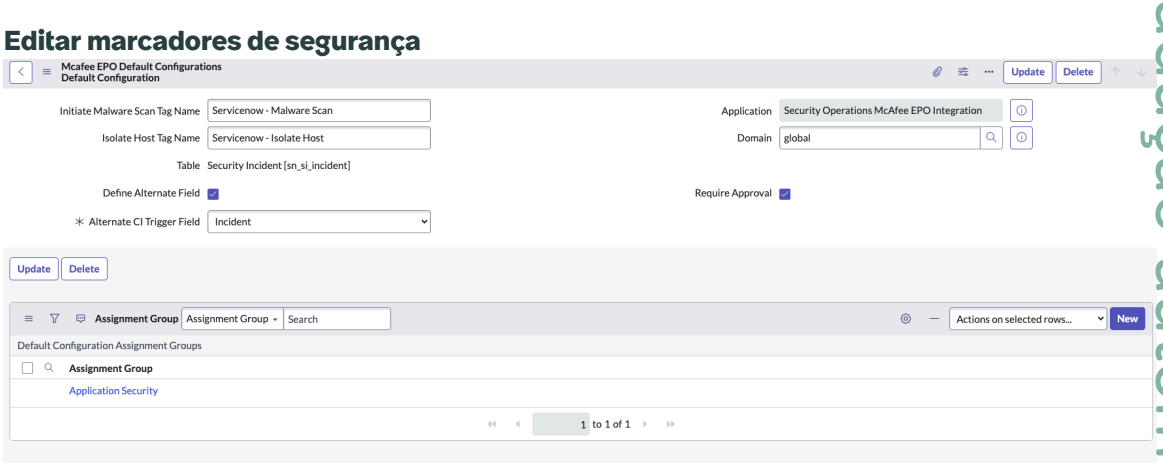
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Integração do McAfee ePO** > **Configurações Padrão**.
2. Para editar o nome do marcador de segurança da integração McAfee ePO, clique em **Configuração padrão**.

   Nota:
   Garante que você execute esta configuração depois de instalar a integração McAfee ePO.

3. No campo Iniciar nome do marcador de verificação de malware, insira o nome do marcador de segurança que você criou no console McAfee ePO para a ação de iniciar verificação.
   Por exemplo, ServiceNow - Verificação de malware
4. No campo Isolar nome do marcador de host, insira o nome do marcador de segurança que você criou no console McAfee ePO para a ação isolar host.
   Por exemplo, ServiceNow - Isolar Host
5. Se você não quiser usar o campo de gatilho de IC na criação do incidente, marque a caixa de seleção **Definir campo alternativo**.
   Quando esta opção está habilitada, a lista de seleção do campo de gatilho de IC alternativo é exibida.



6. Escolha um campo alternativo na lista de seleção para verificar seus critérios de pesquisa de IC.
   Para este exemplo, como usuário com a função sn_si.admin, você acredita que o campo IC não será preenchido no incidente de segurança após a criação do incidente. Como alternativa, você acha que as informações de IC para um FQDN, nome de host ou endereço IP serão preenchidas no campo IC identificado no incidente de segurança e seleciona o campo IC identificado como uma alternativa. O IC Identificado é selecionado para este exemplo, mas você pode usar qualquer campo no incidente de segurança para o IC alternativo.
7. No campo Domínio, selecione um domínio ou grupo para esta configuração usando a opção de pesquisa.
   Por exemplo, global.
8. No campo Requer aprovação, marque a caixa de seleção **Requer aprovação** se você estiver usando os recursos Isolar host e Remover isolamento.

   Nota:
   As capacidades Iniciar verificação de malware, Listar eventos de ameaça e Obter detalhes do sistema não precisam de aprovação.

9. Clique em **Atualizar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O nome do marcador do EPO é atualizado e exibido na lista de configurações padrão do McAfee ePO. O nome do marcador de segurança para a ação de verificação de malware na instância Now Platform corresponde ao nome da verificação no console McAfee ePO.

Você editou com sucesso os nomes de marcador do EPO para a verificação de malware e os recursos de host isolado em sua instância Now Platform. A próxima etapa é criar um perfil para seus recursos.

Tópicos relacionados

Documentação de produto da McAfee

Criar um grupo de aprovação

Crie um grupo de aprovação para a integração McAfee ePO para Security Operations que pode aprovar solicitações para isolar máquinas host, restaurando-as na rede.

Antes de Iniciar

Você não pode reatribuir a autoridade de aprovação a um grupo, a menos que um grupo de aprovação esteja disponível em sua instância.

Nota:
A opção de aprovações em Configurando perfis para a integração McAfee ePO aparece somente para as capacidades Isolar Host e Remover Isolamento de Host.

Função necessária: Now Platform® Administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

As solicitações de aprovação enviadas pelo analista de incidentes de segurança para isolar máquinas host e remover o isolamento são atribuídas ao usuário com a função sn_si.admin por padrão. Como usuário com esta função, você pode reatribuir esta autoridade de aprovação durante a etapa de configuração de um perfil. Antes de reatribuir autoridade a um grupo de aprovação, um grupo de aprovação deve estar disponível na lista Grupos na sua instância Now Platform.

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Grupos**.
2. Na lista de grupos, clique em **Novo**.
3. No formulário, preencha os campos.

Formulário de grupo de aprovação

Campo	Descrição
Nome	Nome do grupo exibido quando uma solicitação de aprovação é enviada, por exemplo, Aprovadores Isolamento de host da McAfee.
E-mail do grupo	Lista de distribuição de e-mail do grupo ou o endereço de e-mail do ponto de contato, como o gerente do grupo, McAfeeapproval@servicenow.com
Gerente	Nome do gerente do grupo. Clique no ícone de pesquisa para exibir a lista.
Primário	(Opcional) Outro grupo do qual este grupo é membro, se este grupo tiver um primário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição	Informações adicionais sobre este grupo.
Incluir membros	Opção para incluir membros neste grupo.
Designado padrão	Opção para escolher um usuário como designado padrão para este grupo. Use a opção Pesquisar para abrir a lista de usuários.
Funções	Opção para selecionar as funções para este grupo. Use a opção Adicionar e Remover para adicionar e remover funções.
Tipo	Opção para escolher uma categoria para este grupo. Use a opção Pesquisar para abrir a lista de tipos de grupo.
Fornecedores	Opção para escolher um fornecedor para este grupo. Use a opção Pesquisar para abrir a lista de fornecedores.

4. Clique em **Enviar**.
   O novo grupo é exibido na lista Grupos.

Este grupo está disponível para processar solicitações quando você habilita a opção **Requer aprovação** durante a configuração deste perfil.

Para monitorar e processar solicitações enviadas por usuários com a função sn_si.analyst, cada membro do grupo de aprovação navega até a guia **Minhas aprovações** no Now Platform.

McAfee ePO perfis de capacidade de integração

Como um usuário com a função de administrador de incidentes de segurança (sn_si.admin), você cria perfis para os recursos McAfee ePO em sua instância Now Platform®. Você agrupa consultas ou ações em perfis e determina quais McAfee ePO recursos deseja executar quando um novo incidente de segurança for criado.

Perfis de capacidade

Você cria perfis™ para poder agrupar McAfee ePO recursos e definir as configurações desses recursos da sua instância Now Platform®. Você tem a flexibilidade para criar vários perfis para esses recursos, o que permite determinar quais ações ou consultas são invocadas quando um incidente Security Incident Response (SIR) é criado. Para atender às necessidades da sua organização, você pode criar um único perfil que executa consultas para obter detalhes do sistema, inicia verificações de malware e isola máquinas host, por exemplo, ou você pode criar vários perfis, cada um com sua própria capacidade McAfee ePO.

Tipos de perfil e capacidades McAfee ePO necessárias

Finalidade primária do seu perfil	Configurar requisitos	Capacidades do McAfee ePO necessárias para este tipo de perfil
Reunir detalhes do sistema	Nenhum(a)	**Obter detalhes do host**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tipos de perfil e capacidades McAfee ePO necessárias

Finalidade primária do seu perfil	Configurar requisitos	Capacidades do McAfee ePO necessárias para este tipo de perfil
Isolar um host	Verifique com o administrador McAfee ePO se você criou os marcadores de segurança para a ação isolar host no console McAfee ePO. Para obter mais informações, consulte Configure seu console McAfee ePO para integrar com Security Incident Response (SIR).	**Isolar Host**
Verifique e pesquise ameaças no seu host	Verifique com o administrador McAfee ePO se você criou os marcadores de segurança para a ação iniciar verificação de malware no console McAfee ePO. Para obter mais informações, consulte Configure seu console McAfee ePO para integrar com Security Incident Response (SIR).	**Iniciar verificação de malware** **Nota:** Como parte da verificação de malware McAfee ePO, o recurso Listar eventos de ameaça é invocado automaticamente. No entanto, você não precisa adicionar o recurso Listar eventos de ameaça ao perfil com o recurso de verificação de malware. Os resultados da verificação de malware são exibidos na guia Detalhes do evento de ameaça no incidente de segurança.
Remover isolamento de um host	Verifique com o administrador McAfee ePO se você criou os marcadores de segurança para a ação isolar host no console McAfee ePO. Para obter mais informações, consulte Configure seu console McAfee ePO para integrar com Security Incident Response (SIR).	**Remover isolamento**
Reúna dados de aprimoramento de ameaça.	Nenhum(a)	**Listar eventos de ameaça**

Criar um perfil de capacidade para a integração McAfee ePO

Crie um perfil e selecione os recursos McAfee ePO que você deseja que o perfil execute.

Tradução automática

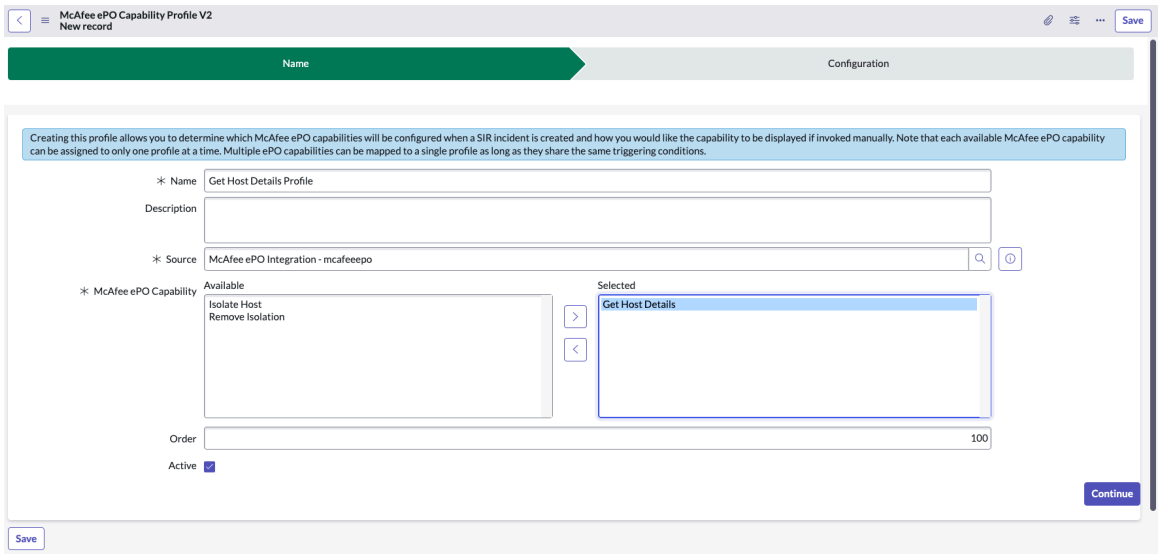
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: Now Platform® Administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa
Para esta etapa da configuração, você cria um perfil para os recursos McAfee ePO. Ao criar perfis, considere a intenção do perfil antes de adicionar recursos McAfee ePO a ele. Consulte a tabela a seguir ao criar perfis.

A tabela a seguir lista os recursos que você precisa adicionar a um perfil se quiser que o perfil execute determinadas consultas ou ações. Crie um único perfil que execute consultas para obter detalhes do host, inicie verificações de malware, remova o isolamento e isole as máquinas host ou crie vários perfis, cada um com sua própria capacidade única.

Procedimento
1. Navegar até **Integração do McAfee ePO** > **Perfis de capacidade do McAfee ePO**.
   A lista de Perfis de capacidade McAfee ePO é exibida.
2. Clique em **Nova**.
3. No formulário, preencha os campos.



4. Para salvar e validar o perfil, clique em **Continuar**.
   Se a validação for bem-sucedida, a página será recarregada e o formulário de **configuração** será exibido.

O que Fazer Depois
A próxima etapa é configurar seu perfil. Antes de definir as configurações do perfil, talvez você prefira revisar os conceitos de configuração de perfis e condições de gatilho. Para obter mais informações, consulte Configure seu console McAfee ePO para integrar com Security Incident Response (SIR) e Definir condições de gatilho com um campo Item de configuração (IC) para um perfil McAfee ePO.

Definir condições de gatilho com um campo Item de configuração (IC) para um perfil McAfee ePO

Depois de criar um perfil e selecionar os recursos McAfee ePO que deseja que o perfil execute, defina as configurações do perfil para que ele seja executado somente quando um conjunto de condições específicas for atendido.

Tradução automática

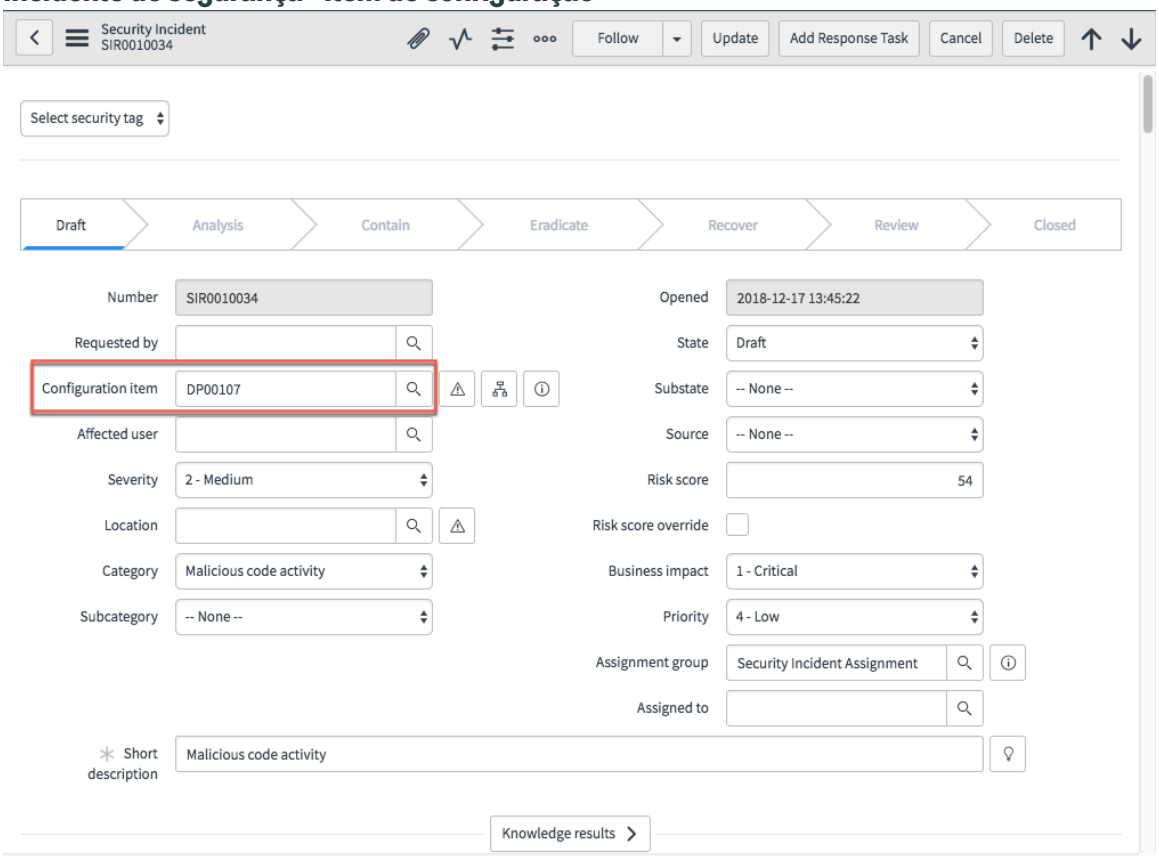
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você tem a flexibilidade de definir essas condições de gatilho para que o perfil seja executado automaticamente com base nos valores de campo padrão que correspondem a um incidente de segurança Now Platform® Security Incident Response. Como alternativa, você pode configurar um perfil para que ele pesquise correspondências nos valores de campo que você identificar especificamente no incidente de segurança.

Uma das chaves para a funcionalidade da integração e como um perfil funciona é o campo Item de configuração (IC) no incidente de segurança Now Platform® Security Incident Response (SIR). O valor deste campo é o valor principal em um incidente de segurança. Este valor é usado para corresponder os IDs de seus ativos às informações armazenadas no banco de dados Now Platform®. Quando um incidente de segurança SIR é criado por um evento de segurança e um perfil é ativado, seus ativos são verificados quanto a um valor correspondente para um nome de domínio totalmente qualificado (FQDN), um nome de host ou um endereço IP com base no valor de o campo Item de configuração.

Em um caso ideal, um valor correspondente é encontrado no banco de dados e os dados podem ser coletados do console McAfee ePO para o ativo correspondente, puxados para sua instância Now Platform® e exibidos nas listas relacionadas de um incidente de segurança. A figura a seguir mostra um exemplo do campo Item de configuração preenchido com um nome de host em um incidente de segurança SIR.

Incidente de segurança - Item de configuração



Nos casos em que o campo Item de configuração (IC) não estiver preenchido no incidente de segurança, ou uma correspondência não puder ser encontrada para um FQDN, um nome de host ou um endereço IP que corresponda ao banco de dados, você poderá selecionar um campo alternativo na segurança incidente para exibir todos os dados de aprimoramento de IC correspondentes encontrados durante a verificação de seus ativos.

Durante a etapa de configuração da configuração do perfil, você pode selecionar um campo de gatilho de IC alternativo para identificação de endpoint para garantir que os dados de

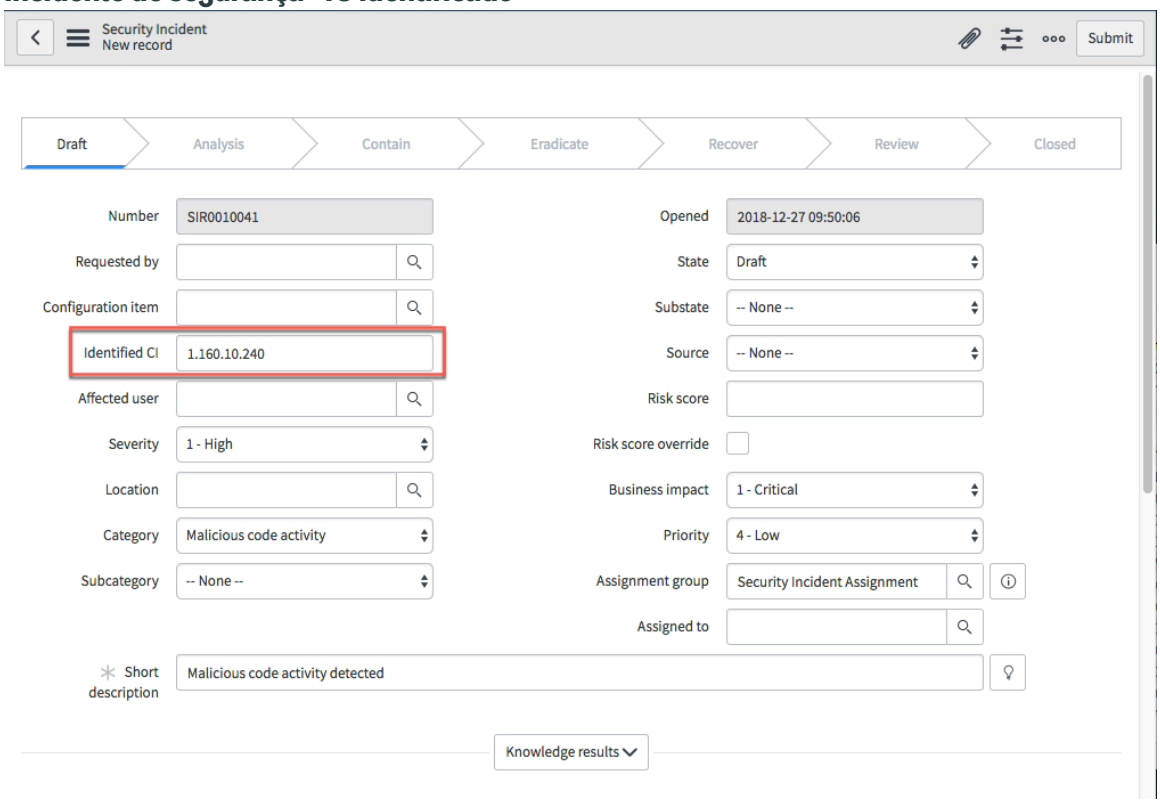
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

aprimoramento de IC da pesquisa McAfee ePO sejam preenchidos no incidente de segurança associado. Você pode selecionar qualquer campo no incidente de segurança como um campo de gatilho de IC alternativo, incluindo campos personalizados que você cria. Ao selecionar este campo de IC alternativo como backup, você garante que seus perfis sejam executados mesmo se o campo de IC não estiver preenchido no incidente de segurança associado na criação do incidente.

Por exemplo, como analista do centro de operações de segurança (SOC), você cria um campo personalizado para um incidente de segurança chamado Endereço IP no meu incidente de segurança. Se você achar que o valor deste campo personalizado não será exibido no campo Item de configuração no incidente de segurança após a criação do incidente, configure o perfil para que ele verifique esse endereço IP. Se correspondido, o endereço IP será exibido no incidente de segurança no campo de sua escolha. Na figura a seguir, o campo IC identificado é selecionado como o campo alternativo para o Endereço IP para este exemplo.

Incidente de segurança - IC identificado

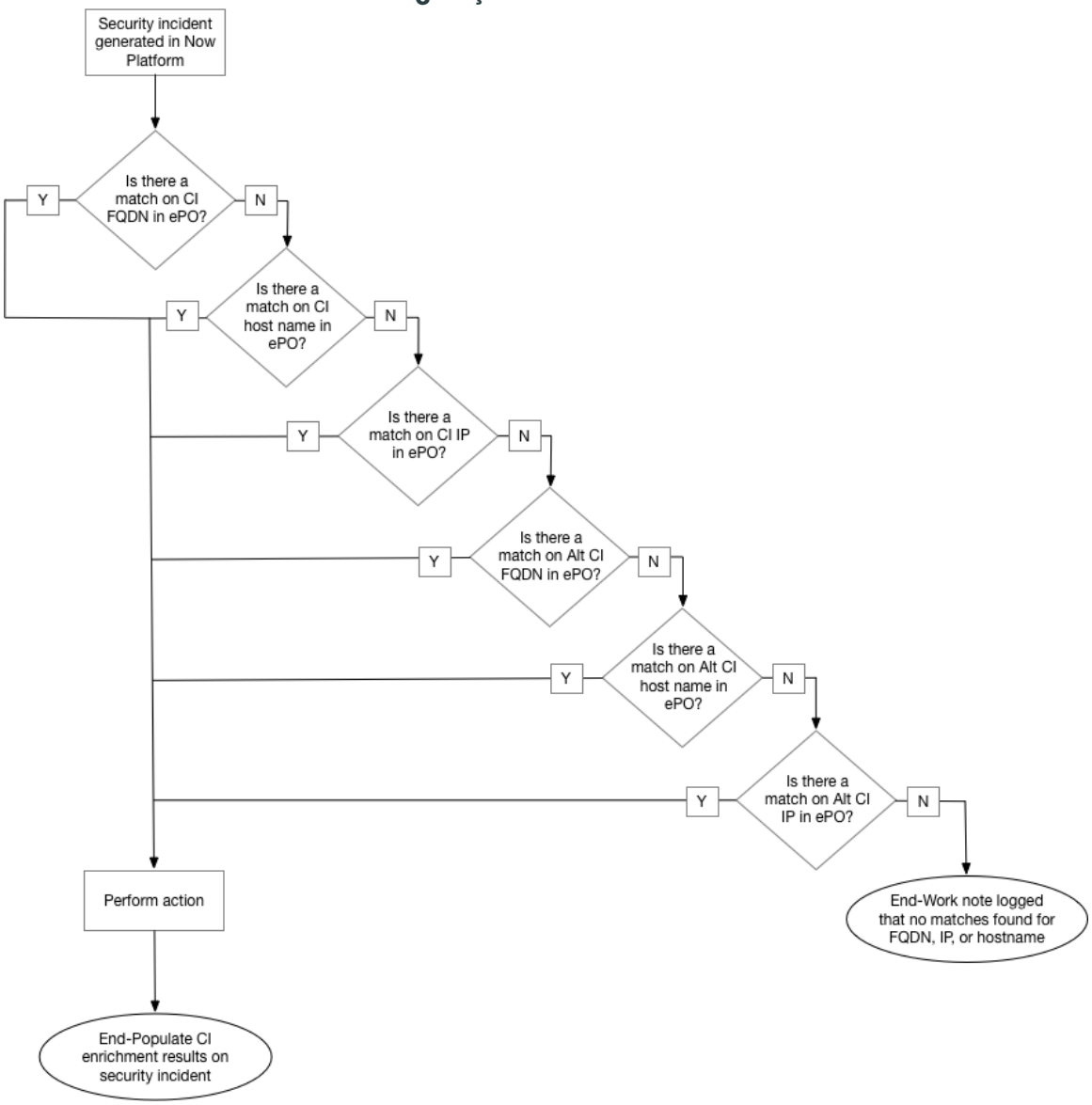


A figura a seguir ilustra como a primeira pesquisa do fluxo de trabalho verifica correspondências para itens de configuração. Se o campo Gatilho de IC alternativo estiver habilitado, a segunda pesquisa verificará correspondências para valores alternativos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de itens de configuração



Se os IDs correspondentes não forem encontrados para o campo de IC ou o campo de IC alternativo, uma anotação de trabalho será registrada e uma mensagem será exibida no incidente de segurança. Quando nenhuma correspondência é encontrada, nenhum dado de aprimoramento é preenchido nos incidentes de segurança relacionados ao evento.

Você habilita o campo de gatilho de IC alternativo e seleciona o campo no qual deseja exibir o ID correspondente durante a etapa de configuração de um perfil. Esta etapa para habilitar o campo de IC alternativo é descrita junto com os outros requisitos de configuração de perfil em Configurando perfis para a integração McAfee ePO.

Configurando perfis para a integração McAfee ePO

Depois de criar um perfil e selecionar os recursos McAfee ePO que você deseja que o perfil execute, defina as configurações para que o perfil seja invocado somente sob as condições específicas que você definir.

Configurando um perfil

Nesta etapa, você configura um perfil de recurso para que ele seja executado somente quando as condições especificadas forem atendidas. Você define quais condições em

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

incidentes de segurança acionam automaticamente os recursos McAfee ePO que você selecionou para o perfil. Você também tem a opção de selecionar um campo de entrada alternativo para o campo Item de configuração (IC) e definir condições de filtragem para que somente os incidentes de segurança relacionados ao evento de acionamento iniciem automaticamente o perfil. A etapa de configuração inclui as seguintes configurações no formulário de configuração do perfil.

Campo de gatilho de item de configuração (IC) alternativo

Nos casos em que o campo Item de configuração (IC) no incidente de segurança Now Platform® Security Incident Response (SIR) não estiver preenchido com um valor ou uma correspondência não puder ser encontrada no banco de dados, você poderá selecionar um campo alternativo no incidente de segurança para exibir qualquer dados de aprimoramento de IC correspondentes encontrados durante a verificação de seus ativos. Para obter mais informações sobre os campos Item de configuração e Item de configuração alternativo em um incidente de segurança, consulte Definir condições de gatilho com um campo Item de configuração (IC) para um perfil McAfee ePO.

Marcadores de segurança

Para ajudá-lo a rastrear o status das máquinas host isoladas e quando as verificações de malware são iniciadas, um recurso de marcação opcional está disponível. Por padrão, esta opção está desabilitada no formulário de configuração dos perfis. Se esta opção for habilitada durante a etapa de configuração, os nomes dos marcadores de segurança serão exibidos no formulário de configuração. Estes são os nomes dos marcadores exibidos em incidentes de segurança relacionados. Esses marcadores informam quando uma ação de isolamento de host é iniciada com sucesso e quando é aprovada. Depois que um host é retornado à rede com sucesso, o marcador de segurança é removido automaticamente do incidente de segurança. Para verificações de malware, um marcador é exibido no incidente de segurança relacionado quando uma verificação é programada. Depois que a verificação for concluída, o marcador programado será substituído automaticamente por um marcador que indica que a verificação foi concluída com sucesso.

Acionar automaticamente com base no incidente

Quando a opção Acionar automaticamente com base no incidente está habilitada, o construtor de condição de filtro está disponível e você deve definir condições de filtragem que especificam quando o perfil é executado automaticamente. Um filtro comum é Categoria é atividade de código malicioso™ e Impacto nos negócios é 1 - Crítico™. Com esses filtros, somente os incidentes de segurança relacionados ao código mal-intencionado e que têm um impacto crítico nos negócios iniciam o perfil. Usar a opção Gatilho automático pode reduzir o número de incidentes de segurança que invocam automaticamente o perfil.

Aprovações

Se sua organização deseja um nível extra de controle sobre ações como isolar máquinas host e iniciar verificações de malware, você pode habilitar a opção Requer aprovação durante a etapa de configuração de um perfil.

Por exemplo, se os recursos de aprovação e marcação estiverem habilitados para um perfil, depois que uma solicitação para isolar uma máquina host ou devolvê-la à rede for enviada para aprovação, o incidente de segurança associado será marcado automaticamente para que a ação seja iniciada. As solicitações são enviadas para aprovação a um usuário com a função sn_si.admin por padrão, mas essa aprovação pode ser reatribuída a outro indivíduo ou a um grupo de aprovação para atender às necessidades da sua organização. Os aprovadores processam solicitações em **Minhas aprovações** em suas instâncias

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Now Platform®. Os marcadores de segurança são exibidos em incidentes de segurança relacionados. Todas as atividades de fluxo de trabalho também são registradas em anotações de trabalho para criar uma trilha de auditoria.

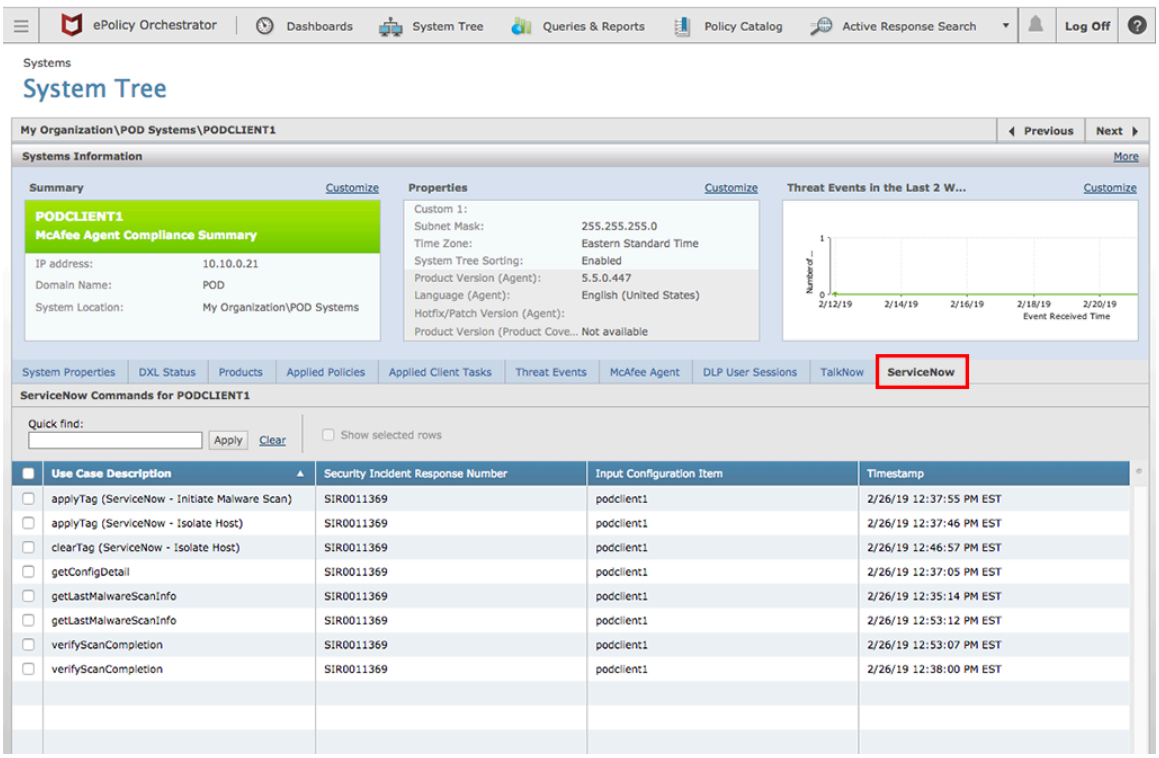
ServiceNow log de auditoria no console McAfee ePO

Na versão 5.10.0 de McAfee ePO, uma guia ServiceNow é exibida com um log de comandos que são iniciados a partir da sua instância Now Platform®. Depois que uma ação ou consulta é invocada de um perfil em sua instância Now Platform® em uma máquina host (endpoint) no console McAfee ePO, um log de auditoria de comandos ServiceNow é criado no console McAfee ePO. Este log é exibido na árvore do sistema no console McAfee ePO e ajuda a auditar os horários dos comandos que são enviados para endpoints específicos. Para exibir eventos ServiceNow registrados em máquinas específicas em um console McAfee ePO, siga estas etapas.

1. Navegue até a Árvore do sistema no console McAfee ePO e localize a guia ServiceNow.
2. Clique na guia para abrir uma lista de máquinas host.
3. Na coluna Nome, clique em um nome de host para abrir o log de auditoria.

Na imagem a seguir, um exemplo de log de um host (PODCLIENT1) é exibido.

Cliente do PODC



Os eventos iniciados a partir dos perfis na sua instância Now Platform® são registrados e exibidos no log. Verificando o status da máquina host, verifique se os eventos listados no log foram concluídos com sucesso no host.

Perfis de exemplo

Os tópicos a seguir incluem exemplos de como configurar perfis e testar incidentes de segurança. Esses exemplos incluem perfis para todos os recursos McAfee ePO que estão disponíveis para esta integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar perfis e incidentes de segurança para consultas de aprimoramento do sistema para a integração McAfee ePO

Defina as configurações de perfil para que o perfil seja acionado somente nas condições que você definir.

Antes de Iniciar

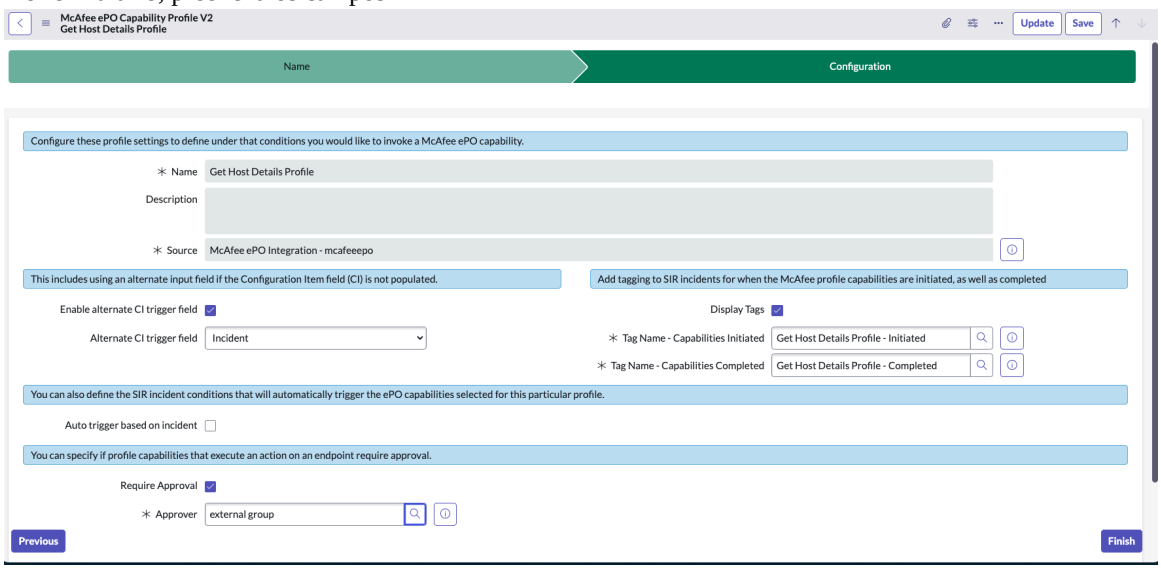
Função necessária: Now Platform® administrador de incidentes de segurança (sn_si.admin)

Por Que e Quando Desempenhar Esta Tarefa

Defina as condições que acionam automaticamente os recursos McAfee ePO que você selecionou para o perfil. Você também pode selecionar um campo de entrada alternativo para o campo Item de Configuração (IC). Neste campo alternativo, você pode definir condições de filtragem para que somente os incidentes de segurança relacionados ao evento de acionamento acionem automaticamente o perfil.

Procedimento

1. Se a página Configuração não for exibida, clique em **Configuração** na barra de andamento.
2. No formulário, preencha os campos



3. Para habilitar a opção de campo de IC alternativo e definir as condições de filtragem que invocam automaticamente este perfil, siga estas etapas.

   a. Marque a caixa de seleção **Habilitar campo de gatilho de IC alternativo**.
   O campo Gatilho de IC alternativo é exibido. Para este exemplo, como usuário com a função sn_si.admin, você acredita que o campo IC não será preenchido no incidente de segurança após a criação do incidente. Como alternativa, você acha que as informações de IC para um FQDN, nome de host ou endereço IP serão preenchidas no campo IC identificado no incidente de segurança e seleciona o campo IC identificado como uma alternativa. O IC Identificado é selecionado para este exemplo, mas você pode usar qualquer campo no incidente de segurança para o IC alternativo.

   b. Na lista de seleção Campo de **gatilho de IC alternativo** exibida, selecione o campo **IC identificado**.

   Todos os campos disponíveis no incidente de segurança são exibidos na lista, incluindo todos os campos personalizados. No campo Gatilho de IC alternativo, IC identificado é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando este perfil é invocado e o campo de IC não é preenchido no incidente de segurança associado após o gatilho de evento inicial, o perfil usa alternativamente o valor do campo de IC identificado na pesquisa.

c. Marque a caixa de seleção **Gatilho automático com base no incidente**.
O construtor de condições de filtro é exibido. Com esta opção, defina as condições de filtragem e especifique quando o perfil é invocado automaticamente na criação de um incidente de segurança.

d. Defina as condições de incidente de SIR que acionarão automaticamente os recursos do ePO selecionados para este perfil específico.

e. Se as capacidades de perfil que executam uma ação em um endpoint exigirem aprovação, marque a caixa de seleção **Requer Aprovação**.

f. Selecione uma aprovação usando o ícone de pesquisa.

4. Clique em **Concluir**.
Você configurou com sucesso o perfil para que ele seja acionado automaticamente na criação do incidente e um campo alternativo seja usado para preencher os resultados de IC correspondentes.

Acionar perfil McAfee ePO manualmente a partir de um incidente de segurança

Acione um perfil de recurso manualmente a partir de um incidente de segurança Now Platform Security Incident Response (SIR).

Antes de Iniciar
Função necessária: sn_si.admin

Nota:
A opção de aprovações em Configurando perfis para a integração McAfee ePO aparece somente para as capacidades Isolar Host e Remover Isolamento de Host.

Por Que e Quando Desempenhar Esta Tarefa
Você pode invocar uma solicitação para Obter detalhes do host, Isolar máquina host ou Remover isolamento de uma máquina automaticamente se as condições de acionamento especificadas no perfil corresponderem às condições em incidentes de segurança. Como alternativa, se você quiser enviar uma solicitação manualmente, envie a solicitação diretamente de um incidente de segurança.

Depois de ativar o perfil, com base nas condições do gatilho configuradas, você pode exibir os resultados da consulta nos Now Platform incidentes de segurança. As integrações McAfee ePO também permitem que você execute recursos individuais em itens de configuração (ICs) sem usar um perfil.

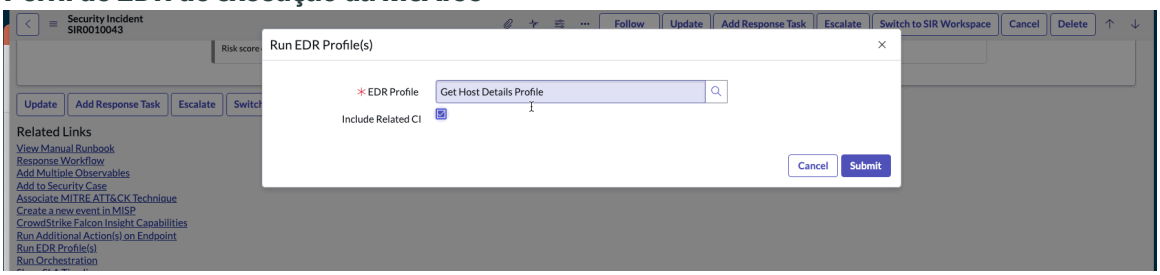
Procedimento

1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações McAfee ePO.
3. Na seção de listas relacionadas, selecione **Executar perfil(is) de EDR**.

Tradução automática

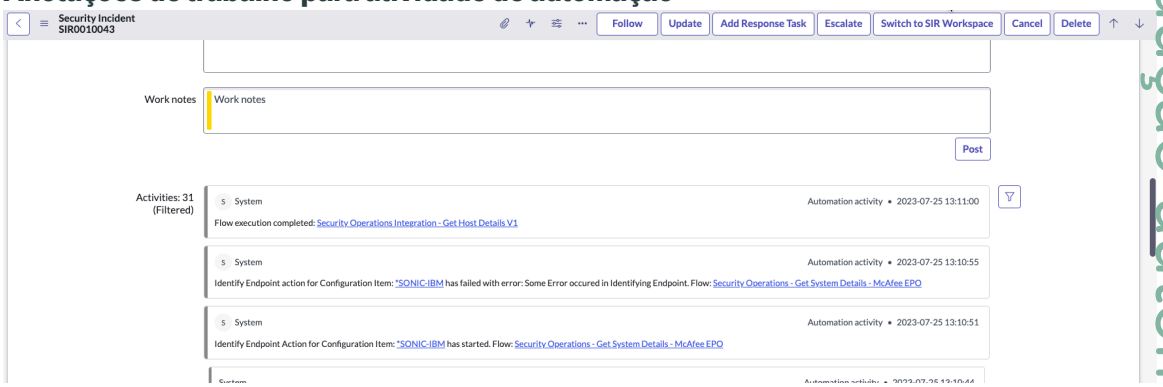
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Perfil de EDR de execução da McAfee



4. Procure e selecione um perfil na lista de perfis disponíveis.
   A lista de perfis disponíveis é Obter detalhes do host, Isolar máquina host e Remover isolamento. Por exemplo, vamos selecionar Obter detalhes do host.
5. Selecione **Incluir IC relacionado** para executar este perfil em todos os ICs relacionados do perfil.
   Por exemplo, se houver cinco ICs associados ao incidente de segurança, o perfil selecionado será executado em todos os cinco ICs.
6. Clique em **Enviar**.
   O perfil selecionado é acionado manualmente. Você pode revisar a seção de anotações de trabalho e atividades e os marcadores iniciados e concluídos pelo perfil na seção de anotações de trabalho.

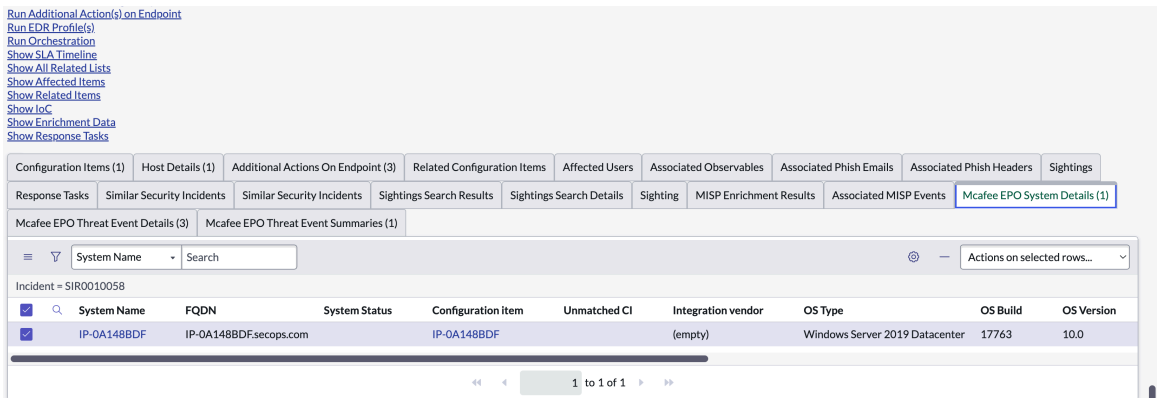
Anotações de trabalho para atividade de automação



Os resultados aparecem na forma de listas relacionadas, como Obter detalhes do host, Isolar máquina host ou Remover isolamento.

Nota:
Todas as tabelas da lista relacionada estendem as tabelas base. Neste exemplo, os Detalhes do sistema do McAfee EPO são uma tabela estendida da tabela base de Detalhes do host.

Listas relacionadas da McAfee



© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Para executar recursos individuais em um item de configuração (IC), execute as seguintes etapas:

   a. Na lista relacionada Itens de configuração, selecione o IC necessário.

   b. Clique na lista suspensa **Ações nas linhas selecionadas...** e selecione a capacidade necessária que você deseja executar para o IC selecionado.
   Por exemplo, Isolar Host.

   c. Clique em **Isolar Host** para executá-lo no IC selecionado.
   O IC selecionado é isolado da rede.

Acionar ações adicionais na integração McAfee ePO

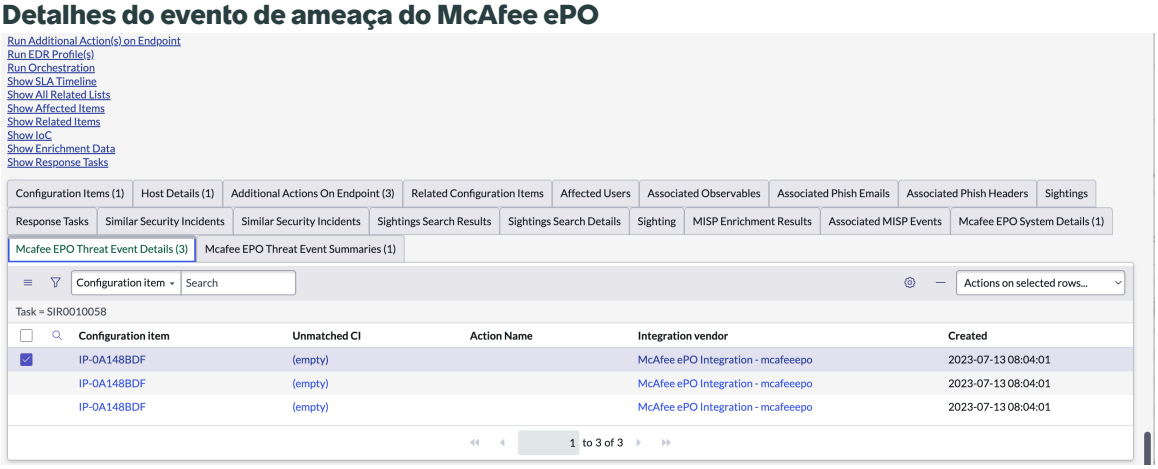
As capacidades Listar eventos de ameaça e Iniciar verificação de malware podem ser acionadas em Executar ações adicionais.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode configurar e acionar ações adicionais na integração McAfee ePO habilita usando **Executar ações adicionais no endpoint**, que incluem os recursos McAfee ePO Listar eventos de ameaça e McAfee ePO Iniciar verificação de malware.

Procedimento
1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança no qual você deseja executar as ações adicionais.
3. Na seção Links relacionados, clique em **Executar ações adicionais no endpoint**.
4. Procure e selecione a implementação da capacidade que você deseja acionar na lista de ações adicionais.
   Por exemplo, McAfee ePO Listar eventos de ameaça.
5. Selecione **Incluir IC relacionado** para executar esta ação adicional em todos os ICs relacionados do perfil.
   Por exemplo, se houver cinco ICs associados ao incidente de segurança, o perfil selecionado será executado em todos os cinco ICs.
6. Clique **em Executar ações adicionais**.

Detalhes do evento de ameaça do McAfee ePO



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Todas as tabelas da lista relacionada estendem as tabelas base. Neste exemplo, a tabela Detalhes do evento de ameaça do McAfee EPO é uma tabela estendida das Ações adicionais na tabela base do endpoint.

7. Exiba e valide os detalhes do evento de ameaça do McAfee ePO nas listas relacionadas.

Usando a integração McAfee ePO no espaço do analista

Use a integração McAfee ePO para aproveitar os recursos McAfee ePO no espaço do analista de SIR.

Antes de Iniciar
Função necessária: sn_si.admin

Antes de usar a integração McAfee ePO no espaço do Security Incident Response, você deve baixá-la do ServiceNow Store e configurá-la. Para obter mais informações, consulte Configure sua instância Now Platform para a integração McAfee ePO.

Por Que e Quando Desempenhar Esta Tarefa
Você pode usar a integração McAfee ePO para fazer ações de correção nos endpoints em tempo real, usar perfis para coletar detalhes sobre o host e fazer consultas ou ações específicas no endpoint usando o espaço Security Incident Response.

A integração McAfee ePO permite que os analistas usem os seguintes recursos [McAfee ePO no espaço do analista Security Incident Response :

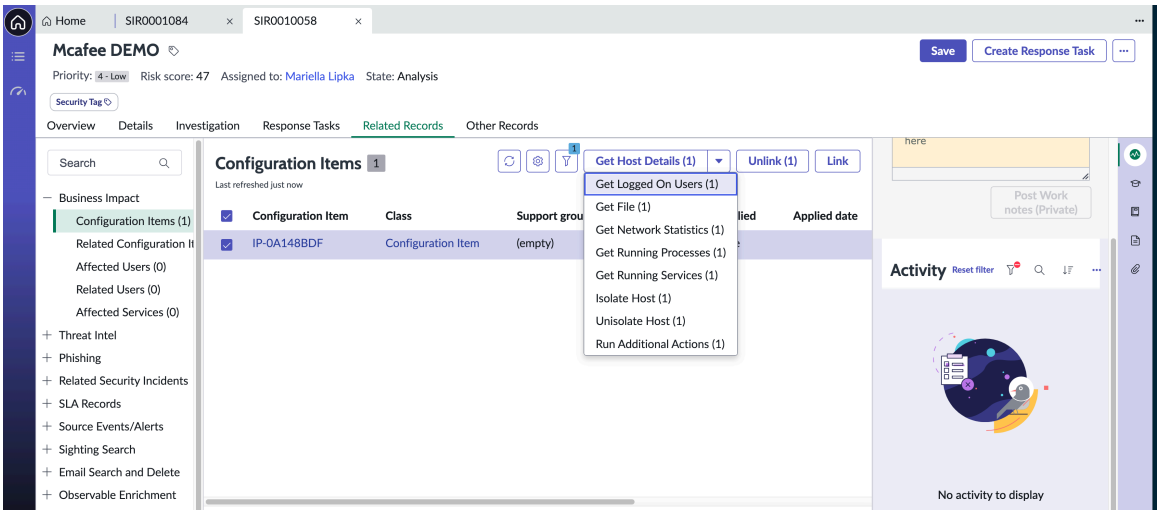
- **Obter detalhes do host**
- **Isolar Host**
- **Remover isolamento**
- **Executar ações adicionais no endpoint**

Procedimento

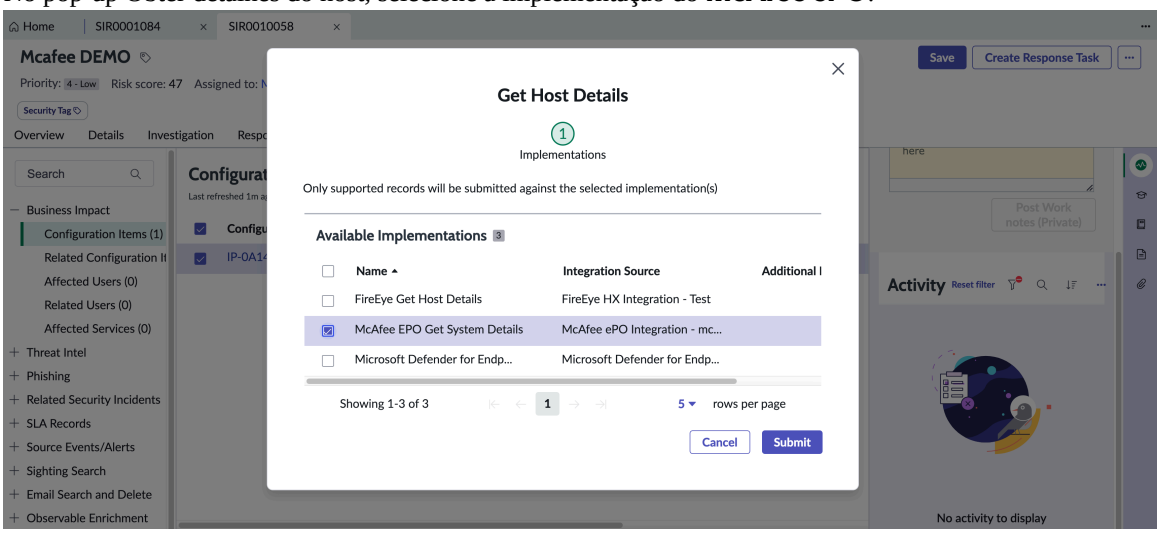
1. Para abrir o incidente de segurança no espaço de SIR, clique em **Alternar para espaço de SIR** no incidente de segurança.
2. No espaço de SIR, selecione a guia **Registros relacionados**.
3. Selecione qualquer **Item de configuração**e escolha um recurso do McAfee ePO para acionar na ação suspensa da lista relacionada.
   Por exemplo, Obter detalhes do host.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No pop-up Obter detalhes do host, selecione a implementação do **McAfee ePO**.

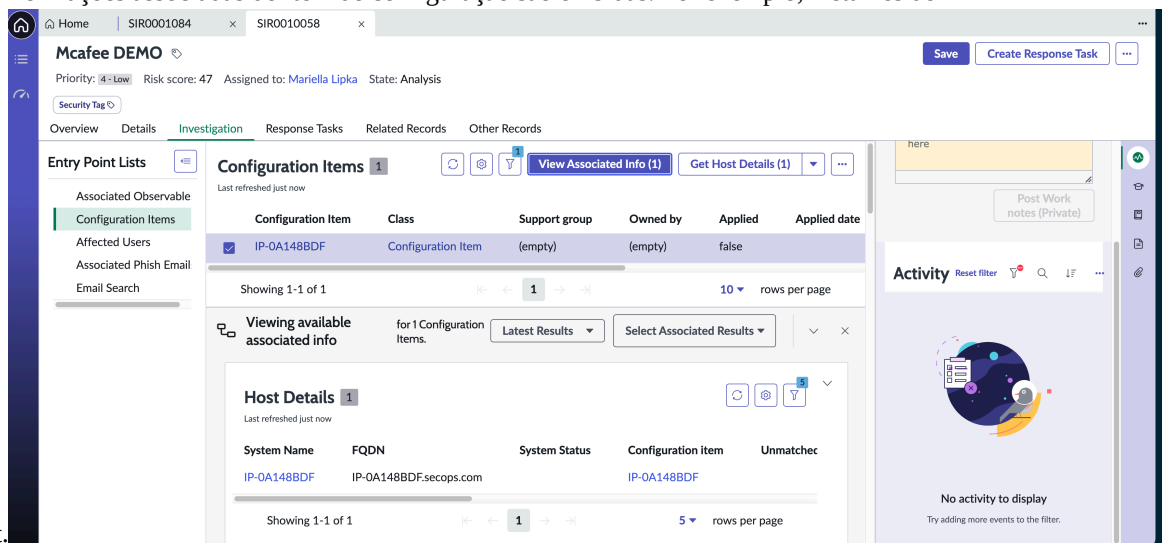


5. Clique em **Enviar**.
   A funcionalidade Obter detalhes do host é invocada no IC. Você pode exibir as anotações de trabalho dos resultados e descobertas.
6. Para exibir os dados da capacidade acionada, selecione a guia **Investigação**.
7. Selecione o **Item de configuração**e clique na ação **Exibir informações associadas**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As informações associadas do item de configuração são exibidas. Por exemplo, Detalhes do host.



8. Clique no **Item de configuração** para exibir os detalhes do host.
   Da mesma forma, você pode tentar usar o outro recurso do McAfee ePO para seus incidentes de segurança no SIR Analyst Workspace.
9. Você pode usar os recursos do McAfee ePO na lista relacionada de **Detecção e resposta de endpoint (EDR)** para análise.
10. Procure e selecione um perfil na lista de perfis disponíveis.
    A lista de perfis disponíveis é Obter detalhes do host, Isolar máquina host e Remover isolamento. Por exemplo, vamos selecionar Obter detalhes do host.
11. Selecione a implementação do **McAfee ePO** e clique em **Enviar**.

McAfee ESM - Integração do analisador de e-mail

A integração ESM - Analisador de e-mail é compatível com um analisador de e-mail que consome notificações por e-mail do ESM para criar incidentes de segurança.

Configurar McAfee ESM - Integração do analisador de e-mails

A integração do McAfee ESM - Analisador de e-mail usa notificações por e-mail do ESM para gerar aprimoramentos e fluxos de trabalho de resposta.

Antes de Iniciar

Função necessária: sn_si_admin

Por Que e Quando Desempenhar Esta Tarefa

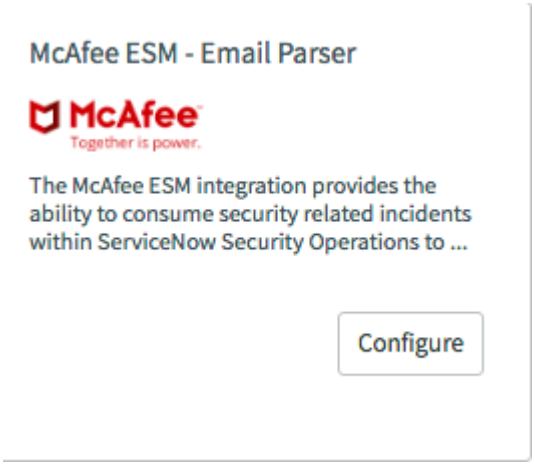
Um modelo de analisador de e-mail do McAfee ESM é fornecido para uso na integração. Ele deve ser configurado e ativado antes que a integração ocorra. Atualizar o analisador o ativa.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. No cartão McAfee ESM - Analisador de e-mail, clique em **Configurar**.
3. Na caixa de diálogo **McAfee ESM - Configuração do analisador de e-mail**, clique no link **Configurar analisador de e-mail**.
4. Clique no link do **McAfee ESM** para editar as configurações no analisador de e-mail do modelo fornecido. Preencha pelo menos o campo O e-mail é de. Para criar seu próprio analisador de e-mail, consulte Criar analisadores de e-mail no Security Operations.
5. Marque a caixa **Ativa**.
6. Clique em **Atualizar** no formulário **Analisador de e-mail**.
   O analisador de e-mail está ativo. Você não precisa retornar para **Configurações de integração**.

McAfee ESM - Integração de aprimoramento de incidente

McAfee ESM - A integração de Aprimoramento de incidentes pesquisa seus logs e adiciona informações de vista relevantes aos seus incidentes de segurança.

Explorar

Integrações do Security Incident Response

Configurar

- Introdução ao McAfee ESM - Incident Enrichment integration
- Criar registros de configuração de pesquisa de vistas

Usar

- Executar uma pesquisa de vistas
- Integração do Security Operations - Fluxo de trabalho de pesquisa de detecções
- Security Operations - Fluxo de trabalho de pesquisa de detecções do McAfee ESM
- Exibir detalhes da pesquisa de detecções
- Exibir Resultados da Pesquisa de Vistas

Desenvolver

- ServiceNow Security Operations diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação

Solucionar problemas e obter ajuda

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Solução de problemas de integração
- Faça ou responda perguntas na comunidade do Security Operations
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Introdução ao McAfee ESM - Incident Enrichment integration

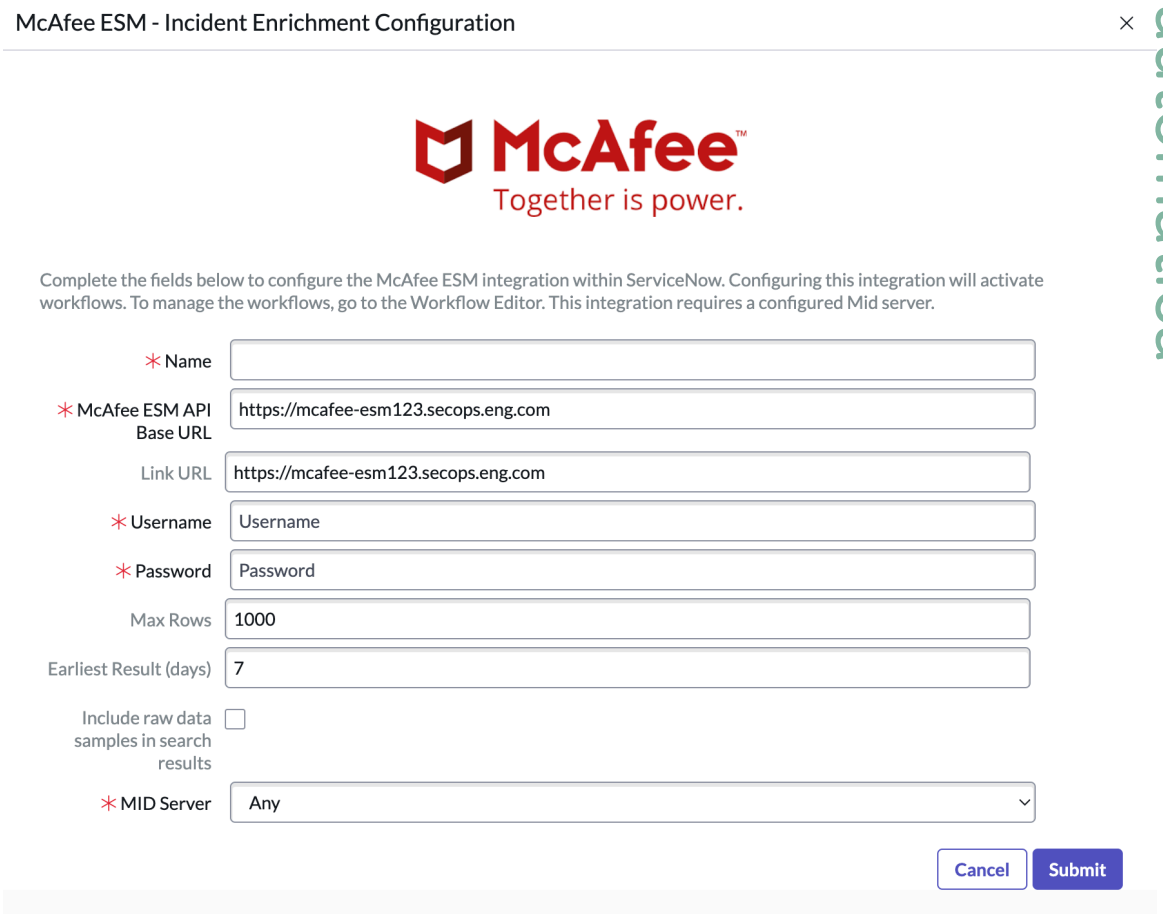
McAfee ESM protege os endpoints contra vírus, Spyware, Cavalos de Tróia e outras ameaças de malware e se integra facilmente com Security Operations. Antes de usar a integração McAfee ESM - Incident Enrichment, você deve baixá-la do ServiceNow Store e adicionar a URL base da API e as credenciais de login apropriadas.

Antes de Iniciar

Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Security Operations** > **Integrações** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão McAfee ESM - Aprimoramento de incidente, clique em **Novo**.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
URL Base da API McAfee ESM	O URL base que você adquiriu no site do McAfee ESM.
URL do Link	[Opcional] A URL do link que vincula a uma instância do McAfee ESM, quando disponível. **Nota:** Se você estiver recebendo um erro, use o URL Base da API do McAfee ESM.
Nome do usuário	Seu nome de usuário do McAfee ESM.
Senha	Sua senha do McAfee ESM.
Máx. de Linhas	O número máximo de linhas que você deseja pesquisar.
Resultado Mais Antigo (dias)	Os resultados mais antigos que você deseja ver em número de dias.
Incluir amostras de dados brutos nos resultados da pesquisa	Selecione esta opção para incluir amostras de dados brutos nos resultados da pesquisa de detecções. A quantidade de dados retornados depende da configuração na propriedade do **número de linhas de dados brutos** nas propriedades do Security Incident Response.
MID Server	Selecione **Qualquer** para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota:
Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho.

5. Clique em **Enviar**.
O cartão de configuração de integração é exibido.
6. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Integração de Microsoft Azure Sentinel

Microsoft Azure Sentinel O é uma solução baseada em nuvem do Security Information Event Management (SIEM) e do Security Orchestration Automated Response (SOAR). Você pode usar a integração Microsoft Azure Sentinel para ingerir incidentes do Azure Sentinel e criar automaticamente incidentes de segurança em Security Incident Response.

Solicitar aplicativos na Store

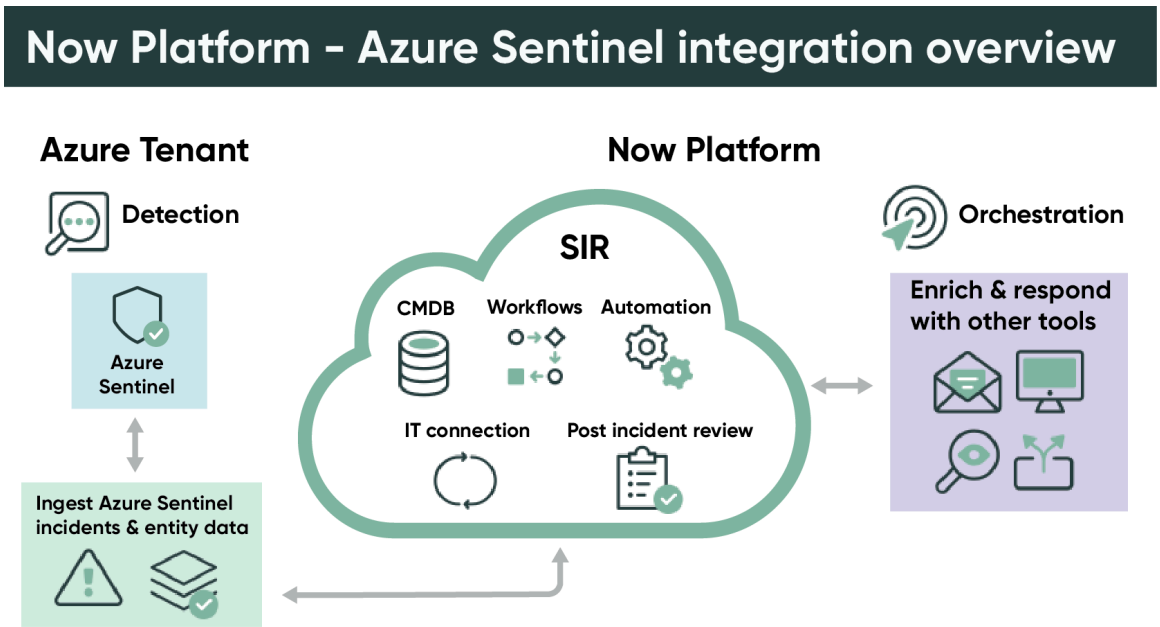
Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

Consulte o diagrama a seguir para saber como Microsoft Azure Sentinel se integra às aplicações Now Platform Security Operations.



Principais recursos

Use os principais recursos desta integração para realizar as seguintes ações:

- Descubra Microsoft Azure Sentinel incidentes que são candidatos a incidentes de segurança e automatize a criação desses incidentes de segurança.
- Mapeie Microsoft Azure Sentinel campos de incidente e entidade para campos de incidente de segurança SIR.
- Filtrar Microsoft Azure Sentinel incidentes.
- Agregue incidentes a incidentes de segurança em aberto existentes para que você não precise criar incidentes de segurança duplicados.
- Automatize Microsoft Azure Sentinel atualizações de status de incidente para o Security Incident Response para que você possa criar e fechar incidentes de segurança.

> **Nota:**
> ServiceNow atualiza o status de Microsoft Azure Sentinel incidentes com base na criação ou no fechamento do incidente de segurança. Esta atualização também inclui comentários de incidentes agregados e novos incidentes.

- Programe a ingestão de incidentes para criar incidentes de segurança periodicamente.
- Sincronize Microsoft Azure Sentinel comentários de incidente com SIR Anotações de trabalho.

Conheça esta integração

Identificador de documento	Título do documento
Microsoft site da documentação do produto	Site de documentação do produto Microsoft

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Identificador de documento	Título do documento
ServiceNow site da documentação do produto	Site de documentação do produto da ServiceNow

Introdução à integração Microsoft Azure Sentinel

Ative e configure o plug-in Microsoft Azure Sentinel – Ingestão de incidentes para Security Operation para interagir com sua instância [Now Platform e produto Security Incident Response.

Antes de Iniciar

Função necessária: Microsoft Azure desenvolvedor de aplicações, Microsoft Azure administrador de locatário

Antes de usar a integração Microsoft Azure Sentinel, você deve baixá-la do ServiceNow Store.

Por Que e Quando Desempenhar Esta Tarefa

Revise a check-list de configuração a seguir e verifique se você concluiu todas as tarefas para uma integração sem problemas.

Check-list

Configuração de tarefa	Descrição
Atribua e verifique as funções Now Platform e Security Incident Response.	As funções a seguir são necessárias para configuração e verificação dos resultados esperados: • A função de administrador instala a integração do ServiceNow Store e atribui a função sn_si.admin. • A função sn_si.admin executa as seguintes tarefas: ◦ Configura a integração. ◦ Cria perfis de incidentes. ◦ Mapeia os campos de dados de incidente Microsoft Azure Sentinel para os campos de incidente de segurança. ◦ Programa a ingestão de incidentes em andamento. ◦ Habilita atualizações de incidentes quando um incidente Security Incident Response é criado ou encerrado. ◦ Atribui a função de analista de incidente de segurança (sn_si.analyst).
Atribua as Microsoft Azure funções necessárias.	As funções a seguir são necessárias em Microsoft Azure para registrar e configurar sua aplicação: • Desenvolvedor de aplicações para registrar a aplicação. • Administrador de locatário para conceder permissões à aplicação chamando o endpoint de consentimento do administrador.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de configurar esta integração.	O plug-in ServiceNow IntegrationHub Starter Pack Installer [com.glide.hub.integrations] é necessário. O plug-in Security Incident Response (com.snc.security_incident) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar os outros aplicativos Security Operations que são necessários para a integração. Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se essas aplicações ainda não estiverem instaladas, você deverá instalar e ativar cada aplicação uma de cada vez na seguinte ordem para garantir uma instalação sem problemas: **1.** Security Incident Response **2.** IU Security Incident Response **3.** Tempo de execução do ServiceNow IntegrationHub (com.glide.hub.integration.runtime) **4.** Etapa de ação do ServiceNow IntegrationHub — REST (com.glide.hub.action_step.rest)
Registre e configure sua aplicação no Microsoft Azure portal.	Registre sua aplicação no portal Microsoft Azure e conceda aos usuários acesso de leitura e gravação à aplicação.

Registrar e configurar o portal Microsoft Azure

Registre sua aplicação no portal Microsoft Azure e conceda aos usuários acesso de leitura e gravação à aplicação.

Antes de Iniciar

Função necessária: Microsoft Azure desenvolvedor de aplicações, Microsoft Azure administrador de locatário

Procedimento

1. Entre no portal Microsoft Azure.

2. Pesquise e selecione **Registros de aplicações**.

3. Clique **em Novo registro**.

Tradução automática

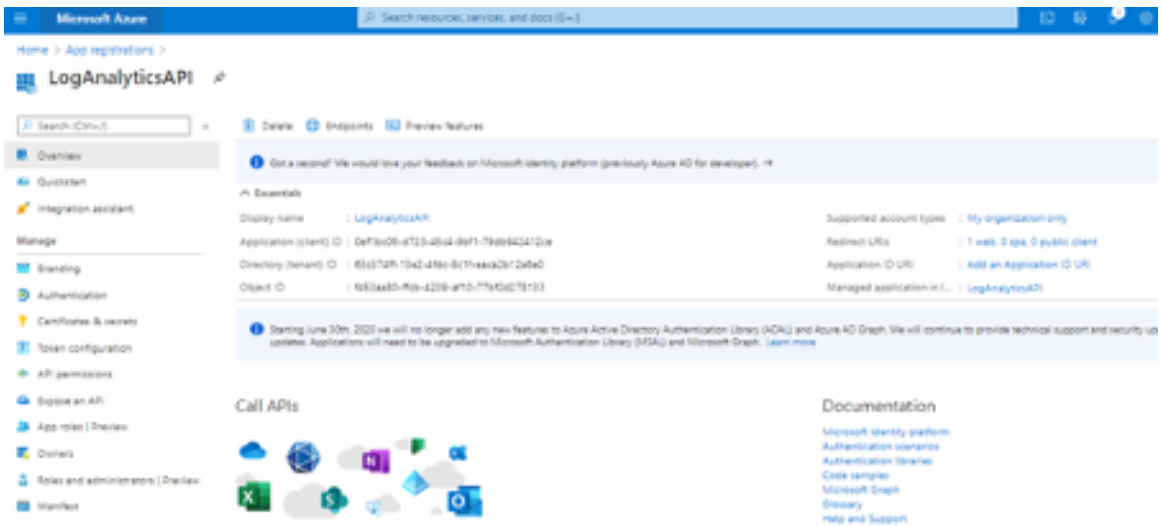
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. No formulário, preencha os campos.

Registrar um formulário de aplicação

Campo	Descrição
Nome	Nome de exibição da aplicação para o usuário. Por exemplo, LogAnalyticsAPI.
Tipos de conta compatíveis	Tipo de conta que pode usar esta aplicação ou acessar a API.
Redirecionar URI	Redirecionar URI. A resposta de autenticação é direcionada para este URI após a autenticação bem-sucedida de um usuário.

5. Clique em **Registrar**.
Depois de registrar a aplicação com sucesso, você verá a página Visão geral.



6. Navegar até **Gerenciar** > **Certificados e segredos**.
7. Na seção Segredos do cliente, clique em **Novo segredo do cliente**.
Você não pode exibir o segredo do cliente mais tarde, portanto, certifique-se de copiar e salvar o segredo do cliente agora nesta etapa. Se você esquecer o segredo do cliente, poderá gerar um novo seguindo as instruções nas etapas 4 e 5.
8. Navegar até **Gerenciar** > **Permissões de API**.
9. Clique **em Adicionar uma permissão**.
10. Na janela Solicitar permissões de API, clique na guia **APIs que minha organização usa**.
11. Pesquise e selecione o nome da aplicação **da API do Log Analytics**.
12. Nas permissões da API do Log Analytics, selecione **Permissões da aplicação**.
Habilitar esta permissão garante que a aplicação seja executada como um serviço ou daemon em segundo plano sem um usuário conectado.
13. Na seção Dados, selecione **Data.Read**
14. Clique **em Adicionar permissões**.
As permissões são atualizadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

15. Habilite a opção **Conceder consentimento do administrador para diretório padrão** para a permissão da API Data.Read que você habilitou na etapa 13.
16. Pesquise e selecione **espaços do Log Analytics**.
17. Selecione o espaço do Sentinel Log Analytics.
    Agora você vê a página Visão geral do espaço do Sentinel Log Analytics.
18. Navegar até **Controle de acesso (IAM)** > **Atribuições de função**.
19. Clique em **Adicionar**e selecione **Adicionar atribuição de função**.
20. No formulário, preencha os campos.

Adicionar formulário de atribuição de função

Campo	Descrição
Função	Tipo de conta que pode usar esta aplicação. Selecione **Respondente do Azure Sentinel**.
Atribuir acesso a	Escopo de permissões que você define. Selecione **Usuário**, **grupo**ou **entidade de serviço**.
Selecionar	Aplicação que você criou anteriormente na etapa 4. Por exemplo, LogAnalyticsAPI.

21. Clique em **Salvar**.

Instalar e configurar a integração Microsoft Azure Sentinel

Instale e configure a integração Microsoft Azure Sentinel do ServiceNow Store na sua instância Now Platform para iniciar a ingestão de incidentes do Azure Sentinel.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Baixe a integração Microsoft Azure Sentinel do ServiceNow Store e instale-a.
2. Navegar até **Security Operations** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco Microsoft Azure Sentinel e clique em **Configurar**.
4. No formulário, preencha os campos.

Microsoft Azure Sentinel - Formulário de configuração de ingestão de incidentes

Campo	Descrição
Nome	Nome da configuração da instância Microsoft Azure Cloud.
URL de identidade	URL de identidade para o locatário Microsoft Azure Cloud. Por exemplo, login.microsoftonline.com. Para obter informações adicionais, consulte a documentação do Microsoft Azure .
Azure Resource Manager	Endpoint do Azure Resource Manager para locatário Microsoft Azure Cloud. Por exemplo, management.azure.com. Para obter informações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	adicionais, consulte a documentação do Microsoft Azure .
ID de locatário	Microsoft Azure Sentinel ID do locatário. Esta é a instância da qual todos os incidentes no portal Microsoft Azure são recuperados.
ID de cliente	ID de cliente da aplicação que você registrou no portal Microsoft Azure.
Segredo do Cliente	Segredo do cliente para sua aplicação registrada.
ID de Assinatura	ID de assinatura da aplicação registrada.
Nome do grupo de recurso	Nome do grupo de recursos para sua aplicação registrada.
Nome do espaço	Nome do espaço da aplicação registrada.

5. Clique em **Enviar**.

Resultado
Depois de validar e enviar a configuração com sucesso, cada configuração do servidor de ingestão de incidente é salva na página Integrações de segurança como um bloco.

Criar um perfil para Microsoft Azure Sentinel

Crie um perfil de incidente em sua instância Now Platform e determine os incidentes Microsoft Azure Sentinel que são adequados para criar incidentes de segurança.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
A integração permite criar diferentes tipos de incidentes, como tentativas de acesso não autorizadas e malware. Esses incidentes são criados com base nos perfis que você configura na instância Now Platform. Todos os incidentes são criados inicialmente para um tipo de incidente configurado em um perfil. Os incidentes criados podem ser filtrados para especificar quais incidentes criam incidentes de segurança.

Todos os incidentes que atendem aos critérios de seleção no seu locatário Microsoft Azure e estão disponíveis na API Microsoft Azure Sentinel são inicialmente ingeridos em sua instância Now Platform.

Procedimento

1. Navegar até **Todos** > **Integração do Microsoft Azure Sentinel** > **Perfil de incidentes do Azure Sentinel**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Microsoft Azure Sentinel - Formulário de configuração de ingestão de incidentes

Campo	Descrição
Nome	Nome do perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Este nome ajuda a identificar o tipo de perfil e também é o nome padrão do marcador de segurança associado a este perfil.
Ativo	Indicador de que o perfil está ativo. Quando o perfil está ativo, isso implica que o Now Platform está pesquisando ativamente os incidentes do Azure Sentinel e que os incidentes de segurança correspondentes são criados em SIR quando as condições de filtragem são correspondidas.
Origem	Microsoft Azure locatário que você configurou para ingerir incidentes. Se você tiver vários locatários configurados, selecione o locatário apropriado para os tipos de incidente que você planeja ingerir para o perfil.
Ordem	Prioridade de fluxo. O valor deste campo indica a ordem em que os fluxos são executados quando dois ou mais perfis compartilham condições de gatilho. O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300, 400. O padrão é 100.
Descrição	Texto extra para ajudar a distinguir este perfil de outros perfis.

4. Para mover para a seção Mapeamento, clique em **Continuar**.

O que Fazer Depois

Mapeie campos de incidentes Microsoft Azure Sentinel individuais para os campos no incidente de segurança Now Platform SIR.

Mapear os campos de incidente Microsoft Azure Sentinel

Mapeie os campos de incidente Microsoft Azure Sentinel individuais para os campos no incidente de segurança SIR para que você possa criar incidentes com os dados mapeados.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Na página de mapeamento, na seção Mapeamento de campo do Azure Sentinel, selecione um dos métodos de ingestão de amostra.

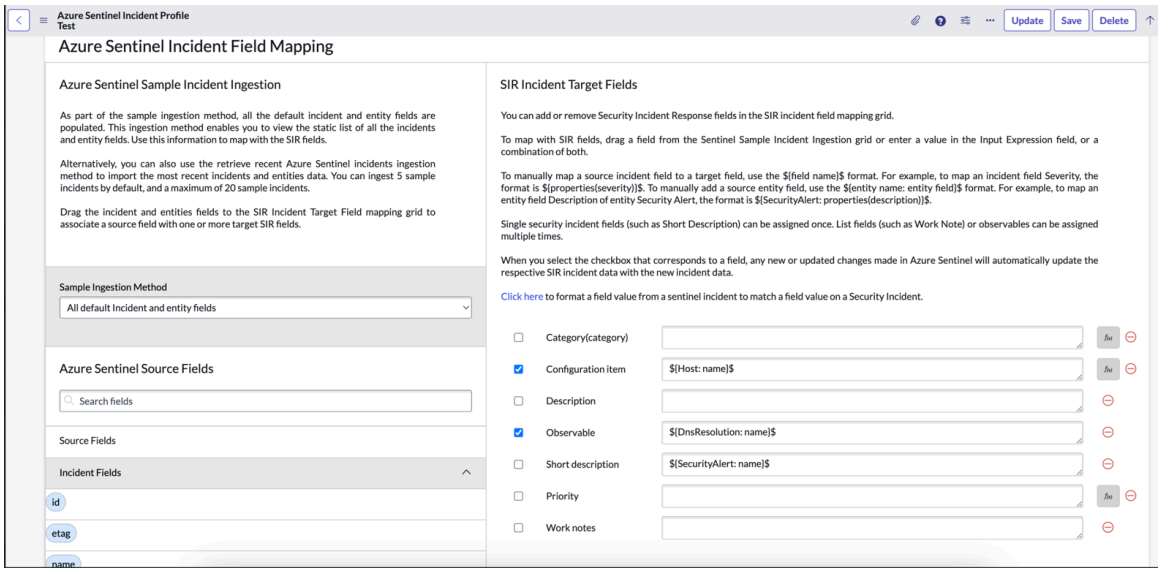
Métodos de ingestão de amostra

Campo	Descrição
Todos os campos padrão de Incidente e entidade	Use este método de ingestão para exibir a lista estática de todos os incidentes e campos de entidade. Este método contém somente nomes de campo padrão sem valores. Você pode usar essas informações para mapear com os campos SIR.
Recuperar incidentes recentes do Azure Sentinel	Use este método de ingestão para importar os dados de incidentes e entidades mais recentes. Se o incidente do Azure Sentinel contiver os dados da entidade, os dados da entidade serão recuperados e ficarão disponíveis para mapeamento na seção Campos de origem do Azure Sentinel. Às vezes, o incidente do Azure Sentinel pode não conter os dados da entidade e, portanto, os campos da entidade não estão disponíveis para mapeamento nesse cenário. Se o incidente do Azure Sentinel contiver vários alertas, o alerta mais antigo que fizer parte do incidente será mostrado na seção de mapeamento. Durante a ingestão, os valores mais antigos do campo de alerta de segurança serão usados. Você pode ingerir 5 incidentes de amostra por padrão e um máximo de 20 incidentes de amostra. Os valores do campo de incidente de amostra são preenchidos quando o perfil ingere os incidentes de amostra. Você pode mapear esses incidentes para os **campos de destino do incidente SIR**. Os campos e valores de incidente aparecem como guias individuais.
Importar dados de amostra	Clique em **Importar dados de amostra** para importar incidentes de amostra do Azure Sentinel. Este botão aparece quando você seleciona o método de ingestão Recuperar incidentes recentes do Azure Sentinel.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	A recuperação de incidentes de amostra do servidor Microsoft Azure Sentinel pode demorar um pouco. Mapeie esses incidentes recuperados para os **Campos de destino do incidente de SIR**. Os campos e valores de incidente aparecem como guias individuais.



2. Para adicionar campos aos campos padrão exibidos no incidente de segurança, execute as seguintes ações:

a. Na seção Campos de destino do incidente de SIR, clique no botão

Botão Mapear outro campo.
Ele mostra uma lista de SIR campos, na qual você pode selecionar um campo para um novo campo a ser exibido.

b. Na coluna Incidente de segurança, expanda a lista exibida e selecione um campo.

> **Nota:**
> Vários observáveis podem ser exibidos no mesmo incidente de segurança. Por exemplo, o campo **Observável** pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos **Item de configuração** e **Anotações de trabalho** oferecem suporte a vários valores. Se você tentar mapear dois valores para um campo que não oferece suporte a vários valores, verá uma mensagem de erro informando que este campo não oferece suporte a vários valores. Da mesma forma, se um campo em um incidente de segurança tiver uma lista na qual você pode escolher várias opções e você tentar mapear uma opção para esse campo que não é exibido na lista, o campo não será preenchido no incidente de segurança.

c. Na seção Campos de origem do Azure Sentinel, arraste e solte o campo para mapeá-lo para o novo campo.

d. Quando você marca a caixa de seleção que corresponde a um campo, todas as mudanças novas ou atualizadas feitas no Azure Sentinel atualizam automaticamente os respectivos dados de incidente SIR com os novos dados de incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
No sistema de base, a propriedade do sistema sn_sec_sentinel.incident_updates é definida por padrão como Verdadeira para receber as Microsoft Azure Sentinel atualizações relacionadas a novos alertas vinculados ao SIR.

- Por padrão, os campos Usuários afetados, Itens de configuração e Observáveis são verificados. Isso significa que sempre que houver novos observáveis ou itens de configuração associados, ou usuários afetados que sejam adicionados ao incidente, essas informações serão automaticamente extraídas e preenchidas nas respectivas listas relacionadas no Security Incident Response (SIR) durante esse intervalo de pesquisa.
- Para quaisquer outros campos, você deve marcar a caixa de seleção que corresponde a um campo para todas as mudanças novas ou atualizadas feitas no registro de incidente do Azure Sentinel no Azure Sentinel. Isso atualizará automaticamente os respectivos dados de incidente de SIR com os novos dados de incidente.

Importante:
É necessário fazer a devida diligência antes de selecionar esta funcionalidade, pois substituir os dados existentes pode resultar em dados instáveis para o analista trabalhar e qualquer outra automação definida, mesmo pelos valores de campo do incidente de segurança, também pode ser afetada. Portanto, é muito importante fazer a devida diligência antes de selecionar qualquer funcionalidade de substituição.

3. Para remover um campo, use o botão Remover Remover item ao lado do campo de expressão de entrada na seção Campos de destino do incidente de SIR.
4. Para mapear um valor de campo da seção Campos de origem do Azure Sentinel para um campo na seção Campos de destino do incidente de SIR, use uma das seguintes ações:

   a. Arraste o nome do campo (por exemplo, id) e solte-o ao lado de um nome de campo na coluna Campos de destino do incidente de SIR.

      Você pode corresponder qualquer valor da seção Campos de origem do Azure Sentinel a um campo na seção Campos de destino do incidente de SIR. Os campos são codificados por cores para que você não ignore ou duplique os campos de incidente no processo de mapeamento. Os campos azul claro indicam que um campo de incidente ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de incidente de entrada a mais de um campo em um incidente de segurança. Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Dessa forma, você pode visualizar quais valores de campo foram adicionados ao incidente de segurança e se alguma informação importante do incidente restante permanece não mapeada.

   b. Você pode adicionar uma combinação de texto e campo.
   Por exemplo, o `nome do incidente é ${name}$`. Aqui, o `nome do incidente é` pode ser inserido manualmente enquanto `${name}$` é mapeado da seção Campos de origem do Azure Sentinel.

   c. Você pode inserir e mapear manualmente um incidente de origem ou campo de entidade para um campo de destino.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para mapear manualmente um campo de incidente de origem, use o formato ${field name}$. Por exemplo, para mapear um campo de incidente Severidade, o formato é${properties(severity)}$.
- Para adicionar manualmente um campo de entidade de origem, use o formato ${entity name: entity field}$. Por exemplo, para mapear um campo de entidade Descrição do alerta de segurança da entidade, o formato é ${SecurityAlert: properties(description)}$.

Esta integração classifica determinados subtipos de observáveis. Quando você mapeia um campo do Azure Sentinel com o campo observável SIR, o Now Platform classifica automaticamente o observável. Se você quiser mapear genericamente o observável do Azure Sentinel de entrada para o tipo de observável em SIR, arraste e solte o campo do Azure Sentinel no campo Observável. No entanto, se você estiver ciente do tipo de observável do observável do Azure Sentinel de entrada em SIR, mapeie especificamente para o campo de tipo de observável SIR. Alguns exemplos de tipos de observáveis específicos em SIR incluem Observável(nome do domínio), Observável(endereço de e-mail), Observável(endereço IP (V4)) e Observável(nome do host).

Se os campos de entrada do Azure Sentinel contiverem informações MITRE-ATT&CK, mapeie-as para o campo MITRE-ATT&CK Técnica. Certifique-se de que o campo de entrada do Azure Sentinel contenha o ID da técnica MITRE-ATT&CK ou o nome da técnica.

Às vezes, os valores de campo de incidente em Microsoft Azure Sentinel podem não ser traduzidos diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de script se quiser formatar valores semelhantes, mas não idênticos.

5. Para formatar uma tradução de campo para um novo campo de um incidente do Azure Sentinel para corresponder a um valor de campo em um incidente de segurança, clique no link **Clique aqui** no cabeçalho **Campos de destino do incidente de SIR**.

6. Para modificar os campos que oferecem suporte à tradução de campo, clique no Formato de campo ícone de tradução de campo de formato de script.
Os campos que oferecem suporte à tradução de campo são **Categoria**, **Item de configuração**e **Prioridade**. Por exemplo, clique no ícone do ao lado da Categoria. O editor de script de tradução de campo do Azure Sentinel é aberto.

7. Insira as mudanças no script e clique em **Atualizar** para salvar as mudanças e retornar à página Mapeamento.
Por exemplo, para Categoria, defina o seguinte no editor de script:

```
"<Incoming Sentinel Incident Field Value>" : "<Category to assign to the Security Incident>".
```

Este mapeamento garante que um perfil use somente categorias configuradas.

8. Continue seu mapeamento adicionando ou removendo valores de campo.
Você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que um incidente de entrada deve satisfazer para criar um incidente de segurança.

9. Para mover para a seção Filtragem e agregação, clique em **Continuar**.

O que Fazer Depois

Defina e defina condições de filtro para que você possa especificar quais incidentes devem criar incidentes de segurança. Você pode usar os mesmos valores de campo (definidos na seção Mapeamento) no construtor Condições de geração de incidente (na seção Filtragem e agregação) para definir critérios adicionais que um incidente de entrada deve satisfazer para criar um incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definição de filtro e critérios de agregação

Você pode definir e definir condições de filtro para que possa especificar quais incidentes Microsoft Azure Sentinel de entrada devem criar incidentes de segurança. Você também pode definir critérios de campo de incidente adicionais que permitem que um incidente de entrada seja anexado a um incidente de segurança em aberto em vez de criar um incidente.

Definir as condições de filtragem para incidentes de segurança

Defina as condições de filtragem para que os incidentes de segurança sejam criados somente quando as condições de filtragem corresponderem.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Este tipo de filtragem ajuda a isolar incidentes de segurança e limita o número de incidentes de segurança que você cria. Se você definir critérios de filtragem adicionais, somente os incidentes necessários serão ingeridos sem precisar mudar a consulta ou a configuração do incidente acionado.

Procedimento

1. Para definir os critérios que um incidente Microsoft Azure Sentinel de entrada deve satisfazer para que um incidente de segurança seja criado, selecione **Filtrar com base em condições**.

   As opções no primeiro campo nas Condições do filtro correspondem aos campos exibidos na seção Ingestão de incidente de amostra do Azure Sentinel para o incidente que você ingeriu. Esses campos são dinâmicos e mudam dependendo do incidente que você ingere. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas. Verifique se os critérios definidos correspondem aos valores do incidente.

   Use a condição de filtro *contém* para os seguintes campos com vários valores:

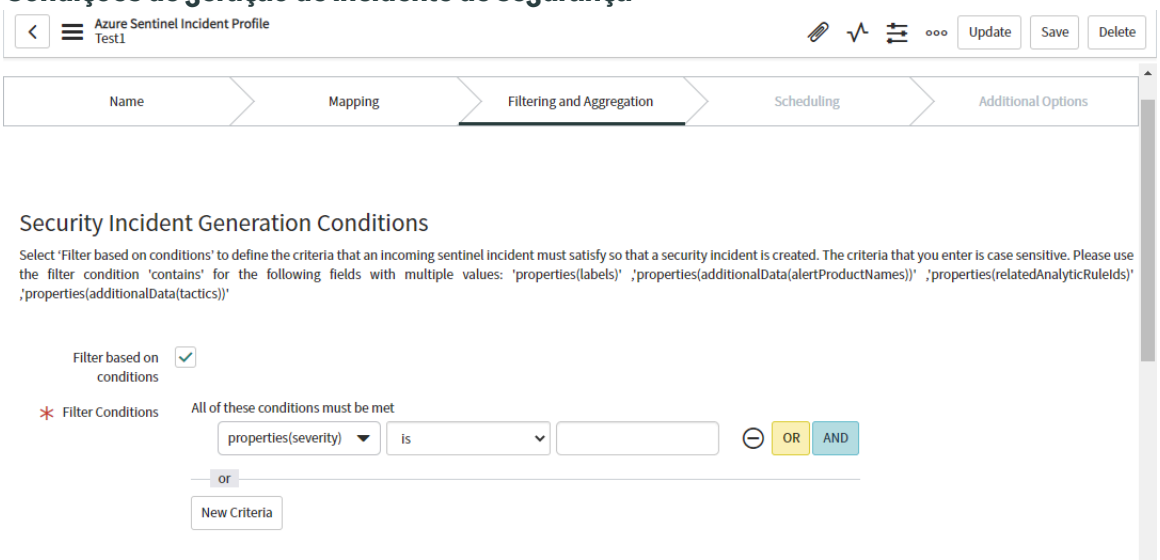
   - properties(labels)
   - properties(additionalData(alertProductNames))
   - properties(relatedAnalyticRuleIds)
   - properties(additionalData(tactics))

   Como a condição do filtro pode recuperar somente cadeias de caracteres, você deve usar a condição do filtro " *contém* " nos campos acima para garantir que os dados sejam filtrados corretamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condições de geração de incidente de segurança



2. Usando as listas e os campos do construtor de condições, defina os filtros para a primeira linha.
3. Para adicionar mais condições, clique em **E** ou **OU**.
   - Se **AND** for selecionado, todas as condições deverão ser correspondidas.
   - Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida.
4. Para definir uma segunda condição de filtro, clique em **Novos critérios**.

Definir condições de agregação

Defina critérios de agregação de incidentes adicionais que agregam um incidente de entrada a um incidente de segurança SIR existente em vez de criar incidentes semelhantes, potencialmente duplicados. Quando você usa critérios de valor de correspondência de campo para cada perfil, essa agregação adicional pode reduzir o número de incidentes de segurança ativos e sobrepostos, colocando todos os dados de incidentes relacionados em um único incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Se um novo incidente corresponder a todos os valores selecionados nas condições de campo de agregação na etapa de mapeamento, o incidente será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os incidentes agregados adicionados em uma lista relacionada em um incidente de segurança.

Todos os incidentes agregados em um incidente de segurança são exibidos na lista relacionada de incidentes agregados do Azure Sentinel. Esta lista detalha os carimbos de data/hora associados e os valores de campos agregados. Essas informações ajudam a entender por que os incidentes são adicionados aos incidentes de segurança existentes.

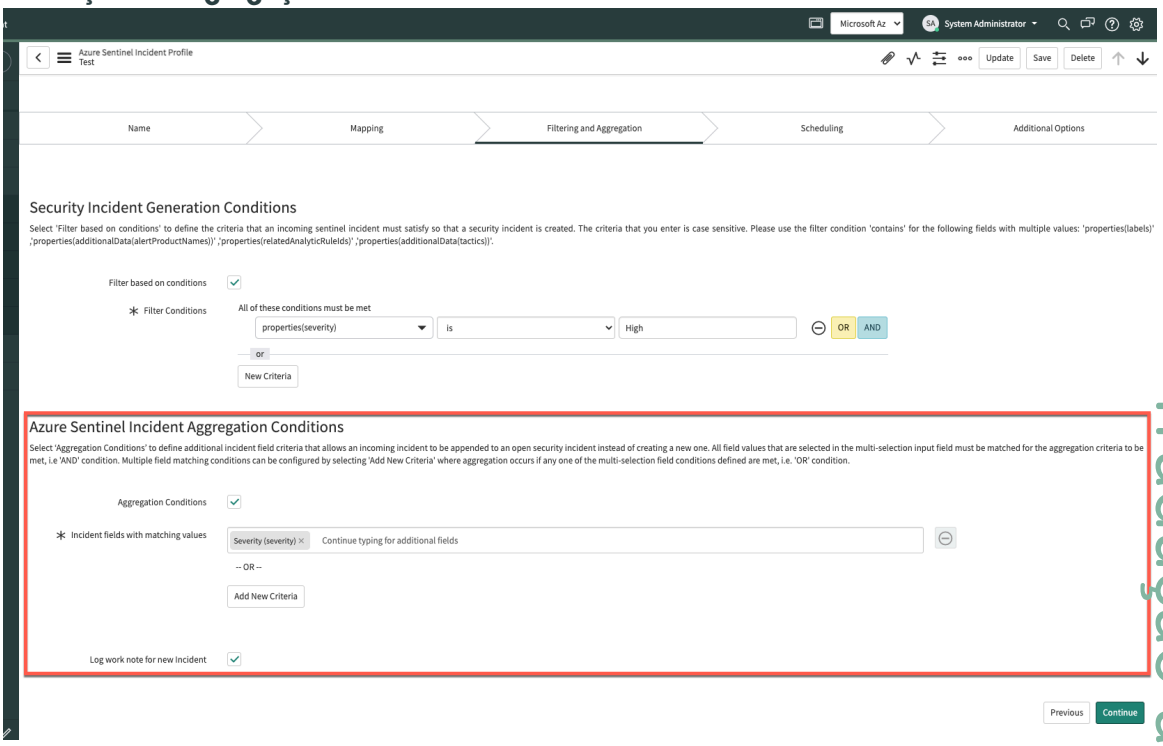
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Para definir critérios de campo de incidente adicionais que permitem que um incidente Microsoft Azure Sentinel de entrada seja anexado a um incidente de segurança aberto em vez de criar um novo incidente, selecione a opção **Condições de agregação**, conforme mostrado na figura a seguir.

Condições de Agregação



2. No campo **Campos de incidente com valores correspondentes**, insira os valores de campo que você deseja corresponder aos incidentes de segurança existentes na sua instância Now Platform.
   Todos os valores de campo selecionados no campo de entrada de seleção múltipla devem corresponder para que os critérios de agregação sejam atendidos e para que este incidente de entrada possa ser anexado a um incidente de segurança existente. Esta seleção implica que é uma condição *E* em que campos, como Observáveis e Itens de configuração que podem ter vários valores de campo, são mapeados para eles. Se apenas um subconjunto dos valores for correspondido, as condições de agregação de incidente do Azure Sentinel não serão atendidas e um novo incidente de segurança será criado.
3. Para adicionar várias condições de correspondência de campo, clique em **Adicionar novos critérios**
   A agregação ocorrerá se qualquer uma das condições do campo de seleção múltipla que você definir forem atendidas. Esta seleção implica a condição *OU*.
4. Para atualizar a anotação de trabalho de um novo incidente quando ele for adicionado a um incidente de segurança, selecione **Registrar anotação de trabalho para novo incidente**.

   A anotação de trabalho registra que um novo incidente foi adicionado e inclui um link para os detalhes do incidente. A anotação de trabalho de log também atualiza mais detalhes que você adiciona ao campo de anotação de trabalho em sua seção de mapeamento.
5. Para configurar a programação, clique em **Continuar**.

O que Fazer Depois

Defina uma programação para recuperar os dados do incidente e os incidentes ingeridos que correspondem aos critérios no perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Programar a Microsoft Azure Sentinel recuperação de incidente

Defina uma programação para recuperar os dados do incidente e para incluir os Microsoft Azure Sentinel incidentes que correspondem aos critérios no perfil.

Antes de Iniciar

Função necessária: sn_sni.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode planejar com que frequência deseja pesquisar futuros Microsoft Azure Sentinel incidentes que correspondam à configuração do perfil de incidente.

Para habilitar a ingestão automatizada de incidentes, você deve configurar a programação e a recuperação de incidentes antes de ativar o perfil. Para definir uma data e hora específicas para a ingestão inicial, habilite **definir tempo de ingestão de incidente**. A ingestão subsequente é baseada no período de intervalo de pesquisa.

O intervalo de pesquisa é configurado para cada perfil individualmente. Os diferentes intervalos de pesquisa podem afetar o desempenho da integração de incidente Microsoft Azure Sentinel. Ao programar, planeje equilibrar a carga do sistema em relação à urgência de um incidente. Um valor padrão de um minuto é definido para todos os perfis. Você pode modificar esta configuração com base na urgência do incidente e na carga antecipada em seu sistema.

Todos os alertas adicionados ao incidente em um intervalo de pesquisa específico, haverá um processo executado e, em seguida, anexado às listas relacionadas de alertas do Azure Sentinel e a anotação de trabalho também será publicada.

Procedimento

1. No formulário de programação, preencha os campos.

   Configure a programação para definir como e quando você extrai incidentes do locatário Microsoft Azure.

   Formulário de programação

Campo	Descrição
Ingestão de incidentes em andamento	Ingestão de incidentes em andamento que a instância Now Platform extrai do locatário Microsoft Azure para novos incidentes. Os incidentes de segurança serão criados se forem encontrados incidentes acionados e os critérios de filtragem de geração de incidentes corresponderem.
Incrementos de pesquisa (minutos)	Frequência de pesquisa definida em minutos.
Definir tempo de ingestão do incidente	Ingestão de incidente que se baseia na data e hora configuradas. Você pode usar esta opção para definir uma data e hora específicas para a ingestão inicial. As adições subsequentes são baseadas no período de intervalo de pesquisa.
Tempo de adição do incidente de entrada	Data e hora que você especifica para a ingestão de incidentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Recuperação Única	Marque esta caixa de seleção para permitir a recuperação única de incidentes históricos do Azure Sentinel e fazer a reconciliação dos dados. Quando você seleciona este check-ox, a aplicação extrai todos os incidentes do Azure Sentinel abertos e fechados pelo período de até 6 meses aproximadamente. Ao processar os dados, os incidentes em andamento e os dados históricos são extraídos, mas o processamento dos incidentes em andamento tem precedência sobre a extração histórica e, caso contrário, a extração histórica pode levar algum tempo com base na duração e no número de incidentes que você está ingerindo . **Nota:** Os incidentes históricos do Azure Sentinel recuperados passam por verificações de desduplicação para evitar duplicações na aplicação Security Incident Response.
Desde a data	A data desde quando os incidentes históricos são ingeridos do Azure Sentinel. **Nota:** Os dados do incidente são extraídos aproximadamente dos últimos 6 meses.

A página de programação permite que você defina como e quando os incidentes são extraídos do locatário Microsoft Azure.

2. Para navegar até a página Opções adicionais, clique em **Continuar**.

Automatizar as atualizações e fechamentos de incidentes pelo status do incidente SIR

Automatize as atualizações e os fechamentos de incidentes pelo status do incidente SIR. A integração Microsoft Azure Sentinel tem uma interface bidirecional que permite que ambos os incidentes criem incidentes de segurança e atualizem os incidentes depois que o incidente de segurança é criado ou encerrado.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. No formulário, preencha os detalhes.
   Siga as instruções para concluir a configuração para atualizar incidentes ao criar ou fechar um incidente de segurança em SIR.

Formulário Automatizando atualizações de incidente

Categoria	Campo	Descrição
Atualizações de criação de incidente	Atualizar status de incidentes do Azure Sentinel após a criação do incidente no SIR	Opção que permite usar a funcionalidade de atualização de incidente automatizada. O status do incidente Microsoft Azure

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Categoria	Campo	Descrição
		Sentinel é atualizado no incidente Microsoft Azure com os comentários depois que o incidente SIR é criado no Now Platform.
	Atualização de status de incidente inicial	Status do incidente inicial que é atualizado no ambiente Microsoft Azure Sentinel. Você pode selecionar **Novo** ou **Ativo** como o status.
	Comentários iniciais retornados para o incidente	Comentários iniciais que são publicados no incidente no ambiente Microsoft Azure Sentinel. Edite o texto padrão exibido na seção de comentários adicionando ou modificando as variáveis de substituição usando o formato ${field name}$ para qualquer campo no formulário de incidente SIR.
Atualizações de fechamento de incidentes	Fechar incidentes do Azure Sentinel após o fechamento do incidente no SIR	Opção que permite usar a funcionalidade de atualização de status de incidente automatizada. Microsoft Azure Sentinel incidentes são encerrados no incidente Microsoft Azure com os comentários fornecidos depois que o incidente SIR é encerrado no Now Platform.
	Atualização de status de incidente de fechamento	Atualização de status no incidente Microsoft Azure Sentinel quando o incidente é encerrado em SIR.
	Comentários de fechamento publicados de volta para o incidente	Comentários que são publicados no incidente no incidente Microsoft Azure Sentinel quando o incidente é encerrado em SIR. Edite o texto padrão exibido na seção de comentários adicionando ou modificando as variáveis de substituição usando o formato ${field name}$ para qualquer campo no formulário de incidente SIR.
	Classificação de incidente e motivo do fechamento	Método para a classificação do incidente e o motivo do fechamento que é usado para fechar o incidente no ambiente Microsoft Azure Sentinel. Selecione a **classificação de incidente padrão e o método de motivo de fechamento** para fechar o incidente no ambiente Microsoft Azure Sentinel. Ao selecionar

Tradução automática

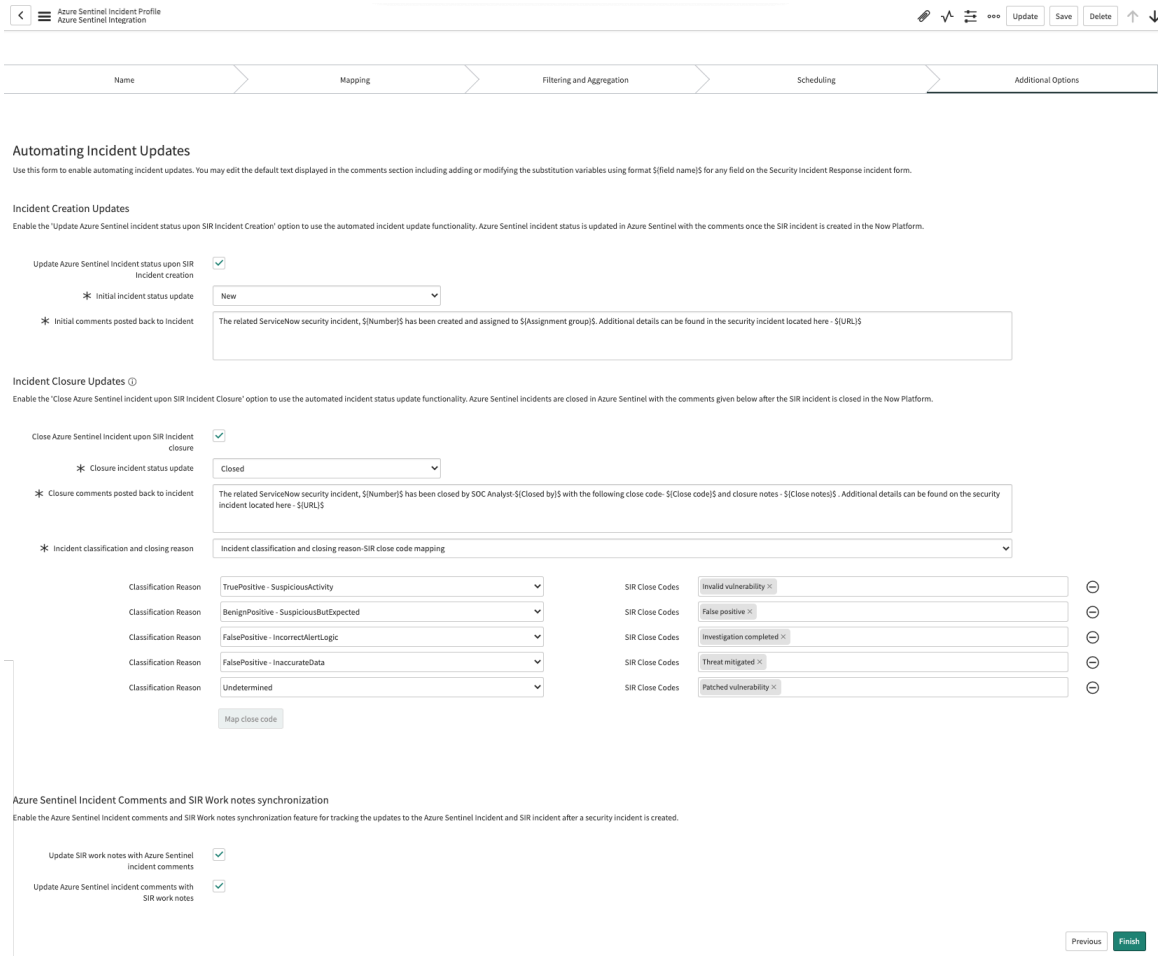
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Categoria	Campo	Descrição
		este método, você deve definir a **classificação de incidente padrão e o motivo de fechamento**. Quando você fecha um incidente no SIR, o status do incidente no Azure Sentinel também é fechado com a **classificação de incidente padrão e o motivo de fechamento**especificados. Selecione o método de **mapeamento de código de encerramento SIR de classificação de incidente e motivo de encerramento** para encerrar os incidentes e mapear os motivos de classificação com os códigos de encerramento SIR. Você pode mapear vários códigos de fechamento SIR para um único motivo de classificação. Depois de fechar um incidente em SIR usando o código de fechamento, o status do incidente no Azure Sentinel também é fechado com a classificação de incidente mapeada e o motivo de fechamento. Se o motivo da classificação e os códigos de encerramento SIR não estiverem mapeados ou uma correspondência não for encontrada, o incidente será encerrado usando o motivo de classificação padrão como "Indeterminado" no ambiente Microsoft Azure Sentinel.
Sincronização de Anotações de trabalho de SIR e comentários de incidente do Azure Sentinel	Atualizar anotações de trabalho SIR com comentários de incidentes do Azure Sentinel	Opção que você pode selecionar para atualizar seus Microsoft Azure Sentinel comentários nas SIR anotações de trabalho. O comentário nas anotações de trabalho SIR aparece com o prefixo `Comentário do Sentinel`. O comentário também contém o ID do Sentinel, os detalhes do analista e o carimbo de data/hora.
	Atualizar comentários de incidentes do Azure Sentinel com anotações de trabalho SIR	Opção que você pode selecionar para atualizar suas SIR anotações de trabalho nos Microsoft Azure Sentinel comentários do incidente. O comentário em Microsoft Azure Sentinel aparece com o prefixo `Comentário da ServiceNow`.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O exemplo a seguir mostra as opções de configuração que estão disponíveis para automatizar as atualizações de incidentes.



2. Clique em **Concluir**.

O que Fazer Depois

O perfil passa para o estado Aguardando. Quando a mensagem de confirmação mostrar que a instalação e a configuração estão concluídas, você poderá ativar o perfil.

Copiar um perfil Microsoft Azure Sentinel

Copie um perfil existente e suas configurações associadas em vez de criar um perfil. Ao criar vários perfis, você pode reutilizar as configurações de um perfil existente copiando esses perfis.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Quando você copia um perfil, o nome do perfil é modificado inicialmente para evitar a criação de perfis duplicados. O perfil copiado também é desativado (definido como falso) para garantir que você não o ative acidentalmente antes de concluir a configuração. Você pode copiar os perfis e usar mapas existentes para incidentes de segurança que você já visualizou e verificou.

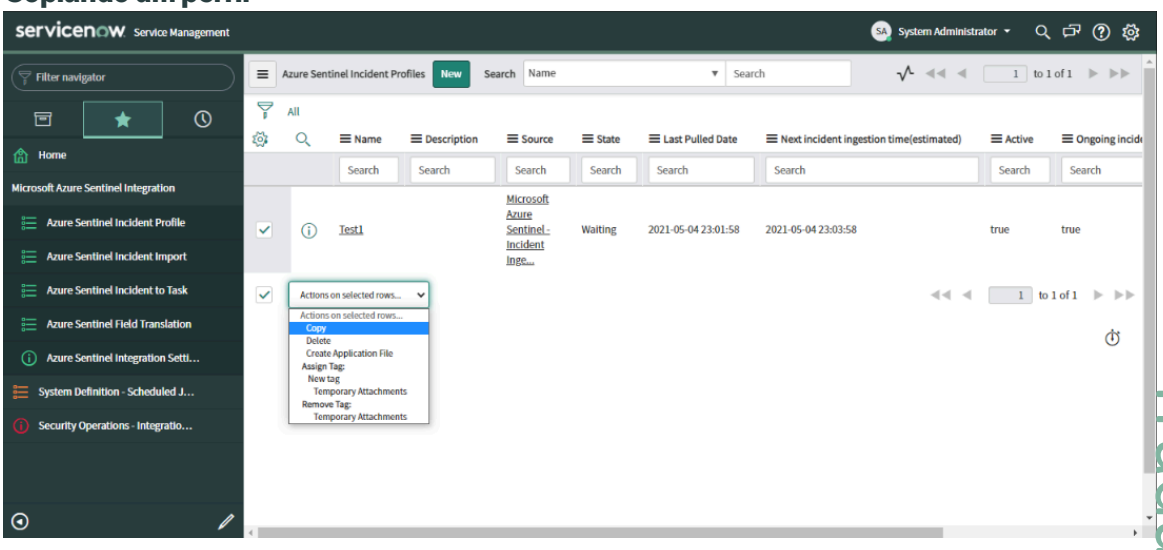
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

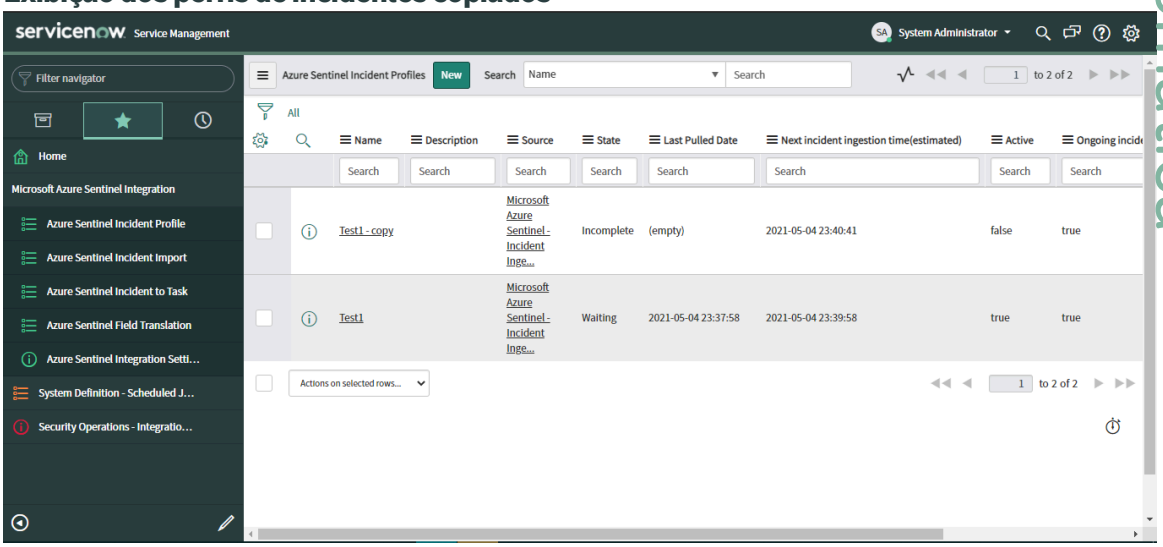
1. Navegar até **Todos** > **Integração do Microsoft Azure Sentinel** > **Perfil do Azure Sentinel**.
2. Na lista Perfis do Azure Sentinel, selecione um perfil que você deseja copiar e, na lista Ações nas linhas selecionadas, clique em **Copiar** conforme mostrado no exemplo a seguir.

Copiando um perfil



O perfil é copiado e exibido na lista, conforme mostrado no exemplo a seguir. A cópia tem todas as configurações do perfil original, incluindo o mapeamento e a configuração de programação. O nome do perfil contém a palavra "cópia". Embora o perfil original esteja habilitado (verdadeiro), a cópia está desativada neste ponto (falso). Você pode preferir editar valores do perfil copiado e renomeá-los para que as definições de configuração se apliquem ao novo perfil, conforme necessário.

Exibição dos perfis de incidentes copiados



Você copiou com sucesso as configurações de um perfil existente para um novo perfil. O status da coluna Ativo é definido como falso, o que significa que o perfil deve ser ativado.

SIR formulário após ingestão de um incidente

Depois que o Now Platform ingere o incidente Microsoft Azure Sentinel, um incidente de segurança é criado e as atualizações são feitas nesse registro de incidente de segurança.

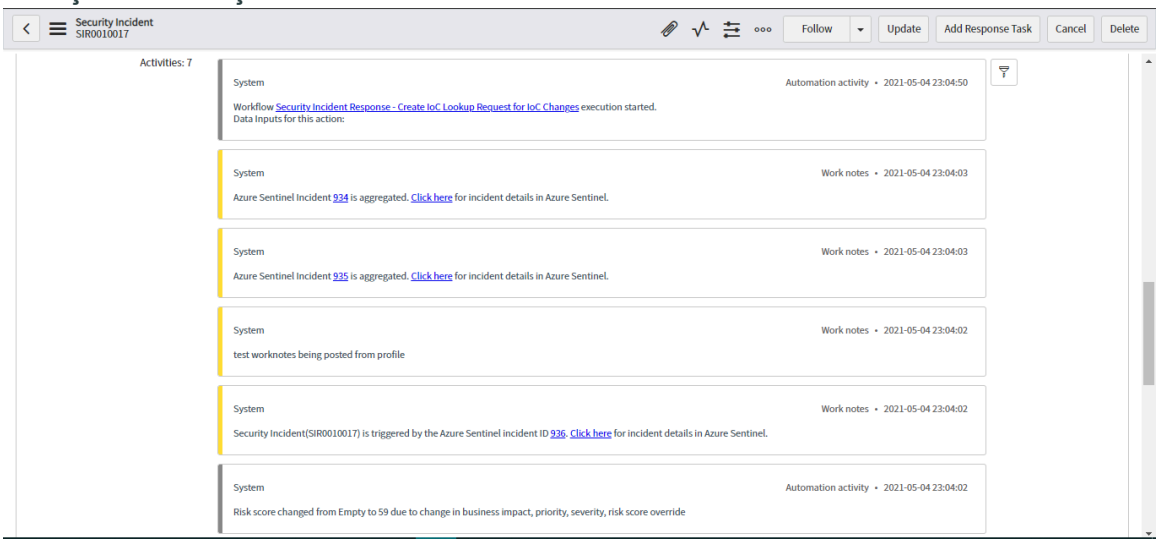
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Anotações de trabalho

Uma anotação de trabalho será publicada quando um incidente for agregado e se você tiver configurado a opção **Registrar anotação de trabalho para novo incidente** nos Critérios de agregaçãode incidente. O exemplo a seguir mostra as anotações de trabalho em SIR.

Exibição de anotações de trabalho no SIR



Ao clicar no número do incidente, você pode exibir o registro de importação do incidente interno que contém os dados brutos do incidente. O exemplo a seguir mostra os dados brutos do incidente em SIR.

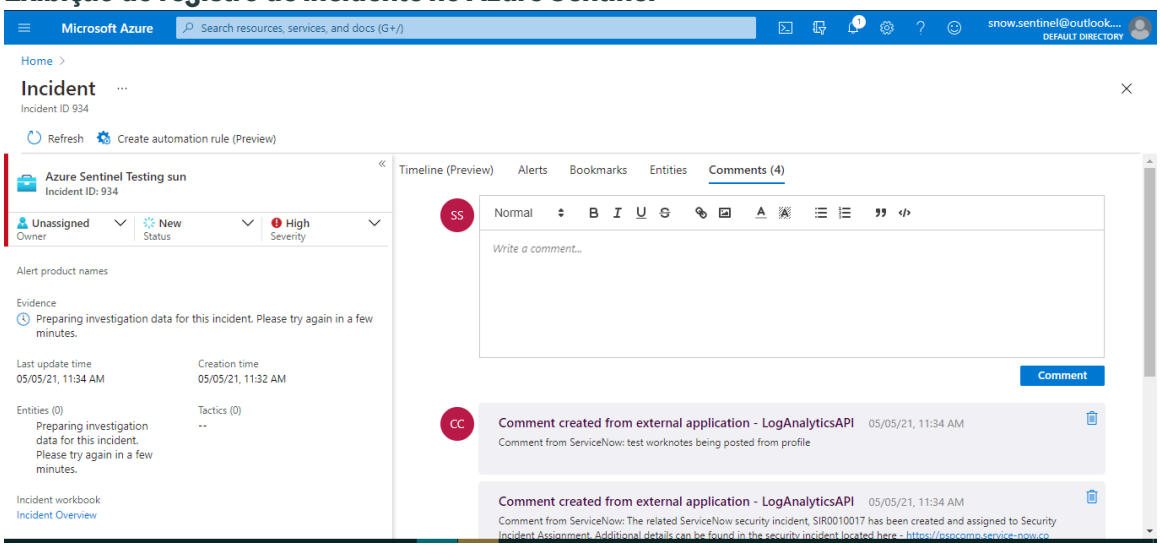
Exibição dos dados brutos do incidente no SIR

Ao clicar no link **Clique aqui**, você pode exibir o registro no ambiente Microsoft Azure Sentinel. O exemplo a seguir mostra o registro no ambiente Microsoft Azure Sentinel.

Tradução automática

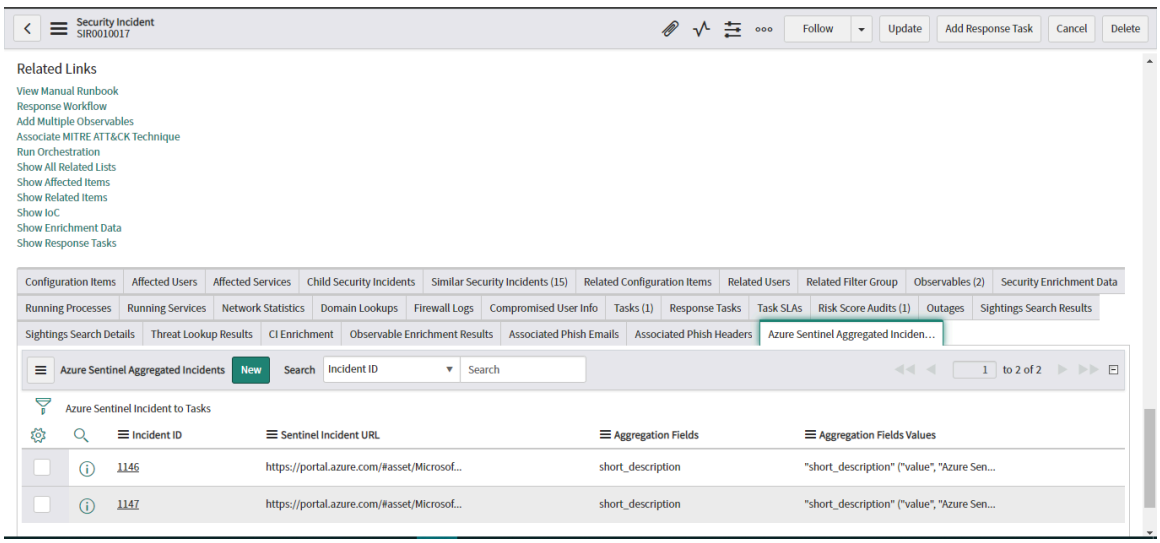
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição do registro de incidente no Azure Sentinel



Incidentes agregados do Sentinel

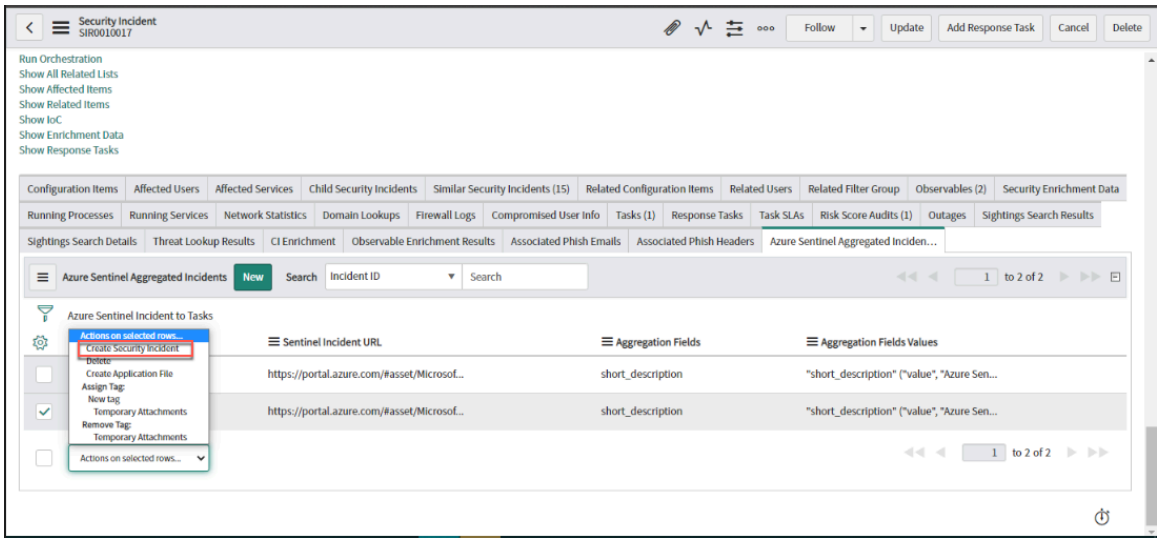
Exibir incidentes agregados do Sentinel: exibe os incidentes que estão agregados ao incidente de segurança. Navegar até **Mostrar Todas as Listas Relacionadas** > **Incidentes agregados do Microsoft Azure Sentinel**.



Criar incidente de segurança: selecione um incidente na lista, clique no menu **Ações** e em **Criar incidente de segurança**. Esta opção cria um novo incidente de segurança para o incidente e este incidente é desagregado do incidente de segurança primário.

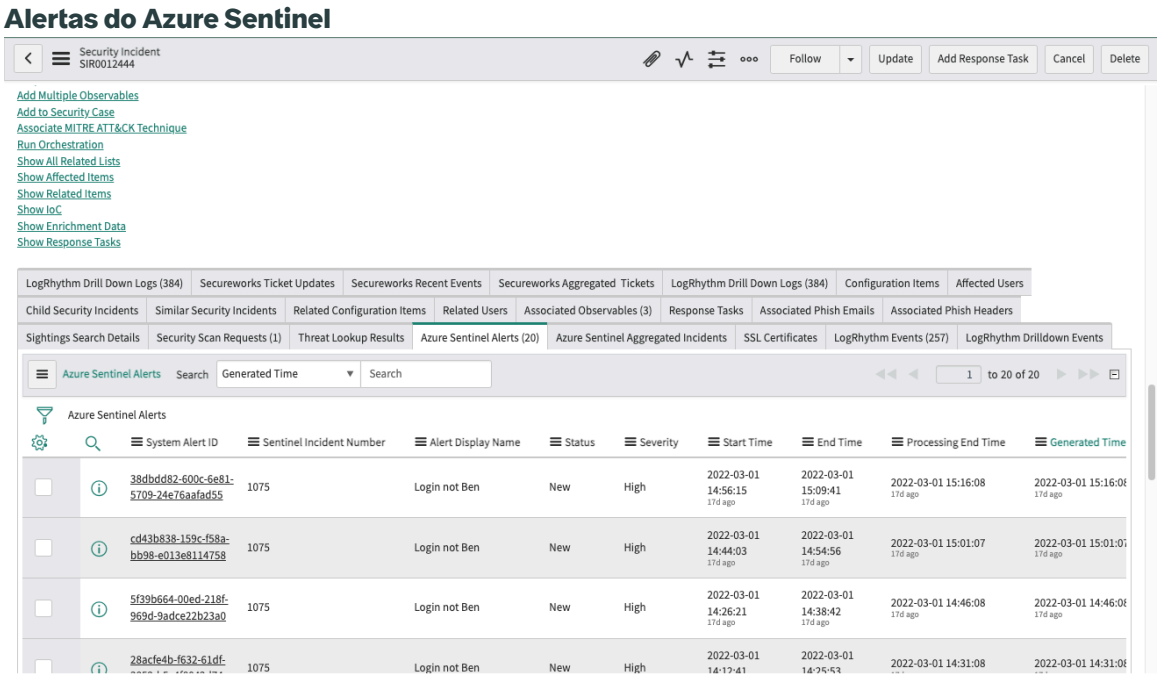
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Alertas do Azure Sentinel

Para exibir os alertas associados ao incidente do Sentinel que acionou o incidente de segurança, navegue até **Mostrar Todas as Listas Relacionadas** > **Alertas do Azure Sentinel**.



Revisar as configurações de integração Microsoft Azure Sentinel

Revise as configurações de integração Microsoft Azure Sentinel para que você possa modificar as propriedades do sistema para adequá-las ao seu ambiente.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Integração do Microsoft Azure Sentinel** > **Configurações de integração do Azure Sentinel**.
2. Modifique as configurações a seguir conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Microsoft Azure Sentinel Configurações de integração

Nome da Propriedade	Descrição
Imponha um limite no número de dias para os quais os dados de amostra podem ser obtidos. sn_sec_sentinel.max_num_of_days_for_sample_data	Número máximo de dias para os quais você pode buscar dados de amostra do ambiente Microsoft Azure Sentinel. Tipo: inteiro Valor padrão: 7
Receba atualizações relacionadas a novos alertas vinculados ao SIR. sn_sec_sentinel.incident_updates	Ative a opção para receber atualizações de incidentes. Tipo: booleano Valor padrão: Verdadeiro
O caractere delimitador para dividir os valores em mapeamentos de campo Microsoft Azure Sentinel. sn_sec_sentinel.delimiter	O caractere delimitador para dividir os valores em mapeamentos de campo Microsoft Azure Sentinel. Tipo: cadeia de caracteres Valor padrão: ', ' (vírgula com espaço)
Imponha um limite no número de incidentes de amostra que podem ser obtidos. sn_sec_sentinel.max_num_of_sample_incidents_per_call	Número máximo de incidentes de amostra que você busca no ambiente Microsoft Azure Sentinel para ingestão. Tipo: inteiro Valor padrão:5 Valor máximo de amostra: 20
Imponha um limite no número de incidentes do Sentinel que podem ser agregados a um único incidente. sn_sec_sentinel.max_aggregations_per_si	Limite de agregação de incidentes de segurança. Por exemplo, se houver 102 incidentes, os primeiros 100 serão agregados ao security incident_1 e os 2 restantes ao security incident_2. Tipo: inteiro Valor padrão: 100
Imponha um limite para o número de incidentes de segurança que podem ser criados em um período de 24 horas. sn_sec_sentinel.max_si_per_day	Número máximo de incidentes de segurança que podem ser criados em um período de 24 horas no Now Platform. Tipo: inteiro Valor padrão: 1000
Limite máximo de paginação para buscar os dados do incidente em uma chamada REST.	Limite de paginação para buscar os dados do incidente em uma chamada REST do ambiente Microsoft Azure Sentinel.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da Propriedade	Descrição
sn_sec_sentinel.max_page_size	Tipo: inteiro Valor padrão: 100
Valor da versão da API para incidentes. sn_sec_sentinel.sentinel_security_incident_api_version	A versão da API da Microsoft para recuperar incidentes do Sentinel. Valor padrão: 2021-10-01
Valor da versão da API para alertas. sn_sec_sentinel.sentinel_security_alert_api_version	A versão da API da Microsoft para recuperar alertas do Sentinel. Valor padrão: 2021-10-01
Valor da versão da API para entidades. sn_sec_sentinel.sentinel_security_entities_api_version	A versão da API da Microsoft para recuperar entidades do Sentinel. Valor padrão: 2021-10-01
sn_sec_sentinel.log.verbosity	O nível de detalhamento do log da aplicação, ou seja, o nome do tipo de informação. Você também pode atualizar o valor para as seguintes opções: ○ **error** ○ **aviso** ○ **informações** ○ **depurar** Valor padrão: **informações**.

3. Clique em **Salvar**.
   Suas configurações de integração modificadas são aplicadas no próximo intervalo de pesquisa, conforme definido no perfil.

Domain Separation e a integração Microsoft Azure Sentinel

A separação de domínio é compatível com esta aplicação. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Básico

- Lógica de negócios: confirme se os dados vão para o domínio adequado para os casos de uso do provedor de serviço de aplicativo.
- O aplicativo oferece suporte à separação de domínio em tempo de execução. O Domain Separation inclui separação de domínio de interface do usuário, chaves de cache, relatórios, acúmulos e agregações.
- O proprietário da instância deve configurar o aplicativo para funcionar em vários locatários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de caso de uso: quando um SP (service provider, provedor de serviço) usa o bate-papo para responder à mensagem de um locatário-cliente, o cliente deve conseguir ver a resposta do SP.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como o Domain Separation funciona na integração Microsoft Azure Sentinel

Siga estas etapas para obter a separação de domínio:

- Crie um usuário com a função sn_si.admin no respectivo domínio.

  Nota:
  Ao criar o perfil, use o seletor de domínio para selecionar um domínio. Não crie o usuário no domínio primário e, posteriormente, altere o domínio do perfil. Você deve ter um usuário para cada domínio do seu perfil com a função sn_si.admin. Use este usuário para criar ou modificar configurações no perfil.

- Desabilite os trabalhos programados existentes.
- Replique os seguintes trabalhos programados para cada domínio:
  - Alertas e entidades de busca do Azure Sentinel
  - Sincronização de comentários do Azure Sentinel
  - Atualização de status do Azure Sentinel
  - Processo de perfil do Azure Sentinel
  - Dados brutos do processo do Azure Sentinel
  - Limpeza de dados do Azure Sentinel
  - Extração de comentário histórico do Azure Sentinel

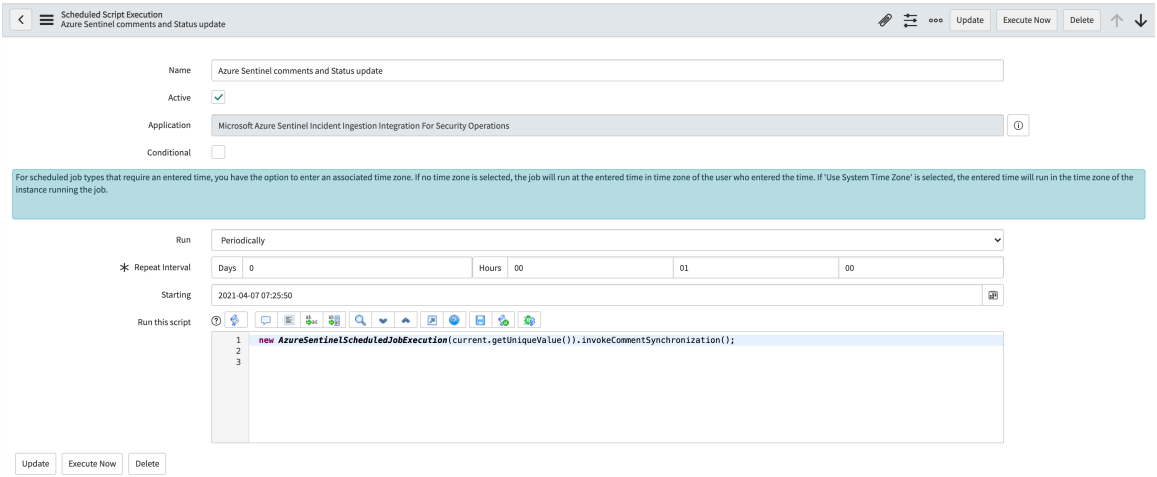
  Nota:
  Depois de replicar os trabalhos programados, use o navegador e pesquise o módulo Políticas de acesso ao módulo, exiba os registros criados recentemente cujo **Script de destino** mostra os trabalhos programados recém-criados. Modifique o valor do campo **Resultado** para **Rastrear**.

- Altere **Executar como** do usuário do sistema para o usuário com a função sn_si.admin no respectivo domínio e execute o trabalho programado.

O exemplo a seguir mostra como replicar os comentários do Azure Sentinel e o trabalho de atualização de status e executar o trabalho como um usuário do sistema.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tópicos relacionados

Domain Separation para provedores de serviço

Comparando integrações Microsoft Azure Sentinel e API de Segurança do Microsoft Graph com SIR

Você pode exibir as diferenças entre as integrações Microsoft Azure Sentinel e API de Segurança do Microsoft Graph e escolher a integração correta com sua instância Now Platform.

Visão geral Microsoft Azure Sentinel – Ingestão de incidentes

Microsoft Azure Sentinel é uma solução baseada em nuvem de gestão de eventos de informações de segurança (SIEM) e resposta automatizada de orquestração de segurança (SOAR). Microsoft Azure Sentinel fornece análise de segurança inteligente e inteligência contra ameaças em toda a empresa. Ele fornece uma solução única para detecção de alertas, visibilidade de ameaças, busca proativa e resposta a ameaças.

Visão geral API de Segurança do Microsoft Graph

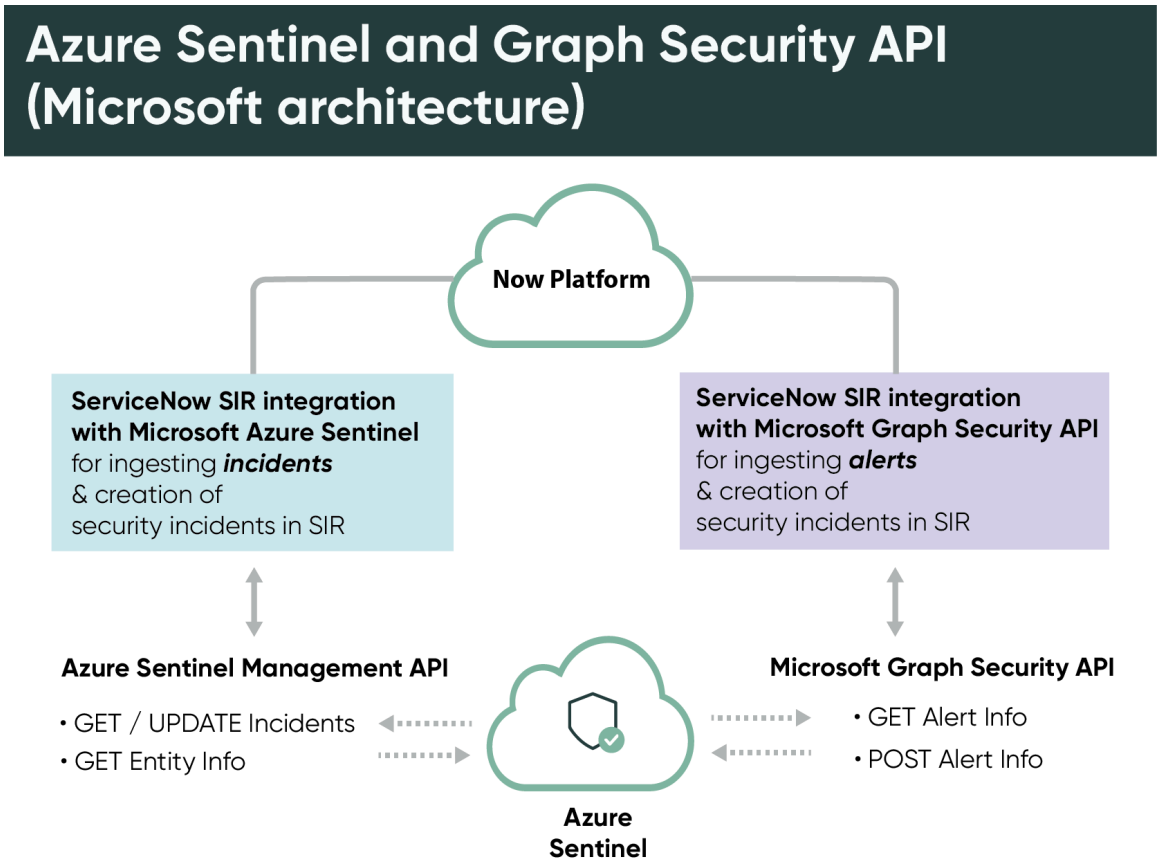
O API de Segurança do Microsoft Graph é um serviço intermediário (ou agente) que fornece uma única interface programática para conectar vários provedores de segurança (nativos da Microsoft, bem como parceiros ServiceNow).

A integração API de Segurança do Microsoft Graph resolve esses problemas usando o API de Segurança do Microsoft Graph para se conectar a diferentes tecnologias de segurança da Microsoft, como Azure Sentinel, Microsoft Defender Advanced Threat Protection e Azure Advanced Threat Protection. Os alertas dos provedores de segurança da Microsoft são ingeridos e os incidentes de segurança são criados automaticamente em Security Incident Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resumo das diferenças de recurso



Microsoft Azure Sentinel versus API de Segurança do Microsoft Graph

Microsoft Azure Sentinel	API de Segurança do Microsoft Graph
Ingere Microsoft Azure Sentinel incidentes junto com informações da entidade (quando disponíveis) e automatiza a criação de incidentes de segurança em SIR.	Ingere alertas de vários provedores de segurança (incluindo o Azure Sentinel) em um esquema padrão e automatiza a criação de incidentes de segurança em SIR.
Automatiza Microsoft Azure Sentinel atualizações de status de incidente para o Security Incident Response para que você possa criar e fechar incidentes de segurança. **Nota:** ServiceNow atualiza o status de Microsoft Azure Sentinel incidentes com base na criação ou no fechamento do incidente de segurança.	Oferece suporte a atualizações de alerta (mudança de status de alerta e fechamento de alerta) para provedores de segurança selecionados. **Nota:** Para obter mais informações sobre os API de Segurança do Microsoft Graph provedores de segurança compatíveis, consulte a documentação da Microsoft.
Use esta integração se o cenário incluir as seguintes condições:	Use esta integração se o cenário incluir as seguintes condições:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Microsoft Azure Sentinel versus API de Segurança do Microsoft Graph

Microsoft Azure Sentinel	API de Segurança do Microsoft Graph
• A investigação de incidente preliminar está em Microsoft Azure Sentinel e a investigação subsequente está em SIR • Ingerir Microsoft Azure Sentinel incidentes para SIR	• Executar investigação de incidentes em SIR. • Inclua Microsoft Azure Sentinel alertas em SIR. • Os incidentes não são criados em Microsoft Azure Sentinel.
O alerta é uma entidade em Microsoft Azure Sentinel. Você não pode recuperar alertas autônomos ou específicos usando a API de gestão Microsoft Azure Sentinel. Você só pode recuperar os dados de alerta associados a um incidente. Os dados de alerta disponíveis usando esta integração são mais avançados do que os dados de alerta disponíveis usando API de Segurança do Microsoft Graph.	Os dados de alerta normalizados Microsoft Azure Sentinel estão disponíveis. Os campos de alerta Microsoft Azure Sentinel que são mapeados internamente em API de Segurança do Microsoft Graphe estão disponíveis em API de Segurança do Microsoft Graphestão disponíveis para uso nesta integração.
	Você não pode atualizar alertas em Microsoft Azure Sentinel usando esta integração.

Integração de Microsoft Defender for Endpoint

O Microsoft Defender for Endpoint permite que você inspecione, analise e contenha proativamente ameaças conhecidas e desconhecidas em qualquer endpoint.

A integração Microsoft Defender for Endpoint ajuda os analistas de segurança a investigar e corrigir incidentes de segurança com eficiência sem precisar navegar entre as ferramentas.

Você pode usar esta integração para criar configurações para recuperar os detalhes do host, detalhes de usuários conectados, detalhes de máquinas relacionadas e outros recursos de aprimoramento. Você pode solicitar para isolar qualquer máquina de acessar as redes ou remover as máquinas do isolamento. As solicitações podem ser aceitas ou rejeitadas pelos aprovadores.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Principais recursos

Microsoft Defender for Endpoint tem os seguintes recursos principais:

- Execute a Pesquisa de segurança corporativa para detectar possíveis observáveis maliciosos nos endpoints e tome medidas de correção.
- Execute ações de resposta, como Isolar host, Remover isolamento, Restringir a execução da aplicação, Executar verificação antivírus, Remover restrição da aplicação e Parar e colocar arquivo em quarentena.
- Crie ou atualize indicadores.
- Execute o aprimoramento observável e recupere dados relacionados a indicadores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Microsoft Defender for Endpoint

Explorar	Instalar	Configurar
Introdução ao Microsoft Defender for Endpoint	Instalar a aplicação e configurar uma origem para a integração	Configurar perfis e incidentes de segurança para o Microsoft Defender for Endpoint
Perfil de capacidade	**Configurações adicionais**	**Diversos**
Crie um perfil de recurso para a integração do Microsoft Defender for Endpoint.	Configurações adicionais que você pode executar no Microsoft Defender for Endpoint	Crie e configure um perfil para pesquisa de vistas e indicadores com o Microsoft Defender para endpoint.

Registrar e configurar o Microsoft Defender for Endpoint no portal Microsoft Azure

Registre a aplicação Microsoft Defender for Endpoint no portal do Microsoft Azure e conceda o acesso de leitura e gravação à aplicação.

Antes de Iniciar

Função necessária: desenvolvedor de aplicações, administrador de locatário.

Procedimento

1. Faça login no portal do Microsoft Azure.
2. Insira Registros do app na caixa Pesquisar e clique em **Clicar em Novo registro**.
3. Insira um nome para sua aplicação e o URI de redirecionamento e clique em **Registrar**.
   Um nome de exemplo é Microsoft Defender for Endpoint. O URI de redirecionamento é usado ao fornecer o consentimento do administrador para a aplicação.
4. Na página **Registros** da aplicação, selecione a aplicação que você registrou na Etapa 3.
5. Em Gerenciar, selecione **Certificados e segredos**.
6. Para criar um segredo do cliente, selecione **Novo segredo do cliente**.
7. Copie o segredo do cliente e salve-o.

   Caso tenha esquecido o segredo do cliente, você pode gerar um novo segredo do cliente.
8. Navegar até **Gerenciar** > **Permissões de API**.
9. Clique **em Adicionar uma permissão**.
10. Na janela Solicitar permissões de API, clique na guia **APIs que minha organização usa**.
11. Pesquise e selecione **WindowsDefenderATP**.
12. Nas permissões do WindowsDefenderATP, selecione **Permissões da aplicação**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Habilitar esta permissão garante que a aplicação seja executada como um serviço ou daemon em segundo plano sem um usuário conectado.

13. Adicione as seguintes permissões de nível de aplicação e conceda o consentimento do administrador para as permissões de API recém-adicionadas.

Permissão	Nome de exibição da permissão
Máquina.Leitura.Todos	Ler todos os perfis de máquina
User.Read.All	Ler perfis de usuário
Isolar.Máquina	Isolar máquina
ExecuçãoRestrita.Máquina	Restringir execução de código
Varredura.Máquina	Verificar máquina
Máquina.PararEmQuarentena	Parar e colocar em quarentena
URL.Leitura.Todos	URLs de Leitura
Arquivo.Leitura.Todos	Ler perfis de arquivo
IP.Leitura.Todos	Ler perfis de endereço IP
Ti.LeituraGravata.Todos	Ler e gravar indicadores

Introdução à integração Microsoft Defender for Endpoint

A seção a seguir lista as tarefas de configuração que você deve concluir em sua instância Now Platform® antes de instalar a aplicação Microsoft Defender for Endpoint da ServiceNow Store.

Antes de Iniciar

Função necessária: administrador

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração sem problemas.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções necessárias da Now Platform e do Security Incident Response (SIR).	As seguintes funções são necessárias: 1. Você deve ter a função de administrador do sistema (admin) para instalar a aplicação para a integração. 2. Você deve ter a função de administrador de incidentes de segurança (sn_si.admin) para configurar a integração, criar, ativar e remover perfis. 3. Você deve ter a função de analista de incidentes de segurança (sn_si.analyst) para trabalhar com incidentes de segurança. Um usuário com esta função pode iniciar qualquer um dos recursos disponíveis na integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
Verifique se as aplicações principais da ServiceNow necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação.	Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se essas aplicações ainda não estiverem instaladas, você deverá instalar e ativar cada aplicação uma de cada vez na seguinte ordem para garantir uma instalação sem problemas: **1.** Security Incident Response **2.** Tempo de execução do ServiceNow IntegrationHub (com.glide.hub.integration.runtime) **3.** Etapa de ação do ServiceNow IntegrationHub — REST (com.glide.hub.action_step.rest)
Antes de habilitar a opção de aprovação para perfis, verifique se você criou um grupo de aprovação.	Um fluxo de trabalho de aprovação opcional está disponível para isolar máquinas host, restaurá-las na rede e executar ações adicionais no endpoint. Se sua organização deseja um nível extra de controle sobre essas ações, habilite a opção Requer aprovação durante a configuração dos perfis. Em um cenário em que o perfil está disponível, a configuração do perfil para aprovação tem precedência. Em um cenário em que o perfil está indisponível, as aprovações são tratadas com base nas configurações padrão. Como administrador de segurança, você pode configurar a aprovação ao configurar os perfis e as configurações padrão. Um grupo de aprovação deve estar disponível na lista Grupos em sua instância. Para monitorar e processar solicitações enviadas pelos usuários com a função sn_si.analyst, cada membro do grupo de aprovação deve navegar até Minhas aprovações no Now Platform®. Como alternativa, os aprovadores podem encontrar as solicitações enviadas exclusivamente para integração Microsoft Defender for Endpoint no módulo Aprovações. Para obter mais informações sobre como criar um grupo de usuários, consulte Criar um grupo de usuários .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Você configurou com sucesso sua instância Now Platform® para a integração Microsoft Defender for Endpoint. A próxima etapa é instalar a aplicação Microsoft Defender for Endpoint da ServiceNow Store para a integração.

Instalar a aplicação e configurar uma origem para a integração

Instale e configure a integração Microsoft Defender for Endpoint do ServiceNow Store na sua instância Now Platform. Comece a criar perfis de capacidade usando as configurações.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

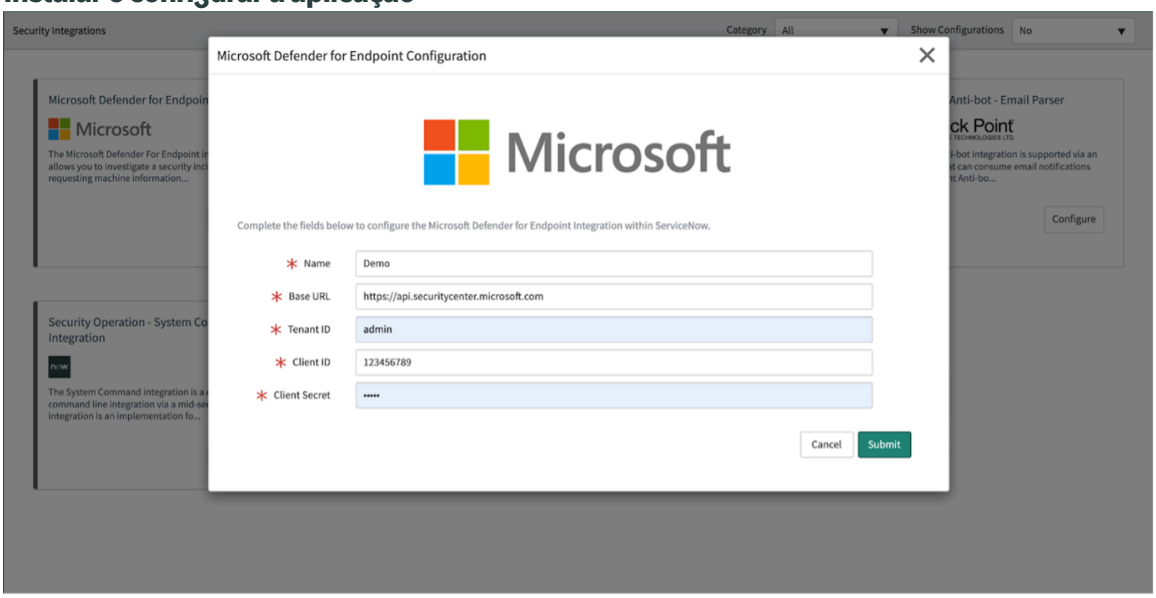
1. Baixe a integração do Microsoft Defender for Endpoint em ServiceNow Store e instale-a.
2. Navegar até **Security Operations** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco Microsoft Defender for Endpoint e clique em **Configurar**.
4. No formulário, preencha os campos a seguir.

Configurar o Microsoft Defender para endpoint

Nome	Nome da configuração da instância Microsoft Defender for Endpoint.
URL base	O URL da base de serviço para Microsoft Defender for Endpoint
ID de locatário	O Microsoft Defender for Endpoint ID de locatário. Todas as ações seriam realizadas nesta instância.
ID de cliente	ID de cliente da aplicação que você registrou no portal do Microsoft Azure.
Segredo do Cliente	Segredo do cliente para sua aplicação registrada.

5. Clique em **Enviar**.

Instalar e configurar a aplicação



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado
A lista de configurações Microsoft Defender for Endpoint é exibida com seu novo registro de configuração. Você concluiu a configuração do Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint Configurações padrão

Há definições de configuração adicionais que você deve executar após concluir a instalação.

Depois de concluir a instalação, você pode encontrar o módulo Configurações padrão na aplicação Microsoft Defender for Endpoint no painel de navegação esquerdo. Ele contém as configurações padrão para diferentes Microsoft Defender for Endpoint funcionalidades.

Funções necessárias: sn_si.admin, sn_si.analyst (somente leitura).

Configurações adicionais

A seguir estão as definições de configuração adicionais:

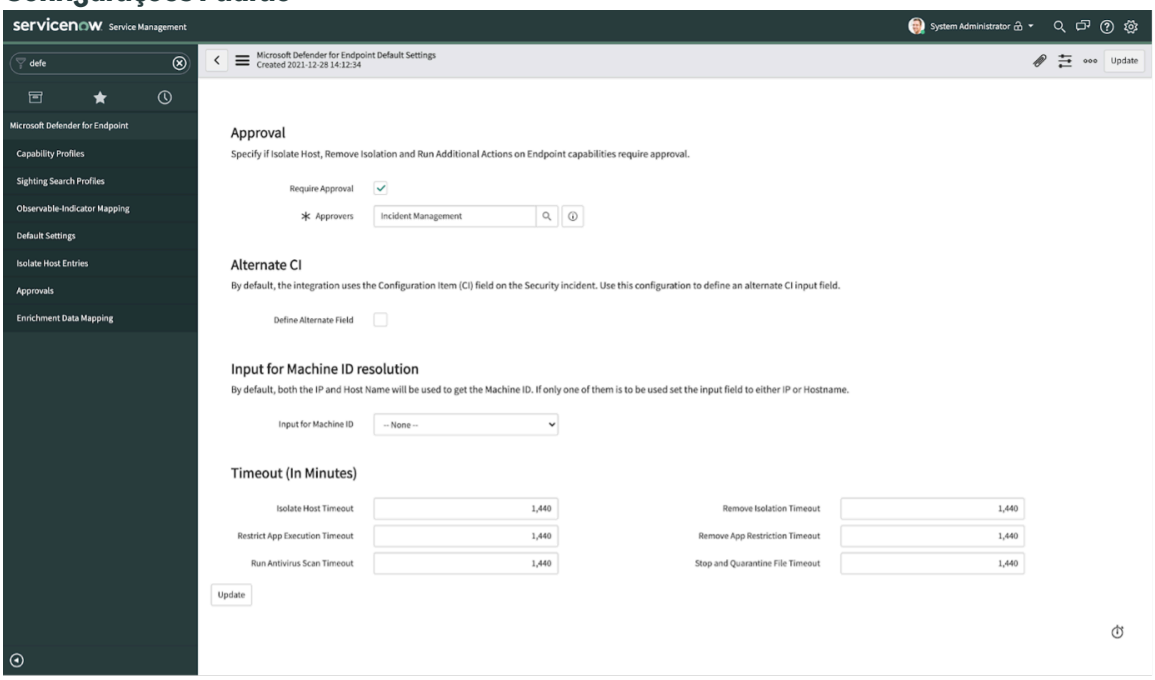
- **Aprovação**: esta aprovação é especificamente para a ação Isolar Host, Remover Isolamento de Host e ações adicionais, como Restringir a Execução da aplicação, Remover Restrição da aplicação e Executar Verificação Antivírus. Você pode usar esta aprovação somente quando as ações são acionadas diretamente da Lista relacionada e se não houver perfis existentes. Se houver perfis para esses recursos, a configuração de aprovação no perfil terá precedência.
  - **Exigir aprovação**: quando você habilita **Requer aprovação**, o campo Aprovadores fica disponível no formulário.
  - **Aprovadores**: lista de grupos de aprovadores. Depois de enviar uma solicitação, a aprovação é necessária do grupo para concluir a solicitação.
- **IC alternativo**: habilitar esta caixa de seleção fornece a lista de campos disponíveis para passar um IC alternativo para o recurso. Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança. Esta configuração é aplicável somente para a funcionalidade Executar ações adicionais no endpoint. Use esta configuração para definir um campo de entrada de IC alternativo para a única funcionalidade Executar ações adicionais no endpoint. Para os outros recursos, use a configuração na seção de perfil. Se os perfis não definirem um IC alternativo, os recursos usarão o campo IC do formulário de Incidente de segurança.
- **Entrada para resolução do ID do agente**: por padrão, o IP e o nome do host são usados para obter o ID do agente. Se você for usar apenas um deles, defina o campo de entrada como IP ou Nome do host.
- **Tempo limite**:
  - **Tempo Limite de Isolar Host (em minutos):** indica o limite de execução dos recursos de Isolar Host.
  - **Remover tempo limite de isolamento (em minutos):** indica o limite de execução para a capacidade Remover tempo limite de isolamento.
  - **Restringir o tempo limite de execução da aplicação (em minutos):** indica o limite de execução da capacidade de Restringir a execução da aplicação.
  - **Tempo Limite para Remover Restrição da Aplicação (em minutos):** indica o limite de execução para a capacidade Remover Restrição da aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Tempo Limite para Executar Verificação Antivírus (em minutos):** indica o limite de execução para o recurso Executar Verificação Antivírus.
- **Interromper e colocar arquivo em quarentena (em minutos):** indica o limite de execução para o recurso Interromper e colocar arquivo em quarentena.

Configurações Padrão



Mapear os tipos de indicador Microsoft Defender for Endpoint

Mapeie o tipo de observável da ServiceNow com o tipo de indicador Microsoft Defender for Endpoint. Este mapeamento seria usado nas ações Aprimoramento de observável e Criar indicador no Microsoft Defender.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst (somente leitura)

Por Que e Quando Desempenhar Esta Tarefa

Em um cenário em que o tipo de observável não está mapeado para um tipo de indicador, esses observáveis não são qualificados para aprimoramento de observável e criação de indicador no Microsoft Defender for Endpoint.

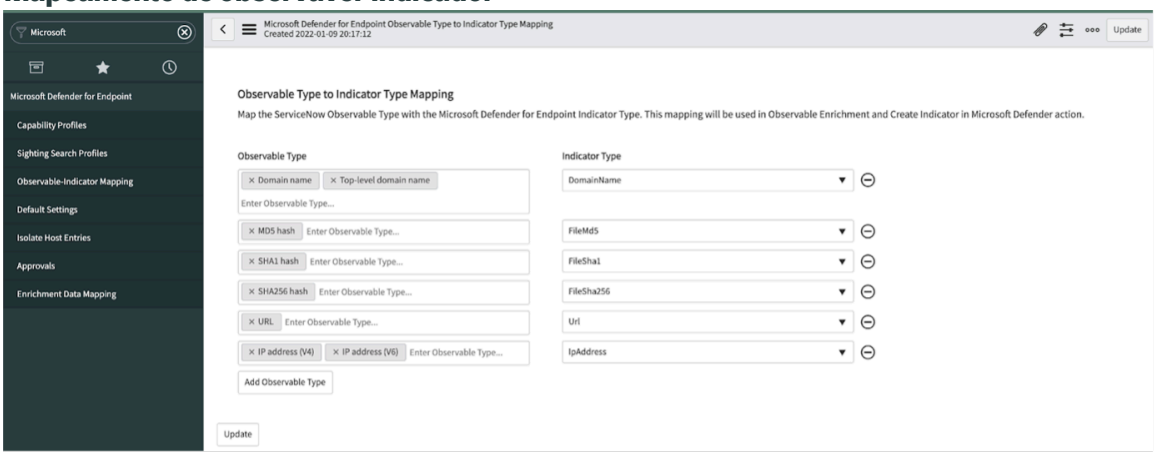
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Microsoft Defender para Ponto de Extremidade** > **Mapeamento de observável-indicador**.

Mapeamento de observável-indicador



2. Adicione ou atualize um tipo de observável de uma das seguintes maneiras:
   - Para adicionar novo mapeamento, clique em **Adicionar tipo de observável**.
   - Para atualizar o Observável para o mapeamento do tipo de Indicador, clique em qualquer linha existente.
3. Para salvar o mapeamento, clique em **Atualizar**.

Criar um perfil de capacidade para a integração Microsoft Defender for Endpoint

Crie um perfil e selecione os recursos Microsoft Defender for Endpoint que você deseja que o perfil execute.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Os perfis são criados para agrupar ou agrupar os recursos, o que ajudaria os analistas a executar a investigação ou a correção com facilidade. Você pode adicionar os seguintes recursos ao perfil:

- Obter detalhes do host
- Obter usuários conectados
- Isolar Host
- Remover isolamento

Você não pode combinar as capacidades Isolar Host e Remover Isolamento de Host com outras capacidades ao criar um perfil. Os perfis para esses recursos devem ser criados individualmente. Por outro lado, os recursos Obter detalhes do host e Obter usuários conectados podem ser combinados. Você pode criar perfis individualmente ou agrupando-os na íntegra ou em partes de acordo com seus requisitos.

Nota:
Depois que uma funcionalidade é incluída em um perfil, ela não pode ser incluída em nenhum outro perfil da mesma origem.

Tradução automática

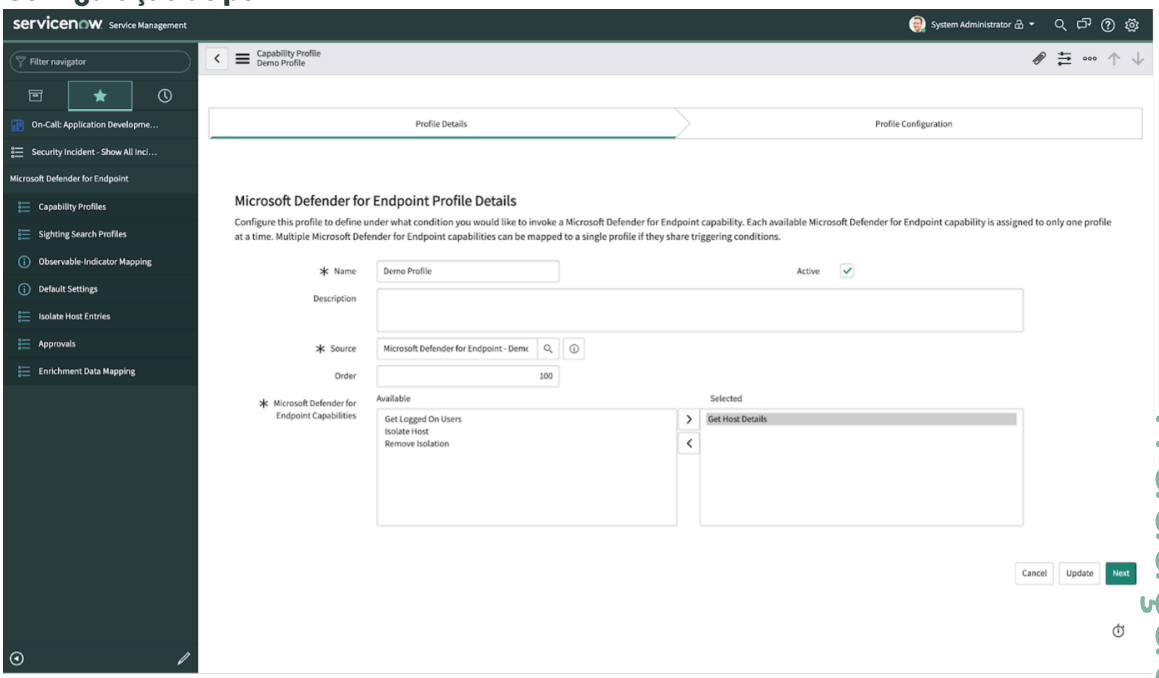
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Microsoft Defender para Ponto de Extremidade** > **Perfis de capacidade**.

   A lista de perfis de recurso do Microsoft Defender for Endpoint é exibida.

Configuração de perfil



2. Clicar **Novo**.
3. No formulário, preencha os campos.

Formulário Perfil de capacidade

Campo	Descrição
Nome	Nome do perfil de recurso Microsoft Defender for Endpoint. Este nome ajuda a identificar o tipo de perfil e a descrevê-lo.
Descrição	Informações adicionais sobre o perfil que descrevem melhor o perfil.
Origem	Nome da origem Microsoft Defender for Endpoint. Somente origens configuradas estão disponíveis na lista.
Recursos do Microsoft Defender para endpoint	Recursos do perfil Microsoft Defender for Endpoint. Selecione os recursos desejados para este perfil na coluna Disponível e mova-os para a coluna Selecionado.
Ordem	Prioridade de fluxo. O padrão é 100. O valor deste campo indica a ordem em que os fluxos são executados quando dois ou mais perfis compartilham condições de gatilho. O fluxo com o número mais baixo tem a prioridade mais alta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300, 400.
Ativo	Opção para indicar que o perfil está ativo. Depois que o perfil estiver ativo, o perfil será acionado automaticamente quando um incidente de segurança for criado que corresponda às condições de filtragem que você especificou na configuração.

4. Para continuar para a Configuração de perfil, clique em **Avançar**.

O que Fazer Depois

A próxima etapa é configurar seu perfil. Antes de definir as configurações do perfil, talvez você prefira revisar como os perfis e as condições configuradas e de gatilho. Para obter mais informações, consulte Condições do gatilho em um item de configuração.

Condições do gatilho em um item de configuração

Depois de criar um perfil e selecionar os recursos Microsoft Defender for Endpoint que você deseja que o perfil execute, defina as configurações do perfil para que o perfil seja executado somente quando um conjunto de condições específicas for atendido.

Como acionar condições em um item de configuração

Você pode definir condições do gatilho para que o perfil seja executado automaticamente sempre que um incidente de segurança for criado que corresponda à condição do gatilho. Se a condição do gatilho não estiver definida, esses perfis poderão ser executados manualmente, clicando no formulário Executar perfil(is) de EDR no incidente de segurança e selecionando o perfil.

Por padrão, a integração usa o campo Item de configuração (IC) no incidente de segurança. Este valor é usado para corresponder os IDs de seus ativos às informações armazenadas no Now Platform Configuration Management Database (CMDB). Quando um incidente de segurança é criado e um perfil é executado automaticamente ou manualmente, o CMDB é pesquisado para recuperar o nome do host ou o endereço IP com base no valor do campo de IC. O nome do host ou IP é usado para resolver o ID do agente em Microsoft Defender for Endpoint para identificar o endpoint.

Em um cenário ideal, um valor correspondente é encontrado no banco de dados e os dados são coletados do console Microsoft Defender for Endpoint para o ativo correspondente. Os dados de vários recursos são inseridos em sua instância Now Platform Configuration Management Database (CMDB) e exibidos nas listas relacionadas de um incidente de segurança. Quando o campo Item de configuração (IC) não estiver preenchido no incidente de segurança com um nome de host com ou um endereço IP que corresponda ao banco de dados, você poderá selecionar um campo alternativo no incidente de segurança que contenha o nome do host ou o IP a ser executado a resolução do ID do agente.

Durante a etapa de configuração da configuração do perfil, você pode selecionar um campo de IC alternativo para identificação do endpoint para garantir que você possa identificar o endpoint em Microsoft Defender for Endpoint. Você pode selecionar qualquer campo no incidente de segurança como um campo de gatilho de IC alternativo, incluindo campos personalizados que você cria. Ao selecionar este campo de IC alternativo como backup, você garante que

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

seus perfis sejam executados mesmo se o campo de IC não estiver preenchido no incidente de segurança associado na criação do incidente.

Nota:
Os campos de IC alternativos são considerados somente para recursos que podem ser adicionados a um perfil. Esses recursos incluem Obter detalhes do host, Obter usuários conectados, Isolar host e Remover isolamento. Para todas as ações adicionais, o IC alternativo deve ser configurado no módulo Configurações padrão.

Configurar perfis e incidentes de segurança para a integração Microsoft Defender for Endpoint

Crie um perfil e selecione os recursos Microsoft Defender for Endpoint que você deseja que o perfil execute. Você precisa definir as configurações para que o perfil possa ser acionado somente nas condições definidas.

Antes de Iniciar
Função necessária: sn_si.admin, sn_si.analyst (somente leitura)

Por Que e Quando Desempenhar Esta Tarefa
Configure o perfil para que ele seja executado somente quando as condições especificadas forem atendidas. Se necessário, você pode selecionar um campo de entrada alternativo para o campo Item de configuração (IC) e definir condições de filtragem para que o perfil possa ser acionado automaticamente quando um incidente de segurança que atende às condições do gatilho for criado.

Nota:
Você pode navegar até a página Configuração do perfil somente depois de inserir a página Detalhes do perfil.

Procedimento

1. Navegar até **Microsoft Defender para Ponto de Extremidade** > **Perfis de capacidade**.
2. Depois de preencher a seção de detalhes do perfil, clique em **Avançar**.
   Revise e configure as seções.
3. Na seção Definir critérios de incidente (Automação), selecione a opção **Definir critérios de incidente** para acionar automaticamente as capacidades Microsoft Defender for Endpoint no perfil.
   Definir critérios de incidente (automação): defina as condições de incidente de segurança que acionarão automaticamente os recursos do Microsoft Defender para endpoint para o perfil. Se você não selecionar a opção **Definir critérios de incidente**, o perfil e os recursos subjacentes poderão ser invocados manualmente a partir do incidente de segurança.

   Nota:
   As capacidades Isolar Host e Remover Isolamento de Host não podem ser acionadas automaticamente.

   a. Em **Condições do filtro**, selecione o campo obrigatório.
   b. Adicione **novos critérios** e defina também a condição **OU** ou **E.**
4. Na seção Aprovações, marque a caixa de seleção **Requer Aprovação** para fornecer um nível extra de controle.

   Se você selecionar esta opção, terá mais controle ao usar os recursos do Microsoft Defender for Endpoint para isolar máquinas host, restaurá-las na rede e obter arquivos.

   A opção Aprovações na configuração do perfil aparece somente para as capacidades Isolar Host e Remover Isolamento de Host, respectivamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Na seção Configuração adicional, selecione a opção **Definir campo** alternativo para definir um campo de entrada alternativo.
   Configuração adicional: quando o campo Item de configuração (IC) não estiver preenchido no incidente de segurança com um nome de host ou um endereço IP que corresponda ao banco de dados, você poderá selecionar um campo alternativo no incidente de segurança para consultar as APIs do Microsoft Defender for Endpoint .

   Nota:
   Para obter mais informações, consulte Condições do gatilho em um item de configuração.

   a. Selecione a opção **Definir campo** alternativo.
   b. Selecione o campo de entrada em **Campo de gatilho de IC alternativo**.
6. Na seção Marcadores, marque a caixa de seleção **Exibir** marcador para habilitar a marcação de incidentes de segurança, o nome do perfil é prefixado ao habilitar o marcador.

   Opcionalmente, você pode marcar incidentes de segurança com marcadores para perfil iniciado, perfil concluído e perfil com falha. Por padrão, esta opção está desativada para todos os perfis.
7. Clicar **Concluído**.

Verificar os filtros de condição do gatilho

Valide o perfil e verifique se os filtros de condição do gatilho que você configurou estão funcionando conforme o esperado.

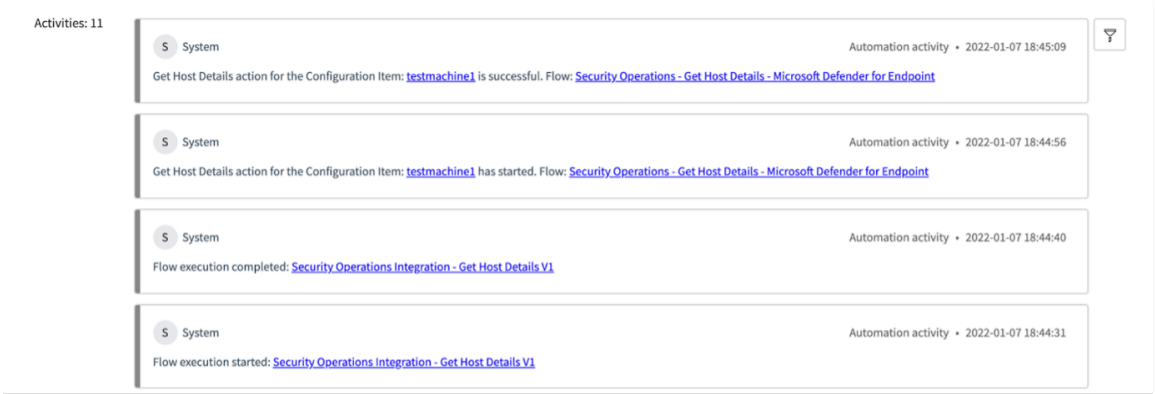
Antes de Iniciar
Função necessária: sn_si.admin ou sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Depois de ativar o perfil, com base nas condições do gatilho configuradas, você pode exibir os resultados da consulta nos Now Platform® incidentes de segurança.

Procedimento
1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Para criar um novo incidente de segurança, selecione **Novo**.
3. Para acionar o respectivo perfil, forneça as condições de filtro conforme fornecidas no perfil de recurso.
4. Clicar **Salvar**.
5. Para validar a seção de atividades e anotações de trabalho, exiba e verifique os registros marcados com o perfil iniciado, perfil concluído ou perfil com falha.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Para validar todos os dados nas listas relacionadas, clique em **Mostrar todas as listas relacionadas**.
7. Clique em qualquer guia **Lista relacionada** para validar os detalhes.
   Por exemplo, Detalhes do host.

Acionar as capacidades Microsoft Defender for Endpoint de Links relacionados

Acione um perfil de recurso manualmente depois de revisar um incidente de segurança de links relacionados.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Além de executar o perfil do IC ou o IC alternativo do incidente de segurança, você também pode executar o perfil dos valores de IC presentes na lista relacionada Item de configuração selecionando **Incluir IC relacionado** na caixa de diálogo. Isso recupera os dados dos valores de IC presentes na lista relacionada também. Como alternativa, você pode executar o perfil apenas para os valores de IC presentes na lista relacionada.

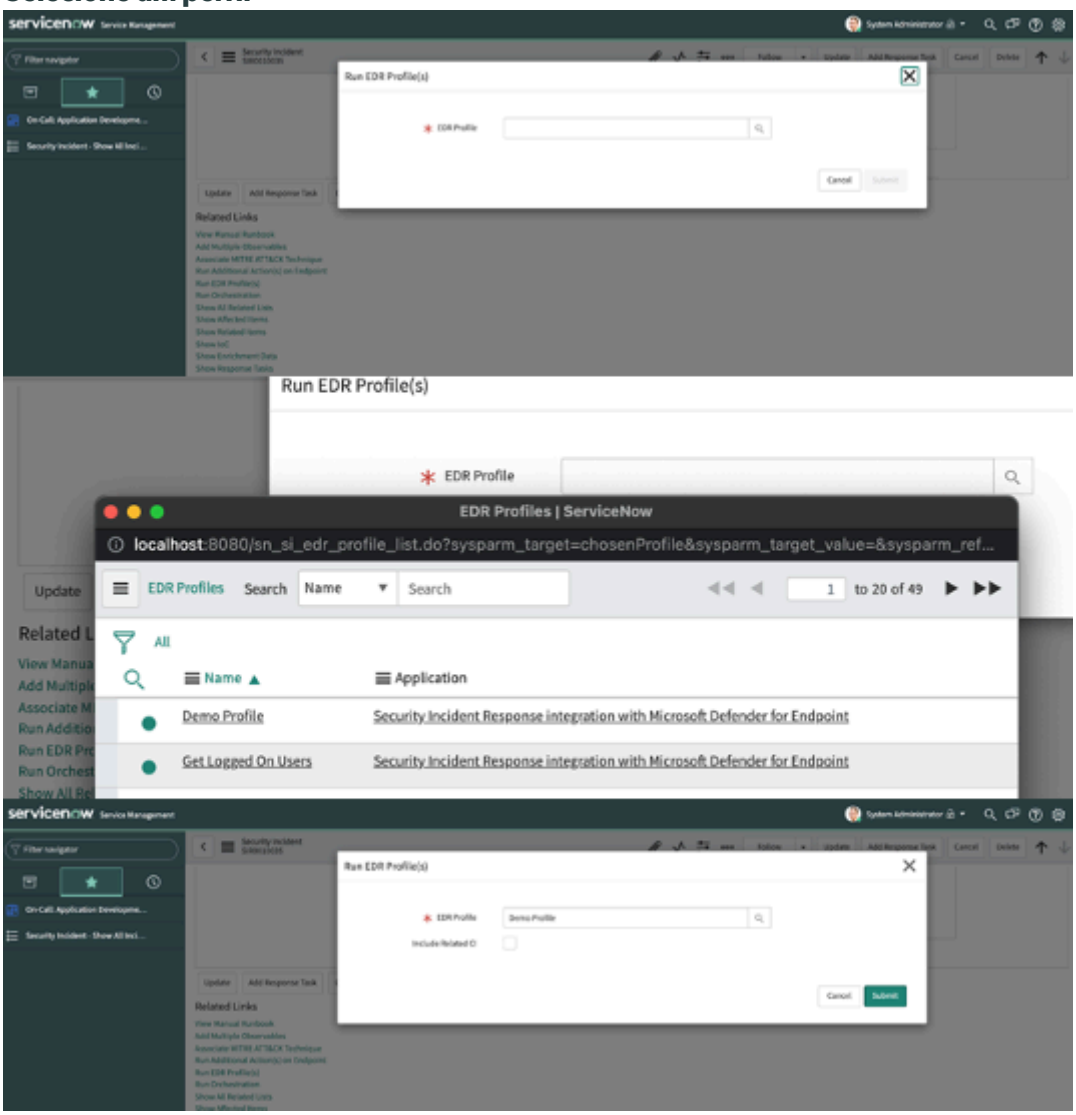
Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações Microsoft Defender for Endpoint.
3. Na seção Links relacionados, clique em **Executar perfil(is) de EDR**.
4. Pesquise e selecione um perfil na lista de perfis disponíveis e clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Selecione um perfil



O perfil selecionado é acionado manualmente.

5. Valide a seção de anotações de trabalho e atividades.
6. Exiba os marcadores e valide os dados nas listas relacionadas.

Acionar o Microsoft Defender for Endpoint da lista relacionada de Item de Configuração

Acione um perfil de recurso manualmente a partir da lista relacionada do item de configuração.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações Microsoft Defender for Endpoint.
3. Clicar **Mostrar Todas as Listas Relacionadas**.
4. Clique na lista relacionada Item de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione os itens de configuração adicionados.
6. Em **Ações** nas linhas selecionadas, selecione um recurso.
   A funcionalidade selecionada é acionada manualmente.
7. Valide a seção de anotações de trabalho e atividades.
8. Exiba os marcadores e valide os dados nas listas relacionadas.

Configurações adicionais em Microsoft Defender for Endpoint

A integração Microsoft Defender for Endpoint oferece suporte à execução de ações adicionais além das ações padrão.

O Microsoft Defender for Endpoint oferece suporte às seguintes configurações adicionais:

Configurar a capacidade Isolar Host no Microsoft Defender for Endpoint

Isole o host de acessar a rede em Microsoft Defender for Endpoint com base na severidade do ataque. Isolar o host da rede permite que você evite outras atividades mal-intencionadas ou possíveis ataques a outros hosts.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Requisitos para a capacidade Isolar Host

Capacidade	Necessários	Descrição
Isolar Host	Tipo de isolamento	(Obrigatório) Tipo de Isolamento (Total ou Seletivo).
	Comentário	(Obrigatório) Comentário a ser associado à ação.

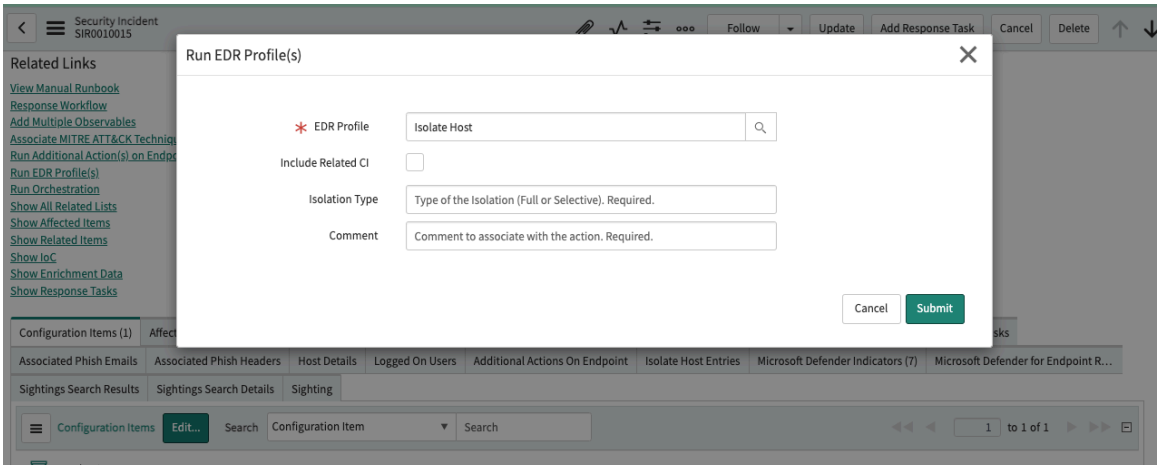
Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender for Endpoint.
3. Na seção Links relacionados, clique em **Executar perfil(is) de EDR**.
4. Procure e selecione um perfil com a **capacidade Isolar Host** selecionada na lista de perfis disponíveis e clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Isolar Host



Como alternativa, você pode executar as seguintes etapas:

a. Na seção de listas relacionadas, clique em **Mostrar todas as listas relacionadas**.

b. Clique na lista relacionada **Item de configuração**.

c. Selecione **Isolar host** e selecione os recursos correspondentes.

5. Valide a atividade de automação e a seção de atividades e certifique-se de que os dados estejam conforme o esperado.
6. Exiba os dados e valide os detalhes do host isolado nas listas relacionadas.

Configure a capacidade Remover isolamento de host no Microsoft Defender for Endpoint

Se necessário, remova o isolamento de um host que foi isolado anteriormente da rede em Microsoft Defender for Endpoint. Você pode impedir outras atividades mal-intencionadas ou possíveis ataques em outros hosts.

Antes de Iniciar

Requisitos para a capacidade de remover isolamento

Capacidade	Entrada necessária	Descrição
Remover isolamento	Comentário	(Obrigatório) Comentário a ser associado à ação.

Função necessária: sn_si.admin ou sn_si.analyst

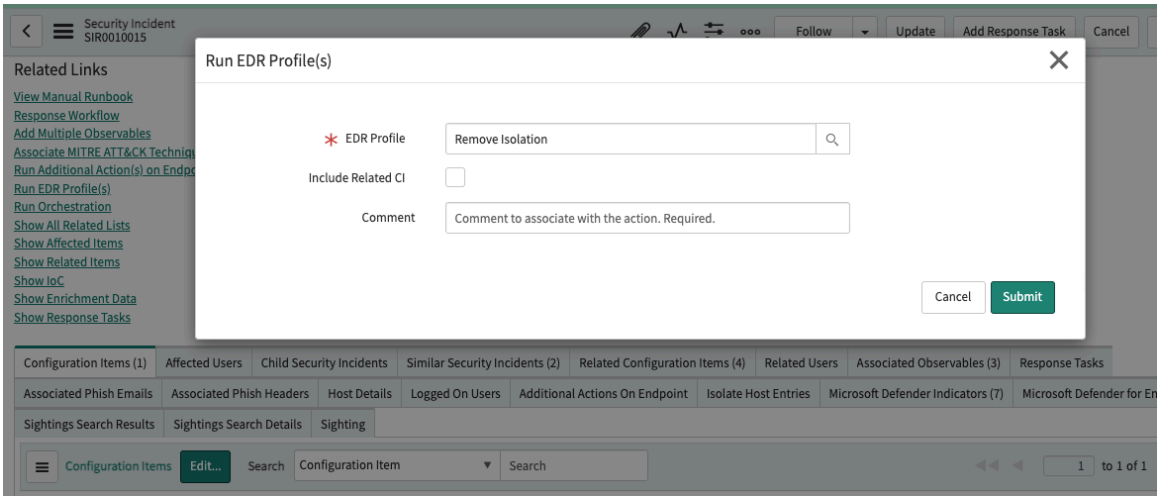
Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender for Endpoint.
3. Na seção Links relacionados, clique em **Executar perfil(is) de EDR**.
4. Procure e selecione um perfil com a **capacidade Remover isolamento** selecionado na lista de perfis disponíveis e clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Remover isolamento



Como alternativa, você pode executar as seguintes etapas:

a. Clique em **Mostrar todas** as listas relacionadas na seção de listas relacionadas.

b. Clique na lista relacionada **Item de configuração**.

c. Selecione **Remover isolamento** e selecione os recursos correspondentes.

5. Valide a atividade de automação e a seção de atividades.
6. Exiba os dados e valide os detalhes do host isolado nas listas relacionadas.
7. Valide as atividades de automação da execução.

Configure a capacidade Executar verificação antivírus no Microsoft Defender for Endpoint

Inicie remotamente uma verificação antivírus para ajudar a identificar e corrigir malware que possa estar presente em um dispositivo comprometido. Execute a verificação como parte da investigação ou do processo de resposta.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Requisitos para a capacidade Executar verificação antivírus

Entrada	Descrição
Tipo de Verificação	(Obrigatório) Tipo de verificação (completa ou rápida).
Comentário	(Obrigatório) Comentário a ser associado à ação.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender for Endpoint.

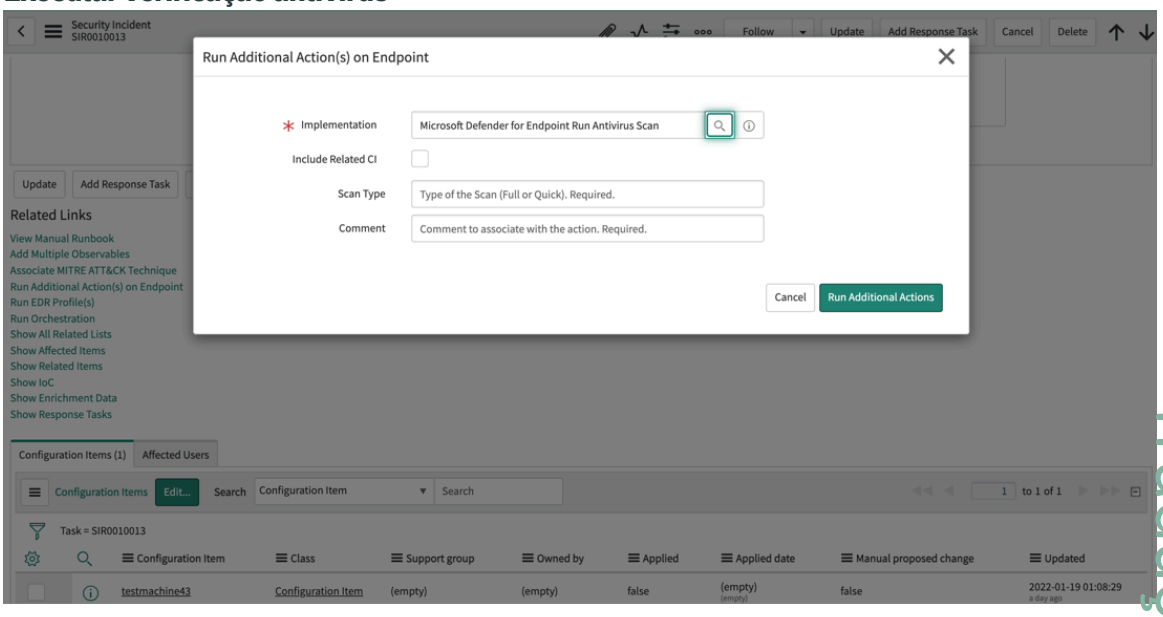
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na seção de links relacionados, clique em **Executar ações adicionais no endpoint**.

b. Procure e selecione o recurso necessário.
Por exemplo, clique no recurso **Executar verificação antivírus**.

Executar verificação antivírus



Como alternativa, você pode executar as seguintes etapas:

a. Na seção de listas relacionadas, clique em **Mostrar todas as listas relacionadas**.

b. Clique na lista relacionada **Item de configuração**.

c. Selecione os itens de configuração adicionados e, em Ações nas linhas selecionadas, selecione **Executar ações adicionais no endpoint**.

Depois de selecionar a implementação do recurso **Executar verificação antivírus**, os campos de entrada **Tipo de verificação adicional** e **Comentário** são exibidos.

3. Selecione o **tipo de verificação** que você deseja executar (Rápida ou Completa) e adicione um comentário antes de executar a verificação.
4. Para iniciar a verificação antivírus, clique em **Executar ação adicional**.
5. Exiba as atividades de automação da execução e valide-as.
6. Valide o status da ação nas Ações adicionais nas listas relacionadas ao endpoint.

Configurar a capacidade de Restringir execução da aplicação no Microsoft Defender for Endpoint

Para conter um ataque, restrinja ou bloqueie um dispositivo e evite que tentativas subsequentes de programas potencialmente mal-intencionados sejam executados.

Antes de Iniciar

Requisitos para a capacidade de Restringir execução da aplicação

Entrada	Descrição
Comentário	(Obrigatório) Comentário a ser associado à ação)

Tradução automática

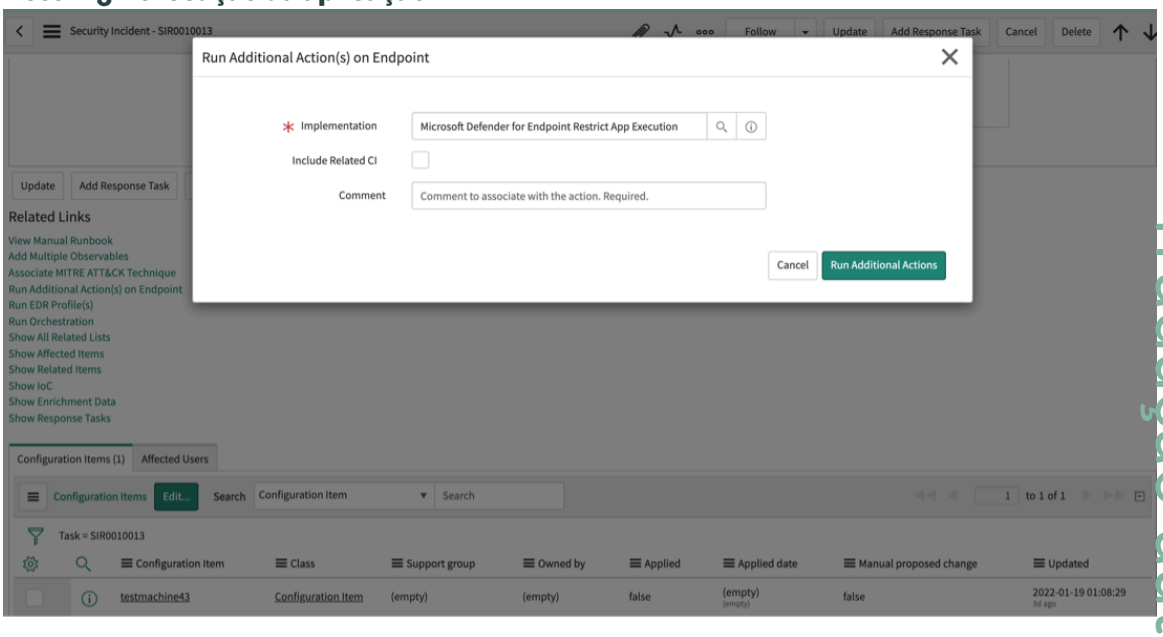
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_si.admin ou sn_si.analyst

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender for Endpoint.
   a. Na seção de links relacionados, clique em **Executar ações adicionais no endpoint**.
   b. Procure e selecione a capacidade **Restringir execução da aplicação**.

Restringir execução da aplicação



Como alternativa, você pode executar as seguintes etapas:

a. Na seção de listas relacionadas, clique em **Mostrar todas as listas relacionadas**.
b. Clique na lista relacionada **Item de configuração**.
c. Selecione os itens de configuração adicionados.
d. Em Ações nas linhas selecionadas, selecione **Executar ações adicionais no endpoint**.

3. Para habilitar Restringir execução da aplicação na máquina, clique em **Executar ação adicional**.
4. Exiba as atividades de automação da execução e valide-as.
5. Valide o status da ação nas Ações adicionais nas listas relacionadas ao endpoint.

Configure a capacidade de Remover Restrição da aplicação no Microsoft Defender for Endpoint

Se necessário, remova as restrições de qualquer aplicação no dispositivo.

Antes de Iniciar

Função necessária: sn_si.admin ou sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

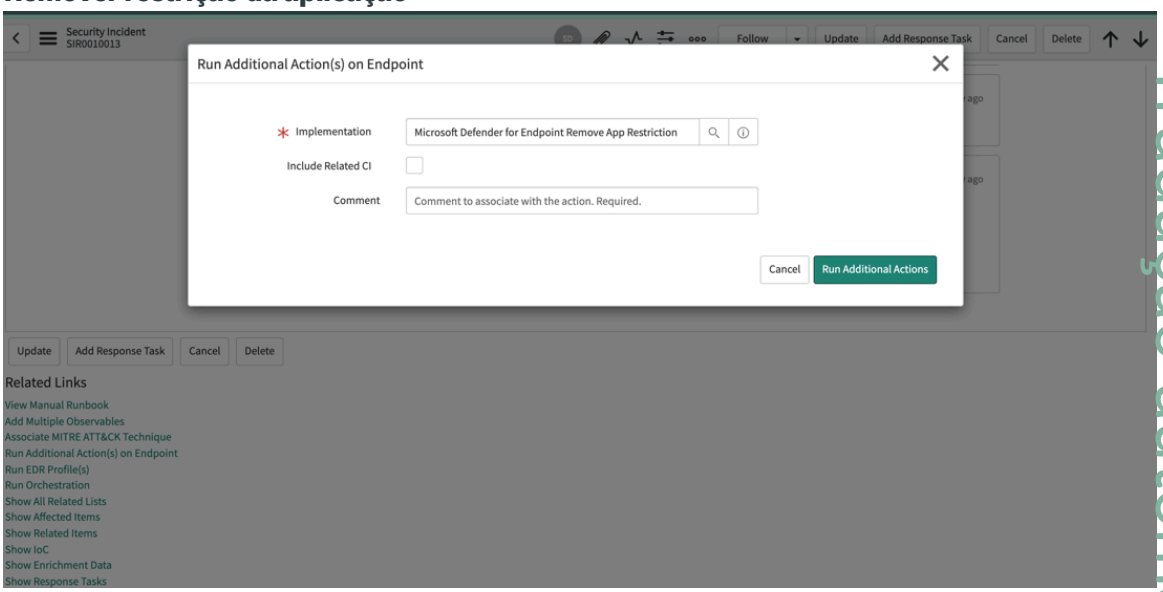
Requisitos para a capacidade de remover restrição da aplicação

Entrada	Descrição
Comentário	(Obrigatório) Comentário a ser associado à ação)

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender for Endpoint.
   a. Na seção de links relacionados, clique em **Executar ações adicionais no endpoint**.
   b. Procure e selecione o recurso **Remover Restrição da aplicação**.

Remover restrição da aplicação



Como alternativa, você pode executar as seguintes etapas:

   a. Na seção de listas relacionadas, clique em **Mostrar todas as listas relacionadas**.
   b. Clique na lista relacionada **Item de configuração**.
   c. Selecione os itens de configuração adicionados.
   d. Selecione **Executar ações adicionais no endpoint**.
   O campo de entrada Comentário adicional é exibido.
3. Para remover a restrição da aplicação, clique em **Executar ação adicional**.
4. Exiba as atividades de automação da execução e valide-as.
5. Valide o status da ação nas Ações adicionais nas listas relacionadas ao endpoint.

Configurar Obter máquinas relacionadas da capacidade do Defender no Microsoft Defender for Endpoint

Obtenha a lista de máquinas relacionadas de observáveis específicos.

Antes de Iniciar

Tipos de observável compatíveis: nome de domínio, hash SHA1 e nome de usuário

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_si.admin ou sn_si.analyst

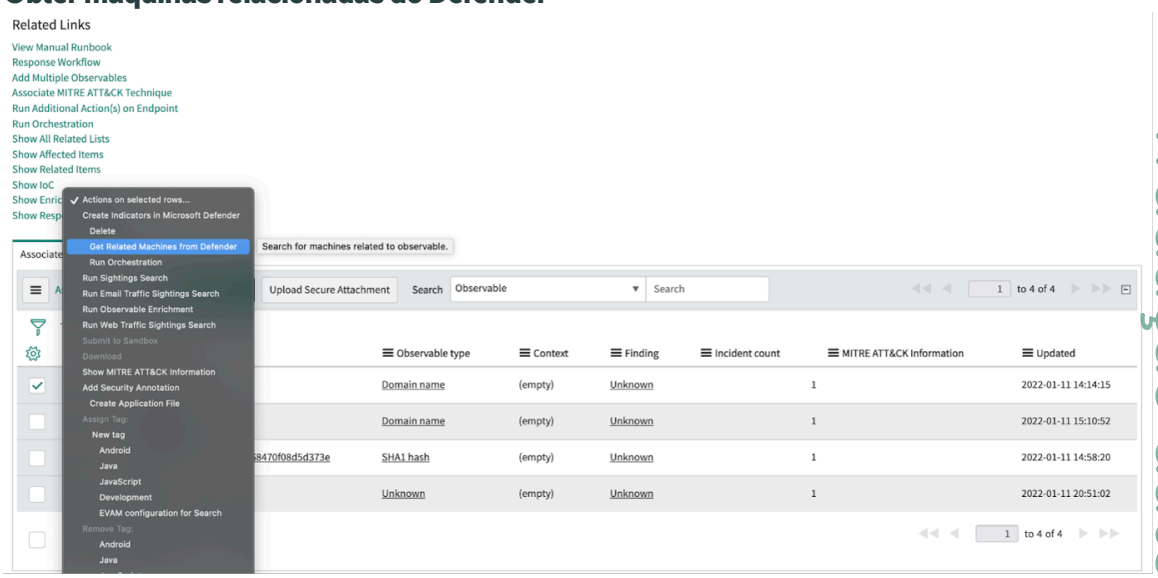
Por Que e Quando Desempenhar Esta Tarefa

Você pode recuperar a lista de máquinas que acessaram os observáveis específicos. Você pode armazenar a lista na tabela Detalhes de máquinas relacionadas ao Microsoft Defender for Endpoint. Você pode acionar a capacidade Obter máquinas relacionadas do Defender na lista relacionada Observáveis associados.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender for Endpoint.

Obter máquinas relacionadas do Defender



3. Na seção Links relacionados, clique em **Mostrar IoC**.
4. Clique na lista relacionada Observáveis associados.
5. Selecione os observáveis associados.
6. Na lista Ações, selecione o recurso **Obter máquinas relacionadas do Defender**.
7. Valide a atividade de automação e a seção de atividades.
8. Exiba os dados e valide os detalhes do Microsoft Defender para máquinas relacionadas ao endpoint nas listas relacionadas.
9. Exiba as atividades de automação da execução e valide-as.

Configurar a capacidade de parar e colocar arquivo em quarentena no Microsoft Defender for Endpoint

Interrompa e coloque em quarentena arquivos da plataforma Microsoft Defender.

Antes de Iniciar

Tipos de observável compatíveis: hash SHA1

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Requisitos para a capacidade de interromper e colocar arquivo em quarentena

Entrada	Descrição
Comentário	(Obrigatório) Comentário a ser associado à ação)

Função necessária: sn_si.admin ou sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Você pode executar a ação Interromper e colocar arquivo em quarentena somente em observáveis específicos do tipo SHA1. Armazene os detalhes na tabela Ações adicionais no endpoint. Você pode acionar o recurso Interromper e colocar arquivo em quarentena na lista relacionada de detalhes do Microsoft Defender para máquinas relacionadas ao endpoint.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender for Endpoint.
3. Na seção de links relacionados, clique em **Mostrar todas as listas relacionadas**.
4. Clique na lista relacionada Detalhes de máquinas relacionadas ao Microsoft Defender for Endpoint.
5. Selecione um ou mais registros.
6. Em **Ações** nas linhas selecionadas, selecione o recurso **Parar e colocar arquivo em quarentena**.
7. Valide a atividade de automação e a seção de atividades.
8. Exiba os dados e valide os dados nas listas relacionadas.
9. Exiba as atividades de automação da execução e valide-as.

Criar e configurar um perfil para pesquisa de vistas com a integração Microsoft Defender for Endpoint

Crie e configure o perfil de pesquisa de vistas automaticamente usando o Microsoft Defender for Endpoint.

Antes de Iniciar
Função necessária: sn_si.admin, sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode usar o fluxo de trabalho Pesquisa de vistas para executar as pesquisas de vista. Este fluxo de trabalho aceita uma lista de observáveis, encontra todos os recursos de implementação, cria as consultas baseadas nas configurações de pesquisa de vista e executa as pesquisas baseadas no fluxo de trabalho configurado.

O Microsoft Defender for Endpoint fornece um perfil de pesquisa de vista do sistema de base que permite configurar as pesquisas de vista automáticas. Com este perfil, você pode acessar as informações de vista observáveis relacionadas de uma organização e também ver as vistas de outras organizações.

Procedimento

1. Navegar até **Integrações** > **Configuração de pesquisa de detecções**.
2. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No formulário, preencha os campos a seguir.

Formulário de Configuração de pesquisa de vistas

Campo	Descrição
Nome	Nome do perfil de pesquisa de vista.
Pesquisa salva	Opção para salvar a configuração de pesquisa. As consultas de configuração de pesquisa salvas são consultas de exemplo. Você pode substituí-los pelos parâmetros do seu ambiente e criar configurações de pesquisa salvas adicionais, conforme necessário.
Origem de pesquisa de vistas	A origem configurada para a pesquisa de vistas na integração Microsoft Defender for Endpoint.
Pesquisar	Cadeia de caracteres de pesquisa nativa que forma uma consulta.
Ativo	Opção para habilitar a configuração de pesquisa salva. Somente configurações de pesquisa ativas podem executar uma pesquisa de vistas.
Tipo de observável	Tipo de categoria de observável. Por exemplo, endereço IP, valor de hash, URL e nome de domínio.
Máximo observável por pesquisa	Número máximo de observáveis que você pode exibir em uma consulta de pesquisa. Defina este valor como 1 para esta integração.
Parâmetros de pesquisa de detecções	Parâmetros para definir consultas mais complexas que incluem lógica e outros operadores compatíveis com o armazenamento de log especificado.

4. Clique em **Enviar**.

Executar uma pesquisa de vista manual no Microsoft Defender for Endpoint

Selecione um ou vários observáveis e execute uma pesquisa de vista manual em Microsoft Defender for Endpoint para determinar a predominância de uma ameaça ao longo do tempo.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Os tipos de observável compatíveis são os seguintes:

- Nome do domínio
- Endereço IP (V4)
- Endereço IP (V6)
- Hash MD5
- Hash SHA1
- Hash SHA256

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Incidentes de segurança**.
2. Abra um SIR existente ou crie um novo SIR.
3. Nos links relacionados, clique em **Mostrar IoC**.
4. Clique nas listas relacionadas de Observáveis associados.
5. Selecione os observáveis.
6. Na lista Ações, clique em **Executar aprimoramento de observável**.
7. Selecione os observáveis em **Ação** nas linhas selecionadas e clique em **Executar pesquisa de detecções**.

   Nota:
   A pesquisa de vista é compatível com os tipos de observáveis Nome de domínio, endereço IP (V4), endereço IP (V6), hash MD5, hash SHA1 e hash SHA256, respectivamente.

8. Especifique o intervalo de tempo da pesquisa e clique em **Pesquisar**.

   Nota:
   O Microsoft Defender para endpoint oferece suporte à pesquisa de vista somente nos últimos 30 dias. Se sua consulta de intervalo for anterior aos últimos 30 dias, a pesquisa de vista não recuperará nenhum dado. Se sua consulta de intervalo se sobrepuser aos últimos 30 dias, as vistas somente dos últimos 30 dias serão recuperadas e, se sua consulta de intervalo estiver nos últimos 30 dias, as vistas da hora de início definida até a hora atual serão recuperadas.

9. Ao concluir a pesquisa, valide os resultados e os detalhes nas listas relacionadas.
10. Clique em **Detalhes da pesquisa** de detecções para exibir os detalhes da pesquisa de detecções.
11. Clique na guia **Vista** para obter detalhes e na guia **Resultados** da pesquisa de Vistas para obter os resultados da pesquisa.

    Você pode exibir informações adicionais relacionadas à vista específica no campo **Resumo**.

Executar um aprimoramento observável automático no Microsoft Defender for Endpoint

Execute um aprimoramento observável automático em Microsoft Defender for Endpoint para aprimorar observáveis com informações adicionais de várias fontes.

Antes de Iniciar

Verifique se você habilitou a propriedade do sistema do **Security Incident Response**. Esta opção aciona a capacidade de aprimoramento do observável no SIR, sempre que um observável estiver associado a um incidente de segurança.

Função necessária: sn_si.admin, sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar esta capacidade durante as investigações de resposta do incidente para conter uma ameaça identificada. Quando novos observáveis são associados ao incidente de segurança, você pode habilitar o enriquecimento do observável na capacidade do Microsoft Defender para Endpoint para ser executado automaticamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender for Endpoint.
3. Valide a atividade de automação depois que os novos observáveis forem associados ao incidente de segurança.
4. Exiba os resultados do aprimoramento na lista relacionada Indicadores do incidente de segurança. Você pode usar a tabela a seguir para obter mais informações sobre o aprimoramento observável.

Indicador do Microsoft Defender

Campo	Descrição
ID do indicador	Identidade da entidade Indicador. Clique em **Abrir** para exibir o registro em detalhes na instância Now Platform
Observável	O observável associado ao resultado.
Título	Título do indicador.
Tipo de Indicador	Tipo do indicador.
Ação	Ação realizada pelo indicador.
Ação recomendada	Ações recomendadas para o indicador.
Fornecedor de integração	Integração de origem do Defender da qual os dados são recuperados.
Data de vencimento	Tempo de expiração do indicador.
Data de recuperação	Data em que o registro de aprimoramento é criado.

Executar um aprimoramento observável manual no Microsoft Defender for Endpoint

Selecione um ou vários observáveis e execute um aprimoramento observável manual para aprimorar os observáveis com informações adicionais de Microsoft Defender for Endpoint.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

A integração Microsoft Defender for Endpoint permite o aprimoramento de observável para todos os tipos de observável que são mapeados no módulo Mapeamento de observável-indicador.

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja revisar com as informações do Microsoft Defender for Endpoint.
3. Clique **em Mostrar todas as listas relacionadas**.
4. Clique na guia **Observáveis associados**.
5. Selecione os observáveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Na lista Ações, clique em **Executar aprimoramento de observável**.
7. Selecione uma **origem** do Microsoft Defender for Endpoint e mova-a para a coluna **Selecionado** para especificar qual implementação você deseja usar para aprimorar os observáveis selecionados.
8. Clique em **Enviar**.
9. Para validar o status da execução, exiba as anotações de trabalho.
10. Para exibir os resultados, clique na guia **Indicador do Microsoft Defender**.
    Você pode usar a tabela a seguir para obter mais informações sobre o aprimoramento observável.

Indicador do Microsoft Defender

Campo	Descrição
ID do indicador	Identidade da entidade Indicador. Clique em **Abrir** para exibir o registro em detalhes na instância Now Platform
Observável	O observável associado ao resultado.
Título	Título do indicador.
Tipo de Indicador	Tipo do indicador.
Ação	Ação realizada pelo indicador.
Ação recomendada	Ações recomendadas para o indicador.
Fornecedor de integração	Integração de origem do Defender da qual os dados são recuperados.
Data de vencimento	Tempo de expiração do indicador.
Data de recuperação	Data em que o registro de aprimoramento é criado.

Como criar Indicadores em Microsoft Defender for Endpoint

Crie indicadores de observáveis associados do incidente de segurança usando o Microsoft Defender for Endpoint.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

A integração Microsoft Defender for Endpoint permite o aprimoramento de observável para todos os tipos de observável que são mapeados no módulo de mapeamento Observable-Indicator.

Criar indicadores fornece a capacidade de definir uma lista de indicadores para detecção e para bloqueio de prevenção e respostas. Você pode criar os indicadores do observável associado do incidente de segurança.

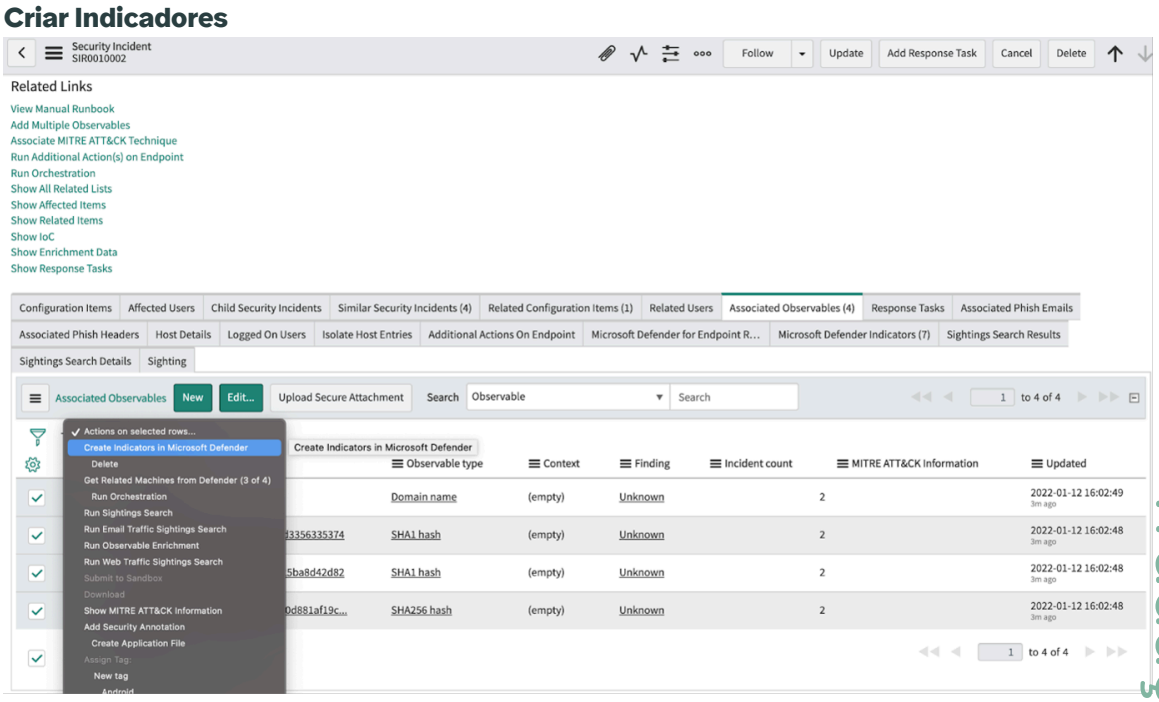
Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja criar indicadores no Microsoft Defender para Endpoint.
3. Clique nas listas relacionadas de Observáveis associados.
4. Adicione observáveis existentes ou crie novos observáveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione os observáveis.
6. Em **Ações** nas linhas selecionadas, clique em **Criar indicador no Microsoft Defender**.



7. No formulário, preencha os campos.

Campo	Descrição
Observáveis selecionados	Observáveis afetados. Esta ação pode ser usada para criar indicadores para vários observáveis. Se você quiser desmarcar um observável, poderá fazer isso desmarcando os observáveis na lista. **Nota:** Se os tipos de observáveis compatíveis não forem mapeados, os indicadores não serão criados no Microsoft Defender para esses observáveis.
Título	Título do indicador.
Descrição	Descrição do indicador.
Tempo de expiração	Tempo de expiração do indicador.
Ações recomendadas	Ações recomendadas que devem ser realizadas para o indicador.
Origem	Configuração de integração para criar o indicador.
Ação	Ações que serão realizadas se o indicador for descoberto na organização. Os valores possíveis são os seguintes: ○ **Aviso** ○ **Bloquear**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **Auditoria** ○ **'Bloquear e corrigir** ○ **Permitido**
Aplicação	A aplicação Microsoft Defender for Endpoint que está associada ao indicador. Este campo é aplicável somente para um novo indicador e não pode ser usado para um indicador existente.
Gravidade	Severidade do indicador. Os valores possíveis são os seguintes: ○ **Baixo(a)** ○ **Média** ○ **Alto**
Nomes de grupo do RBAC	Nomes de grupo do RBAC aos quais o indicador seria aplicado. Os nomes estão em uma lista separada por vírgulas.

8. Clique **em Criar indicador**
9. Valide a atividade e as mensagens de IU.
10. Clique na guia **Indicador do Microsoft Defender** para exibir os resultados.

Atualizar indicadores no Microsoft Defender for Endpoint

Atualize os indicadores existentes em Microsoft Defender for Endpoint no menu de contexto da lista ou na exibição de formulário do indicador do Microsoft Defender, respectivamente.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst

Procedimento

1. Navegar até **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Clique em **Mostrar todas as listas relacionadas** e na guia **Indicadores do Microsoft Defender**.

> **Nota:**
>
> Você deve configurar a lista relacionada para os Indicadores do Microsoft Defender, que aparecerão nas listas relacionadas a Incidentes de segurança. Para obter mais informações, consulte Ações de IU de formulário.

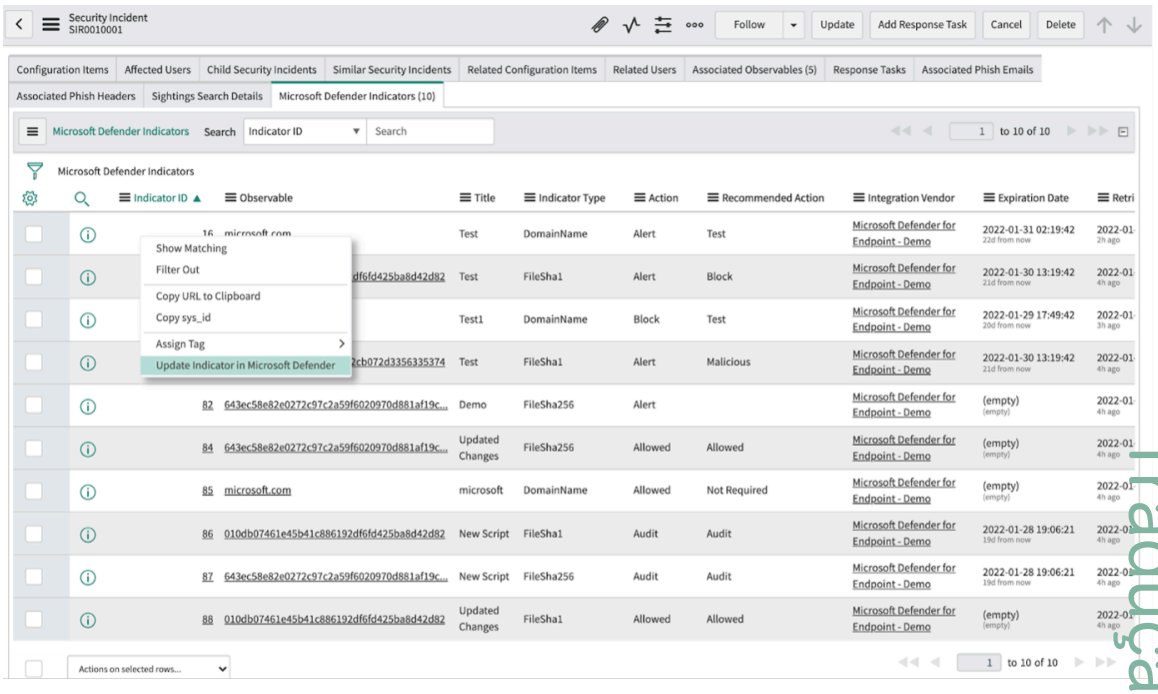
3. Atualize os indicadores do Microsoft Defender for Endpoint de uma das seguintes maneiras:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

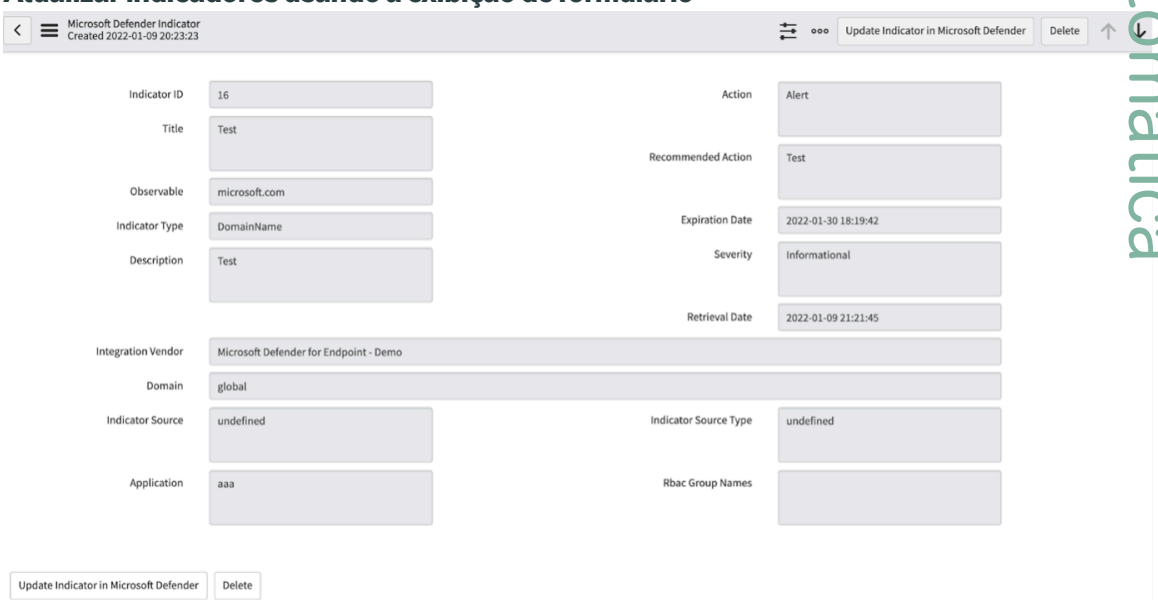
- Para atualizar os indicadores no menu de contexto da lista, selecione a linha do indicador que você deseja atualizar e clique em **Atualizar indicador na opção Microsoft Defender**.

Atualizar indicadores usando o menu de contexto da lista



- Para atualizar os indicadores da exibição de formulário, clique em **Atualizar indicador no Microsoft Defender** na exibição de formulário.

Atualizar indicadores usando a exibição de formulário



4. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de indicador do Microsoft Defender

Campo	Descrição
Título	Título do indicador.
Descrição	Descrição do indicador.
Tempo de expiração	Tempo de expiração do indicador.
Ações recomendadas	Ações recomendadas a serem realizadas para o indicador.
Origem	Configuração de integração para criar o indicador.
Ação	Ações que são realizadas se o indicador for descoberto na organização. Os valores possíveis são os seguintes: ○ **Aviso** ○ **Bloquear** ○ **Auditoria** ○ **Bloquear e corrigir** ○ **Permitido**
Aplicação	A aplicação Microsoft Defender for Endpoint que está associada ao indicador. Este campo é aplicável somente para um novo indicador e não pode ser usado para um indicador existente.
Gravidade	Severidade do indicador. Os valores possíveis são os seguintes: ○ **Baixo(a)** ○ **Média** ○ **Alto**
Nomes de grupo do RBAC	Nomes do grupo do RBAC aos quais o indicador é aplicado. Os nomes estão em uma lista separada por vírgulas.

5. Clique **em Atualizar indicador**.
6. Valide a atividade e as mensagens de IU.

Domain Separation na integração Microsoft Defender for Endpoint

A separação de domínio é compatível com a integração Microsoft Defender for Endpoint.
O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: Básico

Use as seguintes etapas para o Domain Separation:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Crie um usuário com a função sn_si.admin no respectivo domínio.
2. Execute os procedimentos de integração Microsoft Defender for Endpoint no domínio apropriado.

Configuração de limite de taxa na integração Microsoft Defender for Endpoint

Configure o limite de taxa da API e o tempo limite para o limite de taxa para integração Microsoft Defender for Endpoint.

Antes de Iniciar

Função necessária: sn_si.admin, sn_si.analyst (somente leitura)

Procedimento

1. No filtro de navegação, insira sys.properties.list.
   A lista inteira de propriedades na tabela Propriedades do sistema [sys_properties] é exibida.
2. Pesquise e modifique as propriedades a seguir de acordo com seus requisitos.

Nome da Propriedade	Descrição
sn_sec_defender_ep.rate_limit_timeout_in_minutes	Se uma solicitação não for executada dentro do intervalo de tempo especificado, a execução será interrompida e uma mensagem de erro apropriada será exibida. Valor padrão: 75.
sn_sec_defender_ep.request_per_hour_limit	Se a chamada de API configurada for feita no mesmo endpoint em uma hora, a solicitação será enfileirada até que o limite seja atingido ou o tempo limite configurado. Valor padrão: 1500.
sn_sec_defender_ep.request_per_minute_limit	Se a chamada de API configurada for feita no mesmo endpoint em um minuto, a solicitação será enfileirada até que o limite seja atingido ou o tempo limite configurado. Valor padrão: 100.
sn_sec_defender_ep.import_indicator_request_per_minute_limit	Se a chamada de API configurada for feita no endpoint em um minuto, a solicitação será enfileirada até que o limite seja atingido ou o tempo limite configurado. Valor padrão: 30.

Integração de Microsoft Exchange Online

Para a aplicação de integração [Microsoft Exchange Online da ServiceNow, o produto Now Platform® Security Incident Response (SIR) é integrado ao serviço Microsoft Exchange Online, um dos serviços baseados em nuvem no pacote de produtos Microsoft Office 365. Seu analista do Security Operation Center (SOC) pode pesquisar ameaças relacionadas à segurança em seu

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ambiente de e-mail corporativo e remover e corrigir e-mails de phishing com recursos de pesquisa e exclusão de e-mail.

Visão geral

Como analista de incidentes de segurança, você executa a integração a partir da interface do analista de segurança e o fluxo de trabalho retorna detalhes da mensagem de e-mail que correspondem aos critérios de pesquisa. As pesquisas de e-mail são baseadas em critérios que incluem linhas de assunto e endereços de e-mail do remetente e do destinatário. Depois que a pesquisa de e-mail for concluída, você poderá excluir e-mails suspeitos do serviço Microsoft Exchange Online e um processo de aprovação opcional pode ser configurado para solicitar aprovação antes de excluir e-mails.

Esta integração de pesquisa e exclusão de e-mail pode ser usada com um fluxo de trabalho de incidente de resposta de phishing mais amplo ou runbook. Depois que um usuário corporativo ou funcionário recebe um e-mail suspeito e o relata para a equipe de resposta de phishing da empresa ou para a caixa de entrada, o e-mail relatado é encaminhado para o Now Platform e categorizado como um incidente de segurança. Depois de verificar que um e-mail é um ataque de phishing, como analista responsável pela investigação de incidentes de phishing, você pode iniciar uma pesquisa de e-mail para determinar se outros usuários corporativos receberam esse e-mail de phishing. A pesquisa permite localizar e-mails relacionados da mesma campanha de phishing e identificar outras possíveis vítimas que podem ter recebido o e-mail, lido e também clicado em um URL malicioso ou aberto um anexo.

Principais recursos

A integração inclui os seguintes recursos principais:

- Configure os critérios de pesquisa para ameaças de phishing no Security Incident Response com base nas combinações dos campos de remetente, destinatário e assunto das mensagens de e-mail.
- Para pesquisas de e-mail grandes e demoradas, o analista de incidentes de segurança é notificado por e-mail quando a pesquisa é concluída com sucesso, junto com o número de mensagens correspondentes.
- O status de mensagens individuais informa se os destinatários leram ou excluíram e-mails suspeitos.
- Se configurados, os processos de aprovação opcionais garantem que os e-mails suspeitos não sejam excluídos sem aprovação prévia.
- Uma trilha de auditoria completa para solicitações de exclusão que inclui o número de e-mails excluídos é registrada nas anotações de trabalho dos incidentes de segurança.
- Se a marcação estiver configurada, os marcadores de segurança registrarão quando os fluxos de trabalho de pesquisa e exclusão de e-mail forem iniciados e concluídos com sucesso em incidentes de segurança.

Microsoft Exchange Online Versões compatíveis

Esta integração oferece suporte a serviços Microsoft Exchange Online, que fazem parte do pacote do Microsoft Office 365. A integração não é compatível com ambientes do Exchange hospedados Microsoft. Microsoft executa Microsoft Exchange Online serviços na versão do Exchange 2016.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pré-requisitos

O plug-in com.snc.si_dep é necessário para qualquer versão Now Platform. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Security Operations aplicações.

As aplicações Security Operations a seguir devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative um aplicativo de cada vez na ordem listada abaixo para garantir uma instalação sem problemas:

1. Security Integration Framework
2. Security Support Common
3. Orquestração de suporte de segurança
4. Security Incident Response

Arquitetura de integração e conexão de sistemas

Para obter mais informações sobre a arquitetura da integração, incluindo termos-chave e detalhes de conexão de sistemas externos, consulte Arquitetura de integração e conexão de sistemas externos para a integração Microsoft Exchange Online.

Check-list

Os tópicos a seguir são numerados. Siga os tópicos listados abaixo na ordem em que são apresentados para uma instalação e configuração simples da aplicação.

Para obter uma check-list imprimível dessas etapas, consulte Check-list para a integração Microsoft Exchange Online. Você pode usar esta lista para monitorar seu andamento enquanto trabalha nas tarefas de ponta a ponta da configuração de integração, configuração e verificação de resultados.

Limitações

1. A disponibilidade de dados por meio da API Microsoft Threat Hunting está sujeita a atrasos causados pela latência entre o Exchange Server, a Graph API e a API Hunting. A sincronização entre a API de busca e o servidor do Exchange pode levar alguns minutos. O período de latência é variável e pode diferir de uma instância para outra.
2. As limitações da API de busca, cotas e alocação de recursos são explicadas aqui: https://learn.microsoft.com/en-us/graph/api/resources/security-api-overview?view=graph-rest-1.0#advanced-hunting

Configure sua conta do Azure Microsoft para a integração ServiceNow Microsoft Exchange Online

Conclua as seguintes tarefas de configuração no portal do Azure Microsoft antes de instalar a aplicação ServiceNow para esta integração. Esta conta permite acesso ao locatário Microsoft Exchange Online para obter detalhes da mensagem de e-mail.

Antes de Iniciar

Função necessária: Microsoft Administrador do portal do Azure

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta conta é necessária para acessar o locatário Microsoft Exchange Online para coletar detalhes adicionais da mensagem de e-mail e para excluir mensagens de e-mail. Esta conta é configurada no portal do Azure Microsoft.

As imagens nas tarefas a seguir são privilegiadas e proprietárias e são usadas com permissão de Microsoft. Este conteúdo está sujeito a atualizações em Microsoft. Para verificar se você tem acesso ao conteúdo mais atual, consulte o site de documentos da Microsoft .

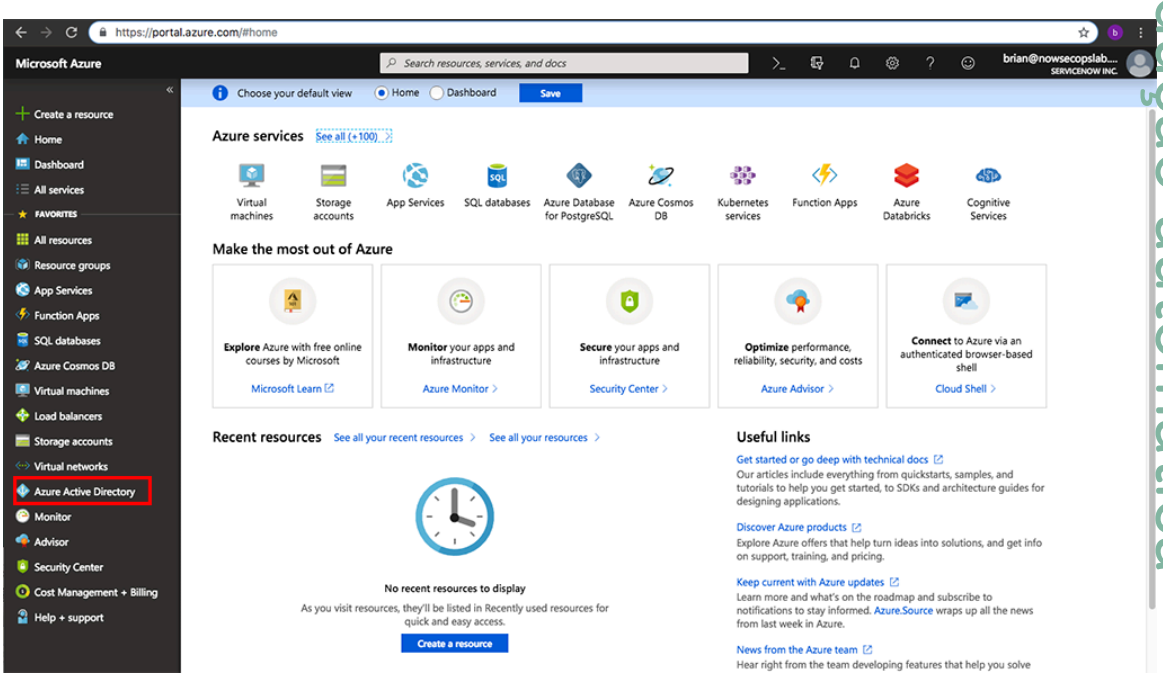
Nas imagens a seguir, ServiceNow Inc. é exibido para o nome da conta nos exemplos do portal do Azure. Na sua conta do portal do Azure, o nome da empresa da sua conta no portal do Azure é exibido.

Procedimento

Se você não criou um ID de aplicação para autenticação OAUTH no portal do Azure Microsoft, siga estas etapas.

a. Faça login no portal do Azure Microsoft usando suas credenciais de administrador do portal do Azure.

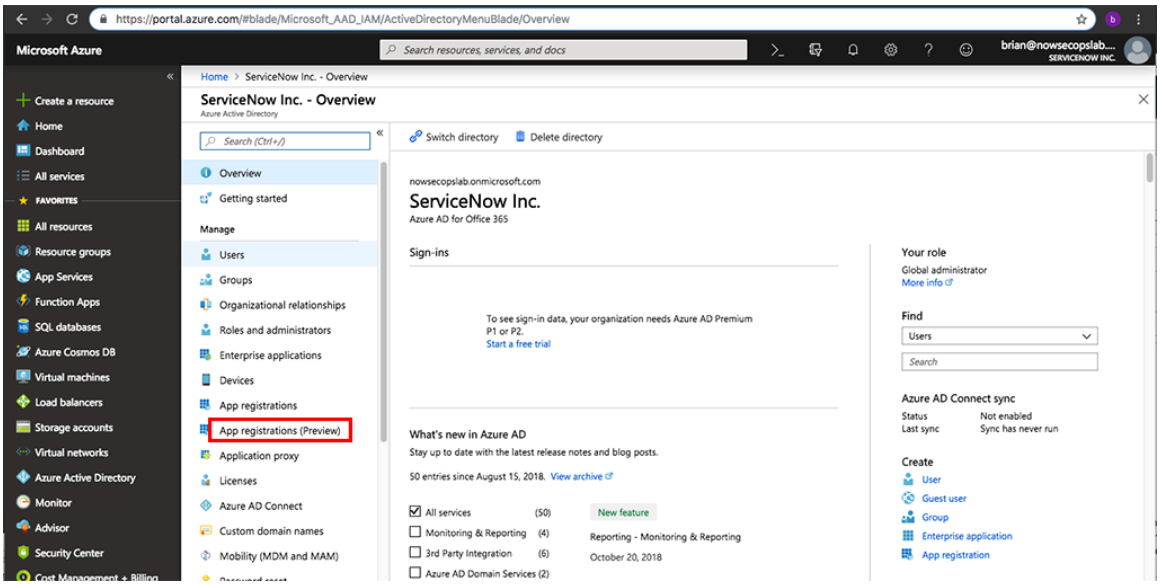
b. No painel de navegação esquerdo do painel inicial, clique em **Azure Active Directory**.



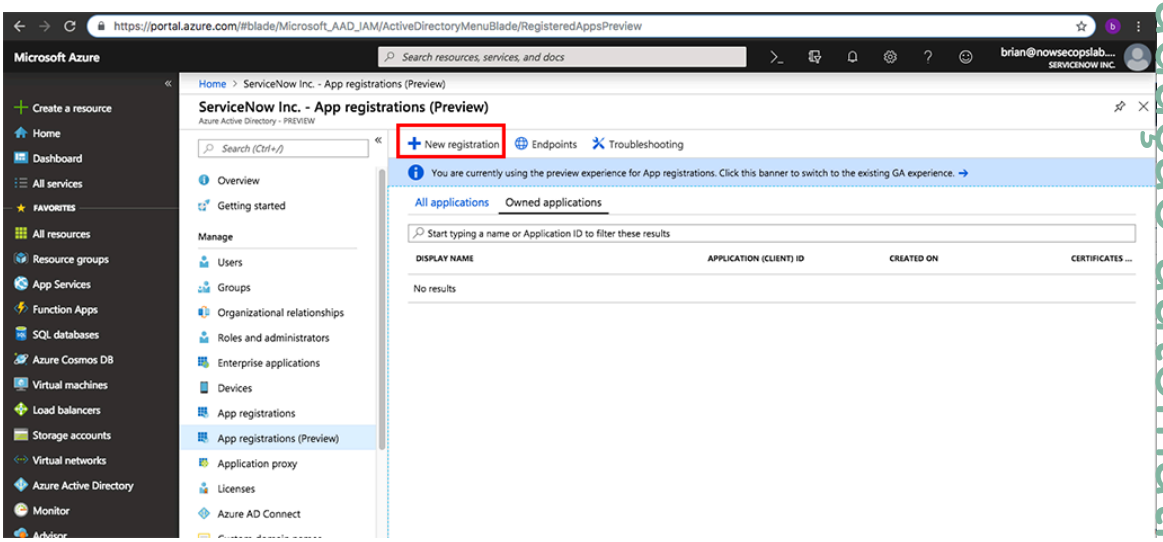
c. No painel Visão geral exibido, clique em **Registros do app (Visualização)**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. No painel Registros do aplicativo (Visualização) exibido, clique em **Novo registro**.



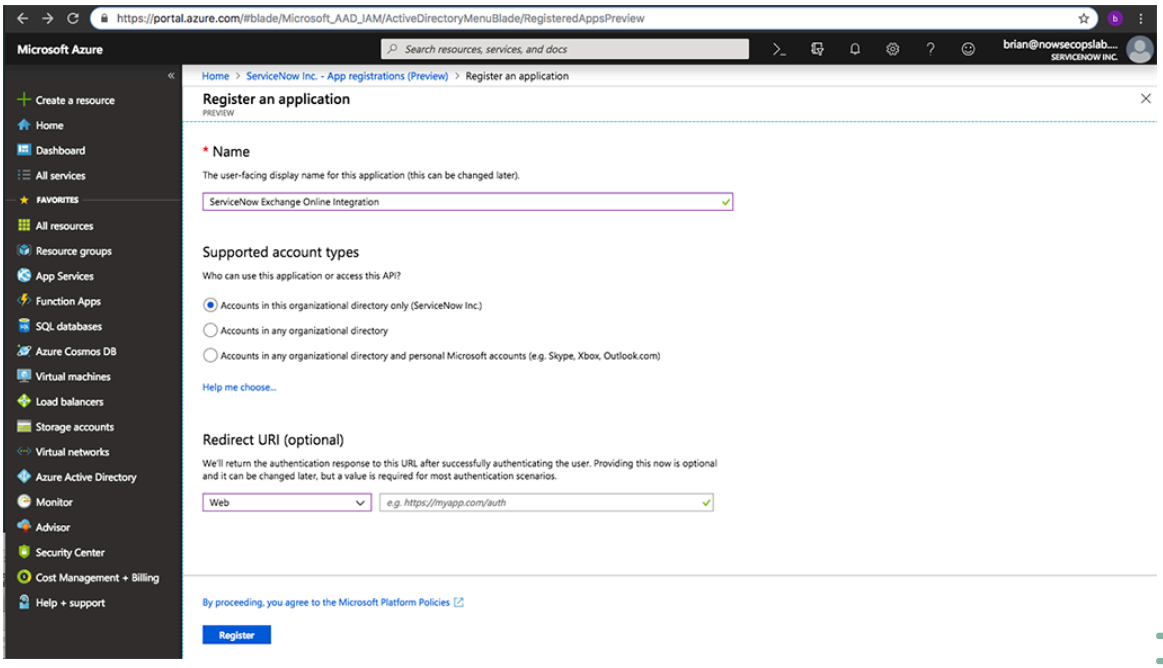
e. Preencha o formulário Registrar uma aplicação que é exibido.

Um exemplo de um formulário preenchido é mostrado após a tabela.

Campo	Descrição
Nome	Nome da aplicação. Neste exemplo, a Integração do Exchange Online da ServiceNow é inserida.
Tipos de conta compatíveis	Para esta conta, em Tipos de conta compatíveis, clique **em Contas neste diretório organizacional somente ServiceNow Inc.)**. Este domínio é usado para as pesquisas de e-mail.
URL de redirecionamento (opcional)	Se você inserir um valor para este campo, ele não será usado pela integração.

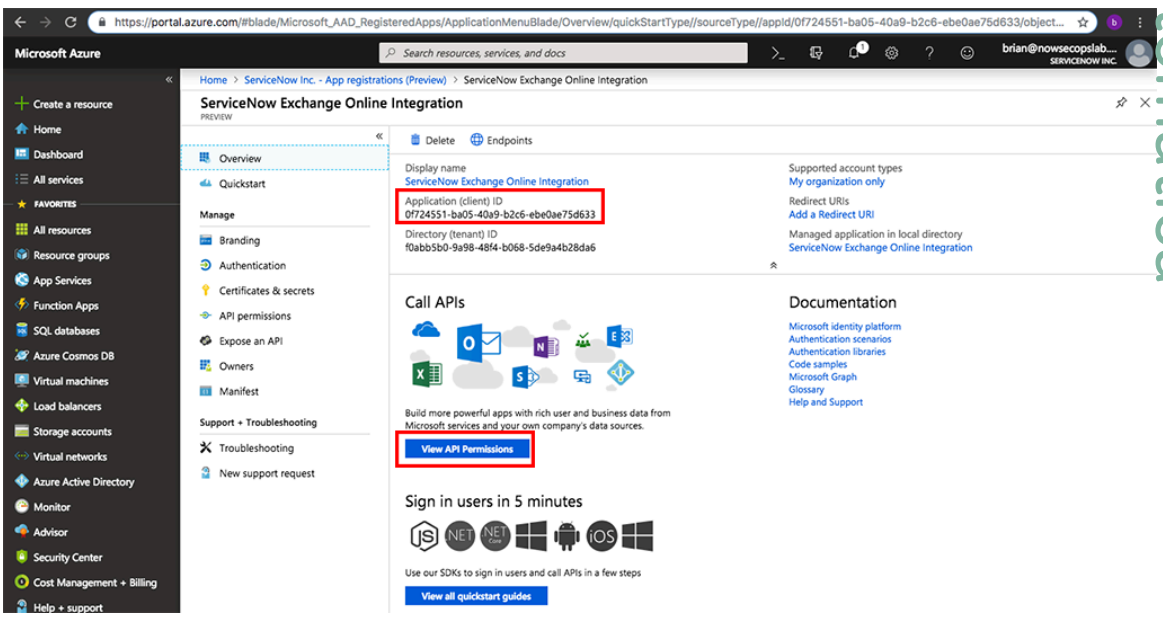
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



f. Clique em **Registrar**.
Um ID de aplicação é criado. Este ID é semelhante a um nome de usuário. Você insere este valor na página de configuração no campo **ID da aplicação OAUTH** durante a etapa de configuração na sua instância Now Platform que é descrita em Configure a integração Microsoft Exchange Online com sua instância Now Platform.

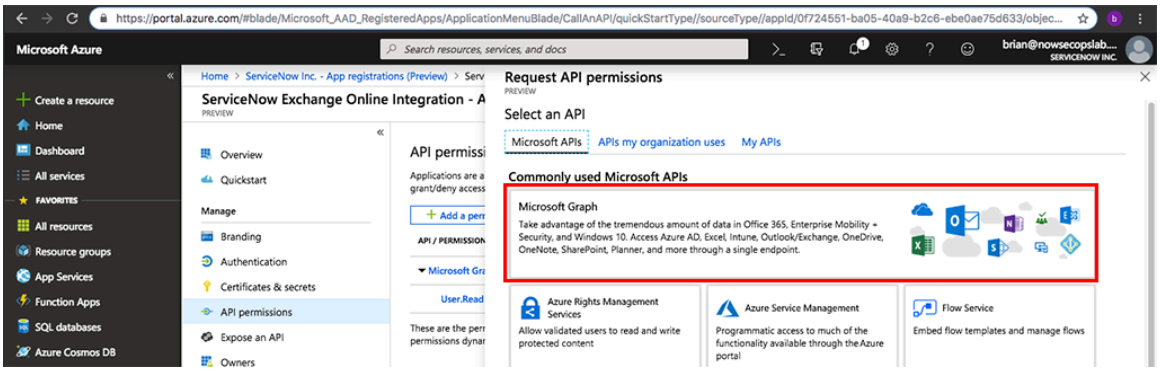
g. Com o ID da aplicação (cliente) exibido no painel de Integração do Exchange Online da ServiceNow, clique em **Exibir permissões de API**.



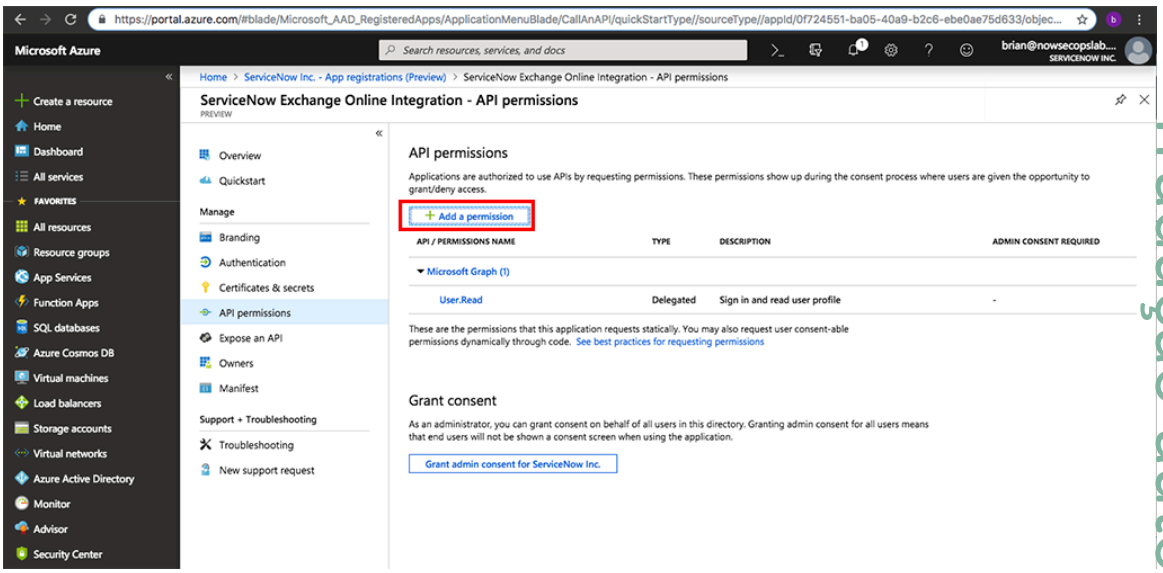
h. No painel Solicitar permissões de API exibido, clique em **Microsoft Graph**.

Tradução automática

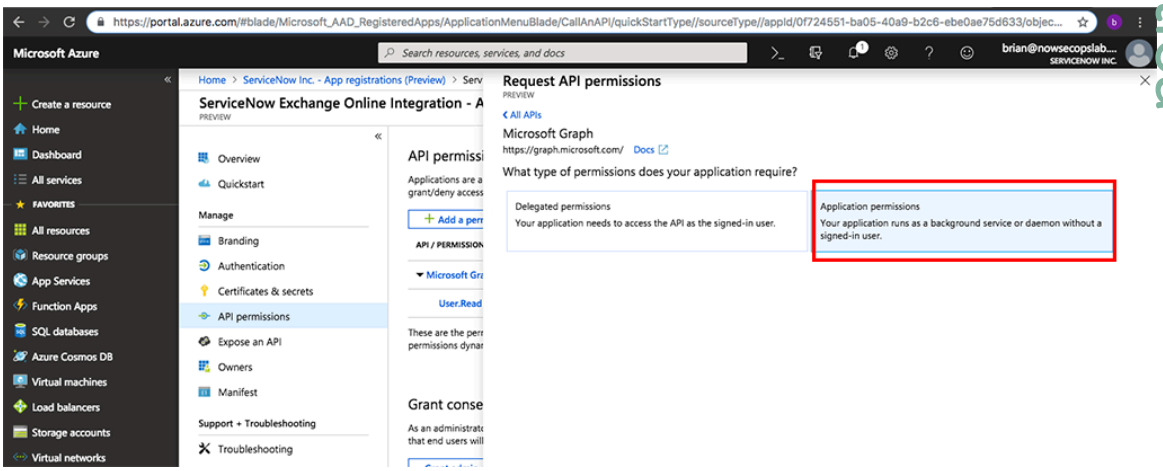
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



i. No painel Integração do Exchange Online da ServiceNow - Permissões de API exibido, clique em **Adicionar uma permissão**.



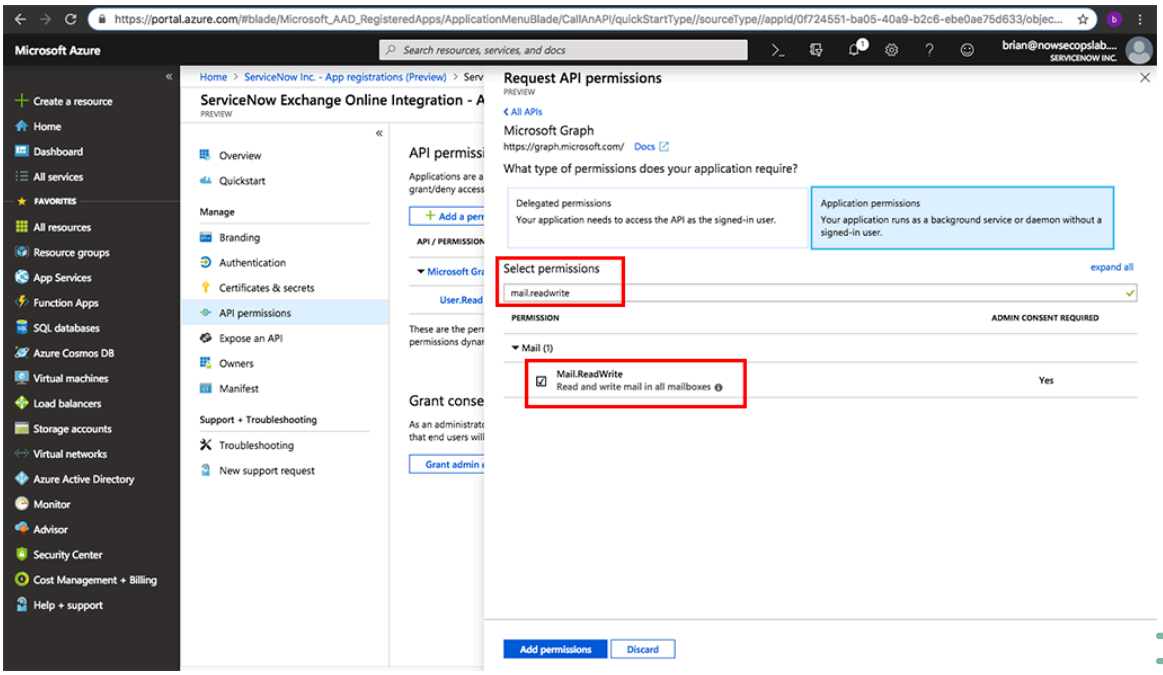
j. No painel Solicitar permissões de API exibido, clique em **Permissões da aplicação**.



k. No campo Selecionar permissões exibido, insira **Mail.ReadWrite** e marque a caixa de seleção **Mail.ReadWrite**.

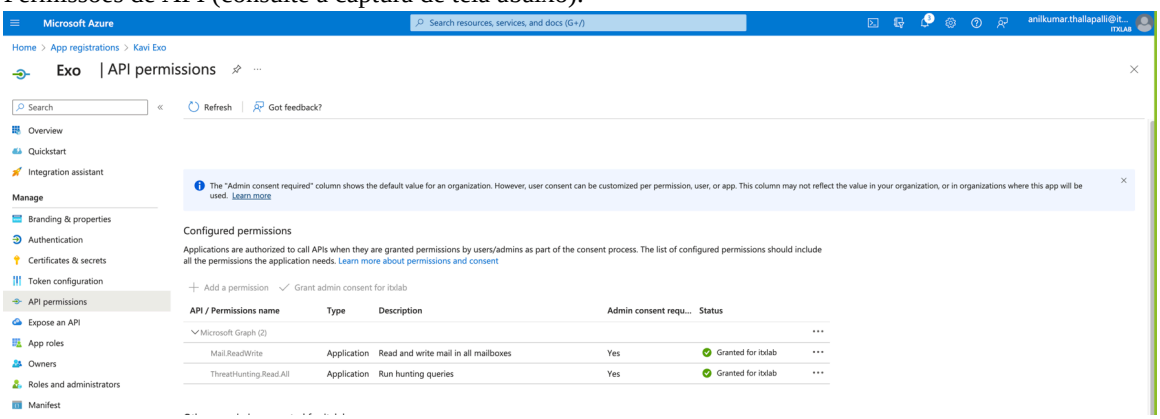
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



l. Clique **em Adicionar permissões**.

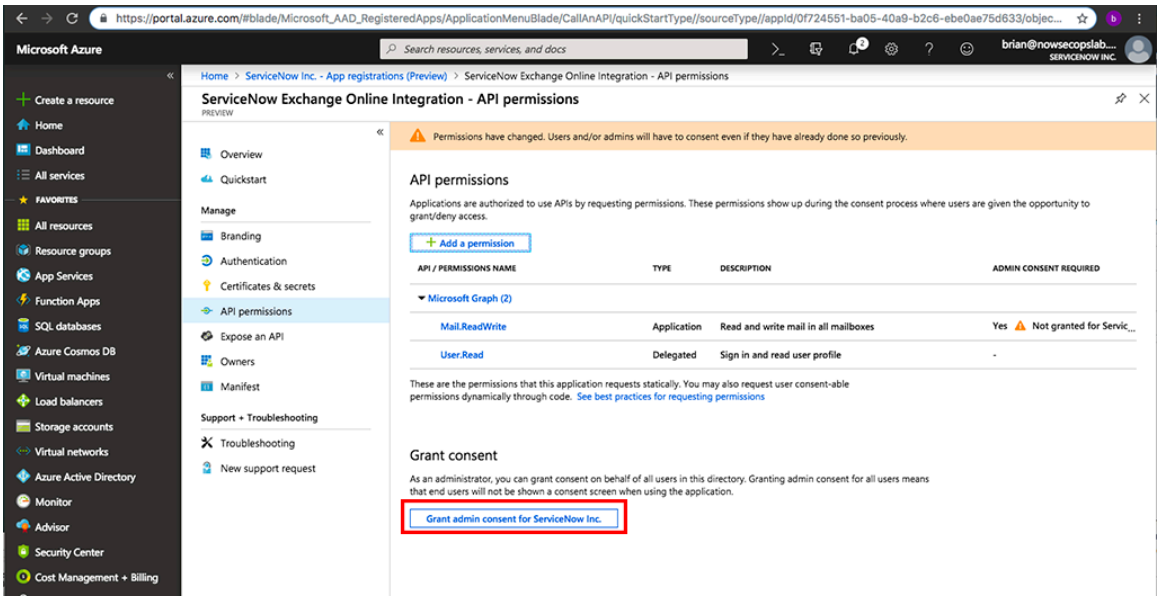
m. Repita as etapas da etapa i à etapa l para adicionar mais uma permissão, ThreatHunting.Read.All à lista de Permissões de API (consulte a captura de tela abaixo).



n. No painel Integração do Exchange Online da ServiceNow - Permissões de API exibido, clique em **Conceder consentimento do administrador para**<your organization name> .

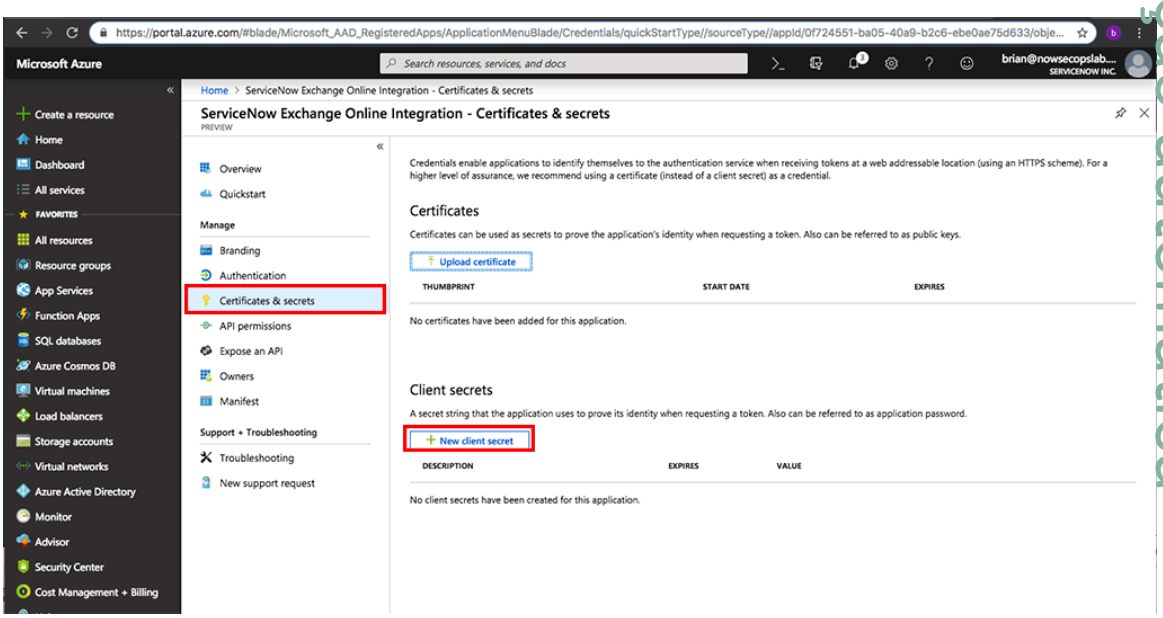
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



o. Para confirmar a seleção de API anterior (Microsoft Graph API) que você inseriu, clique em **Confirmar**.

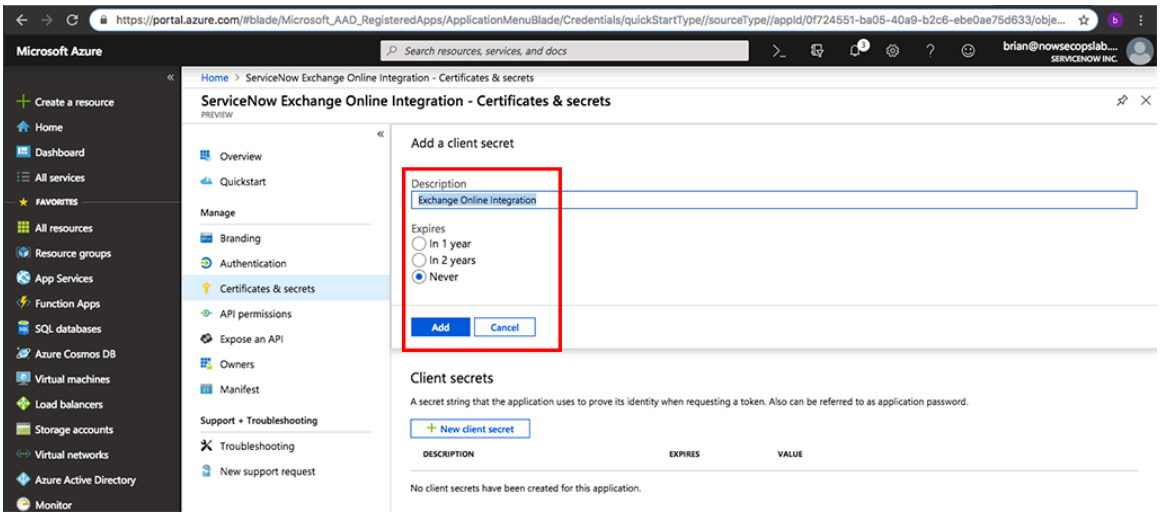
p. No painel ServiceNow Exchange Online Integration - Certificates & Secrets, clique em **Certificados e segredos**, seguido por **Novo segredo do cliente** (senha).



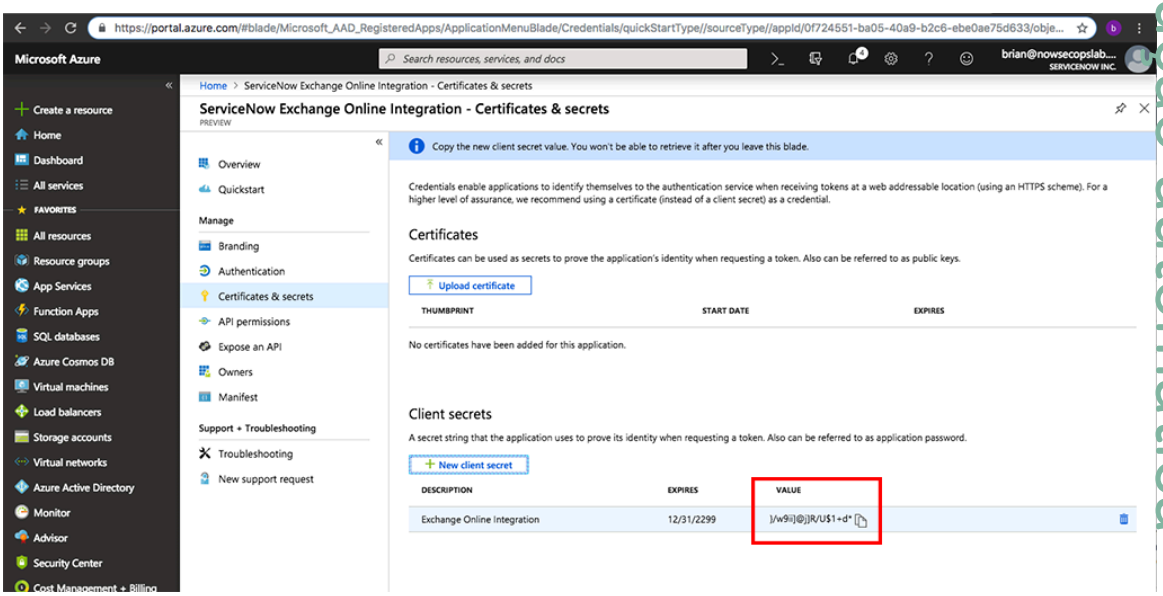
q. No formulário exibido no painel Integração do Exchange Online da ServiceNow - Certificados e segredos, insira o nome da aplicação no campo Descrição, clique em uma opção de expiração e clique em **Adicionar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



No painel Certificados e segredos exibido, na seção **Segredos do cliente**, em Valor, a linha é preenchida com o novo segredo do cliente (senha). Salve esta senha em um local seguro. Depois de sair desta página, este valor de senha não estará mais visível. Você insere essa senha no campo **Segredo do cliente OAUTH** na página de configuração durante a etapa de configuração da integração na sua instância Now Platform. As etapas de configuração da integração são descritas em Configure a integração Microsoft Exchange Online com sua instância Now Platform.



Você criou com sucesso um ID de aplicação para autenticação OAuth no portal do Azure Microsoft.

O que Fazer Depois

Você está pronto para configurar sua instância Now Platform® para a integração.

Configurar integração do Exchange Online com o Security Incident Response

Uma integração inicial é necessária para autenticação usando objetos da aplicação. A aplicação e a entidade de serviço são usadas de forma intercambiável, mas uma aplicação é como um objeto de classe, enquanto uma entidade de serviço é como uma instância da classe.

Para obter mais informações sobre objetos principais de serviço e aplicação no Azure Active Directory, consulte Objetos principais de serviço e aplicativo no Azure Active Directory . Para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

obter um fluxo visual detalhado sobre como criar aplicações no Azure AD, consulte Criar uma aplicação Azure Active Directory e entidade de serviço que pode acessar recursos .

Execute as seguintes etapas para configurar:[store-future: BEGIN review]

1. Registre a aplicação no Azure AD.
2. Atribua permissões de API à aplicação.

   Para que o objeto da aplicação acesse os recursos, ele precisa ter a permissão da aplicação `ThreatHunting.Read.All` e `Mail.ReadWrite`.

3. [store-future: BEGIN review]Gere um certificado autoassinado e conceda acesso à chave privada.

   Crie e configure um certificado X.509 autoassinado, que é usado para autenticar sua aplicação no Azure AD, ao solicitar o token de acesso somente da aplicação. Os certificados de última geração (CNG) não são compatíveis com a autenticação somente de app com o Exchange. Os certificados CNG são criados por padrão nas versões modernas do Windows. Você deve usar um certificado de um provedor de chaves CSP. `(-Provider = 'Provedor de criptografia forte da Microsoft')`.

   [End]
4. [store-future: BEGIN review]Anexe o certificado à aplicação do Azure AD.[End]
5. [store-future: BEGIN review]Atribua funções do Azure AD à aplicação.

   A aplicação precisa ter a função `Administrador de conformidade do` Azure AD atribuída.

   [End]
6. [store-future: BEGIN review]Crie uma nova entidade de serviço.[End]

[End]

Etapa 1: registrar a aplicação no Azure AD

1. Abra o portal do Azure AD .
2. Na caixa **Pesquisar** na parte superior da página, digite **Registros do app**.
3. Selecione **Registros do aplicativo** nos resultados da seção Serviços e selecione Registros do aplicativo nos resultados da seção **Serviços**.

   Como alternativa, você pode navegar até a página **Registros do aplicativo** usando https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade .
4. Na página **Registros do aplicativo**, selecione **Novo registro**.
5. Na página **Registrar uma aplicação**, defina as seguintes configurações:

Campo	Descrição
Nome	Insira algo descritivo. Por exemplo, ExO PowerShell CBA.
Tipos de conta compatíveis	Verifique se **Contas somente neste diretório organizacional (** <YourOrganizationName> somente - Locatário único) está selecionado. Para tornar a aplicação multilocatária para cenários delegados do Exchange Online,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	selecione o valor Contas em qualquer diretório organizacional (Qualquer diretório do Azure AD - Multilocatário).

6. Depois de concluir o registro do app, selecione **Registrar** e feche a página do app.

Etapa 2: atribuir permissões de API à aplicação

Os procedimentos nesta seção substituem todas as permissões padrão que foram configuradas automaticamente para o novo app. O app não precisa das permissões padrão que foram substituídas.

1. Na página do app, selecione **Manifesto** em Gestão.
2. Na página Manifesto, localize a entrada `obrigatórioResourceAccess` (na linha 52 ou próximo a ela).
3. Modifique os valores de `resourceAppId`, `resourceAccess id` e `resourceAccess type` conforme mostrado no seguinte snippet de código:

```
"requiredResourceAccess": [
    {
        "resourceAppId": "00000003-0000-0000-c000-000000000000",
        "resourceAccess": [
            {
                "id": "e2a3a72e-5f79-4c64-b1b1-878b674786c9",
                "type": "Role"
            },
            {
                "id": "dd98c7f5-2d42-42d3-a0e4-633161547251",
                "type": "Role"
            }
        ]
    }
],
```

4. Selecione **Salvar**.
5. Na página **Manifesto**, selecione **Permissões de API** em Gestão.
6. Na página de **permissões de API**, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
API/Nome de permissões	Verifique se o valor ThreatHunting.Read.All e Mail.ReadWrite é mostrado.
Status	O valor incorreto atual é **Não concedido para**<Organization> e este valor precisa ser alterado. Selecione **Conceder consentimento do administrador para**<Organization> , leia a caixa de diálogo de confirmação que é aberta e selecione **Sim**. O valor do status agora deve ser **Concedido para**<Organization> .

7. Feche a página de permissões de API atual (não a guia do navegador) para retornar à página de registros do app.

[store-future: BEGIN review]

Etapa 3: gerar um certificado autoassinado e conceder acesso à chave privada

Crie um certificado x.509 autoassinado executando o seguinte:

- Use os cmdlets New-SelfSignedCertificate , Export-Certificate e Export-PfxCertificate em uma sessão elevada (executada como administrador) do Windows PowerShell para solicitar um certificado autoassinado e exportá-lo para .cer e .pfx (SHA1 por padrão). Por exemplo:

```
# Create certificate
$mycert = New-SelfSignedCertificate -DnsName "snowsecops.onmicrosoft.com"
 -CertStoreLocation "cert:\LocalMachine\My" -NotAfter (Get-Date).AddYears(2) -KeySpec
 KeyExchange -Provider "Microsoft Strong Cryptographic Provider"

# Generate password fro private key
$mypwd = ConvertTo-SecureString -String '<password>' -Force -AsPlainText

# Export certificate to .pfx file
$mycert | Export-PfxCertificate -FilePath mycert.pfx -Password $mypwd

# Export certificate to .cer file
$mycert | Export-Certificate -FilePath mycert.cer
```

- Forneça acesso de chave privada ao usuário do serviço MID usando as seguintes etapas:
  1. Abra **o MMC (Console de gestão da Microsoft)**.
  2. No Microsoft Management Console (MMC), navegue até **Certificados (computador local)** > **Pessoal** > **Certificados**.

     (Se o MMC não tiver nenhum item de menu, adicione-o navegando até **Arquivo** > **Adicionar Remover Snap-in**.
  3. Clique com o botão direito do mouse no certificado que você gerou.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Expandir **Todas as tarefas** > **Gerenciar chaves privadas**
5. Adicione o **usuário do serviço MID** à lista de acessadores.

[End]

[store-future: BEGIN review]

Etapa 4: anexar o certificado à aplicação do Azure AD

Depois de registrar o certificado com sua aplicação, você pode usar a impressão digital para autenticação.

1. Na guia **Aplicativos** próprios na página de **registro** de aplicativos no final da Etapa 2, selecione seu aplicativo.

   Se você precisar voltar para a página de **registro de aplicações**, use https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/%7E/RegisteredApps , verifique se a guia **Aplicações** próprias está selecionada e selecione sua aplicação.

2. Selecione **Certificados e segredos** em Gerenciar.
3. Na página **Certificados e segredos** que é aberta, selecione **Carregar certificado**.
4. Navegue até o certificado autoassinado (arquivo.cer) que você criou na Etapa 3.
5. Após concluir, selecione **Adicionar**.

   O certificado agora é mostrado na seção Certificados.

6. Anote CertificateThumbImprima e feche a página atual de **Certificados e segredos**.

[End]

[store-future: BEGIN review]

Etapa 5: atribuir funções do Azure AD à aplicação

1. Abra o portal do Azure AD .
2. No campo **Pesquisar** na parte superior da página, procure por **Funções e Administradores**.
3. Selecione **Funções e administradores do Azure AD** nos resultados na seção Serviços.

   Como alternativa, você pode navegar até a página de **funções e administradores do Azure AD** usando https://portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade .

4. Na página **de funções e administradores do Azure AD**, localize e selecione uma das funções compatíveis clicando no nome da função (não na caixa de seleção) nos resultados.

   Encontre e selecione a função de **Administrador de conformidade**.

5. Na página **Atribuições**, selecione **Adicionar atribuições**.
6. No pop-up **Adicionar atribuições**, localize e selecione o app que você criou na Etapa 1.
7. Após concluir, selecione **Adicionar**.
8. Volte para a página **Atribuições** e verifique se a função foi atribuída ao app.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

[End]

[store-future: BEGIN review]

Etapa 6: criar uma nova entidade de serviço

Importante:
Certifique-se de estar conectado ao **Security & Compliance PowerShell** antes de concluir as etapas para criar uma nova entidade de serviço. Criar uma nova entidade de serviço sem se conectar ao PowerShell não funcionará (seu ID do app do Azure e o ID do objeto são necessários para criar a nova entidade de serviço).

1. Execute o seguinte comando para armazenar os detalhes da aplicação Azure que você registrou na Etapa 1 (<AppName>) em uma variável:

```
Install-Module -Name AzureAD
Import-Module -Name AzureAD
Connect-AzureAD
$AADApp = Get-AzureADServicePrincipal -SearchString"<AppName>"
```

   Para obter informações detalhadas de sintaxe e parâmetro, consulte Get-AzureADServicePrincipal .

2. Na mesma janela do PowerShell, conecte-se ao Security & Compliance PowerShell :

```
Import-Module ExchangeOnlineManagement
Connect-IPPSSession -CertificateThumbPrint "<Your_Certificate_ThumbPrint>" -AppID
 $AADApp.AppId -Organization "<Your_organization>
```

   Execute os seguintes comandos para criar um objeto principal de serviço para a aplicação Azure:

```
New-ServicePrincipal -AppId $AADApp.AppId -ObjectId $AADApp.ObjectId -DisplayName
"<Descriptive Name>"
```

   Para obter informações detalhadas de sintaxe e parâmetro, consulte New-ServicePrincipal .

[End]

Tradução automática

Configure sua instância Now Platform® para a integração Microsoft Exchange Online

A seção a seguir lista as tarefas de configuração que você deve concluir em sua instância Now Platform® antes de instalar a aplicação Microsoft Exchange Online. Revise a check-list e verifique se você concluiu essas tarefas antes de baixar e instalar a aplicação Microsoft Exchange Online para a integração a fim de garantir uma instalação e configuração sem problemas.

Antes de Iniciar

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform® e Security Incident Response (SIR) necessárias.	As seguintes funções ServiceNow são necessárias: • O administrador do sistema (admin) instala aplicações e atribui a função de administrador de incidentes de segurança (sn_si.admin).

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	• O administrador de incidentes de segurança (sn_si.admin) configura a aplicação para a integração. Se necessário, a função de administrador de incidentes de segurança também atribui ao analista de incidentes de segurança (sn_si.analyst) as funções de leitura e gravação de e-mail (sn_sec_cmn.cap_email_write e sn_sec_cmn.cap_email_read). As funções (sn_sec_cmn.cap_email_read) e (com.snc.security_incident) são instaladas com o produto Security Incident Response. Eles são atribuídos ao administrador de incidentes de segurança por padrão e podem ser reatribuídos conforme necessário. • O analista de incidentes de segurança (sn_si.analyst) executa pesquisas de e-mail e exclui e-mails. Esta função também verifica se os e-mails foram excluídos e funciona com incidentes de segurança. ◦ A função de gravação permite que o sn_si.analyst edite, crie e execute pesquisas de e-mail e exclua mensagens. Não há nenhuma função separada necessária para excluir mensagens. ◦ A função de leitura permite que o sn_si.analyst exiba os resultados em listas relacionadas em incidentes de segurança. **Nota:** O sn_si.analyst deve ter as funções (sn_sec_cmn.cap_email_read) e (sn_sec_cmn.cap_email_write) para exibir os resultados da pesquisa de e-mail e criar e executar consultas de pesquisa de e-mail. Se não for atribuído, as etapas a seguir descrevem como atribuir as funções (sn_sec_cmn.cap_email_read) e (sn_sec_cmn.cap_email_write) ao analista de incidente de segurança. Para obter mais informações sobre como atribuir funções em Security Incident Response, consulte Funções instaladas com SIR.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão	O plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário

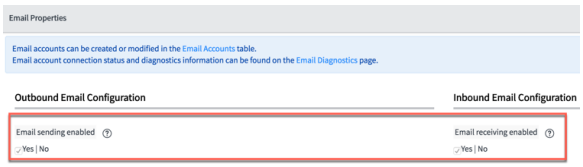
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
instaladas e ativadas antes de instalar a aplicação para a integração.	e instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras aplicações Security Operations necessárias para a integração. Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Orquestração de suporte de segurança Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.
Se sua organização planeja usar Now Platform notificações por e-mail, verifique se a funcionalidade de envio/recebimento de e-mail está habilitada.	Siga estas etapas para verificar se a funcionalidade de envio e recebimento de e-mail está habilitada na sua instância Now Platform®. Esta capacidade notifica os usuários por e-mail quando as pesquisas e solicitações de exclusão foram iniciadas e concluídas com sucesso. **1.** Navegar até **Propriedades do e-mail** > **Administração** > **Propriedades do E-mail**. **2.** Em Configuração de e-mail de saída, verifique se Envio de e- mail habilitado e Recebimento de e-mail habilitado estão selecionados. Esta funcionalidade de envio/recebimento de e-mail é necessária para que o analista de incidentes de segurança receba notificações por e-mail enviadas pelo Now Platform®. Se o recurso de aprovação de exclusão estiver habilitado, as solicitações para excluir e-mails também serão enviadas aos aprovadores por e-mail. Além de habilitar esta propriedade de e-mail, não há nenhuma outra configuração necessária para enviar e receber e-mails no Now Platform®.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Como administrador de incidente de segurança Now Platform (sn_si.admin), as funções de leitura e gravação de e-mail (sn_sec_cmn.cap_email_read) e (sn_sec_cmn.cap_email_write) são atribuídas automaticamente a você ao baixar o produto Security Incident Response (SIR). Como administrador de incidentes de segurança, você atribui essas funções ao analista de incidentes de segurança (sn_si.analyst) ou a outra função. Se você não atribuiu essas funções ao analista de incidente de segurança ou a outra função, siga estas etapas para atribuí-las.

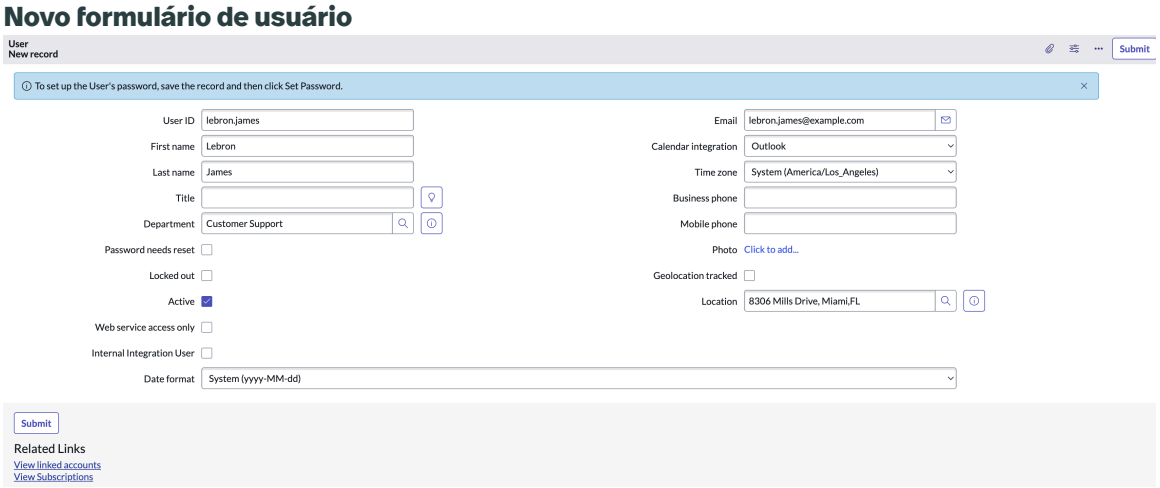
Procedimento

1. Navegar até **Organização** > **Usuários**.
2. Clique no módulo **Usuários**.
   a. Na lista Usuários exibida, clique em **Novo**.
   b. No novo formulário de usuário exibido, preencha o formulário.

Campo	Descrição
UserID	ID do usuário para a função de analista de incidente de segurança Now Platform, por exemplo, jferguson.
E-mail	Endereço de e-mail da empresa. As notificações dos resultados da pesquisa de e-mail e as confirmações de exclusão de e-mail são enviadas para este endereço de e-mail. Para este exemplo, jferguson@servicenow.com é usado, mas qualquer endereço de e-mail da empresa pode ser usado para receber essas notificações por e-mail, conforme exigido pela sua organização.
Nome	Nome
Sobrenome	Sobrenome
Título	Analista deincidentesde segurança, Analista de segurança ou Analista doSecurity Operations Center (SOC), por exemplo.

Tradução automática

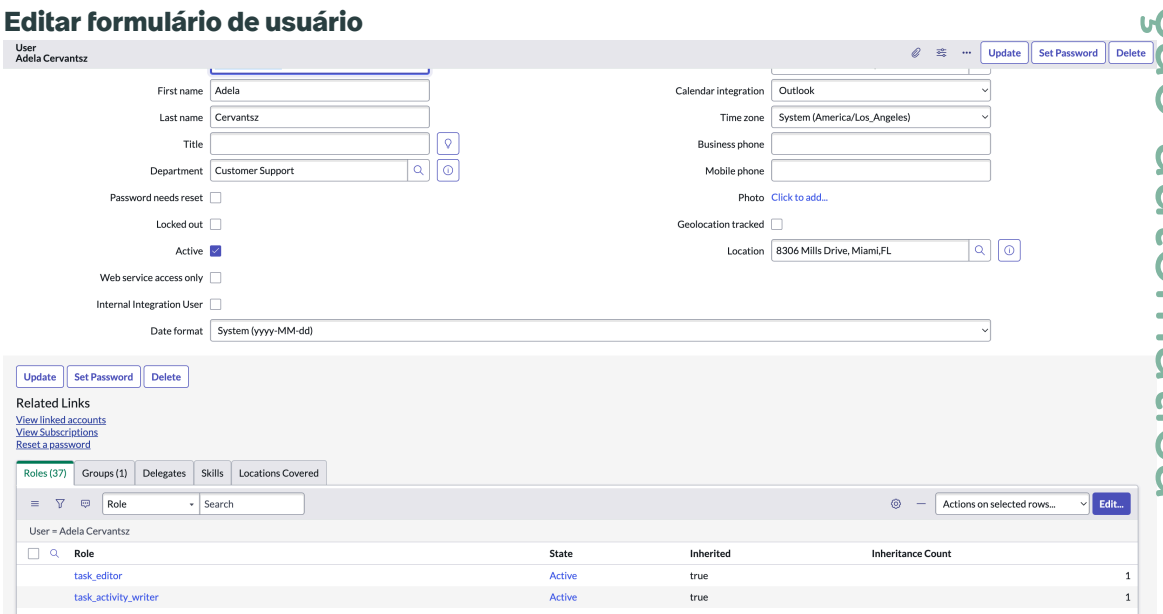
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Clique em **Enviar**.
O novo usuário é exibido na lista Usuários.

3. Na lista Usuários na coluna ID do usuário, clique no nome do usuário ao qual você deseja atribuir as funções `sn_sec_cmn.cap_email_read` e `sn_sec_cmn.cap_email_read`.

4. No registro aberto na seção Links relacionados, clique em **Editar**.



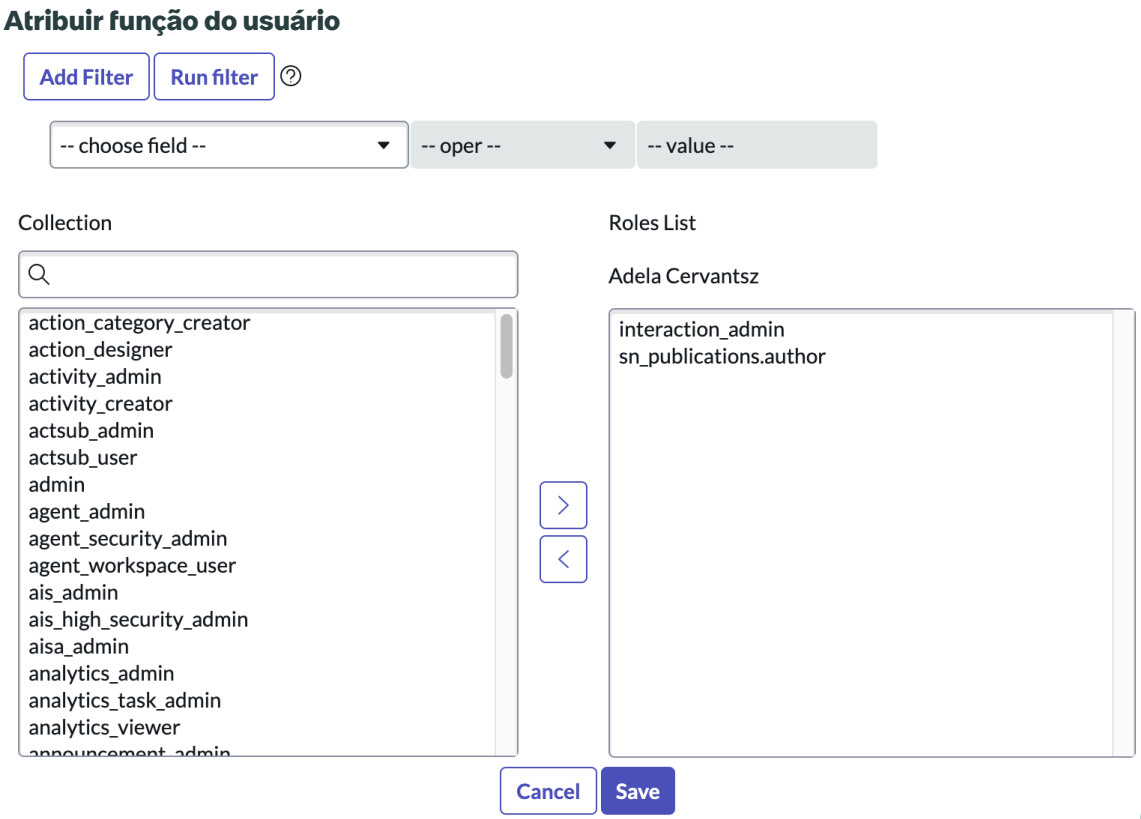
5. No formulário Editar membros exibido, insira `sn_sec_cmn.cap_email_read` no campo de coleta.

Nota:
A coluna abaixo do campo é preenchida automaticamente. Se o usuário não tiver sido atribuído à função sn_si.analyst, insira `sn_si.analyst` no campo Coleção também. Na figura a seguir, a função sn_si.analyst já foi atribuída a Joe Ferguson.

6. Na coluna Coleção, selecione e mova `sn_sec_cmn.cap_email_read` e `sn_sec_cmn.cap_email_read` e `sn_si.analyst` (se ainda não estiverem atribuídos) para a Lista de funções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

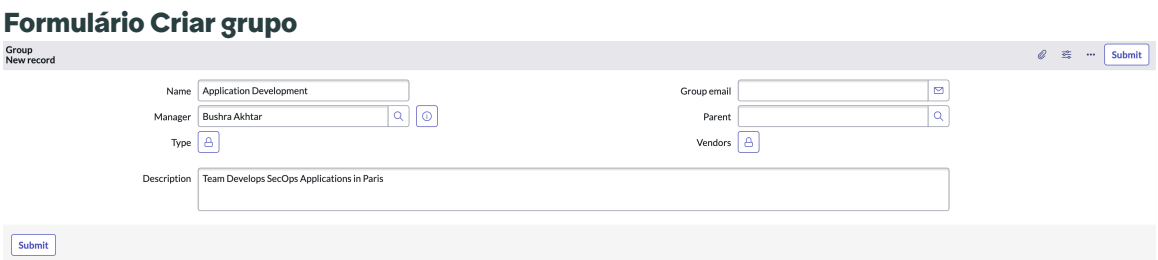


7. Clique em **Salvar**.
   As funções sn_sec_cmn.cap_email_read e sn_sec_cmn.cap_email_read são atribuídas ao analista de segurança (jferguson).
8. Adicione usuários e atribua funções conforme necessário para sua organização.
9. **Opcional:** Se você quiser habilitar o recurso de aprovação para solicitações de exclusão de e-mail, siga estas etapas para criar um grupo de aprovação.

   a. Navegar até **Administração de usuários** > **Grupos**.

   b. Na lista Grupos exibida, clique em **Novo**.

   c. No formulário, preencha os campos.



   Para obter mais informações sobre como criar grupos e atribuir funções, consulte Criar um grupo de usuários .

   d. Clique em **Enviar**.
   Na coluna Nome, o novo grupo é exibido na lista Grupos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode adicionar mais usuários a este grupo. Um usuário herda funções de todos os grupos aos quais o usuário pertence. Você também pode atribuir funções diretamente a um usuário. Para obter mais informações, consulte Managing roles. Cada usuário pode aprovar solicitações de exclusão de e-mail enviadas pelo analista de segurança. É necessário apenas um usuário para aprovar ou rejeitar a solicitação.

Se sua organização deseja um nível extra de controle sobre a exclusão de e-mails com esta integração, habilite o recurso de aprovação opcional. Marque a caixa de seleção **Habilitar** na guia Configurações adicionais durante a etapa de configuração para habilitar as aprovações. No exemplo anterior, cada usuário do grupo de Aprovadores do Exchange Online está disponível para processar solicitações de exclusão por meio de notificação por e-mail.

Instalar a aplicação Microsoft Exchange Online para a integração ServiceNow Microsoft Exchange Online

Antes de executar a integração em sua instância, instale a aplicação Microsoft Exchange Online para a integração do ServiceNow Store.

Antes de Iniciar

Antes de instalar a aplicação da ServiceNow Store na sua instância Now Platform, conclua todas as tarefas listadas nas check-lists de pré-requisito.

Função necessária: administrador

Importante:
Se você instalar dados de demonstração, uma configuração de demonstração sem credenciais será criada automaticamente. Isso pode causar erros. Para obter detalhes, consulte KB0755880.

Procedimento

1. Se você não instalou a aplicação para a integração, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.
2. Depois de instalar a aplicação do ServiceNow Store, configure-o para se conectar à sua instância Now Platform.

Tópicos relacionados

Configure sua conta do Azure Microsoft para a integração ServiceNow Microsoft Exchange Online

Configurar integração do Exchange Online com o Security Incident Response

Configure sua instância Now Platform para a integração Microsoft Exchange Online

Configure a integração Microsoft Exchange Online com sua instância Now Platform

Depois de instalar a aplicação do ServiceNow Store, configure-o para se conectar à sua instância Now Platform. Esta ativação ativa os fluxos de trabalho de pesquisa e exclusão.

Antes de Iniciar

Função necessária: sn_si.admin

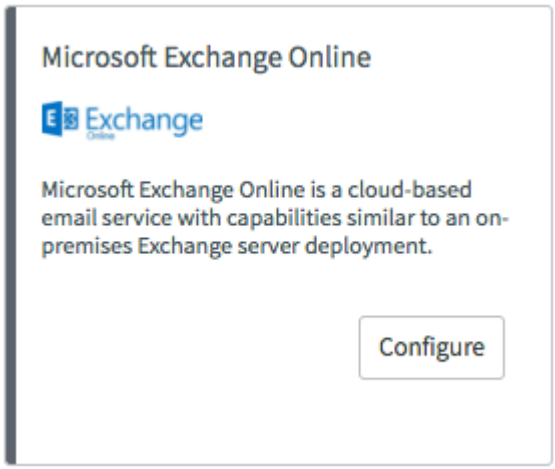
Procedimento

1. Em sua instância Now Platform, navegue até **Security Operations** > **Integrações** > **Configurações de Integração**.
2. Localize o bloco Microsoft Exchange Online.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

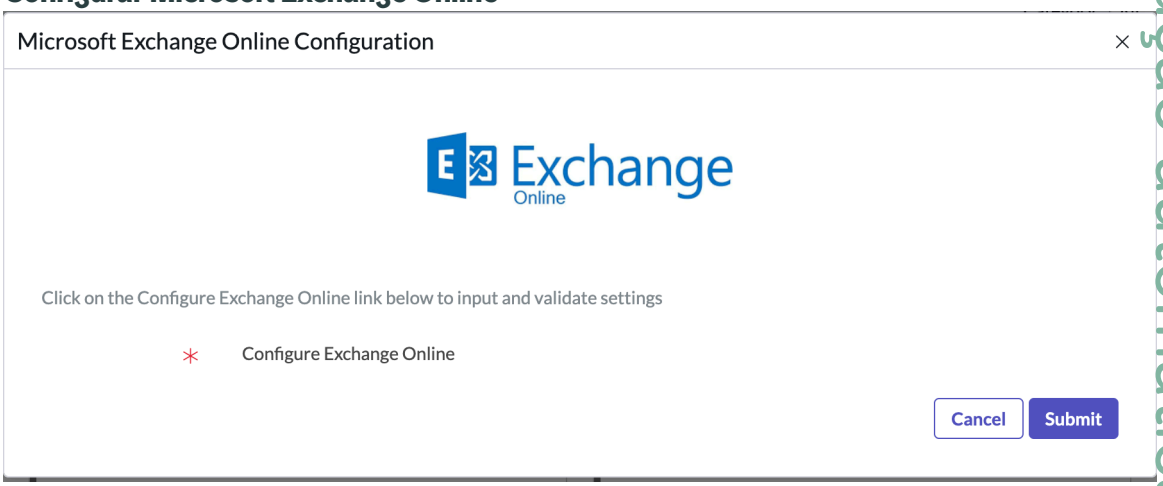
3. Clique em **Configurar**.



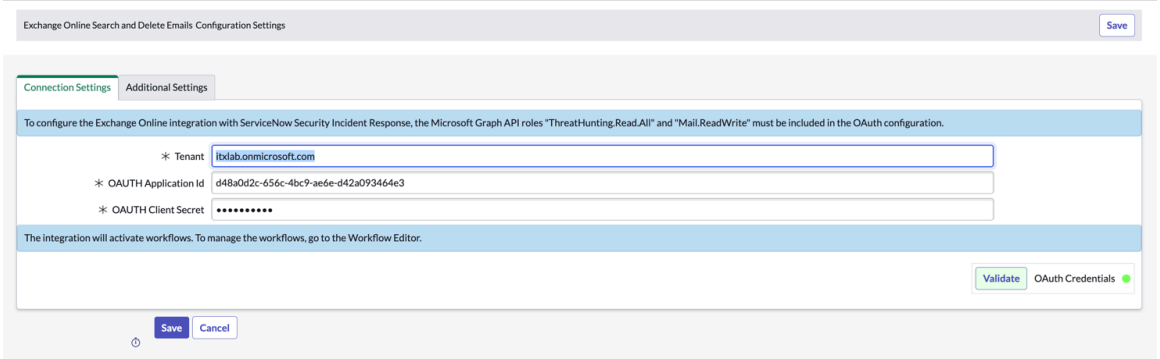
4. Na caixa de diálogo de configuração Microsoft Exchange Online exibida, clique em **Configurar Exchange Online**.

   Um exemplo de um formulário preenchido e validado segue a tabela.

Configurar Microsoft Exchange Online



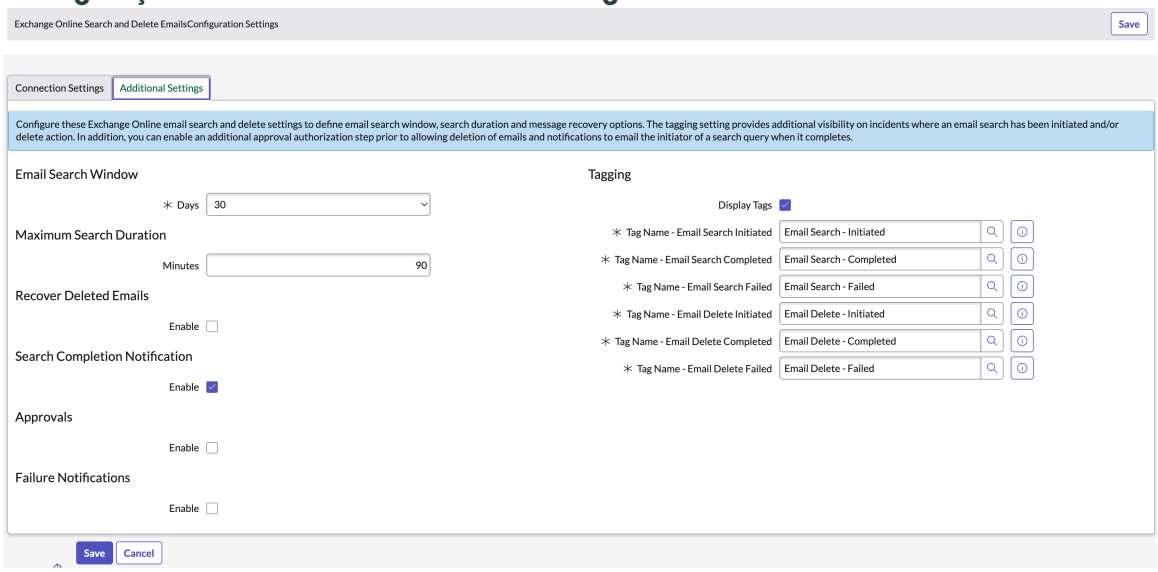
Configurações de conexão do Microsoft Exchange Online



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações adicionais do Microsoft Exchange Online



5. Escolha um para continuar.

Trouble?
Se uma mensagem de erro for exibida ou um ou mais dos indicadores à direita do botão Validar estiverem vermelhos, verifique se as credenciais da conta do usuário inseridas são válidas. Insira suas credenciais e clique em **Salvar** novamente.

Validação malsucedida

Consulte a tabela a seguir para obter mais informações sobre o botão **Validar** e os ícones coloridos.

Estado do botão Validar e dos indicadores	Descrição
O botão Validar está verde.	Indica que o OAuth é válido.
O botão Validar está vermelho claro.	O botão de credenciais do OAuth do Exchange Online está vermelho: indica que as credenciais do OAuth do Exchange Online são inválidas. **Nota:** Se algum dos campos de conexão, como ID do locatário, ID do cliente ou Segredo do cliente, for inválido, as mensagens de erro correspondentes serão exibidas. Certifique-se de fornecer os detalhes de conexão válidos.

Definir critérios de pesquisa de e-mail e solicitar uma pesquisa no serviço Microsoft Exchange Online

Como um usuário com a função sn_si.analyst, defina os critérios de pesquisa e envie uma solicitação de pesquisa de e-mail com base nos detalhes do incidente em um registro de incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.analyst

Os números neste procedimento são mostrados com os **formulários** com guia selecionados em Configurações do sistema. Para obter mais informações sobre como selecionar e limpar formulários com guias, consulte a seção intitulada Exibir formulários com guias em Configuração do layout de formulário no site de Documentação de produtos da ServiceNow .

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
O status de mensagens individuais que correspondem à consulta de pesquisa e os resultados da pesquisa são relatados no registro de incidente de segurança. Se as notificações por e-mail estiverem habilitadas, você poderá exibir os resultados da pesquisa de uma mensagem de e-mail.

Os critérios de pesquisa podem incluir endereços do remetente da mensagem, endereços do destinatário ou nomes do assunto. As seguintes combinações de parâmetros de pesquisa Assunto, Remetente e Destinatário da mensagem geralmente são usadas para encontrar mensagens de e-mail relacionadas a phishing que podem fazer parte de uma única campanha de phishing:

- Encontrar todos os e-mails originais enviados por uma conta de phishing: pesquisar por remetente.
- Encontrar todos os e-mails originais de uma única campanha de phishing: pesquisar por assunto e remetente.
- Encontrar todos os e-mails recebidos para uma única campanha de phishing (original e encaminhado, qualquer remetente): pesquisar por assunto.
- Encontrar todos os e-mails encaminhados para um único e-mail de phishing de um único usuário: pesquisar por destinatário + assunto.
- Encontrar todos os e-mails relacionados a phishing enviados para um único usuário: pesquisar por remetente + destinatário.

Nota:
As pesquisas são realizadas em e-mails enviados ou recebidos nos últimos 30 dias corridos, a menos que uma janela de pesquisa mais curta seja configurada durante a configuração inicial. Uma pesquisa de e-mail bem-sucedida é necessária antes que você possa excluir e-mails.

O exemplo a seguir mostra como iniciar uma pesquisa a partir de um incidente de segurança Now Platform. Um incidente de segurança é criado com base no e-mail original de um ataque de phishing suspeito no servidor Microsoft Exchange Online da sua organização. Para este exemplo, o critério de pesquisa é Remetente (De) mais Assunto, em que De é phisher@cbamyx.come o Assunto é login na sua conta.

Os resultados de pesquisas sobre assuntos são retornados quando a pesquisa encontra cadeias de caracteres de texto que contêm palavras-chave que correspondem aos critérios de pesquisa inseridos. Neste exemplo, o assunto é faça login na sua conta. Use o operador **E** para separar as condições de pesquisa De e Assunto para retornar resultados para todas as mensagens de e-mail que contêm esses critérios de pesquisa fornecidos. As etapas a seguir descrevem como configurar uma pesquisa que encontra somente e-mails que contêm texto de linha de assunto enviado por uma conta de phishing específica.

Tradução automática

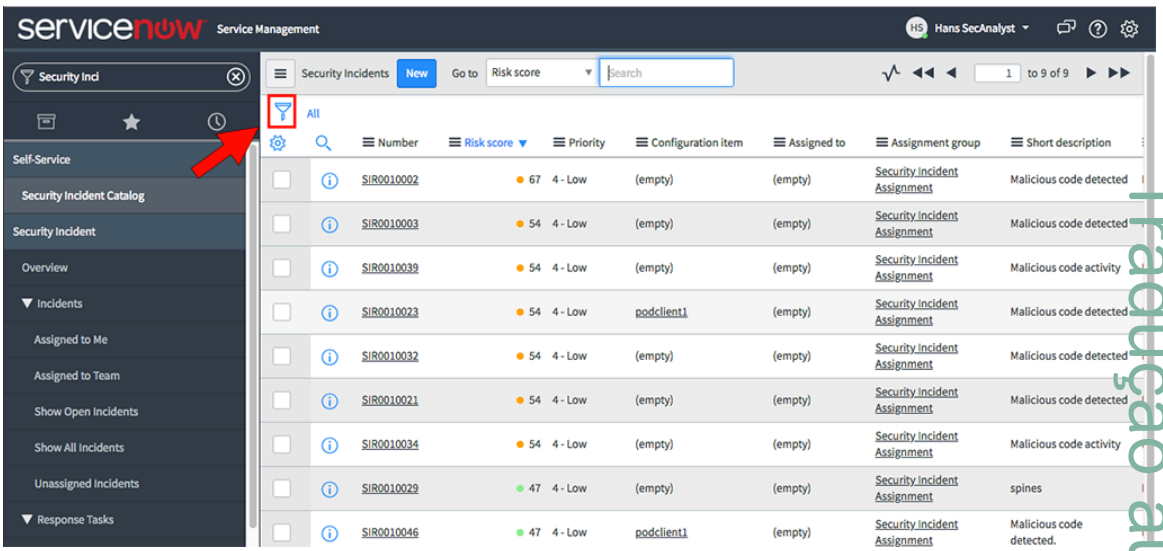
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar Todos os Incidentes** e localize o incidente de segurança com o qual você está trabalhando.
2. Como alternativa, siga estas etapas para definir e executar um filtro para que somente os incidentes de segurança criados por eventos de phishing sejam exibidos.

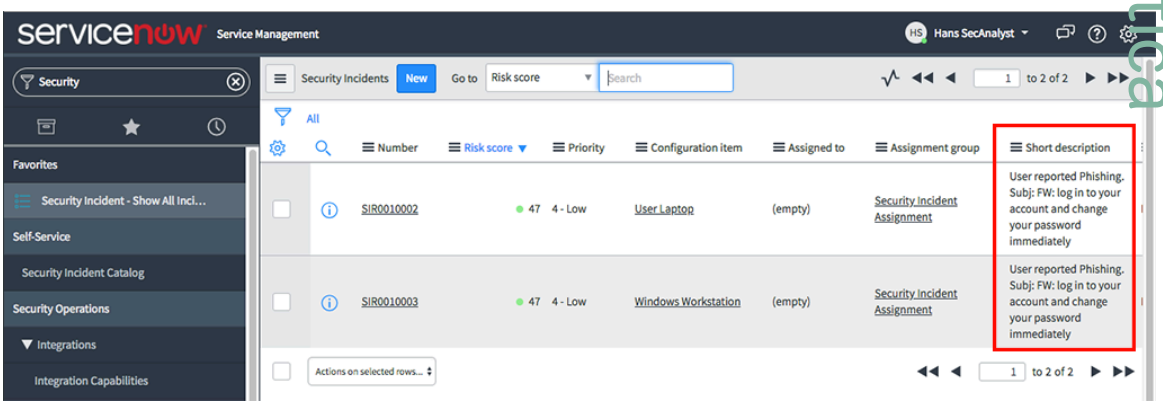
   a. Navegar até **Incidente de segurança** > **Mostrar Todos os Incidentes** para abrir a lista de Incidentes de segurança.

   b. No canto superior esquerdo da lista exibida, clique no ícone de filtro.



   c. Nos campos exibidos, selecione **Descrição resumida** > **contém** nas listas de seleção, insira **phishing relatado pelo usuário** e clique em **Executar**.

   Os incidentes de segurança relacionados ao phishing são exibidos.



   d. Use o texto na coluna Descrição resumida para ajudá-lo a localizar o incidente de segurança com o qual você está trabalhando.

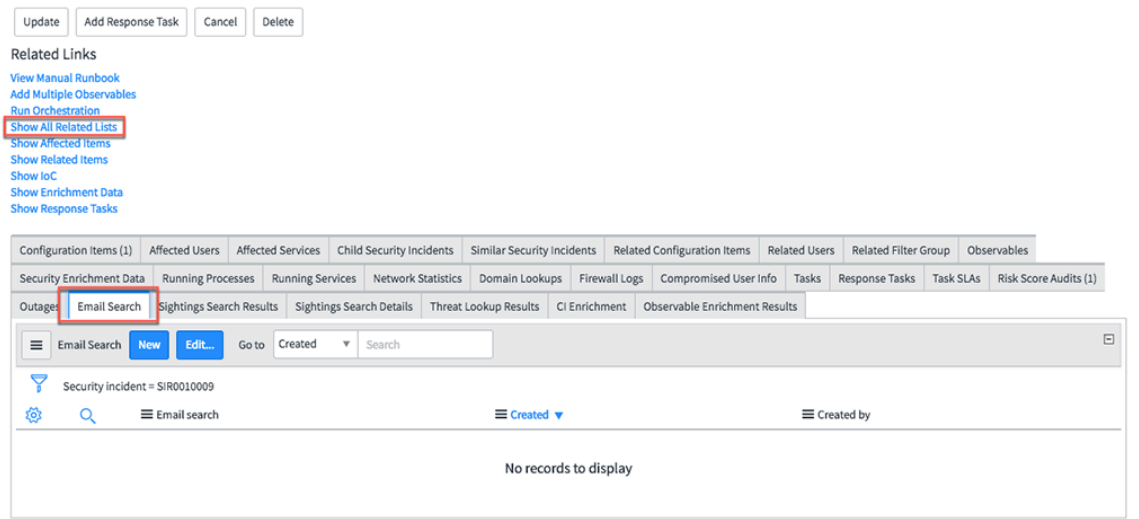
   e. Na coluna Número, clique em um incidente de segurança para abrir um registro.

3. Role até a parte inferior do registro de Incidente de segurança e clique na lista relacionada Pesquisa de e-mail.

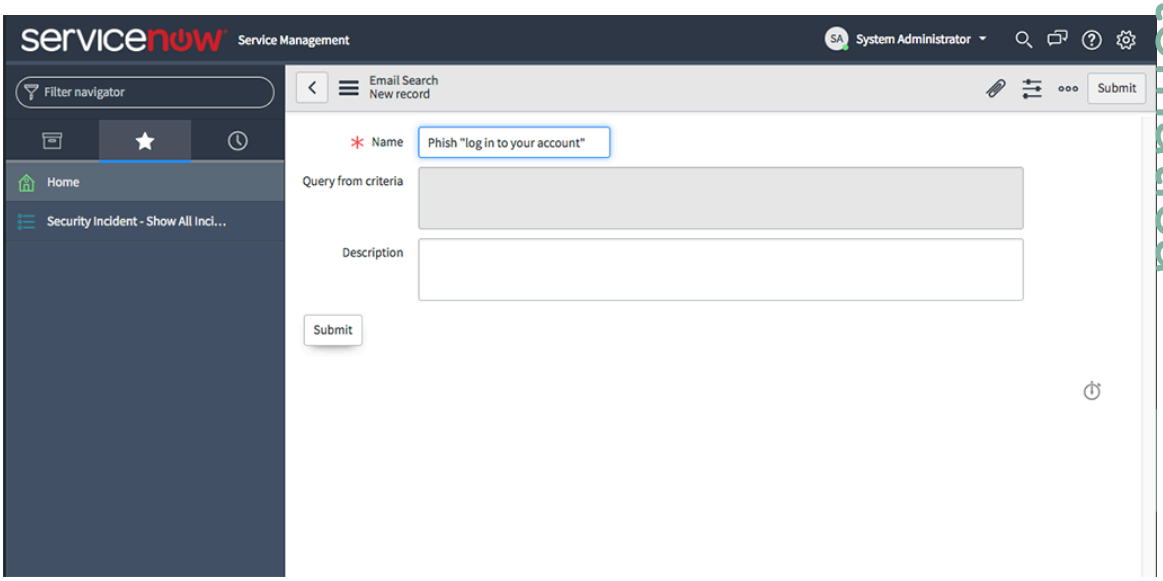
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se a lista relacionada Pesquisa de e-mail não for exibida, clique no link relacionado **Mostrar todas as listas** relacionadas para exibir essa lista relacionada.



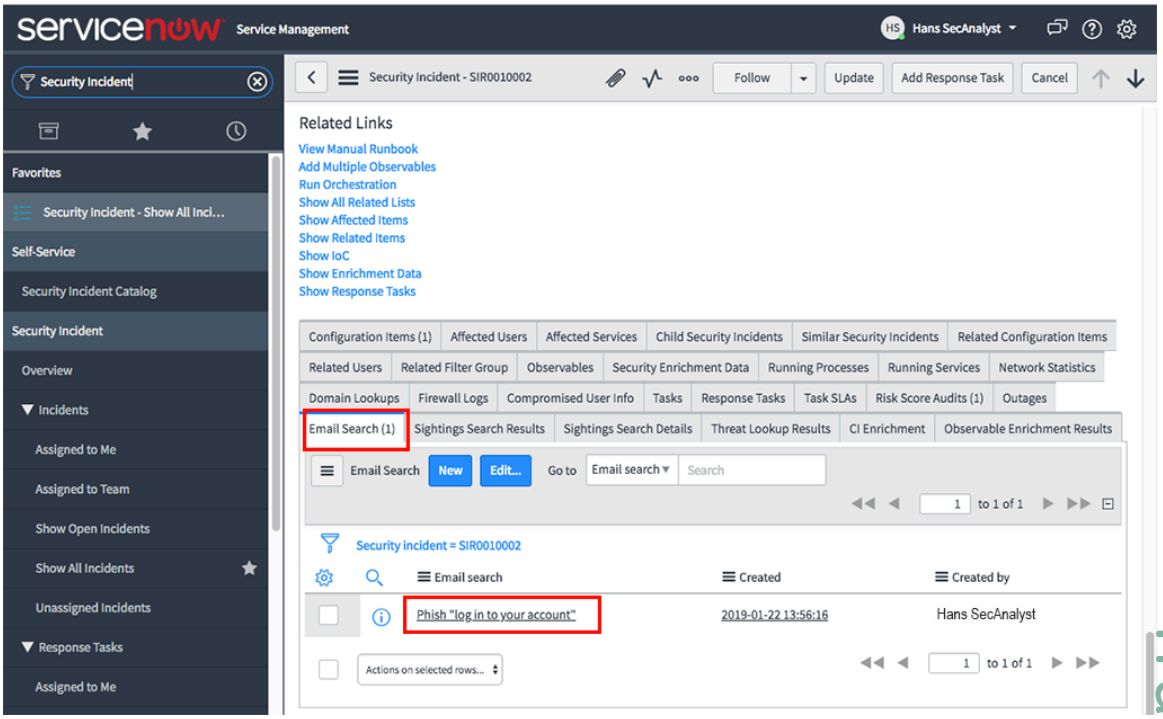
4. Na lista relacionada Pesquisa de e-mail, clique em **Novo** para criar um novo registro de pesquisa de e-mail. O formulário Pesquisa de e-mail é exibido. Se você determinar que deseja executar novamente esta consulta de pesquisa para o mesmo incidente relacionado a phishing com pequenas modificações, poderá usar este registro de consulta de pesquisa novamente. No entanto, é improvável que você use essa pesquisa para um incidente diferente relacionado ao phishing, porque as campanhas de phishing são dinâmicas e os campos do remetente e da mensagem mudam com frequência.
5. **Opcional:** Para editar um registro de consulta de pesquisa existente, clique em **Editar**.
6. No formulário Pesquisa de e-mail, preencha os campos.



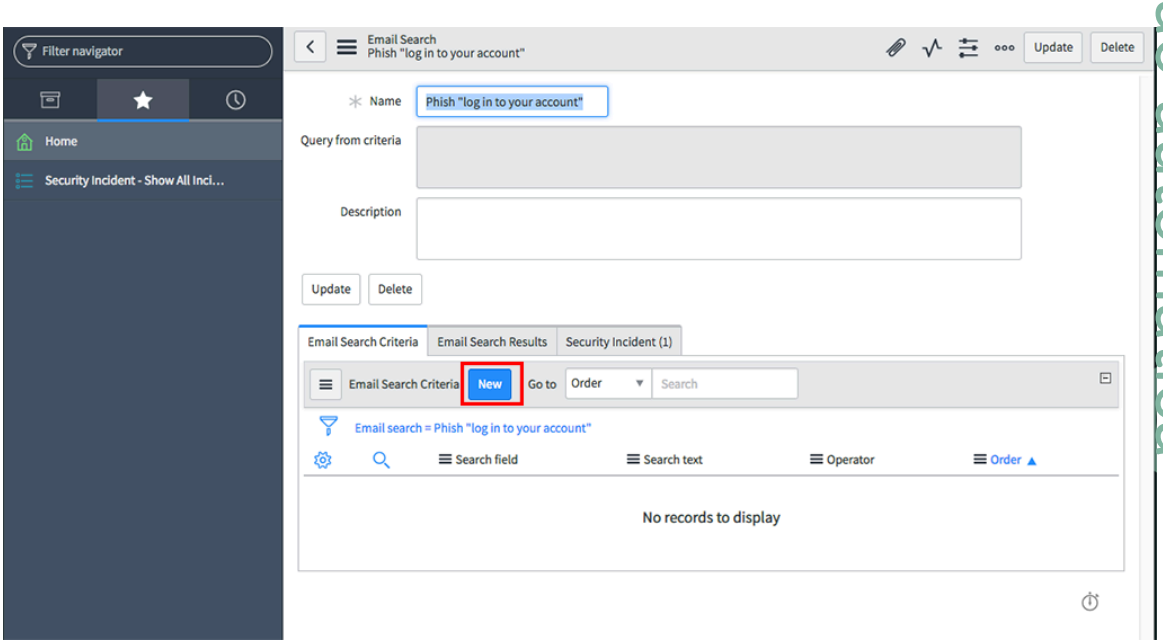
7. Clique em **Enviar**.
O incidente de segurança é exibido e o nome da pesquisa de e-mail é exibido na coluna Pesquisa de e-mail na lista relacionada Pesquisa de e-mail. Antes de usar esta nova consulta de pesquisa, os critérios de pesquisa devem ser definidos para o registro de pesquisa.
8. Para definir critérios de pesquisa, com a lista relacionada Pesquisa de e-mail selecionada, na coluna Pesquisa de e-mail, clique em **Phish "faça login na sua conta"**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. No registro de pesquisa de e-mail exibido, clique na lista relacionada Critérios de pesquisa de e-mail e clique em **Novo**.

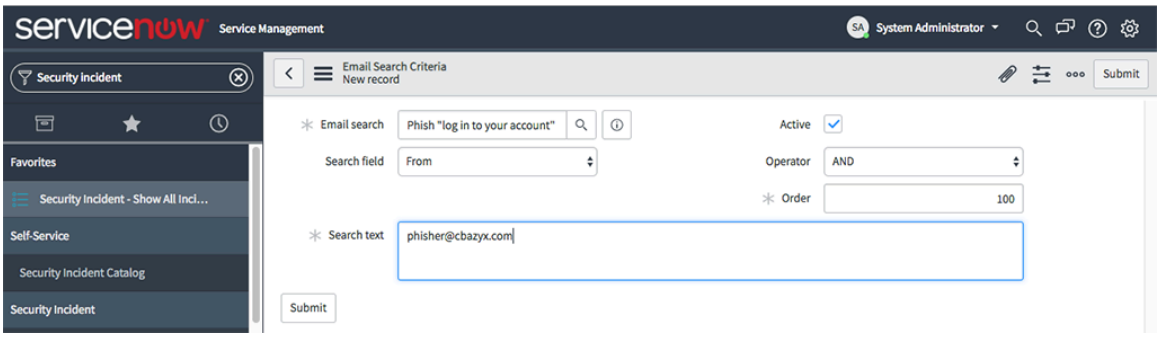


10. No formulário Critérios de pesquisa de e-mail, preencha os campos.

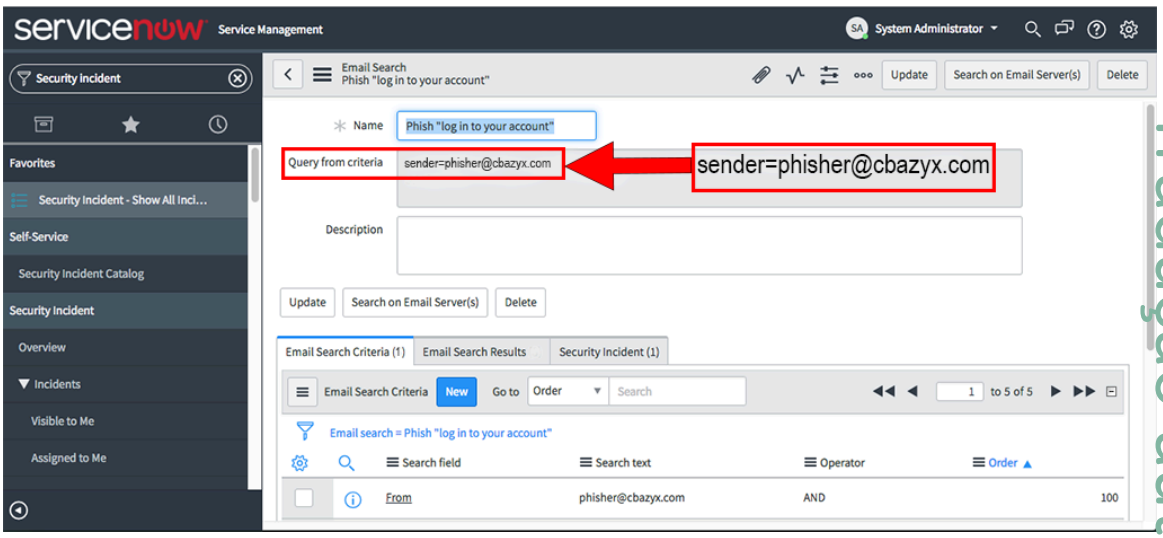
Um exemplo de formulário preenchido segue a tabela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

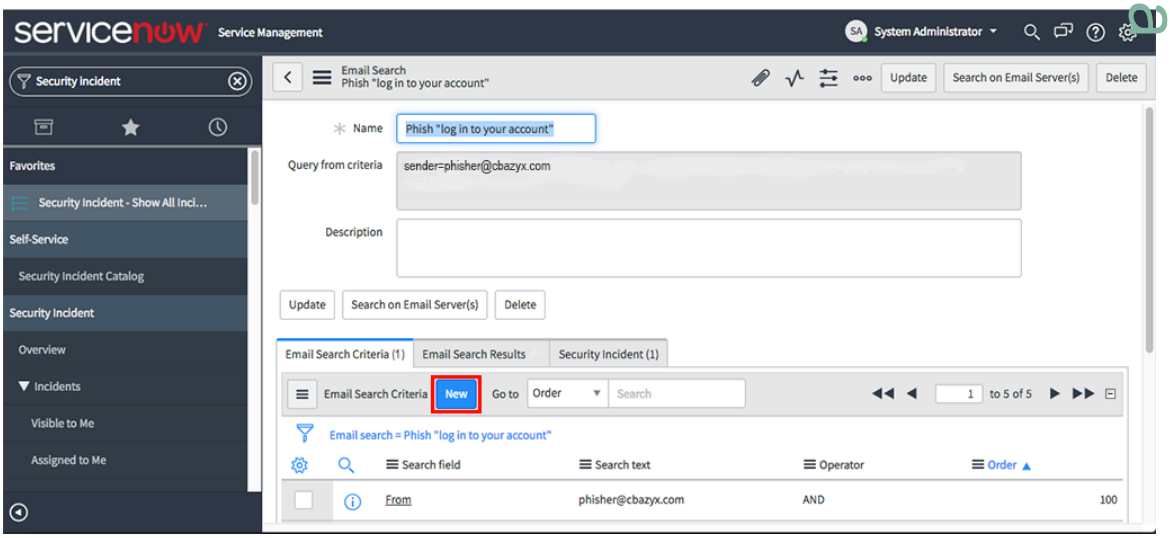


11. Clique em **Enviar**.
O registro de pesquisa de e-mail é exibido. No campo **Consultar de critérios**, os critérios de pesquisa que você adicionou para o Remetente (De) são exibidos.



12. Para atualizar esses critérios de pesquisa de e-mail com mais informações para que a consulta inclua a condição de assunto mais remetente desejada, siga as etapas para adicionar outra condição de pesquisa.

a. Na lista relacionada Critérios de pesquisa de e-mail, clique em **Novo**.



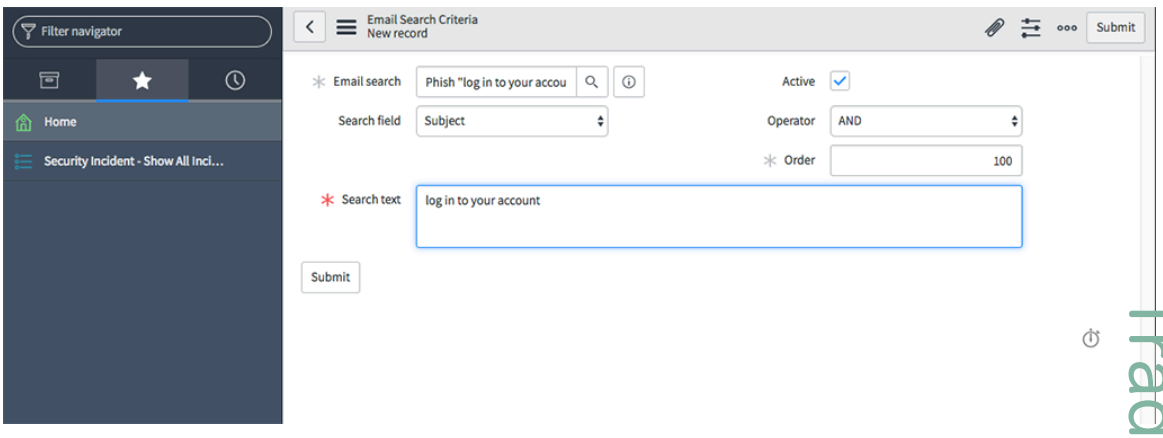
b. Na lista **Campo**de pesquisa do registro Critérios de pesquisa de e-mail exibido, selecione **Assunto**.

Tradução automática

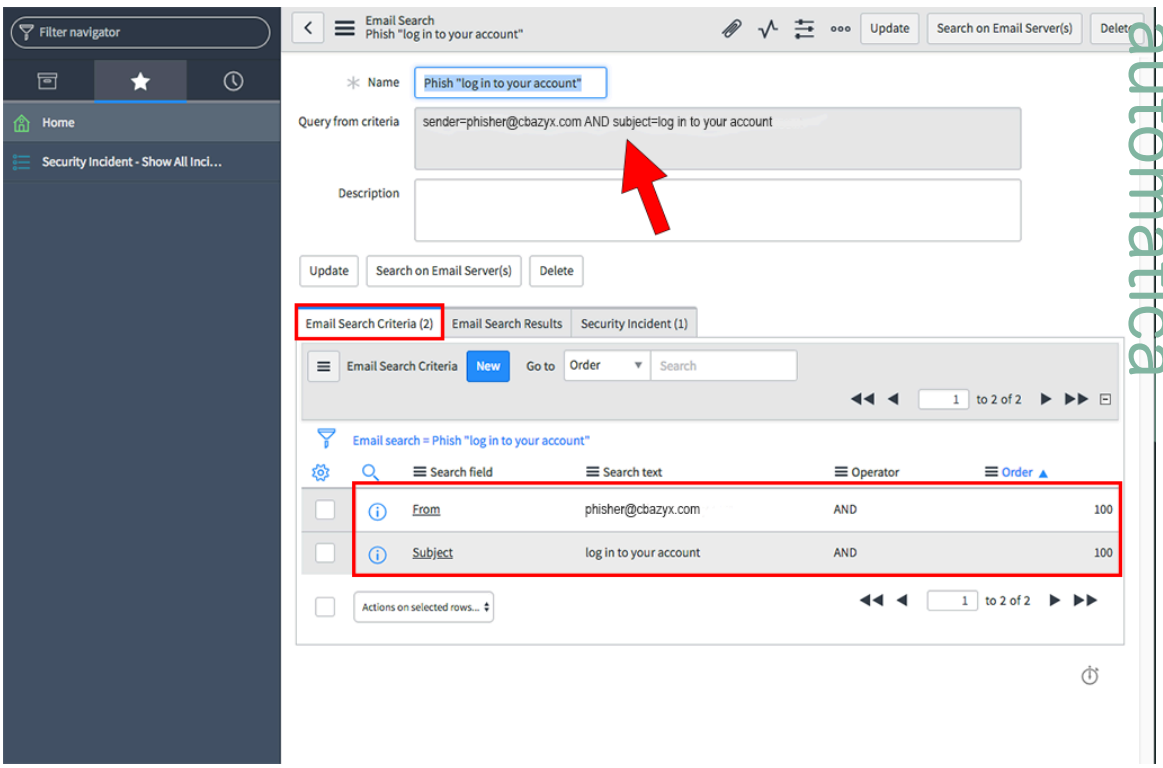
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Na lista Operador, selecione**E** ou **OU**.
Se você selecionar **OU**, a pesquisa retornará resultados se as palavras-chave na cadeia de caracteres de texto da linha de assunto forem correspondidas ou se a condição do endereço de e-mail for correspondida. **E** está selecionado para este exemplo para que a pesquisa retorne resultados somente para e-mails que contenham as palavras-chave da cadeia de caracteres do texto do assunto e que correspondam ao endereço de e-mail do remetente.

d. No campo **Texto de pesquisa**, insira o valor do texto da linha de assunto e `faça login na sua conta`.



e. Clique em **Enviar**.
A nova condição é exibida na lista relacionada Critérios de pesquisa de e-mail e as duas condições são exibidas no campo **Consultar de critérios** separados pelo operador **AND**.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

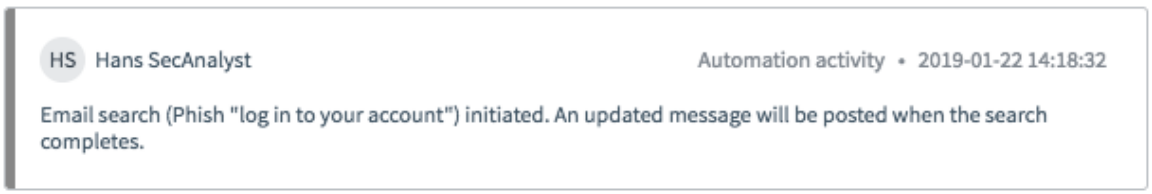
f. **Opcional:** Se você tiver mais de duas condições de pesquisa e selecionar **E** para separar cada condição, defina o valor do pedido para priorizá-las.

g. Continue a adicionar, modificar ou remover critérios de pesquisa conforme desejado e clique em **Atualizar** para salvar suas mudanças no registro.

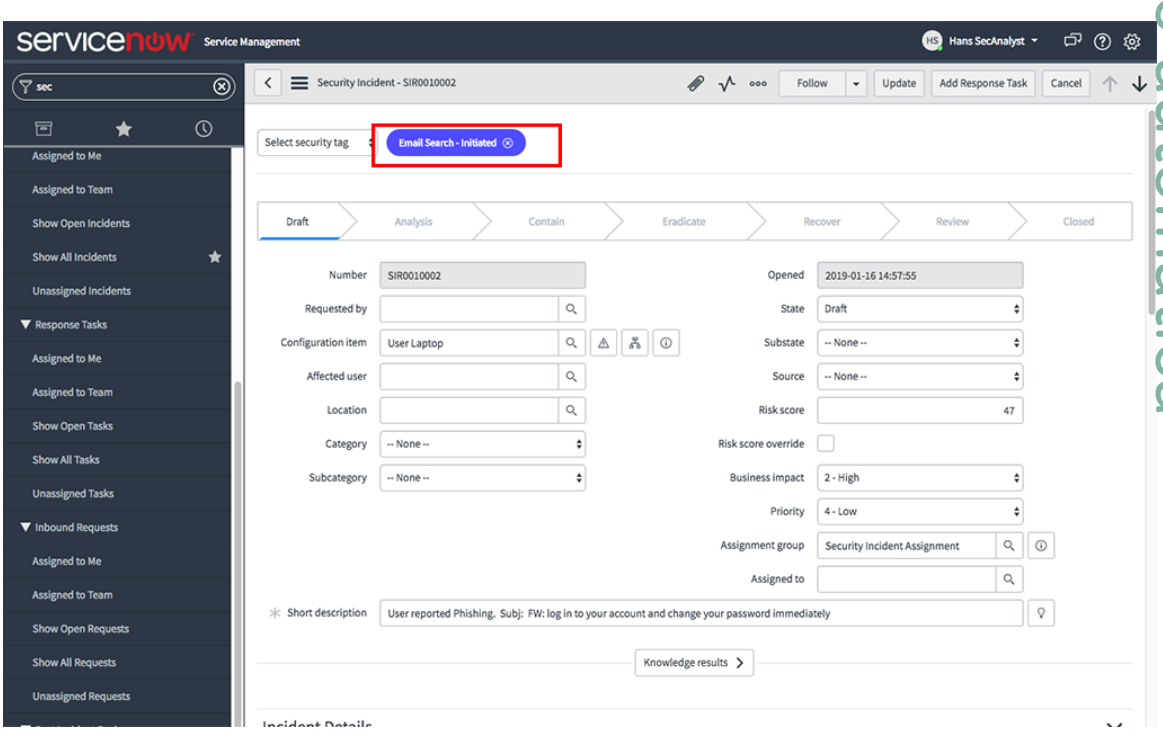
13. Escolha uma opção para continuar.

14. Para iniciar uma pesquisa de e-mail, no registro de pesquisa de e-mail, clique **em Pesquisar em servidores de e-mail**.
Uma mensagem é exibida indicando que a solicitação de pesquisa foi enviada.

No registro de Incidente de segurança, uma anotação de trabalho é exibida indicando que uma pesquisa foi iniciada.



Se a marcação estiver habilitada, na parte superior do registro de Incidente de segurança, o marcador de segurança Pesquisa de e-mail - Iniciada será exibido.



Depois que a pesquisa for concluída com sucesso, se as notificações por e-mail estiverem habilitadas, um e-mail será enviado para o endereço de e-mail do indivíduo que iniciou a pesquisa.

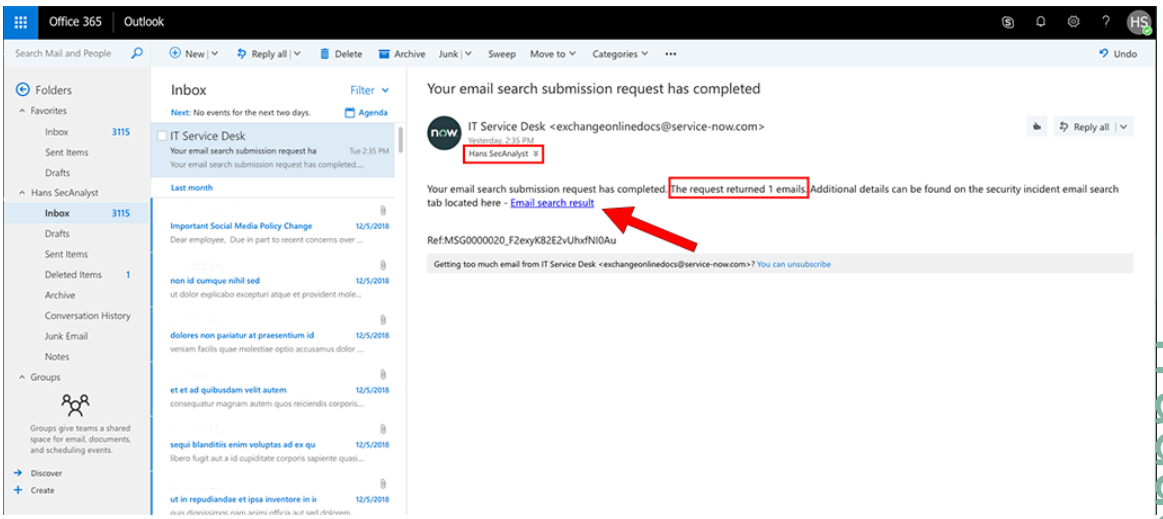
Neste exemplo, o usuário com a função sn_si.analyst, Hans SecAnalyst, enviou esta pesquisa. A imagem a seguir mostra que esta notificação é enviada para uma conta em

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Microsoft Exchange Online. No entanto, essas notificações podem ser enviadas para um serviço de e-mail diferente, conforme necessário.

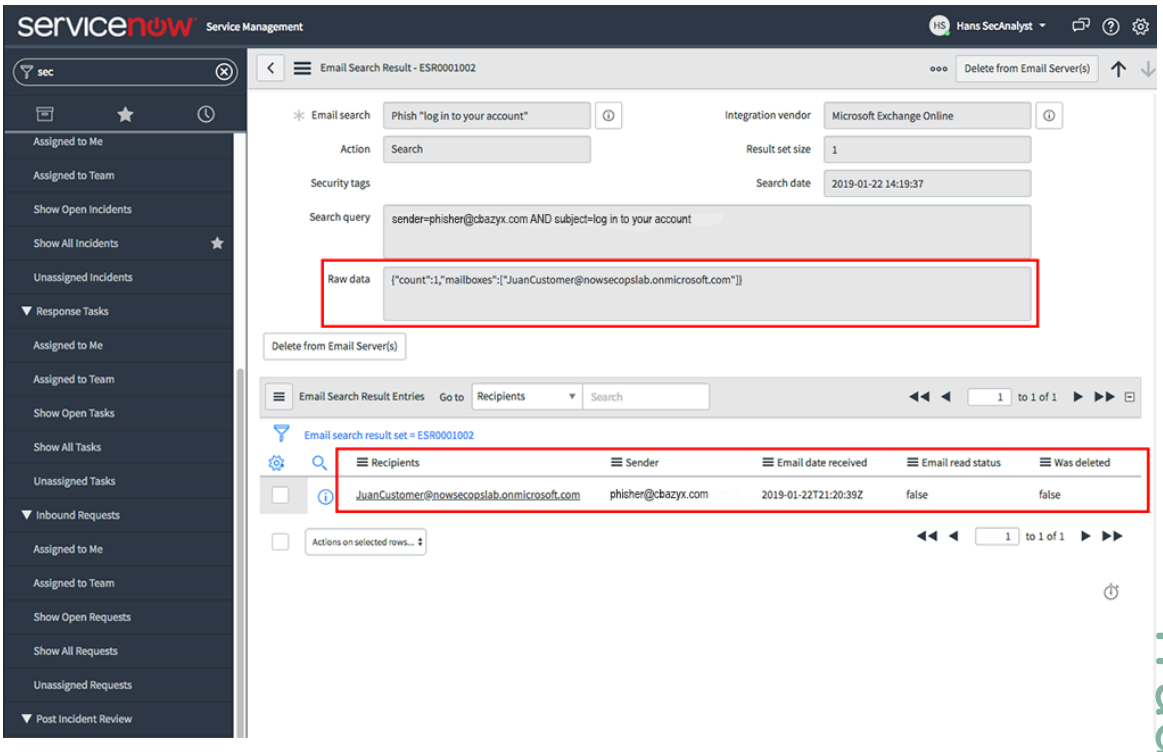
Esta notificação permite exibir todos os resultados correspondentes que exigem acompanhamento e exclusão. O exemplo a seguir mostra que há um e-mail que corresponde aos critérios de pesquisa. Um link de resultado de pesquisa de e-mail para o registro de resultado de pesquisa de e-mail na sua instância Now Platform também é fornecido. Se você quiser exibir o registro de pesquisa, clique neste link.



15. Nesse e-mail, para exibir os resultados da pesquisa, clique no link Resultado da pesquisa de e- **mail**.
O registro do resultado da pesquisa de e-mail é exibido. Neste registro, você pode verificar e revisar os dados a seguir.
    - No campo **Dados brutos**, a contagem de e-mail para o número de e-mails que corresponderam aos critérios de pesquisa {"count":1}e os endereços da caixa de correio onde os e-mails foram encontrados são exibidos ["JuanCustomer@nowsecopslab.onmicrosoft.com"].
    - Na coluna Destinatários, o destinatário é (JuanCustomer@nowsecopslab.onmicrosoft.com).
    - Na coluna Remetente, a origem do e-mail é exibida.
    - Na coluna Data de recebimento do e-mail, a data e a hora em que o e-mail foi recebido são exibidas para ajudá-lo a rastrear os cronogramas da campanha de phishing.
    - Na coluna Status de leitura do e-mail, o e-mail neste exemplo não foi lido (falso). Se um e-mail tiver sido lido, verdadeiro será exibido.
    - Na coluna Foi excluído, o e-mail neste exemplo não foi excluído. Se um e-mail tiver sido excluído, verdadeiro será exibido.

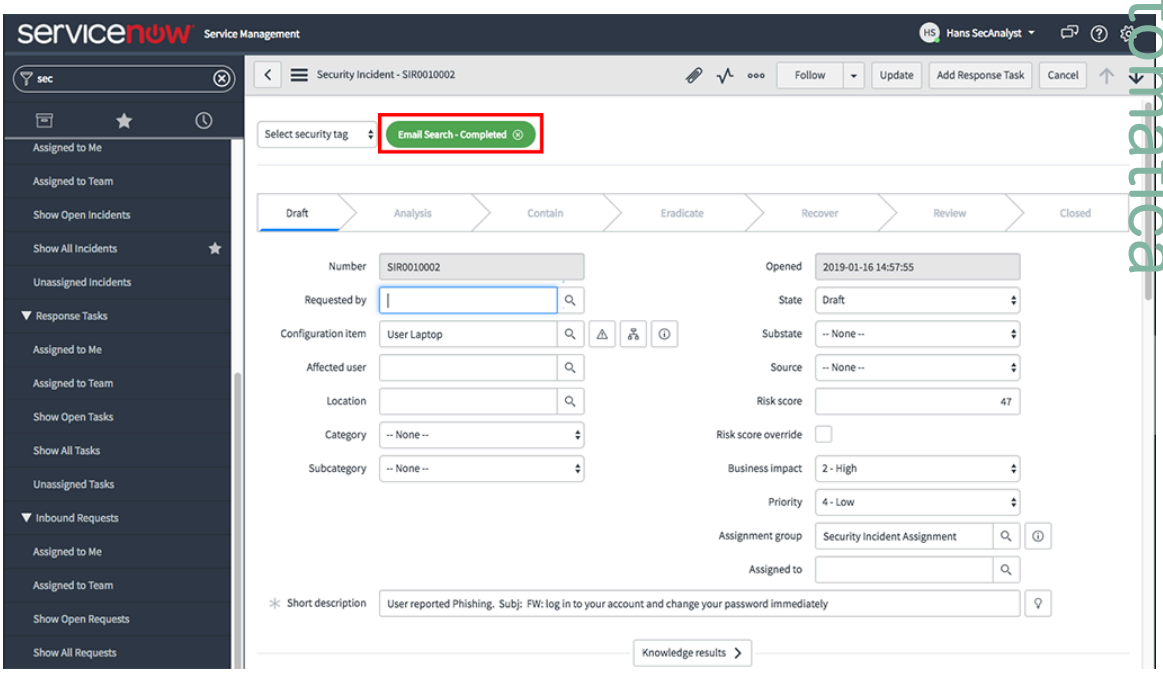
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



16. Como alternativa, para exibir os resultados da pesquisa do incidente de segurança, siga estas etapas.

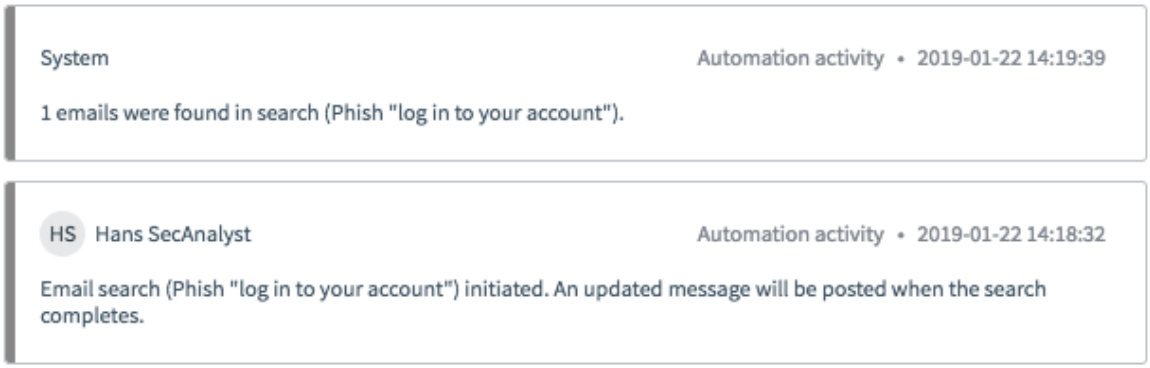
a. Navegar até **Incidente de segurança** > **Incidentes** e abra o incidente de segurança com o qual você está trabalhando.
Na parte superior do registro, quando a pesquisa é concluída com sucesso, o marcador de segurança Pesquisa de e-mail - Concluída substitui o marcador de segurança Pesquisa de e-mail - Iniciada.



As anotações de trabalho são exibidas informando que a pesquisa foi concluída com sucesso e que um e-mail correspondente foi encontrado.

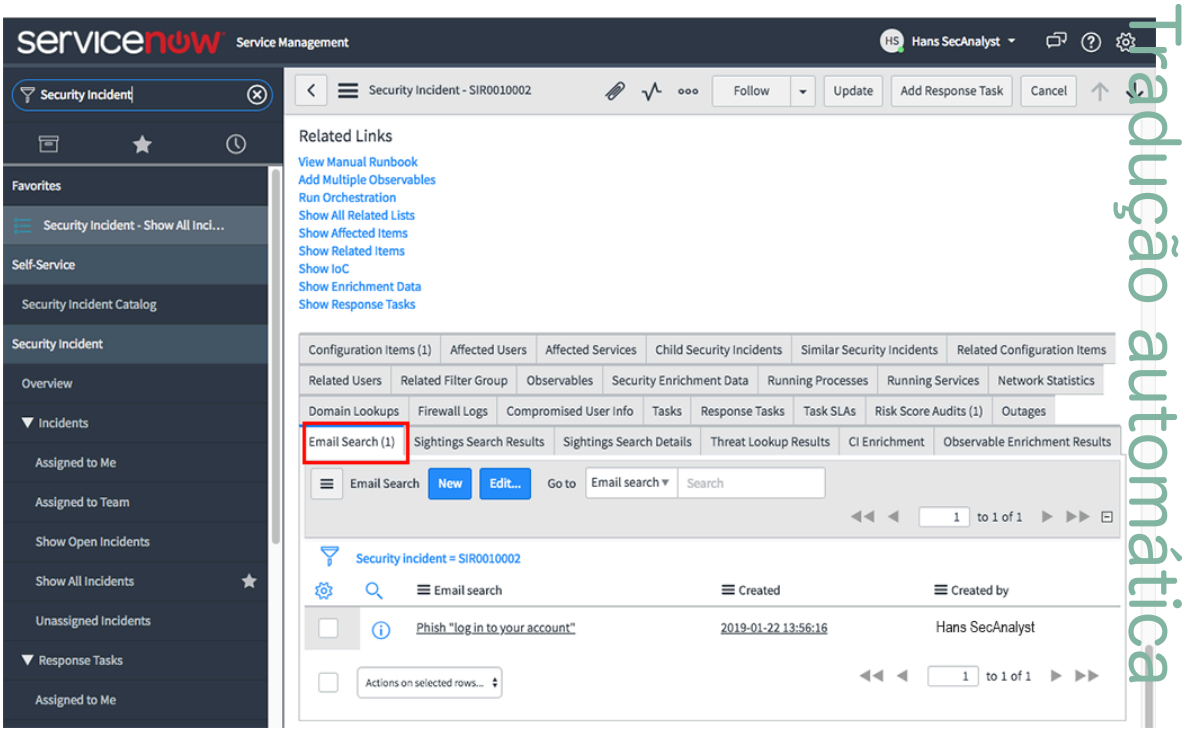
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



b. Role até a parte inferior do registro de Incidente de segurança e clique na lista relacionada Pesquisa de e-mail.

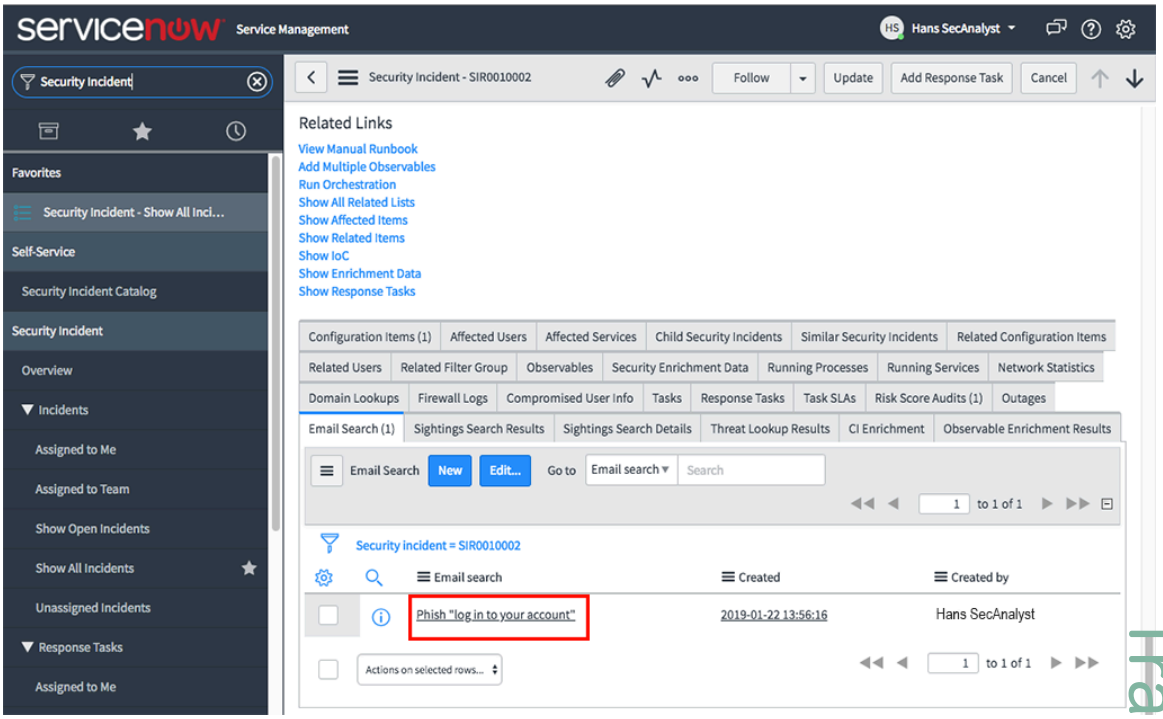
Se a lista relacionada Pesquisa de e-mail não for exibida, clique no link relacionado**Mostrar todas as listas** relacionadas para exibir essa lista relacionada.



Tradução automática

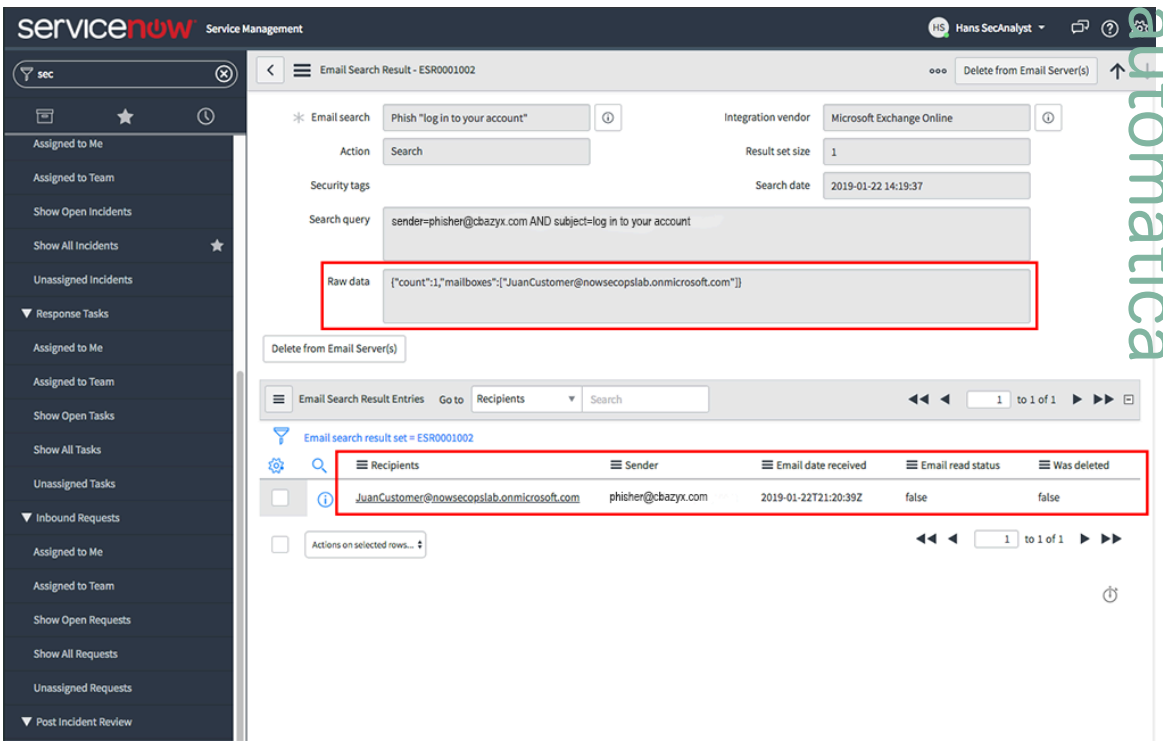
c. Com a lista relacionada Pesquisa de e-mail selecionada, na coluna Pesquisa de e-mail, clique no nome da sua pesquisa.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. No registro Pesquisa de e-mail, clique na lista relacionada Resultados da pesquisa de e-mail.

e. Na coluna Data da pesquisa, clique na data da pesquisa para exibir os dados.
O registro do resultado da pesquisa de e-mail é exibido.



Depois que uma pesquisa de e-mail for concluída com sucesso, avalie os resultados. Se você determinar que os e-mails precisam de correção, agora está pronto para excluir e-mails ou solicitar aprovação de exclusão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitar aprovação de exclusão para e-mails no serviço Microsoft Exchange Online

Depois que uma pesquisa de e-mail for concluída com sucesso e as mensagens correspondentes forem identificadas, você poderá excluir permanentemente todos os e-mails suspeitos do serviço online do Microsoft Exchange que estão relacionados ao incidente de segurança e à campanha de phishing.

Antes de Iniciar

Função necessária: sn_si.analyst

O sistema executa exclusões nos resultados de pesquisa bem-sucedidos mais recentes.

Por Que e Quando Desempenhar Esta Tarefa

Se as aprovações e notificações por e-mail estiverem habilitadas, envie uma solicitação para excluir e-mails para um grupo de aprovação antes da remoção do e-mail.

Os resultados da pesquisa de e-mail são exibidos com todas as mensagens recebidas. Para garantir que os e-mails de phishing sejam excluídos com sucesso, os resultados da exclusão são publicados nas anotações de trabalho do incidente de segurança associado. Se a marcação estiver habilitada, um marcador de segurança também será exibido no incidente de segurança relacionado. Se o e-mail não for excluído com sucesso, você também será notificado nas anotações de trabalho.

Dependendo das políticas organizacionais, pode ser necessário solicitar aprovação antes de excluir e-mails de phishing. O processo de aprovação de exclusão requer informações sobre o número de e-mails a serem excluídos e, potencialmente, acesso a outros detalhes da mensagem. Para processar a solicitação de exclusão, em uma notificação por e-mail, um aprovador recebe a contagem de mensagens de e-mail correspondente, o link do incidente de segurança para acessar os detalhes completos da mensagem e os links de aprovação ou rejeição. Os links neste e-mail permitem que um aprovador aceite ou rejeite a solicitação de exclusão da notificação por e-mail. Também está disponível uma trilha de auditoria completa com um carimbo de data/hora que rastreia quando o status de aprovação foi alterado nas anotações de trabalho. Se um grupo de aprovação for atribuído, um usuário do grupo poderá processar a solicitação para o grupo inteiro. Cada membro do grupo de aprovação recebe uma notificação por e-mail da solicitação.

Como um usuário com a função sn_si.analyst, se você determinar que os e-mails precisam de correção, siga as etapas necessárias para excluir e-mails. Se as aprovações estiverem habilitadas, solicite aprovação para excluir e-mails do serviço Microsoft Exchange Online.

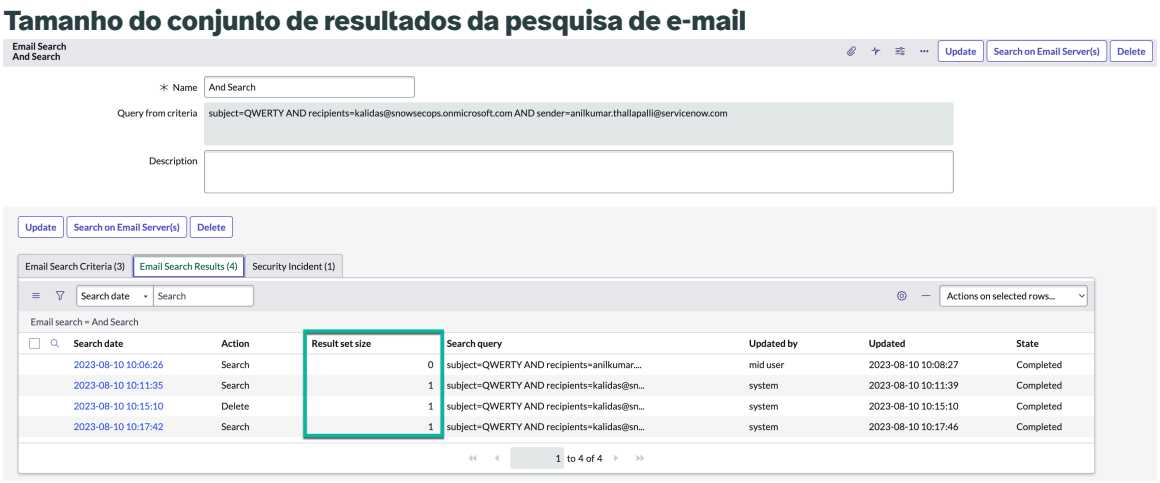
Procedimento

1. Navegar até **Todos** > **Incidente de segurança > Mostrar todos os incidentes**.
2. Clique na lista relacionada **Pesquisa de e-mail**.
3. Com a lista relacionada Pesquisa de e-mail selecionada, na coluna Pesquisa de e-mail, clique no nome da sua pesquisa.
   Os resultados da pesquisa são exibidos na lista relacionada Resultados da pesquisa de e-mail.

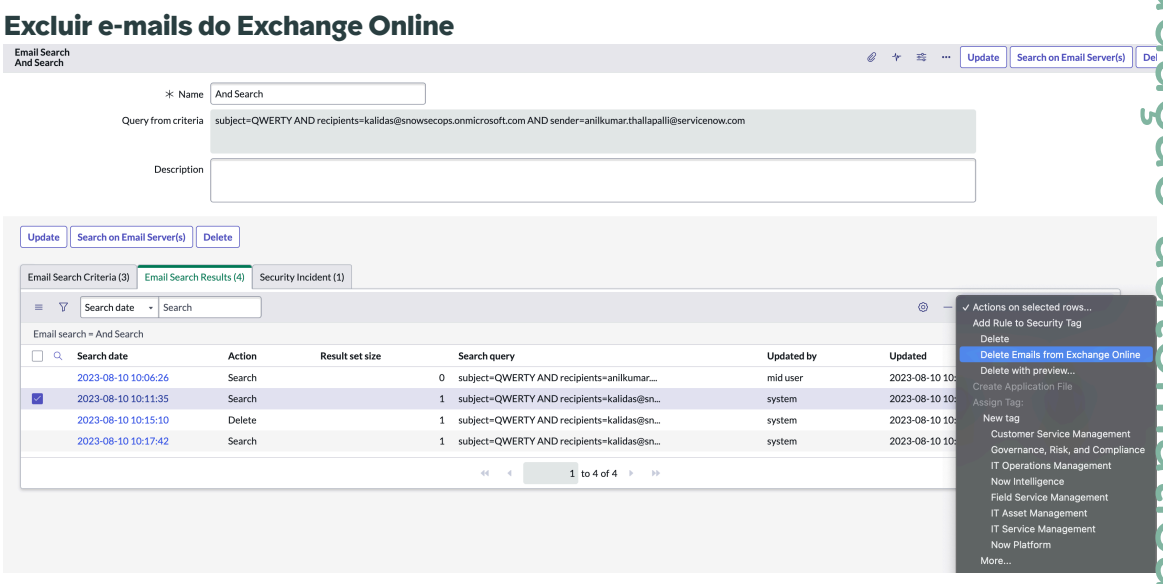
   Para este exemplo, esta pesquisa encontrou e-mails que correspondem aos seus critérios de pesquisa. Há duas ações de pesquisa listadas no registro. Uma pesquisa não tem correspondências (0) e a outra pesquisa tem um e-mail correspondente (1).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Para excluir itens de e-mail associados a uma pesquisa, à esquerda da coluna Data de pesquisa, marque a caixa de seleção de um conjunto de resultados de pesquisa.
   Você pode selecionar um único conjunto de resultados ou vários conjuntos de resultados na lista.
5. Selecione os conjuntos de resultados que você deseja excluir.



6. Na parte inferior da lista relacionada Resultados da pesquisa de e-mail, na lista Ações nas linhas selecionadas, selecione **Excluir e-mails do Exchange Online** para excluir todos os itens de e-mail associados a um ou mais conjuntos de resultados do servidor do Exchange Online.
   Se um conjunto de resultados contiver mais de um e-mail, você não precisará abrir o registro de resultado da pesquisa de e-mail e selecionar e-mails individuais para excluí-los. Todos os itens de e-mail com um status falso na coluna Foi excluído no registro Resultado da pesquisa de e-mail serão excluídos depois que você selecionar **Excluir e-mails do Exchange Online**.

   Se um item de e-mail em um conjunto de resultados já tiver sido excluído, o status na coluna Foi excluído no registro de resultado da pesquisa de e-mail será verdadeiro. Esses itens não serão excluídos novamente.

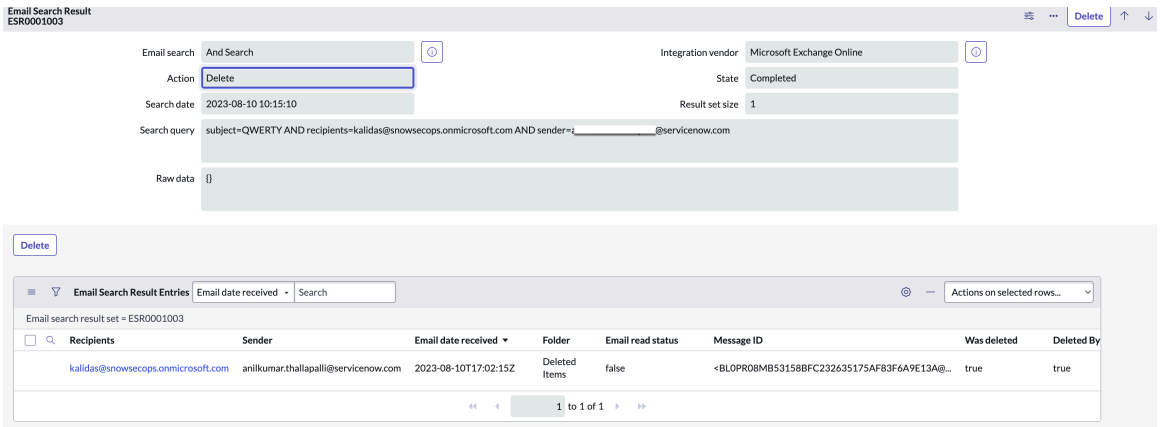
   Se a opção de aprovação estiver desabilitada durante a etapa de configuração, depois de selecionar **Excluir e-mails do Exchange Online**, os e-mails associados ao conjunto de resultados serão excluídos. O próprio conjunto de resultados não é excluído. No entanto, o status de todos os itens de e-mail excluídos do conjunto de resultados é atualizado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para verdadeiro na coluna Foi excluído do registro de resultado da pesquisa de e-mail. Para obter mais informações sobre o recurso de aprovação, consulte Configure a integração Microsoft Exchange Online com sua instância Now Platform.

Detalhes de exclusão de e-mail



Esses e-mails são excluídos do locatário Microsoft Exchange Online em que você executou as pesquisas. Uma anotação de trabalho será exibida se os e-mails forem excluídos com sucesso.

No registro de incidente de segurança, o marcador de segurança Exclusão de e-mail - Concluída é exibido.

Exclusão de e-mail - Marcador de segurança concluído

Se as aprovações estiverem desabilitadas para solicitações de exclusão, você excluiu e-mails do locatário Microsoft Exchange Online.

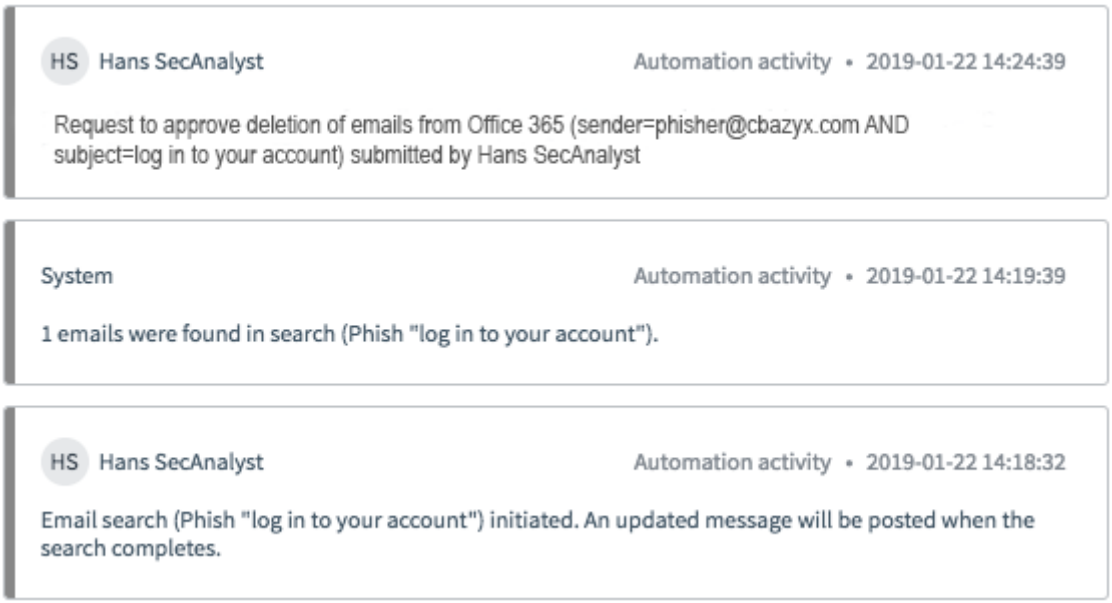
Se as aprovações estiverem habilitadas para solicitações de exclusão durante a etapa de configuração, depois de selecionar **Excluir e-mails do Exchange Online**, uma notificação por e-mail será enviada a cada membro do grupo de aprovação selecionado durante a etapa de configuração.

Se a marcação estiver habilitada durante a etapa de configuração, o marcador de segurança Exclusão de e-mail - Iniciada será exibido no registro do incidente de segurança relacionado. Para obter mais informações sobre marcação, consulte Configure a integração Microsoft Exchange Online com sua instância Now Platform.

As anotações de trabalho são exibidas de que uma solicitação para excluir e-mails é enviada pelo usuário com a função sn_si.analyst (Hans SecAnalyst).

Tradução automática

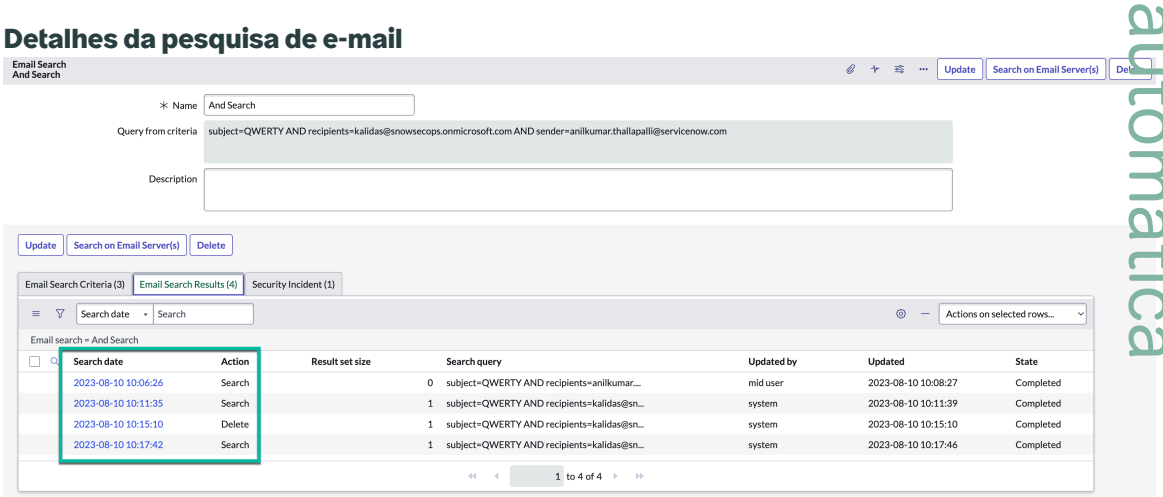
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se as aprovações estiverem habilitadas, a próxima etapa será processar a solicitação de exclusão.

7. Como alternativa, se você quiser exibir os detalhes e itens de e-mail individuais de um registro de pesquisa antes de excluí-lo ou enviar uma solicitação de exclusão, siga estas etapas.

a. Com a lista relacionada Resultados da pesquisa de e-mail selecionada, na coluna Data da pesquisa, clique na data de uma pesquisa que você deseja revisar.



As seguintes informações sobre os e-mails são exibidas:

- Destinatários
- Remetente
- Data de recebimento do e-mail
- Status de leitura do e-mail (verdadeiro ou falso)
- Foi excluído (verdadeiro ou falso)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Excluído por integração (verdadeiro ou falso)

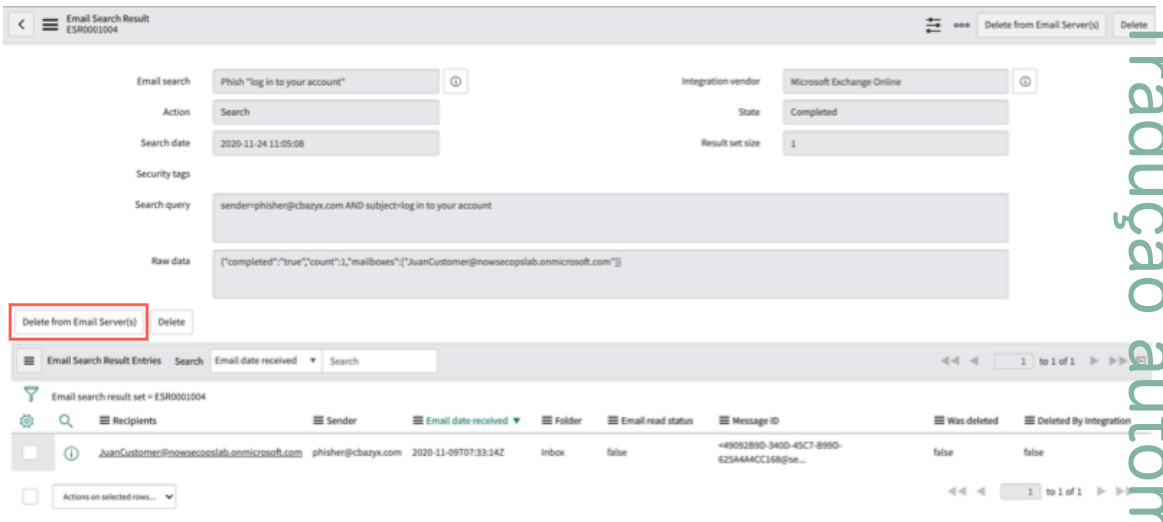
Nota:

O valor é definido como verdadeiro quando o e-mail é excluído quando o analista inicia a opção Excluir do(s) servidor(es) de e-mail.

As anotações de trabalho são atualizadas com o número total de registros excluídos, que inclui os registros excluídos pela integração e pelo usuário.

b. Depois de revisar os dados, para excluir todos os e-mails ou enviar uma solicitação para excluir todos os e-mails, clique em **Excluir do(s) servidor(es) de e-mail**.

Conforme descrito no exemplo anterior, se houver mais de um e-mail listado no registro do resultado da pesquisa, você não precisará selecionar os e-mails individuais para removê-los. A solicitação de exclusão remove todos os e-mails associados à pesquisa quando falso é exibido na coluna Foi excluído dos resultados da pesquisa mais recentes.



Se as aprovações estiverem habilitadas, você enviou com sucesso uma solicitação para excluir e-mails. Os marcadores de segurança e as anotações de trabalho são exibidos no registro de incidente de segurança relacionado, conforme descrito no exemplo anterior. Como aprovador, a próxima etapa é processar a solicitação de exclusão.

Aprovar solicitações de exclusão de e-mail para a integração Microsoft Exchange Online

Se a opção de aprovação estiver habilitada na sua instância Now Platform, as solicitações para excluir e-mails serão enviadas para cada membro do grupo de aprovação por e-mail. Você seleciona o grupo de aprovação durante a etapa de configuração. As aprovações fornecem à sua organização um nível adicional de controle sobre a exclusão de e-mails.

Antes de Iniciar

Verifique se a opção **Aprovações** está selecionada na guia Configurações adicionais do formulário Configurações de pesquisa e exclusão de e-mails do Exchange Online.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verifique se você habilitou as opções **Envio**de e- **mail habilitado e Recebimento de e-mail habilitado** em sua instância Now Platform para solicitações de aprovação. Para obter mais informações, consulte Configure sua instância Now Platform para a integração Microsoft Exchange Online.

Quando o usuário com a função sn_si.analyst envia solicitações de exclusão de e-mail, por padrão, essas solicitações são enviadas por e-mail para o sn_si.admin. Se você tiver criado um grupo de aprovação, cada membro do grupo receberá uma notificação. Os aprovadores podem processar solicitações de exclusão de e-mail diretamente da notificação por e-mail. Como alternativa, as solicitações podem ser processadas a partir dos registros de resultado da pesquisa de e-mail em Now Platform instâncias. Este tópico mostra os dois métodos de aprovação.

As informações a seguir descrevem a solicitação na notificação por e-mail:

Número de registro do resultado da pesquisa de e-mail

Número exclusivo atribuído ao registro de pesquisa pelo Now Platform como parte da trilha de auditoria.

Nome do analista que enviou a solicitação

Nome da pessoa que enviou a solicitação como parte da trilha de auditoria.

Link para o incidente de segurança

Um link para o incidente de segurança relacionado ao evento de phishing. Exiba o incidente de segurança com as anotações de trabalho, pesquisas de e-mail e resultados de pesquisa de e-mail diretamente do e-mail.

Aprovar ou rejeitar links

Links para aprovar ou rejeitar a solicitação da notificação por e-mail. Depois de clicar em qualquer link, o sistema inicia automaticamente o fluxo de trabalho relacionado e uma anotação de trabalho é publicada no registro do incidente de segurança.

Função necessária: sn_si.admin ou todos os membros de um grupo de aprovação atribuído.

Procedimento

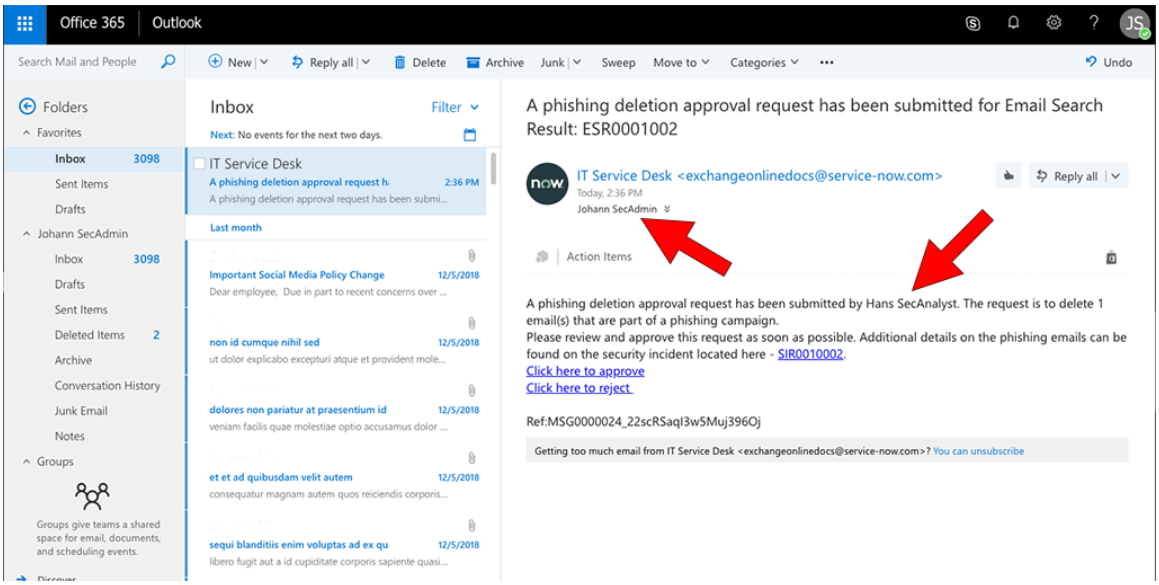
1. Para processar a solicitação de exclusão da notificação por e-mail, siga estas etapas.

   a. Como aprovador, localize o e-mail de notificação na conta de e-mail que você configurou em sua conta de usuário Now Platform.

      Neste exemplo, o usuário com a função sn_si.analyst (Hans SecAnalyst) envia uma solicitação para excluir um e-mail. Joan SecAdmin é um membro do grupo de aprovação.

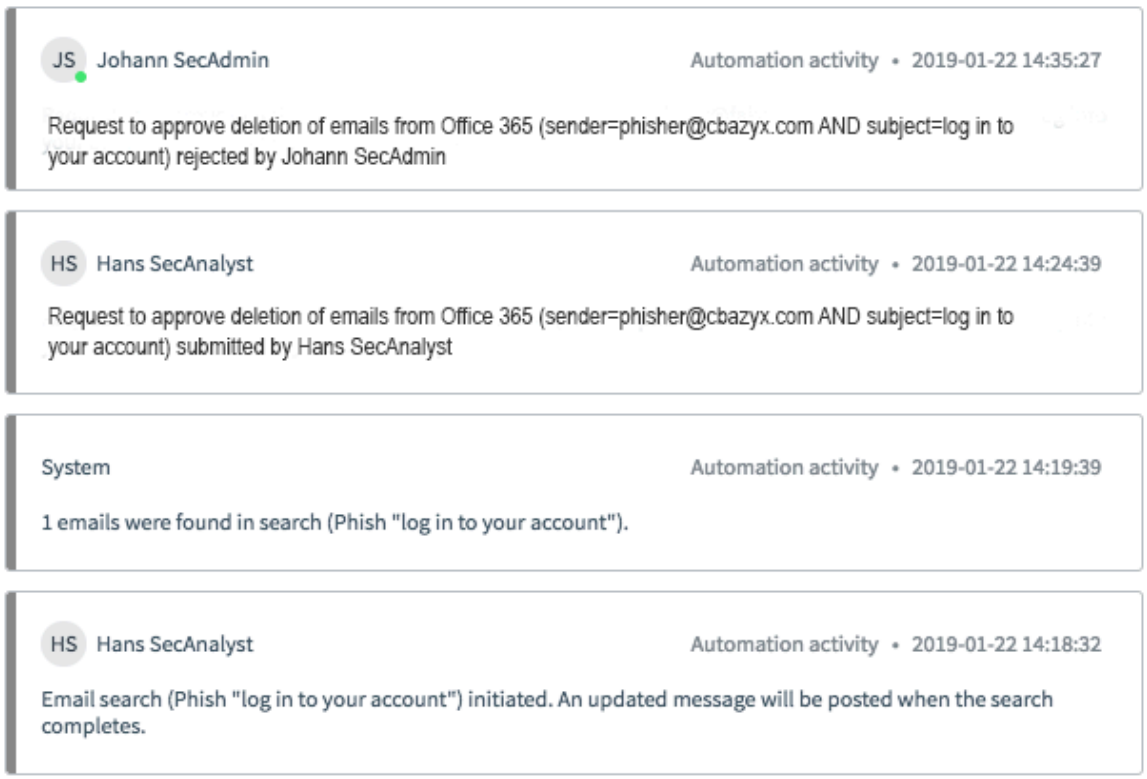
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



b. Na notificação por e-mail, escolha uma opção para continuar.

A imagem a seguir mostra um exemplo da trilha de auditoria criada pelas anotações de trabalho no registro de incidente de segurança relacionado para este exemplo. Quando a solicitação é rejeitada pela notificação por e-mail por um aprovador, uma anotação de trabalho é publicada com pela pessoa que rejeitou a solicitação. O SecAdmin de Joan rejeita esta solicitação.



Na instância Now Platform da pessoa que rejeitou a solicitação (Johann SecAdmin), em **Autoatendimento > Minhas aprovações**, Rejeitado será exibido na coluna Estado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

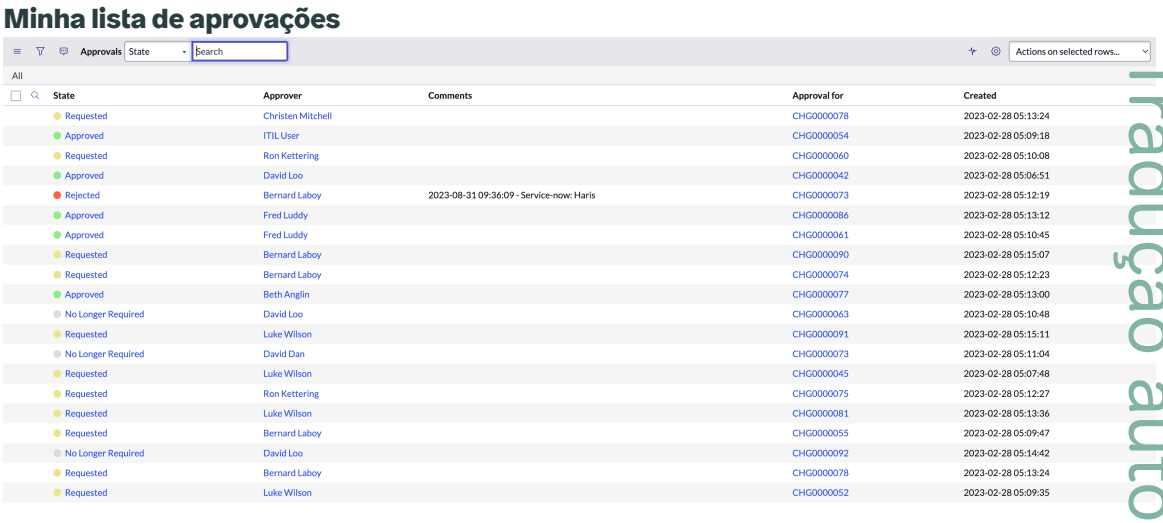
Depois que uma solicitação é rejeitada por qualquer membro do grupo de aprovação, como o usuário com a função sn_si.analyst, você deve enviar uma nova solicitação para excluir esses e-mails se determinar que eles devem ser excluídos.

Para este exemplo, depois que a solicitação é rejeitada, o usuário com a função sn_si.analyst envia uma nova solicitação.

Outro membro do grupo de aprovação, John Approver, recebe um e-mail semelhante ao mostrado no exemplo anterior. O aprovador John também pode processar esta solicitação.

2. Como alternativa, os aprovadores podem navegar até **Autoatendimento > Minhas aprovações** em suas instâncias Now Platform para exibir e processar solicitações de exclusão.
Para processar uma solicitação de **Minhas aprovações**, siga estas etapas.

   a. Navegar até **Autoatendimento > Minhas aprovações**.

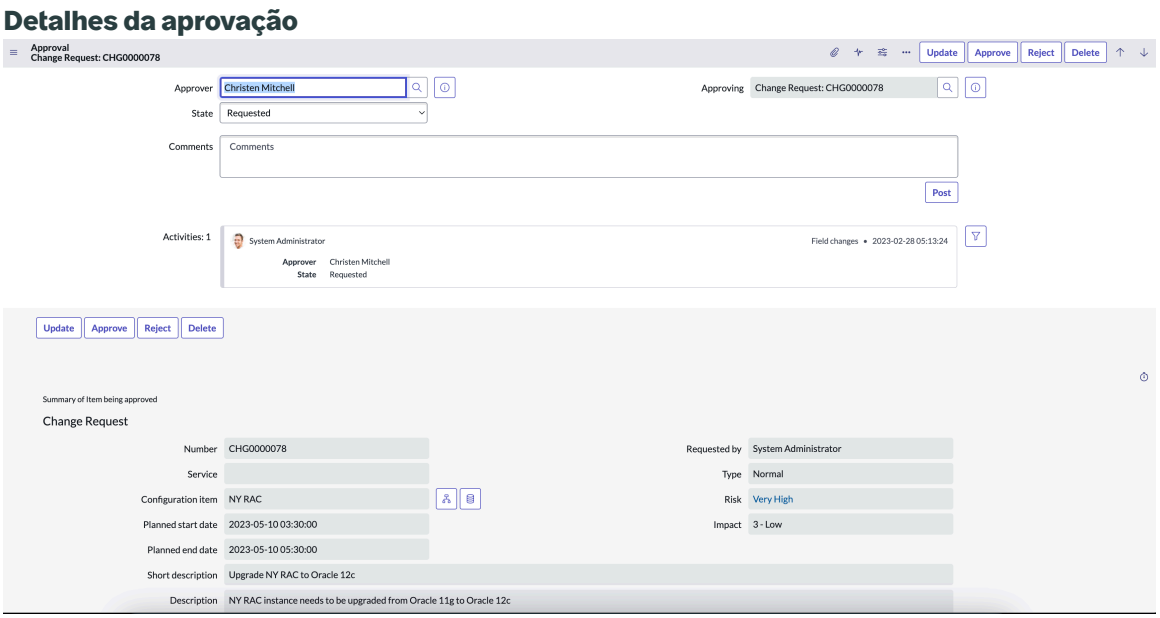


   b. Na coluna Estado, clique no item solicitado.

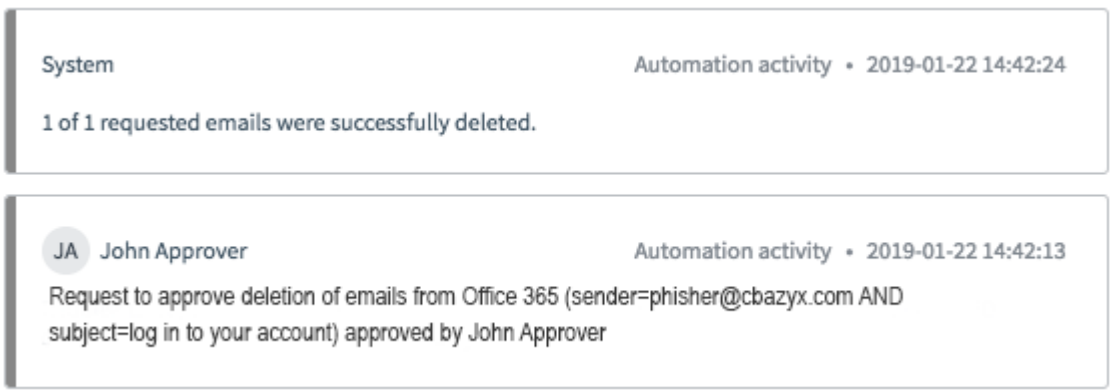
      No registro de aprovação exibido, os dados sobre a pesquisa, a solicitação de pesquisa e os resultados da pesquisa são listados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Nesse registro, clique em **Aprovar** para aprovar a solicitação.
Depois que a solicitação é aprovada, o sistema inicia o fluxo de trabalho de exclusão para remover os e-mails. A imagem a seguir mostra um exemplo da trilha de auditoria criada pelas anotações de trabalho no registro de incidente de segurança relacionado para este exemplo. Depois que esta solicitação de exclusão for enviada novamente, ela será aprovada. Independentemente de qual método seja usado para aprovar uma solicitação, o número de e-mails excluídos com sucesso é publicado em uma anotação de trabalho.



Depois que os e-mails forem excluídos com sucesso, no registro de incidente de segurança relacionado, se a marcação estiver habilitada, o marcador Exclusão de e-mail - Concluído substituirá o marcador Exclusão de e-mail - Iniciado.

Recebido(a) **Autoatendimento > Minhas aprovações** para o aprovador (Aprovador John), o estado muda de Solicitado para Aprovado.

Recebido(a) **Autoatendimento > Minhas aprovações** para outros membros do grupo de aprovação, por exemplo, Joan SecAdmin, o estado muda para Não é mais necessário depois que a solicitação é aprovada.

3. Como alternativa, para confirmar que os e-mails foram excluídos no registro de resultado da pesquisa de e-mail no registro de incidente de segurança relacionado, siga estas etapas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

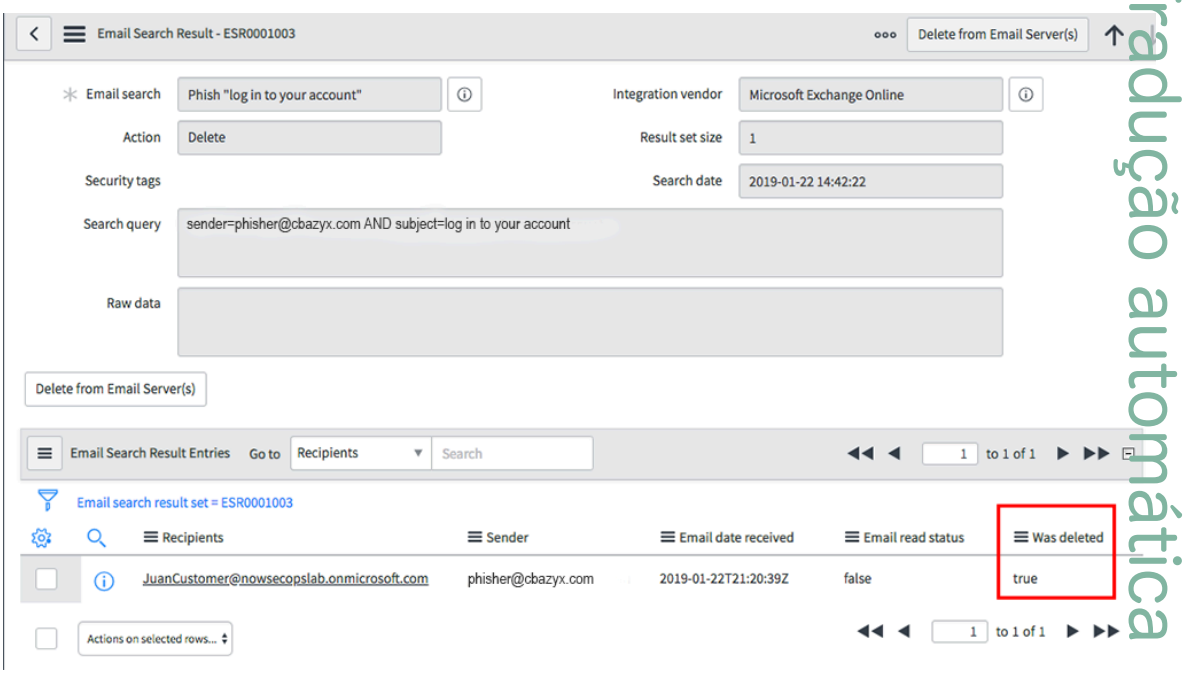
a. Navegar até **Incidentes de segurança > Mostrar todos os incidentes** e localize o incidente de segurança relacionado ao phishing.
Na parte inferior do registro, as listas relacionadas são exibidas.

b. Clique na lista relacionada **Pesquisa de e-mail**.

c. Clique no nome da pesquisa na coluna de pesquisa de e-mail (Phish "faça login na sua conta").
O registro de pesquisa de e-mail é exibido. Se a lista relacionada Pesquisa de e-mail não estiver visível, clique no link **Mostrar todas as listas**relacionadas.

d. Clique na lista relacionada **Resultados da pesquisa de e-mail**.
Na coluna Data de pesquisa, as ações de pesquisa e exclusão de e-mail são exibidas com as datas correspondentes.

e. Na coluna Data de pesquisa, clique no item que corresponde à ação de exclusão.
No registro Resultado da pesquisa de e-mail exibido, o status da coluna Foi excluído mostra que o e-mail foi excluído (verdadeiro).



Você aprovou com sucesso solicitações de exclusão de e-mail de uma notificação por e-mail e um registro de aprovação e confirmou que os e-mails foram excluídos. Para obter mais informações sobre como localizar o registro de resultado da pesquisa de e-mail, consulte Definir critérios de pesquisa de e-mail e solicitar uma pesquisa no serviço Microsoft Exchange Online.

Arquitetura de integração e conexão de sistemas externos para a integração Microsoft Exchange Online

A arquitetura de integração Microsoft Exchange Online foi desenvolvida para oferecer suporte aos recursos de pesquisa e exclusão de ameaças de e-mail no serviço Microsoft Exchange Online. Esta introdução explica por que há etapas de configuração que você deve concluir em suas contas Microsoft antes de instalar a aplicação ServiceNow.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A arquitetura de integração é baseada em avaliações das interfaces de programação de aplicações disponíveis no momento e com a consulta da Microsoft equipe de integração. Essas informações, bem como a terminologia principal sobre o serviço Now Platform e Microsoft Exchange Online, são fornecidas para esclarecer a operação conceitual da integração.

Termos-chave usados para esta integração

Os termos-chave a seguir são usados durante a instalação e a configuração. Para obter mais informações sobre os termos a seguir, consulte o site de documentação do produto da ServiceNow e o site de documentos da Microsoft.

[store-future: BEGIN review]

Now Platform

Um produto empresarial ServiceNow. O Now Platform é a base sobre a qual componentes individuais, como Security Incident Response (SIR), IT Service Management (ITSM) e outros produtos são criados.

Security Incident Response (SIR)

Uma aplicação Now Platform que rastreia o andamento dos incidentes de segurança desde a descoberta e a análise inicial, passando pela contenção, erradicação e recuperação, até a revisão e fechamento pós-incidente finais.

Microsoft Exchange Online

A oferta de serviço de e-mail para Microsoft Exchange Online, que faz parte do pacote Office 365 de produtos Microsoft.

Graph API global

A API fornecida por Microsoft que é usada para acessar informações de caixa de correio em Microsoft Exchange Online.

[store-future: BEGIN review]Autenticação baseada em certificados[End]

[store-future: BEGIN review]Essa autenticação permite que os clientes permitam ou exijam que os usuários se autentiquem diretamente com certificados X.509 no Azure Active Directory (Azure AD) para aplicações e login do navegador.[End]

Autenticação OAUTH

Um ID criado no portal do Azure Microsoft usado para coletar detalhes adicionais da mensagem de e-mail e para excluir e-mails em Microsoft Exchange Online. Aqui, o ID do cliente e o segredo do cliente da Microsoft são usados para autenticar os usuários.

[store-future: BEGIN review]Host do Windows[End]

[store-future: BEGIN review]O tipo específico de máquina virtual usada nesta integração.[End]

[store-future: BEGIN review]MID Server[End]

[store-future: BEGIN review]Uma aplicação Now Platform que facilita a comunicação e a movimentação de dados entre Now Platform e aplicações externas, fontes de dados e serviços. Um MID Server normalmente é necessário para integração com tecnologias locais, mas um MID Server pode ser implantado em determinados casos entre o Now Platform e uma oferta baseada em nuvem quando um componente fornecido pelo cliente é necessário para a integração. Para esta integração de serviços Microsoft Exchange Online, o MID Server facilita a comunicação entre o Now Platform e o servidor PowerShell.[End]

[store-future: BEGIN review]Servidor PowerShell[End]

[store-future: BEGIN review]O servidor PowerShell é uma aplicação da Microsoft que requer suas credenciais de conta da Microsoft.[End]

Administrador de incidentes de segurança (sn_si.admin)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O usuário com a função sn_si.admin supervisiona a configuração da integração com o produto SIR em sua instância Now Platform. O usuário com esta função também aprova solicitações de exclusão de e-mails por padrão e atribui a função sn_si.analyst conforme necessário. O usuário com esta função também tem controle total sobre todos os dados Gestão de serviços.

Analista de incidentes de segurança (sn_si.analyst)

O usuário com a função sn_si.analyst interage e analisa os incidentes de segurança no produto SIR.

[End]

Conexão de sistemas externos para pesquisa e exclusão de e-mail

[store-future: BEGIN review]Esta aplicação usa o serviço PowerShell do Centro de conformidade e segurança do Office 365 e o serviço Global Graph API para recuperar informações do locatário do serviço Exchange Online do Office 365. Uma conexão HTTPS de saída do MID Server para este ambiente é necessária para que a integração funcione corretamente.[End]

[store-future: BEGIN review]A arquitetura de integração oferece suporte a uma capacidade de pesquisa e exclusão de e-mail no serviço Microsoft Exchange Online. A arquitetura de integração tem como alvo e-mails de phishing, bem como outras ameaças de e-mail que podem comprometer a segurança da sua organização. Para obter e-mails que correspondam a determinados critérios de consulta de pesquisa, o Now Platform se conecta a um locatário de serviço Microsoft Exchange Online usando um MID Server que executa o PowerShell em um servidor Windows.[End]

Esta aplicação usa a abordagem baseada em REST para buscar os dados da Microsoft.

Depois que o Now Platform é conectado ao serviço Microsoft Exchange Online, a integração oferece suporte a vários níveis de pesquisas de e-mail.

A versão atualizada da integração do Security Incident Response com o Microsoft Exchange Online é uma integração SIR nova e robusta, que opera utilizando o ID da aplicação, o ID do locatário (organização) e o segredo do cliente para adquirir um token de portador (JWT) por meio de REST APIs. Esta nova integração não requer nenhum MID Server ou recursos adicionais do PowerShell. O objeto de aplicação estabelecido no Azure AD é atribuído a uma função de diretório, que é refletida em um token de acesso.

[store-future: BEGIN review]

- As mensagens correspondentes: esta pesquisa é realizada por meio do cmdlet do Microsoft PowerShell por meio de um MID Server do Windows que é um componente do Now Platform. Esta pesquisa é baseada em critérios que você configura no Now Platform de um incidente de segurança. O primeiro componente da pesquisa retorna todas as mensagens de e-mail que correspondem aos critérios de pesquisa configurados, além dos endereços de caixa de correio específicos onde essas mensagens podem ser encontradas em Microsoft Exchange Online. Os parâmetros de pesquisa compatíveis são Assunto, Remetente e Destinatário da mensagem de e-mail (o valor exibido no campo Para em uma mensagem de e-mail).
- Os detalhes da mensagem: depois que a pesquisa inicial baseada em cmdlet do PowerShell identifica as mensagens correspondentes, essa pesquisa recupera informações adicionais da mensagem usando a Microsoft Global Graph API. Os resultados de e-mail retornados incluem os seguintes detalhes da mensagem:
  - Status de leitura: o status verdadeiro ou falso é rastreado quando os usuários leram e-mails.
  - Endereço do remetente.

Tradução automática

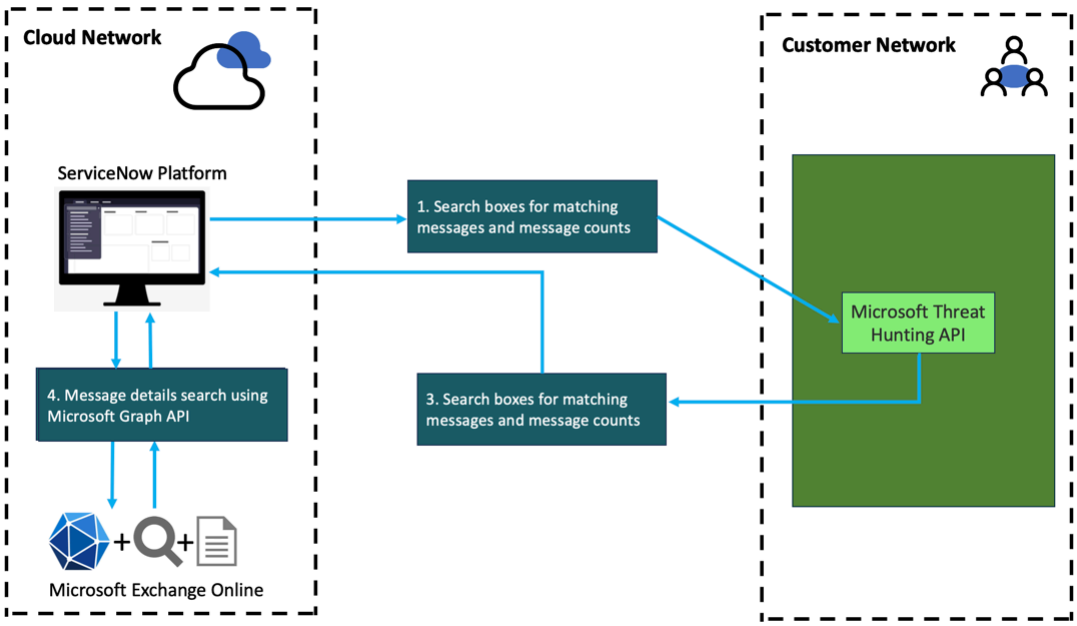
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Endereço do destinatário: esses endereços incluem indivíduos, um grupo e indivíduos que estão em cc e cco nas mensagens.
- Excluir status: o status verdadeiro ou falso rastreia e-mails excluídos.
- ID da mensagem: o identificador alfanumérico das mensagens de e-mail.

[End]

O fluxo de dados básico do e-mail pesquisa o número de mensagens e os detalhes da mensagem são ilustrados na figura a seguir.

Pesquisa de e-mail para o número de mensagens e detalhes da mensagem



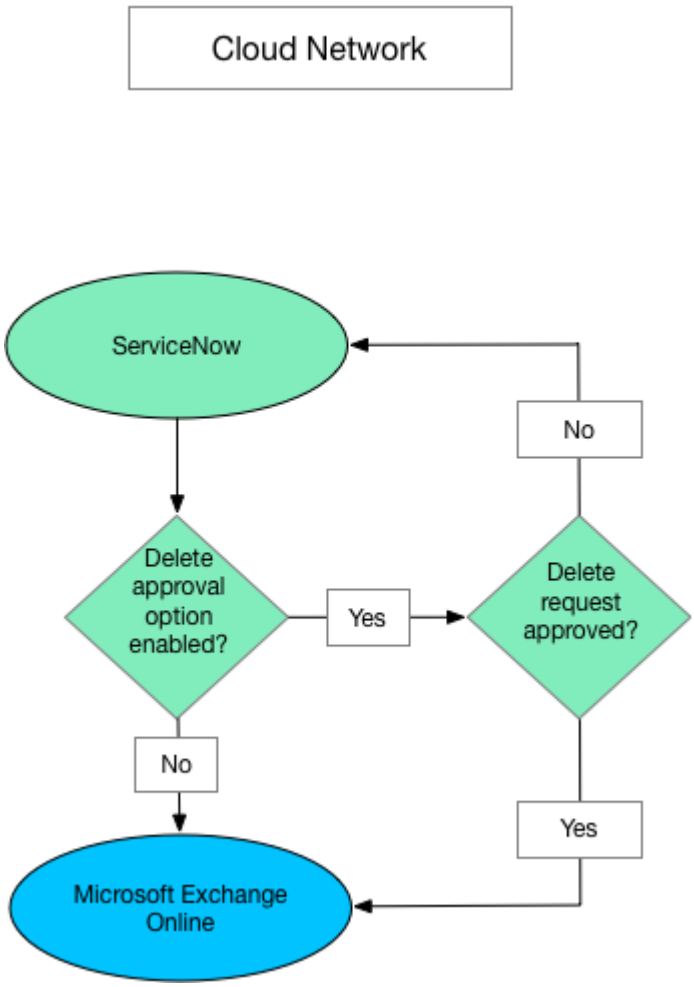
Para excluir e-mail, a integração usa a Graph API global. A recuperação de e-mails excluídos está disponível como uma opção durante a etapa de configuração e é descrita com mais detalhes em Configure a integração Microsoft Exchange Online com sua instância Now Platform.

O fluxo de dados para exclusão de e-mail com o processo de aprovação pré-configurado é ilustrado na figura a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exclusão de e-mail



Workflows

A aplicação Microsoft Exchange Online para pesquisa e exclusão de e-mail inclui os seguintes fluxos de trabalho:

- Exchange Online - Exclusão de e-mails
- Obter detalhes do e-mail do Exchange Online.
- Microsoft Exchange Online - Pesquisa e exclusão de e-mails.

Para obter mais informações, consulte Introdução aos fluxos de trabalho .

Agora você está pronto para configurar as contas necessárias para a integração.

Recuperar e-mails excluídos no serviço Microsoft Exchange Online

(Opcional) Como administrador do Microsoft Exchange, você pode recuperar e-mails excluídos se a correção do incidente exigir que você recupere os e-mails excluídos pelo fluxo de trabalho desta integração.

Antes de Iniciar

Para obter mais informações sobre como essa integração exclui e-mails, consulte Configure a integração Microsoft Exchange Online com sua instância Now Platform.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre a função administrativa no produto Microsoft Office 365, incluindo informações sobre como recuperar itens excluídos em uma caixa de correio do usuário, consulte Sobre a função de administrador do Exchange Online .

Função necessária: administrador, administrador do Microsoft Exchange

Por Que e Quando Desempenhar Esta Tarefa

Se você selecionar a opção **Recuperar e-mails excluídos** na guia Configurações adicionais durante a etapa de configuração, habilitará a recuperação de e-mails excluídos no seu locatário Microsoft Exchange Online. Os e-mails excluídos usando o fluxo de trabalho de exclusão desta integração são colocados na subpasta Itens excluídos da pasta Itens recuperáveis na caixa de correio do usuário no serviço Microsoft Exchange Online. Se a conta do usuário estiver configurada no locatário Microsoft Exchange Online para que o usuário possa exibir a pasta Itens excluídos, o usuário poderá recuperar esses e-mails usando o serviço Microsoft do Outlook na Web. Como alternativa, o administrador Microsoft Exchange Online pode recuperar e-mails excluídos de uma pasta de itens excluídos de um usuário. Consulte Recuperar itens ou e-mails excluídos no Outlook Web App para obter mais informações.

Função necessária: Microsoft Exchange Online administrador ou Microsoft administrador global para recuperar e-mails excluídos.

Função necessária: sn_si.admin no Now Platform para habilitar a opção Recuperar e-mails excluídos.

Função necessária: sn_si.analyst no Now Platform para concluir uma pesquisa bem-sucedida de e-mails e verificar se os e-mails foram excluídos com sucesso antes da recuperação.

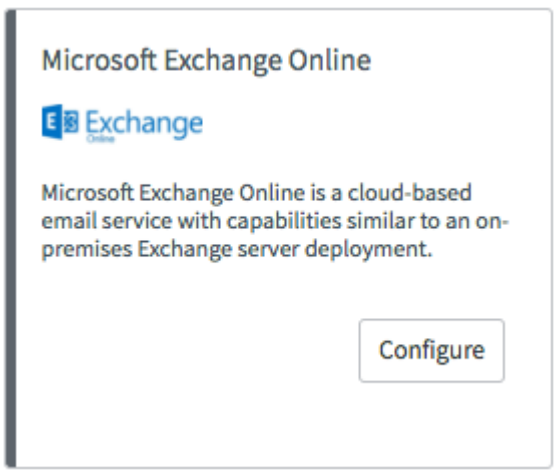
Procedimento

Para habilitar a opção de recuperação de e-mail, siga estas etapas.

a. Navegar até **Security Operations** > **Integrações** > **Configurações**.

b. Localize o bloco Microsoft Exchange Online.

c. Clique em **Configurar**.

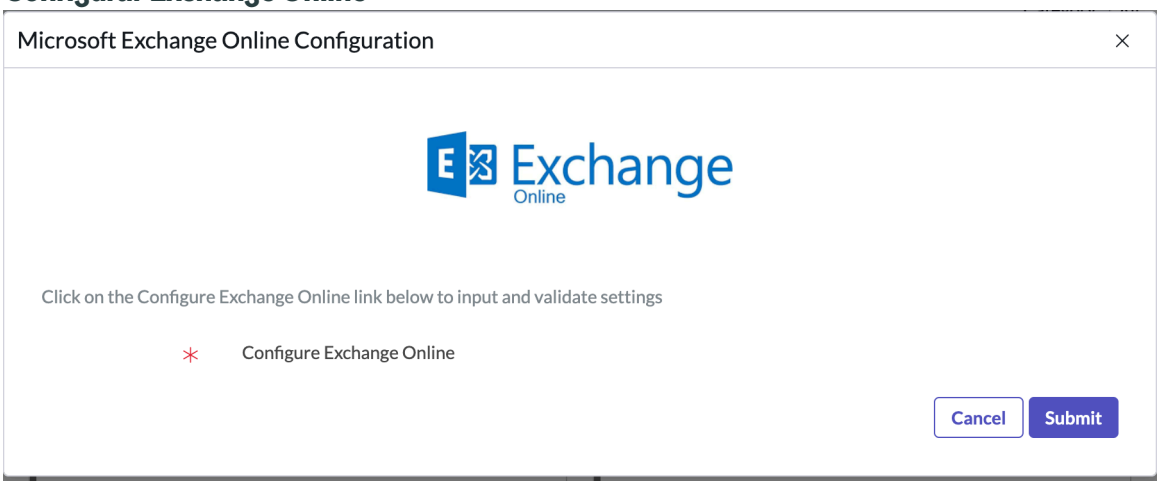


d. Na caixa de diálogo Microsoft Exchange Online Configuração exibida, clique em **Configurar Exchange Online**.

Tradução automática

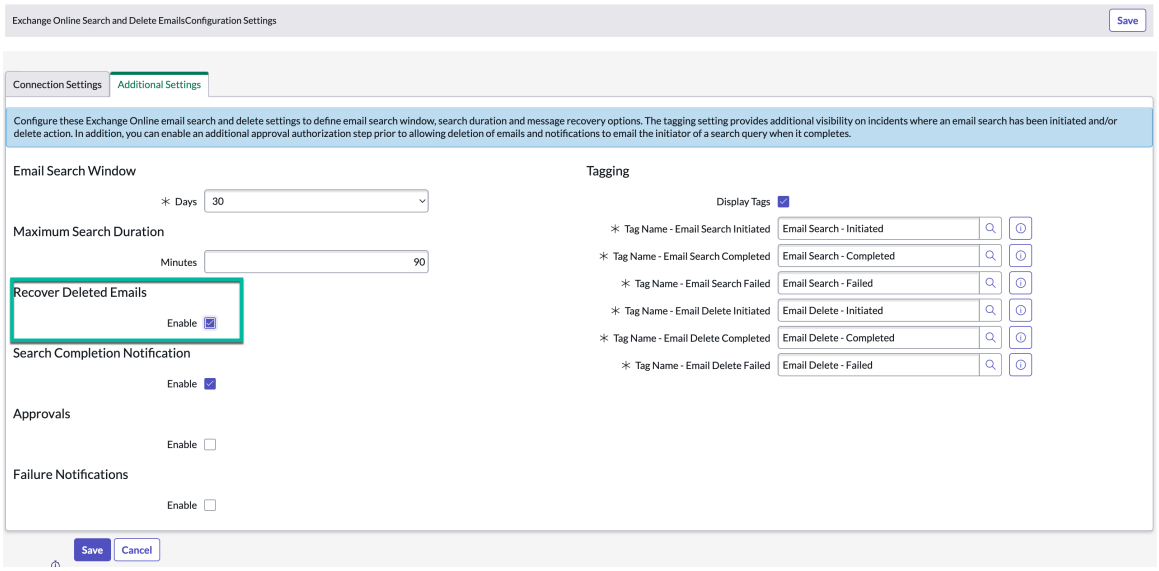
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar Exchange Online



e. Na guia Configurações adicionais, em Recuperar e-mails excluídos, marque a caixa de seleção **Habilitar**.

Recuperar e-mails excluídos



f. Verifique todas as outras configurações e clique em **Enviar**.

g. Para verificar se uma pesquisa e exclusão de mensagens de e-mail foram concluídas com sucesso para as mensagens de e-mail que você deseja recuperar, navegue até o incidente de segurança que registrou a pesquisa de e-mail e exclua os fluxos de trabalho.

h. Localize as anotações de trabalho e verifique se o sistema excluiu as mensagens com sucesso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

i. Como administrador Microsoft Exchange Online ou administrador global, faça login na sua conta Microsoft do Office 365.

j. Siga as etapas descritas em Recuperar itens excluídos ou e-mail no Outlook Web App no site de documentação Microsoft.

Editar marcadores de segurança na Now Platform para a integração Microsoft Exchange Online

Você pode editar os nomes e as cores dos marcadores de segurança em sua instância Now Platform® para a integração Microsoft Exchange Online. Esses marcadores de segurança ajudam a identificar rapidamente quando a pesquisa de e-mail é concluída ou falha. Eles também identificam quando as solicitações para excluir e-mails são iniciadas e quando os itens de e-mail são excluídos com sucesso.

Antes de Iniciar

Por padrão, os marcadores de segurança serão habilitados na sua instância Now Platform® se você selecionar a opção **Exibir** marcadores durante a etapa de configuração. Você pode editar cores e nomes de marcadores e atribuir marcadores a grupos de marcadores de segurança para ajudá-lo a organizá-los em sua instância Now Platform®. Por exemplo, você pode mudar as cores dos marcadores para que o marcador de início de um recurso seja de uma cor e o marcador de conclusão seja de outra cor para corresponder aos outros marcadores de segurança habilitados na sua instância Now Platform®. Essas cores diferentes podem ajudar a identificar rapidamente quando os fluxos de trabalho são iniciados e concluídos com sucesso. Se você decidir que não precisa de um marcador específico, sem desabilitar a marcação para a integração, também poderá desabilitar um único marcador do registro de marcador. Se desabilitado, este marcador não será mais exibido nos incidentes de segurança relacionados. Para obter mais informações sobre como configurar grupos e marcadores de segurança, consulte Configuração de grupos e marcadores de segurança no site de documentação do produto da ServiceNow .

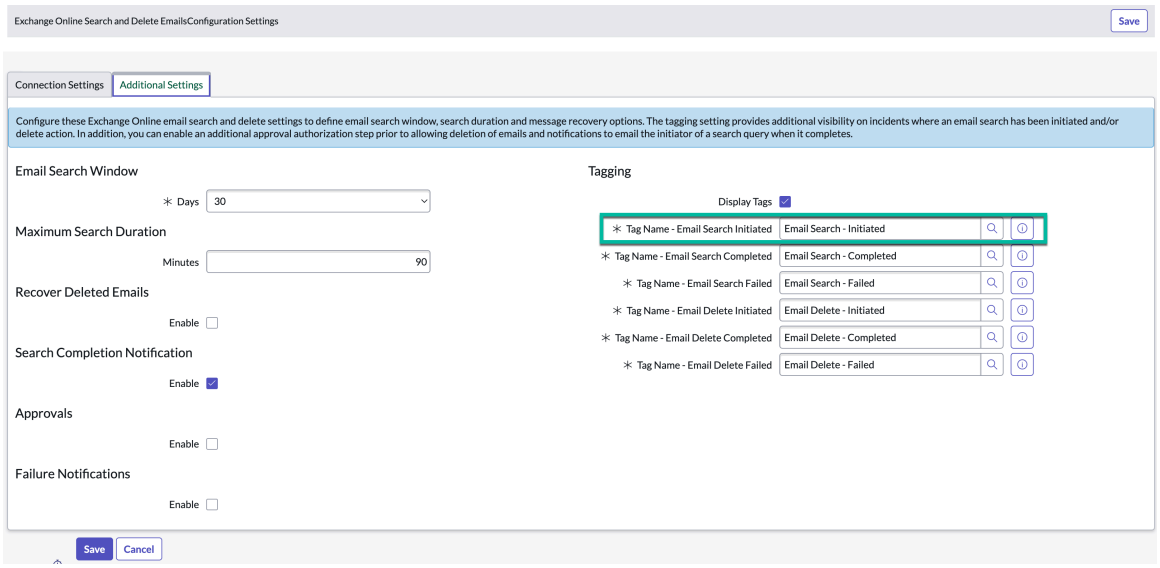
Função necessária: sn_si.admin

Procedimento

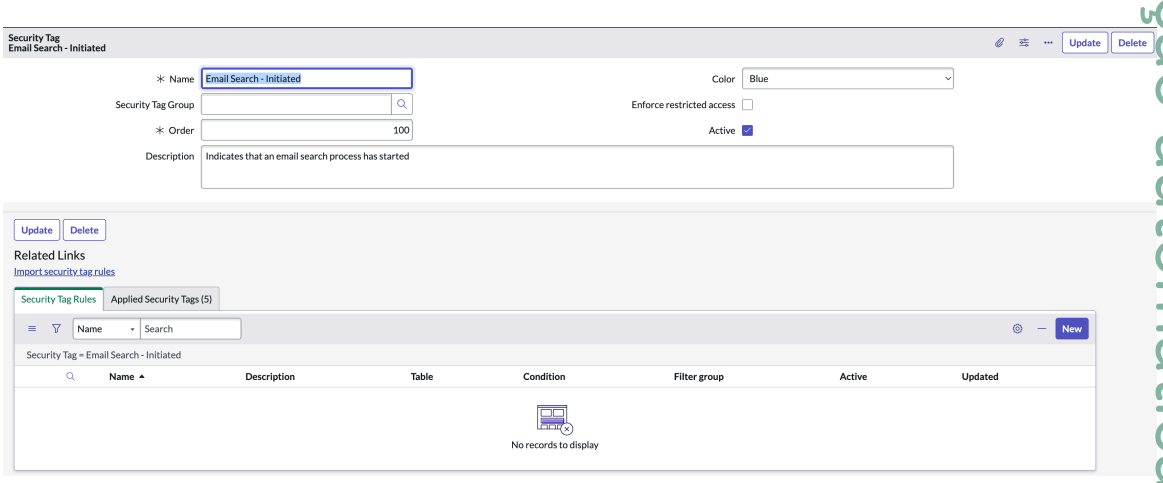
1. Navegar até **Todos** > **Security Operations** > **Integrações** > **Configurações do Exchange Online**.
2. Clique na guia **Configurações adicionais** para selecioná-la.
3. Na guia exibida, se a opção **Exibir** marcadores estiver desmarcada, selecione-a para exibir os nomes dos marcadores.
4. Com os nomes de marcador exibidos, à direita de um marcador, clique no ícone de informações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Na caixa de diálogo Marcador de segurança exibida, clique em **Abrir registro**.
6. No registro exibido, edite os campos.
7. Clique em **Atualizar** para salvar suas mudanças.



Você editou com sucesso o registro do marcador para um marcador de segurança.

Check-list para a integração Microsoft Exchange Online

Use esta check-list para orientar você nas tarefas de ponta a ponta da integração. A check-list a seguir inclui tarefas de configuração e instalação, exemplos de casos de uso e resultados esperados para a aplicação.

Antes de Iniciar

Acompanhe seu progresso com a instalação e configuração da integração com a tabela a seguir. Conclua todas as tarefas de uma etapa antes de passar para a próxima. Cada etapa identifica as funções necessárias para executar as tarefas e faz referência aos tópicos numerados do guia de instalação e configuração desta integração.

Funções necessárias: as funções são listadas para cada etapa na tabela a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

Para acompanhar o andamento da integração, siga as etapas na tabela na ordem em que são apresentadas

Check-list

☐	Como administrador do Microsoft Office 365, configure sua conta Microsoft do Office 365. Crie uma conta de API que permita o acesso ao Centro de segurança e conformidade no Microsoft Office 365.
☐	Como administrador do Microsoft Azure, configure sua conta Microsoft do Azure. Crie uma conta que usa um ID de aplicação para coletar detalhes adicionais da mensagem de e-mail e excluir mensagens de e-mail. Para obter as etapas de configuração da conta, consulte Configure sua conta do Azure Microsoft para a integração ServiceNow Microsoft Exchange Online.
☐	Como administrador Now Platform, configure sua instância Now Platform para a integração. Para tarefas e mais informações, consulte Configure sua instância Now Platform para a integração Microsoft Exchange Online. **a.** Atribua Now Platform funções. **b.** Instale as aplicações Now Platform (SIR) e Security Operations de ServiceNow Store e ative-as em sua instância. **c.** Habilite os recursos de envio e recebimento de e-mail. **d.** Atribua a função de leitura e gravação de e-mail ao sn_si.analyst. **e.** Crie um grupo de aprovação.
☐	Como administrador do Now Platform, instale a aplicação para a integração do ServiceNow Store. Para obter as etapas de instalação, consulte Instalar a aplicação Microsoft Exchange Online para a integração ServiceNow Microsoft Exchange Online.
☐	Como sn_si.admin, conclua as guias de definições de configuração para estabelecer a conectividade e ativar os fluxos de trabalho de pesquisa e exclusão. Para obter as definições de conexão e configuração, consulte Configure a integração Microsoft Exchange Online com sua instância Now Platform.
☐	Como sn_si.analyst, configure os critérios de pesquisa de e-mail e solicite uma pesquisa de e-mails correspondentes no servidor Microsoft Exchange Online. Para obter um exemplo, consulte Definir critérios de pesquisa de e-mail e solicitar uma pesquisa no serviço Microsoft Exchange Online. **a.** Localize incidentes de segurança relacionados a eventos de phishing. **b.** Configure os critérios de pesquisa de e-mail.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	c. Solicite uma pesquisa de e-mails. **d.** Localize os resultados da pesquisa e os detalhes da mensagem nas listas relacionadas ao incidente de segurança.
☐	Como sn_si.analyst, exclua e-mails do servidor Microsoft Exchange Online. Para obter um exemplo, consulte Solicitar aprovação de exclusão para e-mails no serviço Microsoft Exchange Online. **a.** Localize o incidente de segurança com os resultados da pesquisa. **b.** Exclua e-mails ou solicite aprovação para excluir e-mails. **c.** Verifique se os e-mails foram excluídos dos resultados publicados nas anotações de trabalho e nas listas relacionadas no incidente de segurança.
☐	Como sn_si.admin ou, como membro de um grupo de aprovação, processe solicitações de exclusão de e-mail por meio de notificações por e-mail. Para obter um exemplo, consulte Aprovar solicitações de exclusão de e-mail para a integração Microsoft Exchange Online.

Você concluiu com sucesso as etapas de configuração e verificou os resultados esperados para a integração.

Solução de problemas da integração do Microsoft Exchange Online

Se a permissão `ThreatHunting.Read.All` não estiver visível, verifique a licença do Defender for Office 365.

Para obter mais informações, consulte Comparação de segurança do Microsoft Defender for Office 365 .

Integração do Microsoft Exchange no Local

A integração Microsoft Exchange no local fornece ferramentas para os analistas de segurança conterem e erradicarem ameaças de e-mail de phishing e de Spear Phishing em instâncias locais.

Explorar

Integrações do Security Incident Response

Configurar

Introdução à integração do Microsoft Exchange no local

Usar

Pesquisar e excluir e-mails de phishing

Desenvolver

- ServiceNow Security Operations diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	• Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Faça ou responda perguntas na comunidade do Security Operations • Pesquise artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Introdução à integração do Microsoft Exchange no local

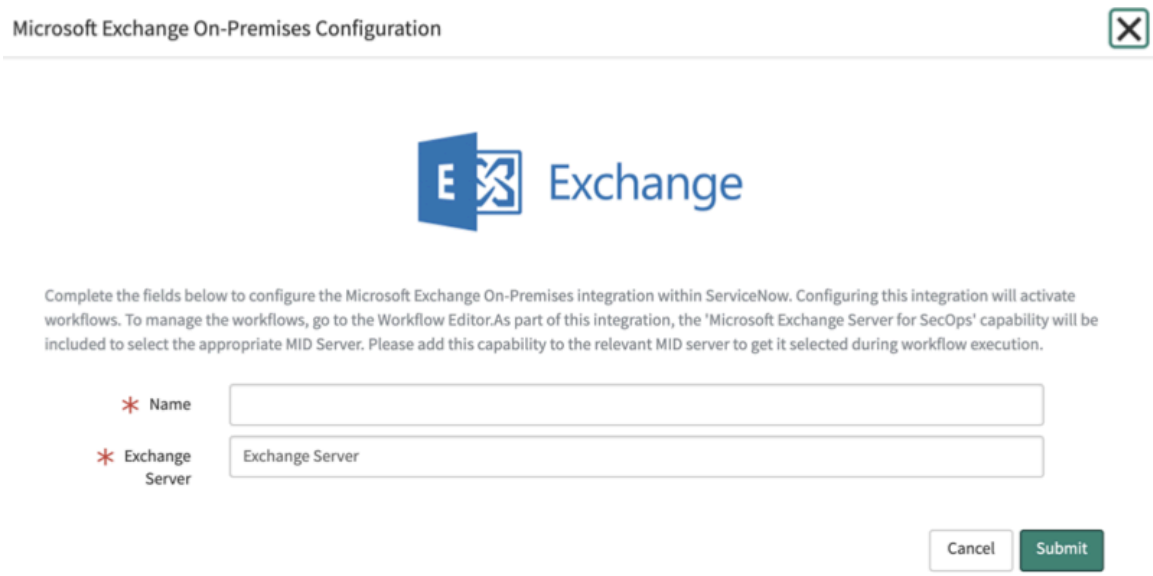
A integração Microsoft Exchange no local fornece ferramentas para os analistas de segurança conterem e corrigirem ameaças de e-mail de phishing e de Spear Phishing em instâncias locais. Antes de usar a integração Microsoft Exchange no local, você deve baixá-la do ServiceNow Store e identificar os servidores Exchange e MID apropriados.

Antes de Iniciar

Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação do sistema operacional for concluída, navegue até **Security Operations** > **Integrações** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão Microsoft Exchange No local, clique em **Novo**.



4. Preencha os campos, conforme necessário.

Tradução automática

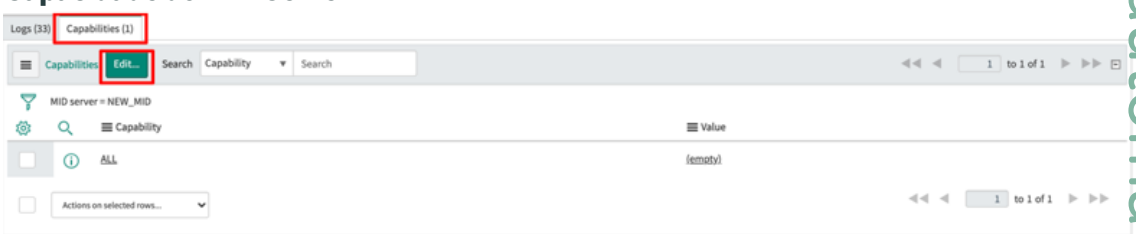
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	O nome desta configuração.
Exchange Server	Especifique o servidor do Exchange a ser usado.

Nota:
Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho.

5. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
6. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
7. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.
8. Navegar até **Orquestração** > **MID Servers**.
9. Abra o registro e verifique o status do MID Server que pode ser acessado pelo Exchange Server e se a opção **Status** está definida como **Ativo** e a opção **Validado** como **Sim**.
10. Adicione o recurso do MID Server:
    - Selecione o respectivo MID Server para adicionar o recurso.
    - Clique na lista relacionada **Recursos** e clique em **Editar**.

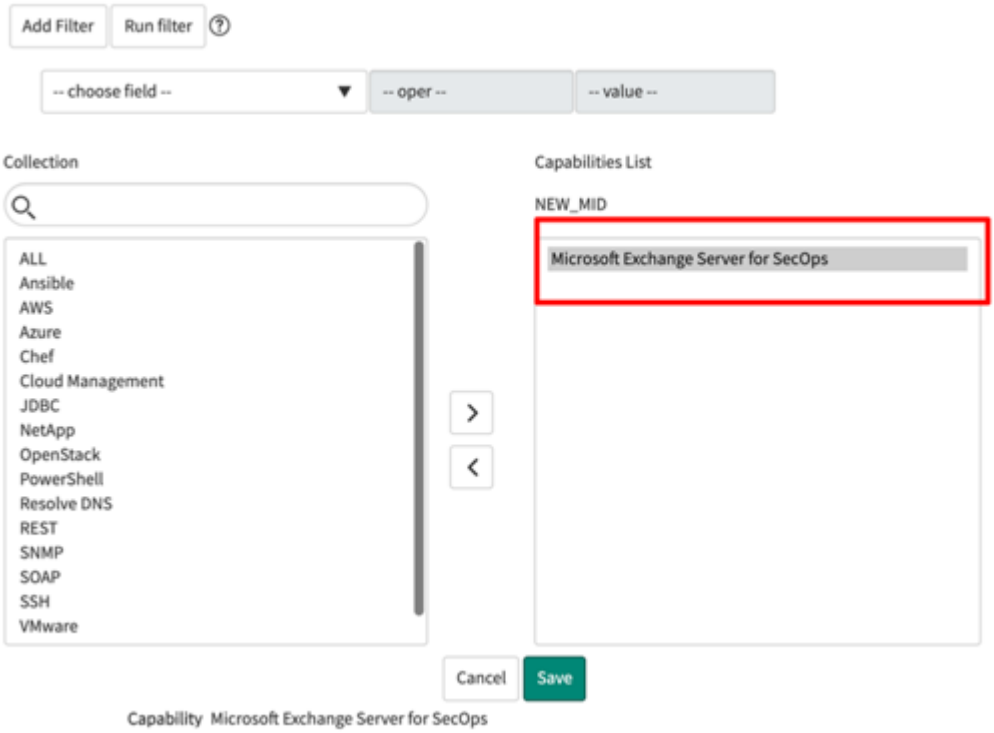
Capacidade do MID Server



    - Remover **tudo** e adicionar **Microsoft Exchange Server para SecOps**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



- Selecione os **Intervalos de IP** na seção **Listas relacionadas** e defina o valor como **TODOS** ou qualquer valor desejado.
- Selecione as **Aplicações compatíveis** na seção **Listas relacionadas** e defina o valor como TODOS ou Orchestration.
- **Salve** o registro.

11. Valide as conexões e credenciais.
12. Depois que as credenciais forem validadas, a configuração na instância da ServiceNow estará concluída e pronta para executar operações de pesquisa e exclusão de e-mail usando esta integração.

Microsoft Exchange - Executar fluxo de trabalho de pesquisa e exclusão de e-mail

Quando o fluxo de trabalho **Microsoft Exchange - Executar pesquisa e exclusão de e-mail** é executado, ele pesquisa o servidor do Exchange usando a consulta de pesquisa fornecida e retorna os detalhes para a instância local.

Antes de Iniciar

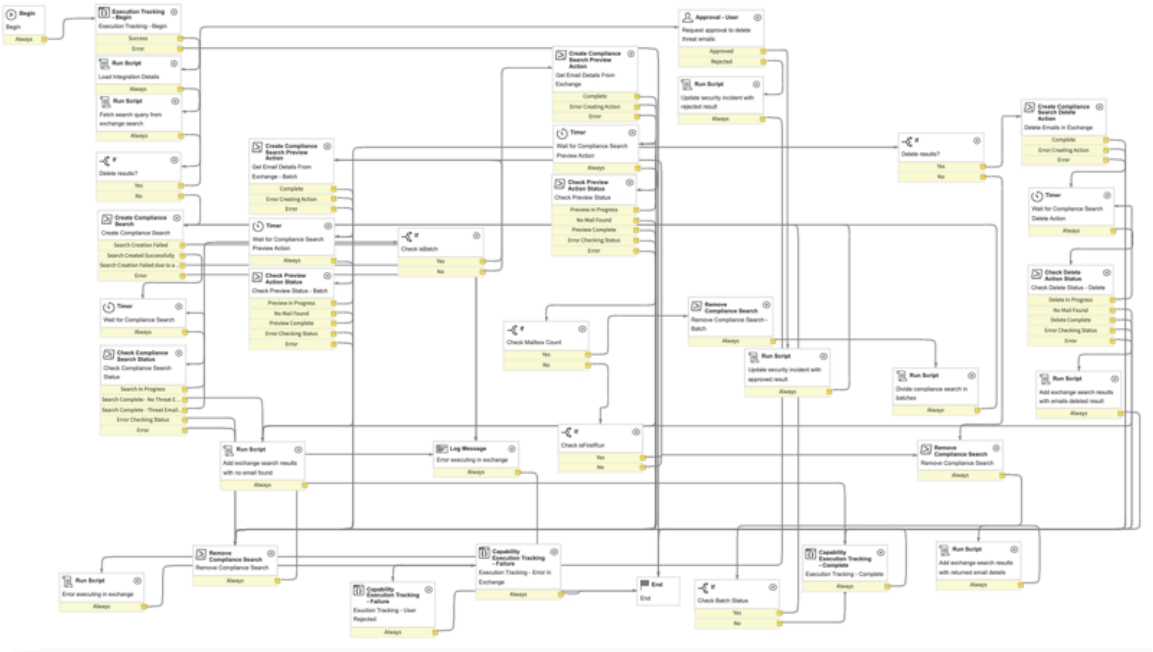
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho **Microsoft Exchange - Executar pesquisa e exclusão de e-mail** é executado quando as pesquisas de e-mail são configuradas e o botão **Excluir de servidores de e-mail** ou **Pesquisar em servidores de e-mail** é pressionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Atividades específicas para esta integração são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Criar atividade de pesquisa de conformidade

A atividade Criar pesquisa de conformidade cria uma pesquisa de conformidade para e-mails no(s) servidor(es) do Exchange designado(s) usando as consultas de pesquisa definidas e retorna o nome da pesquisa de conformidade criada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
search_query	Consulta de pesquisa obrigatória usada para encontrar e-mails no Exchange Server em todas as caixas de correio.
Exchange Local	Campo de local obrigatório usado para pesquisar no local definido. Os valores são: • Todos • Nome da caixa de correio específica
targetId	Campo de identificador de host de destino obrigatório onde o Exchange Server está localizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Nome da pesquisa de conformidade criada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condições de Saída

As possíveis condições de saída para esta atividade são:

Condições de Saída

Variável	Descrição
Falha na criação da pesquisa	Quando a criação da pesquisa falha devido a uma exceção no Exchange Server.
Pesquisa criada com sucesso	Quando a criação da pesquisa é bem-sucedida.
Falha na criação da pesquisa devido a um erro de análise	Quando a criação da pesquisa falha devido a um problema de análise.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Verificar atividade de status de pesquisa de conformidade

A atividade Verificar status de pesquisa de conformidade verifica o status da pesquisa de conformidade criada no Exchange Server e, se o status for concluído, retorna as informações sobre a pesquisa de e-mail encontrada para a pesquisa de conformidade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
targetId	Campo de identificador de host de destino obrigatório onde o Exchange Server está localizado.
searchName	Nome obrigatório da pesquisa de conformidade criada no Exchange Server.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Contém o status da pesquisa de conformidade e o número de e-mails encontrados no servidor de troca para a pesquisa de conformidade.

Condições de Saída

As possíveis condições de saída para esta atividade são:

Condições de Saída

Variável	Descrição
Pesquisa em andamento	Quando o status da pesquisa de conformidade está em andamento.
Pesquisa concluída - Nenhum e-mail de ameaça encontrado	Quando o status da pesquisa de conformidade é concluído e nenhum e-mail é encontrado como parte da pesquisa de conformidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condições de Saída

Variável	Descrição
Pesquisa concluída - E-mails de ameaça encontrados	Quando o status da pesquisa de conformidade é concluído, e os e-mails são encontrados como parte da pesquisa de conformidade.
Erro ao verificar status	Quando a verificação de status falha devido a uma exceção no Exchange Server.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Criar atividade de ação de visualização da pesquisa de conformidade

A atividade Criar ação de visualização de pesquisa de conformidade cria uma nova ação de pesquisa de conformidade do tipo visualização no servidor de troca para a pesquisa de conformidade criada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
targetId	Campo de identificador de host de destino obrigatório onde o Exchange Server está localizado.
searchName	Nome obrigatório da pesquisa de conformidade criada no Exchange Server.

Condições de Saída

As possíveis condições de saída para esta atividade são:

Condições de Saída

Variável	Descrição
Concluir	Quando a ação de pesquisa de conformidade é criada com sucesso.
Erro ao criar ação	Quando a criação da ação de pesquisa de conformidade falha devido a uma exceção no Exchange Server.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Verificar atividade de status da ação de visualização

A atividade Visualizar status da ação verifica o status da ação de pesquisa de conformidade do tipo visualização e retorna as informações de visualização dos e-mails encontrados, como destinatário, remetente, assunto e data do e-mail recebido.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
targetId	Campo de identificador de host de destino obrigatório onde o Exchange Server está localizado.
searchName	Nome obrigatório da pesquisa de conformidade criada no Exchange Server.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Contém o status da ação de pesquisa de conformidade e as informações de visualização do e-mail encontrado como parte da pesquisa de conformidade.

Condições de Saída

As possíveis condições de saída para esta atividade são:

Condições de Saída

Variável	Descrição
Visualização em andamento	Quando o status da ação de pesquisa de conformidade está em andamento.
Nenhum e-mail encontrado	Quando o status da ação de pesquisa de conformidade é concluído e nenhum e-mail é encontrado como parte da pesquisa de conformidade.
Exibição concluída	Quando o status da ação de pesquisa de conformidade é concluído e os e-mails são encontrados como parte da pesquisa de conformidade.
Erro ao verificar status	Quando a verificação de status falha devido a uma exceção no Exchange Server.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Criar atividade de ação de exclusão de pesquisa de conformidade

A atividade Criar ação de exclusão de pesquisa de conformidade cria uma nova ação de pesquisa de conformidade do tipo limpar no servidor de troca para a pesquisa de conformidade criada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
targetId	Campo de identificador de host de destino obrigatório onde o Exchange Server está localizado.
searchName	Nome obrigatório da pesquisa de conformidade criada no Exchange Server.

Condições de Saída

As possíveis condições de saída para esta atividade são:

Condições de Saída

Variável	Descrição
Concluir	Quando a ação de pesquisa de conformidade é criada com sucesso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condições de Saída

Variável	Descrição
Erro ao criar ação	Quando a criação da ação de pesquisa de conformidade falha devido a uma exceção no Exchange Server.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Verificar atividade de status da ação de exclusão

A atividade Verificar status da ação de exclusão verifica o status da ação de pesquisa de conformidade do tipo limpar e executa a operação de exclusão reversível no servidor de troca dos e-mails encontrados como parte da pesquisa de conformidade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
targetId	Campo de identificador de host de destino obrigatório onde o Exchange Server está localizado.
searchName	Nome obrigatório da pesquisa de conformidade criada no Exchange Server.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Contém o status da ação de pesquisa de conformidade e a contagem de e-mails excluídos que foram encontrados como parte da pesquisa de conformidade.

Condições de Saída

As possíveis condições de saída para esta atividade são:

Condições de Saída

Variável	Descrição
Exclusão em Andamento	Quando o status da ação de pesquisa de conformidade está em andamento.
Nenhum e-mail encontrado	Quando o status da ação de pesquisa de conformidade é concluído, nenhum e-mail é excluído como parte da pesquisa de conformidade.
Exclusão concluída	Quando o status da ação de pesquisa de conformidade é concluído, os e-mails são excluídos como parte da pesquisa de conformidade.
Erro ao verificar status	Quando a verificação de status falha devido a uma exceção no Exchange Server.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Remover atividade de pesquisa de conformidade

A atividade Remover pesquisa de conformidade remove a pesquisa de conformidade criada do servidor do Exchange.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
targetId	Campo de identificador de host de destino obrigatório onde o Exchange Server está localizado.
searchName	Nome obrigatório da pesquisa de conformidade criada no Exchange Server.

Integração de ingestão de alerta da API de segurança do Microsoft Graph

Use a integração API de Segurança do Microsoft Graph para ingerir alertas de provedores de segurança do Microsoft Graph e criar incidentes de segurança automaticamente.

Visão geral

O API de Segurança do Microsoft Graph é um serviço intermediário (ou agente) que fornece uma única interface programática para conectar vários provedores de segurança (nativos da Microsoft, bem como parceiros da ServiceNow).

A integração API de Segurança do Microsoft Graph resolve esses problemas usando o API de Segurança do Microsoft Graph para se conectar a diferentes tecnologias de segurança da Microsoft, como Azure Sentinel, Microsoft Defender Advanced Threat Protection e Azure Advanced Threat Protection. Os alertas dos provedores de segurança da Microsoft são ingeridos e os incidentes de segurança são criados automaticamente em Security Incident Response.

Principais recursos

Esta integração inclui os seguintes recursos principais:

- Descoberta de API de Segurança do Microsoft Graph alertas que são candidatos a incidentes de segurança e automatizam a criação de incidentes de segurança.
- Mapeamento de campos de alerta para campos de incidente de segurança.
- Agregação de alertas semelhantes a incidentes de segurança em aberto existentes em vez de criar incidentes de segurança duplicados.
- Visualize os valores do campo de alerta e valide seus mapeamentos no incidente de segurança.
- Atualização automática de status de alerta para criação e fechamento de incidente de segurança.
- Configure a ingestão programada de alertas para criar incidentes de segurança periodicamente.

Configure sua instância da Now Platform para a integração da API de segurança do Microsoft Graph

A seção a seguir lista as tarefas de configuração que você deve concluir em sua instância Now Platform® antes de instalar a aplicação do ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração sem problemas.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform® e Security Incident Response.	As funções a seguir são necessárias para a instalação, configuração e uso da integração na sua instância Now Platform®. • Um usuário com a função de administrador Now Platform® (admin) instala a aplicação a partir do ServiceNow Store e atribui a função de administrador de incidente de segurança (sn_si.admin). • Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no Now Platform®: ◦ Nomeia, cria e edita perfis de alerta. ◦ Seleciona e mapeia os campos de dados de alerta da API de segurança do Microsoft Graph para os campos de incidente de segurança. ◦ Visualiza os detalhes do incidente de segurança para precisão antes de finalizar a configuração. ◦ Programa a ingestão de alertas em andamento. ◦ Habilita atualizações de alerta quando um incidente Security Incident Response é criado e encerrado. ◦ Atribui a função de analista de incidente de segurança (sn_si.analyst). ◦ Usuários com o sn_si.analyst trabalham com incidentes de segurança. Para obter mais informações sobre funções e atribuição de funções a usuários, consulte Funções no site de documentação do produto da ServiceNow .
Registre sua aplicação no portal Microsoft Azure.	Antes de ingerir alertas, você deve configurar sua aplicação no portal Microsoft Azure. Consulte Configurar o portal do Microsoft Azure para mais detalhes.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	1. Security Incident Response **2.** Ingestão de eventos e alertas para Security Operations: esta aplicação requer: ○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub Runtime ○ com.glide.hub.action_step.rest => Etapa de ação do ServiceNow IntegrationHub - REST **Nota:** Os componentes do Integration Hub são instalados junto com o plug-in Event and Alert Ingestion. Se eles não estiverem instalados, entre em contato com o Suporte ao cliente para obter assistência. Para obter mais informações sobre como instalar as aplicações principais Security Operations, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

Configurar o portal do Microsoft Azure

Para recuperar alertas de segurança para uma aplicação disponível no locatário do Microsoft Azure usando o API de Segurança do Microsoft Graph, você deve registrar a aplicação no portal Microsoft Azure e conceder acesso de leitura e gravação ao evento de segurança para a aplicação.

Antes de Iniciar

Função necessária:

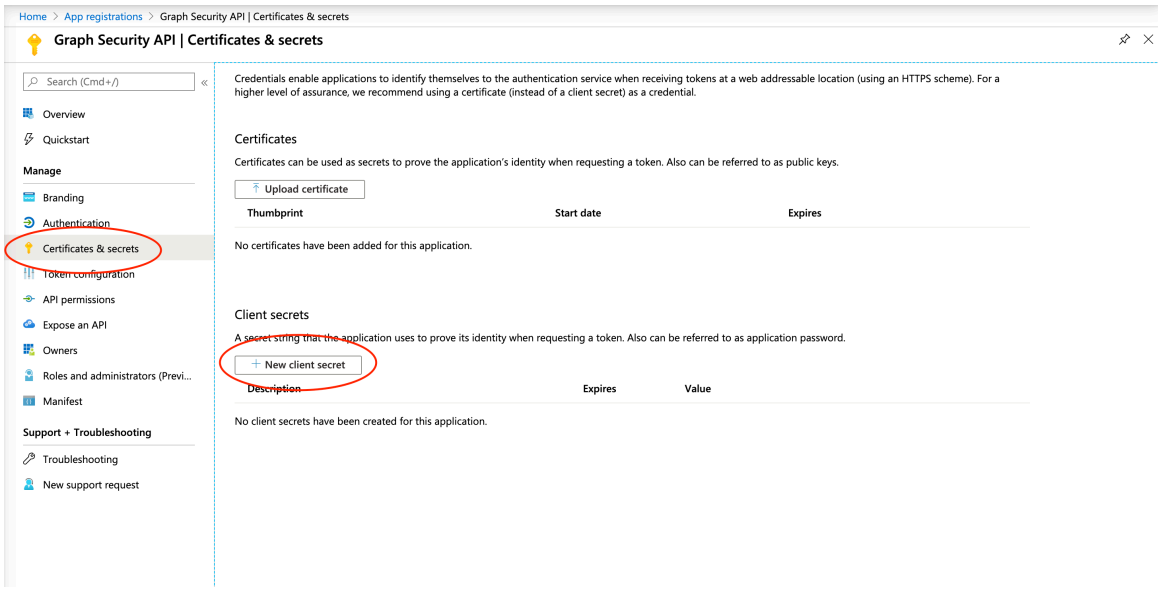
- Desenvolvedor de aplicações: necessário para registrar a aplicação.
- Administrador de locatário: o administrador de locatário Microsoft Azure deve conceder permissões à aplicação fazendo uma chamada para o endpoint de consentimento do administrador.

Procedimento

1. Faça login no portal Microsoft Azure.
2. Insira **Registros do app** na caixa **Pesquisar**.
3. Clique **em Novo registro**.
4. Insira um nome para sua aplicação e o URI de redirecionamento, por exemplo, http://localhost e clique em **Registrar**.
   O URI de redirecionamento é usado ao fornecer o consentimento do administrador para a aplicação.
5. Na página Registros da aplicação, selecione a aplicação que você registrou, por exemplo, Graph Security Demo.
6. Em **Gerenciar**, selecione **Certificados e segredos**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

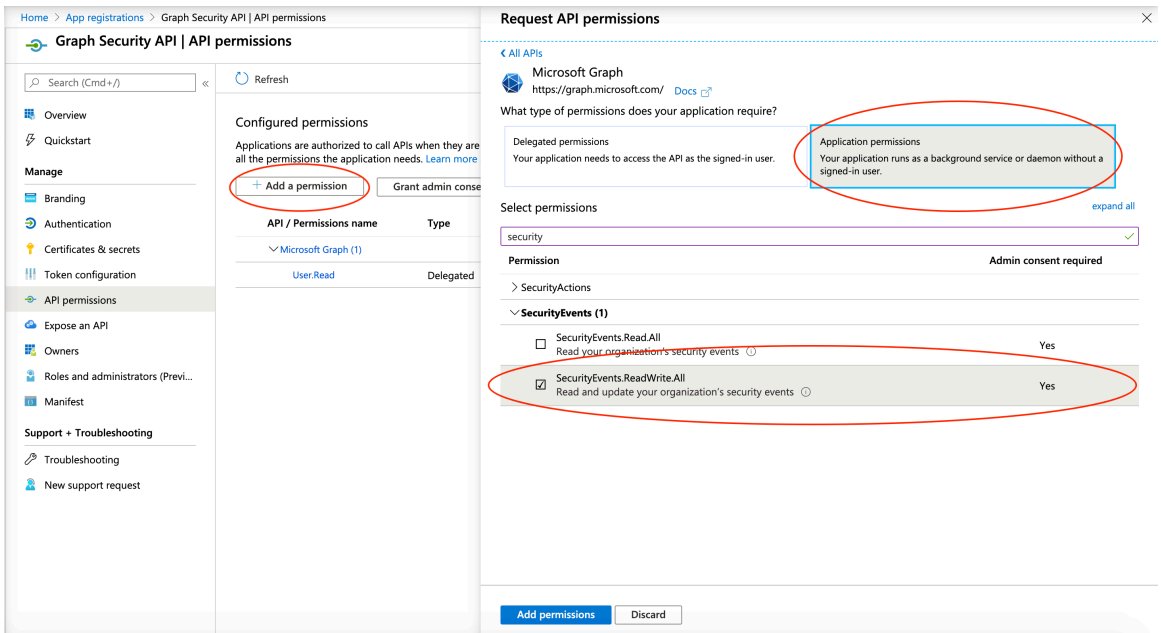


7. Selecione **Novo segredo do cliente** para criar um segredo do cliente.
   Copie o segredo do cliente e salve-o, pois ele não ficará visível mais tarde. Caso tenha esquecido o segredo do cliente, você pode gerar um novo segredo do cliente.

   Nota:
   Se você esquecer o segredo do cliente, poderá gerar um novo seguindo as instruções nas etapas 4 e 5.

8. Clique em **Exibir permissões de API** na página Visão geral.

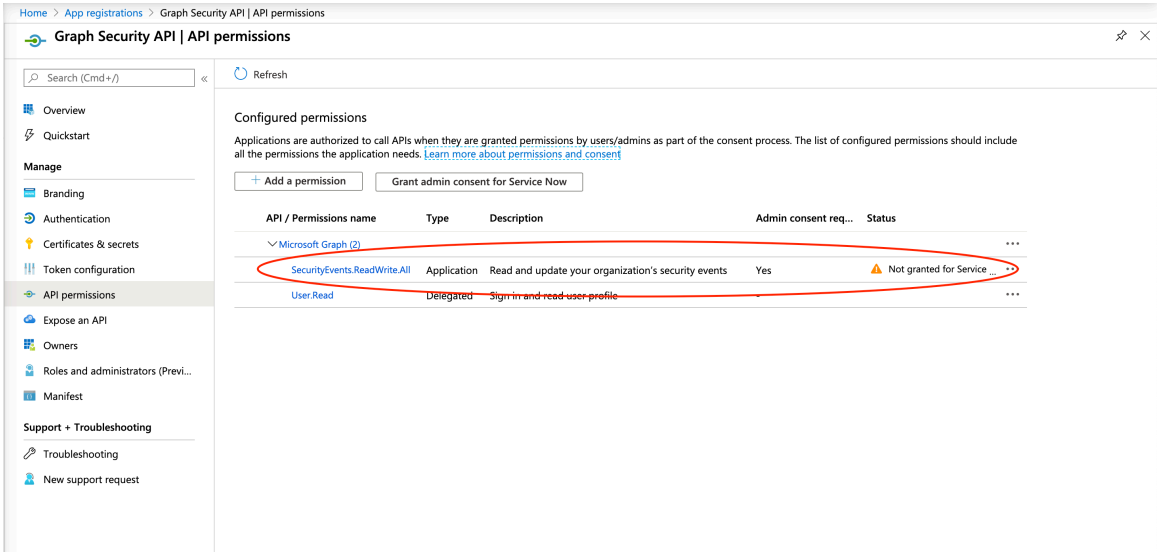
9. Adicione novas permissões de API no nível da aplicação para eventos de segurança SecurityEvents.ReadWrite.All.



10. Conceda consentimento de administrador para as permissões de API recém-adicionadas.
    Para obter mais informações, consulte a Referência de permissões do Microsoft Graph Modelo de permissão do Microsoft Graph.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



11. Faça login como administrador de locatários e forneça consentimento para a aplicação.
As etapas são fornecidas abaixo:

    a. Navegue até o seguinte URL: https://login.microsoftonline.com/common/adminconsent?client_id=APPLICATION_ID&state=12345

    Insira o APPLICATION_ID da aplicação que você registrou.

12. Clique em **Aceitar** para aceitar as permissões solicitadas pela aplicação criada acima.
Você pode usar a aplicação para ler eventos de segurança. Consulte a documentação de autorização de segurança do Microsoft Graph para obter mais detalhes.

Instalar e configurar a aplicação ServiceNow para integração de ingestão de alertas da API de segurança do Microsoft Graph

Antes de executar a integração na sua instância Now Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente aos produtos Security Incident Response e Security Operations na sua instância Now Platform.

Antes de Iniciar

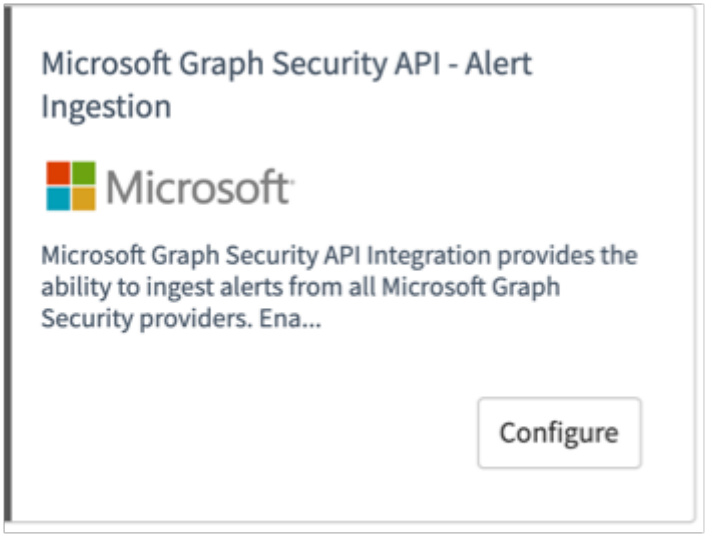
Função necessária: sn_si.admin

Procedimento

1. Se você não instalou a aplicação [API de Segurança do Microsoft Graph de ServiceNow Store para a integração, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.
2. Depois de instalar a aplicação com êxito, navegue até **Integrações** > **Configurações de integrações** e localize o bloco Microsoft Graph Security API - Alert Ingestion.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para configurar a aplicação, clique em **Configurar**.
4. Na caixa de diálogo Configuração de ingestão de alertas exibida, preencha os campos.
5. Clique em **Enviar**.
   Depois de validada e enviada com sucesso, cada configuração de servidor de ingestão de alertas é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista de seleção Mostrar configurações, clique em **Sim**.

O que Fazer Depois
Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar um perfil de alerta.

Criar um perfil para a integração de ingestão de alertas da API de segurança do Microsoft Graph

Como um usuário com a função sn_si.admin, você cria um perfil de alerta em sua instância Now Platform e determina quais alertas criam incidentes de segurança. Antes que os incidentes de segurança sejam criados a partir de alertas ingeridos, os valores de campo dos alertas são exibidos em um layout de um incidente de segurança Now Platform para que você possa visualizar como o incidente de segurança real será exibido.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
A integração permite ingerir diferentes tipos de alertas, como tentativas de acesso não autorizado e malware, por exemplo. Esses alertas são ingeridos com base nos perfis que você configura no ambiente Security Operations da sua instância. Todos os alertas são ingeridos inicialmente para um tipo de alerta configurado em um perfil. Os alertas ingeridos podem ser filtrados para especificar quais alertas criam incidentes de segurança.

Por exemplo, você pode preferir filtros que criem incidentes de segurança somente para alertas identificados como de alto risco. Antes de um perfil ser ativado e criar incidentes de segurança a partir de alertas ingeridos, os valores de campo individuais nos alertas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

filtrados são mapeados para campos correspondentes em um layout de incidente de segurança para uma visualização. Todos os alertas que atendem aos critérios de seleção no seu locatário Microsoft Azure e estão disponíveis em API de Segurança do Microsoft Graph são inicialmente ingeridos em sua instância Now Platform.

Identifique a origem do perfil

Especifique o nome e a origem do perfil.

Antes de Iniciar

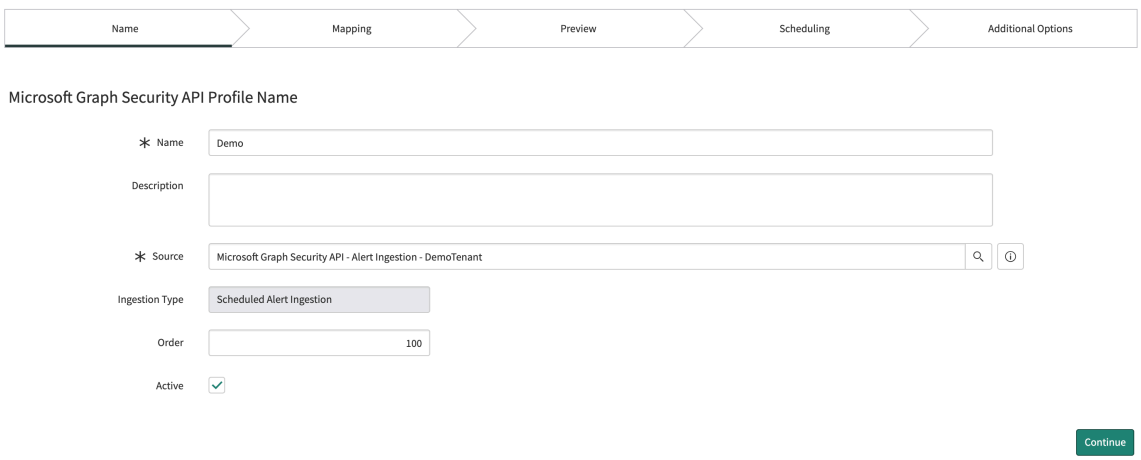
Função necessária: sn_si.admin

Procedimento

1. Para criar um perfil para um alerta em sua instância Now Platform, navegue até **Microsoft Graph Security API Integration** > **Perfil da API de Segurança do Microsoft Graph**.
2. Clique em **Nova**.
3. Preencha os campos.

   Um exemplo de formulário preenchido segue a tabela.

   A figura a seguir é um exemplo de um formulário preenchido.



O que Fazer Depois

A próxima etapa é mapear os campos de alerta.

Mapeamento de campos de alerta para integração de ingestão de alertas da API de segurança do Microsoft Graph

Depois de identificar as origens para ingestão de alerta programada, a próxima etapa é mapear campos de alerta individuais para os campos em um incidente de segurança Now Platform SIR.

Para a etapa de mapeamento, você deve primeiro ingerir alertas de amostra do locatário Microsoft Azure. Em seguida, você deve garantir que todos os dados de campo de alerta relevantes sejam mapeados para o local apropriado no formulário de incidente SIR e, em seguida, visualizar o incidente SIR na seção de visualização.

O mapeamento dos campos de alerta de amostra envolve o seguinte:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Ingerir alertas de amostra da API de segurança do Microsoft Graph
- Mapeamento de alertas para campos de resposta a incidentes de segurança

Ingerir alertas de amostra da API de segurança do Microsoft Graph

Inclua alertas de amostra do seu locatário Microsoft Azure.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

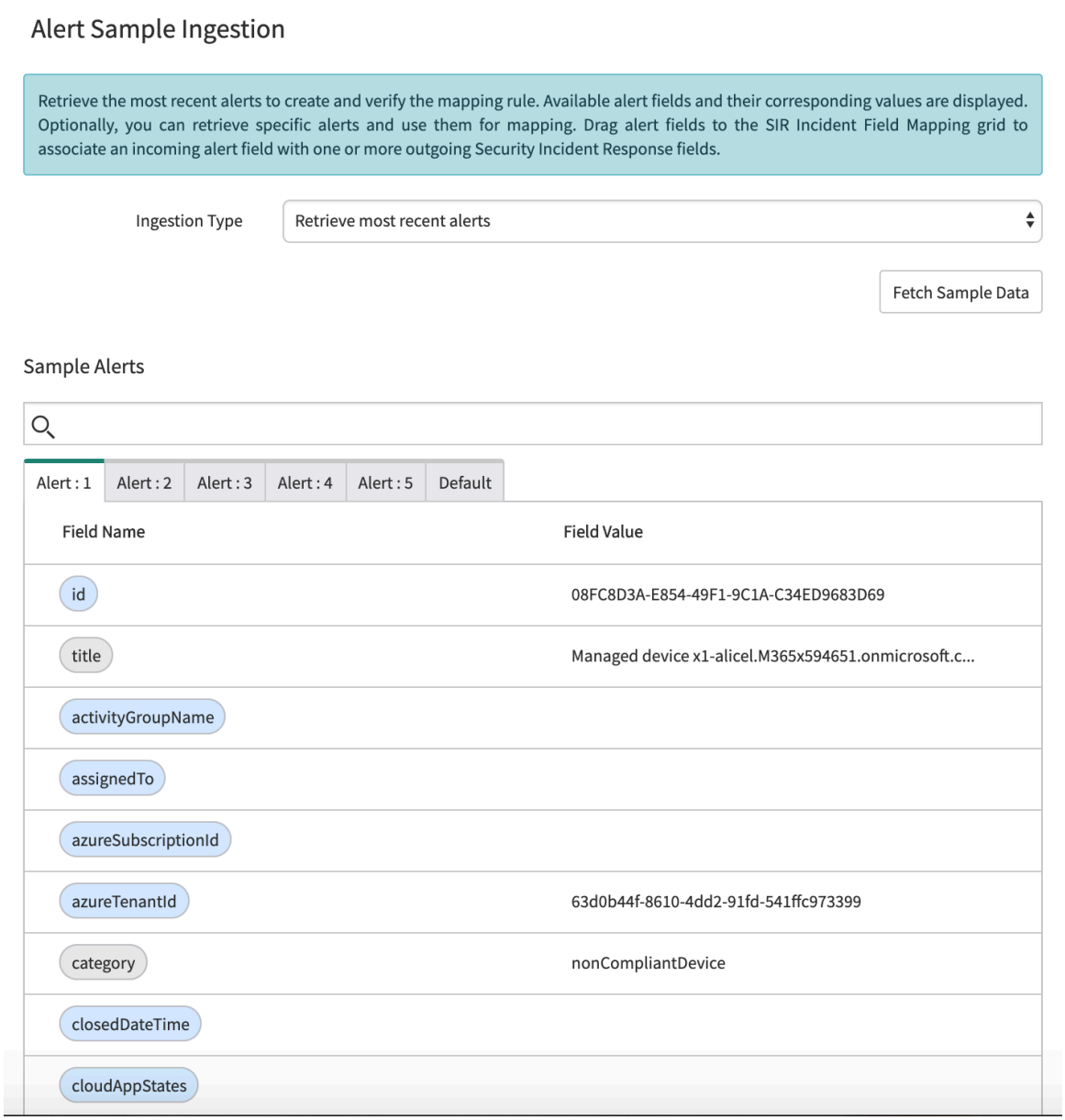
1. Você pode extrair os 5 alertas de amostra mais recentes ou fornecer os IDs de alerta exclusivos para os alertas específicos que deseja usar para sua experiência de mapeamento.
   Na lista de seleção **Preferência de ingestão**, selecione uma das seguintes opções:
   - Recuperar alertas mais recentes: os 5 alertas mais recentes são recuperados.
   - Selecionar alertas com base no ID de alertas: especifique o ID dos alertas a serem recuperados. Você pode especificar no máximo 5 IDs de alerta separados por vírgulas.
2. Clique em **Buscar dados de amostra** para extrair os dados de alerta de amostra mais recentes do locatário Microsoft Azure.
   A extração de alertas de amostra pode levar alguns minutos.

   Os valores do campo de alerta de amostra são preenchidos no lado esquerdo do formulário quando os alertas de amostra são ingeridos pelo perfil. Esses são os alertas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

que você mapeia para os campos de incidente de segurança SIR. Os campos de alerta e os resultados dos valores são exibidos como guias individuais.



O que Fazer Depois

Depois de buscar os dados de amostra, a próxima etapa é mapear os campos de alerta para o incidente de segurança.

Mapeamento de alertas para campos de resposta a incidentes de segurança

Mapeie campos de alerta individuais de alertas acionados para campos em um incidente de segurança Now Platform.

Mapeamento de campo de alerta

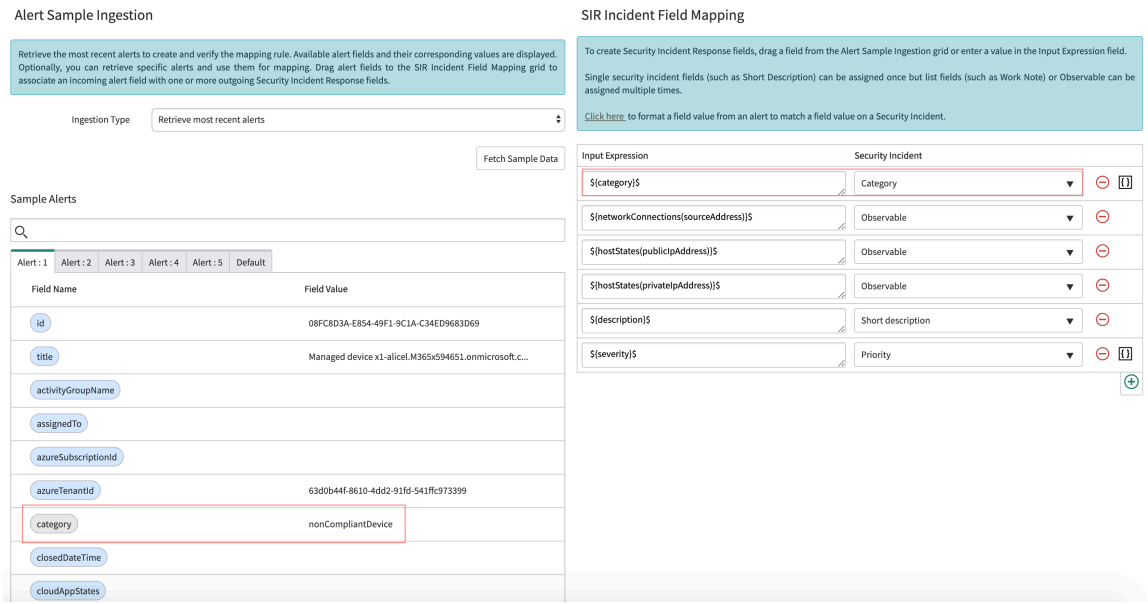
Como um usuário com a função sn_si.admin, use os campos da seção Alertas de amostra à esquerda e mapeie-os para os campos de incidente de segurança na coluna Mapeamento de campo de incidente SIR no painel direito. Edite a configuração de mapeamento arrastando os campos de alerta do lado esquerdo e soltando-os na seção de mapeamento de incidente SIR à direita. O mapeamento à direita associa o campo de alerta de entrada a um campo de incidente de segurança de saída.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Depois de buscar os dados de amostra, a próxima etapa é mapear os campos de alerta para o incidente de segurança. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e mantenha pressionado um nome de campo azul no lado esquerdo do formulário.
2. Arraste o nome do campo, por exemplo, categorye solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.

   O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, a categoria é mapeada para o campo Categoria no incidente de segurança.



No entanto, você pode corresponder qualquer valor do lado esquerdo a um campo do lado direito. Verifique se o valor está mapeado corretamente no incidente de segurança durante a etapa de visualização.

Para ajudar a garantir que nenhum campo de alerta seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. A codificação por cores dos campos de alerta ajuda a rastrear os valores de alerta que você já mapeou conforme eles se tornam esmaecidos, enquanto todos os campos não mapeados restantes aparecem em azul. Isso ajuda a visualizar melhor quais valores de campo foram adicionados ao incidente de segurança e se alguma informação de alerta importante restante permanece não mapeada.

Os campos azul claro à esquerda indicam que um campo de alerta ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de alerta de entrada a mais de um campo em um incidente de segurança. Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação de cores ajuda a rastrear o mapeamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

a. Para inserir manualmente um valor no campo Expressão de entrada, insira-o no formato ${fieldname}$. O campo de alerta será mapeado para o campo de incidente de segurança.

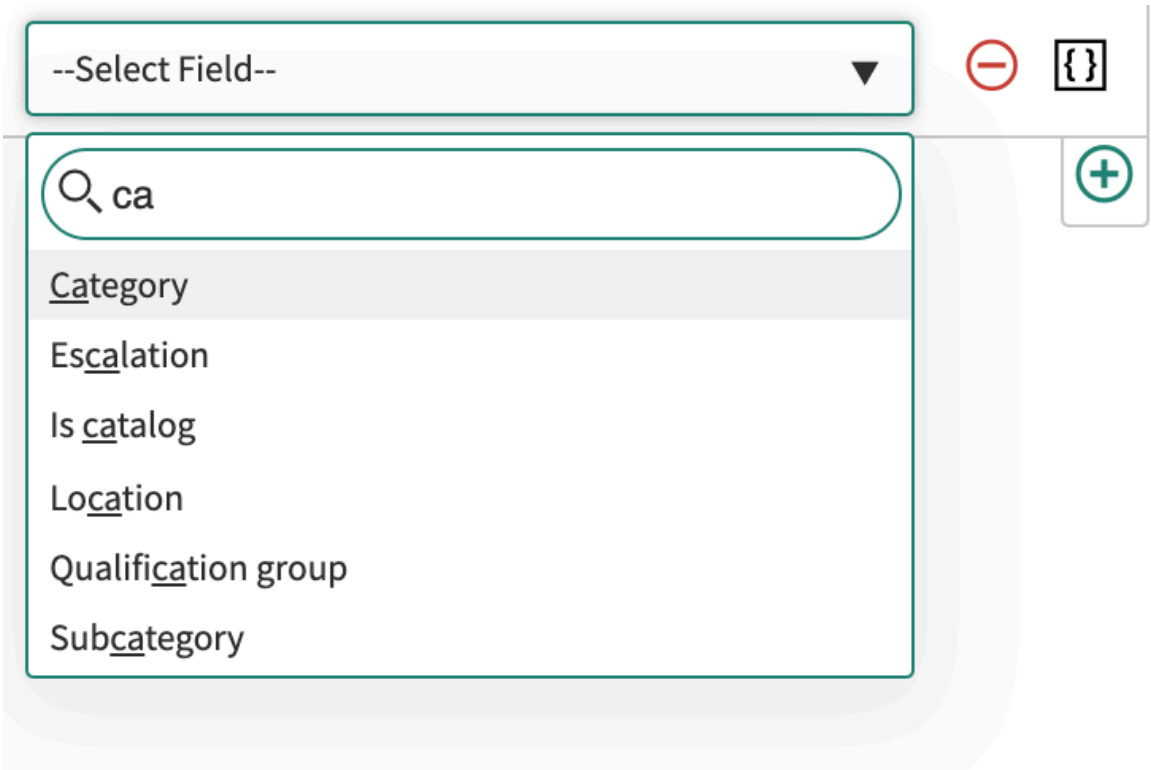
b. Não é possível mapear alertas ingeridos para os campos Estrutura MITRE-ATT&CK na seção de mapeamento de incidente de segurança. Se você ainda mapear os campos, as informações não estarão disponíveis como parte do cartão MITRE-ATT&CK] na seção de estrutura MITRE-ATT&CK no formulário de incidente de segurança. Para associar as técnicas MITRE-ATT&CK, use o recurso de extração automática disponível como parte da estrutura MITRE-ATT&CK] no módulo Inteligência contra ameaças.

3. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas.

a. À direita do formulário na seção SIR Mapeamento de campo de incidente, na parte inferior da grade, clique no ícone de adição (+). Um novo campo é exibido.

b. Na coluna Incidente de segurança, expanda a lista de seleção exibida e selecione um campo.

Na lista de seleção expandida para o novo campo, alguns campos estão sombreados. Na figura a seguir, Categoria tem um plano de fundo cinza porque foi mapeada no incidente de segurança. Semelhante à codificação de cores dos campos de alerta no lado esquerdo do formulário, essa codificação de cores para os campos de incidente de segurança à direita ajuda a rastrear os campos de incidente SIR já mapeados.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Como vários observáveis podem ser exibidos no mesmo incidente de segurança, o campo Observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho oferecem suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, será exibida uma mensagem de erro informando que não há nenhum valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista de seleção na qual você pode escolher várias opções e você tentar mapear uma opção para esse campo que não é exibido na lista de seleção, o campo não será preenchido no incidente de segurança.

c. Como alternativa, digite um valor no campo Pesquisar da nova linha.

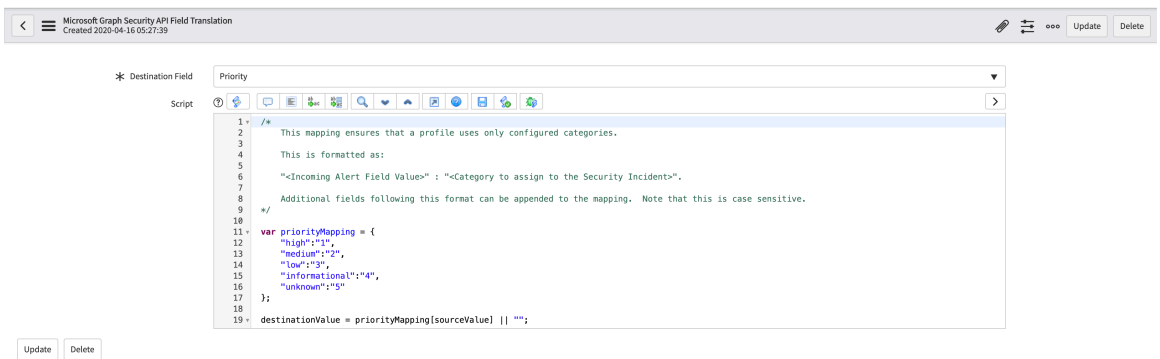
d. No lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar o ID de alerta desejado no campo Expressão de entrada. Com o recurso de arrastar e soltar, mapeie-o ao lado do novo campo.

4. Continue mapeando adicionando ou removendo valores de campo para o mapeamento.
5. Depois de concluir as etapas de mapeamento de campo anteriores, você pode usar os mesmos valores de campo no construtor Condições de geração de incidente para definir critérios adicionais que um alerta de entrada deve satisfazer para criar um incidente de segurança. Para definir condições de geração de incidentes, siga estas etapas.

Formatar tradução de campo

Em determinados casos, os valores do campo de alerta em API de Segurança do Microsoft Graph podem não ser traduzidos diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de script se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de script, um valor de categoria de Alerta de malware e Infecção de vírus pode ter valores de campo diferentes para a categoria de origem, mas ambos os valores podem ser convertidos em uma Atividade de código malicioso comum no campo Categoria no incidente de segurança SIR usando o formato Funcionalidade de tradução de campo.

Para usar o editor de script, clique no ícone {}. O editor de script é exibido.



Condições de geração de incidentes

Depois que a seção de mapeamento estiver concluída, você poderá definir condições de filtro para especificar quais alertas devem criar incidentes de segurança e quais alertas devem ser filtrados, por exemplo, alertas de prioridade baixa. Você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que um alerta de entrada deve satisfazer para criar um incidente de segurança. Para definir condições de geração de incidentes, siga estas etapas.

Tradução automática

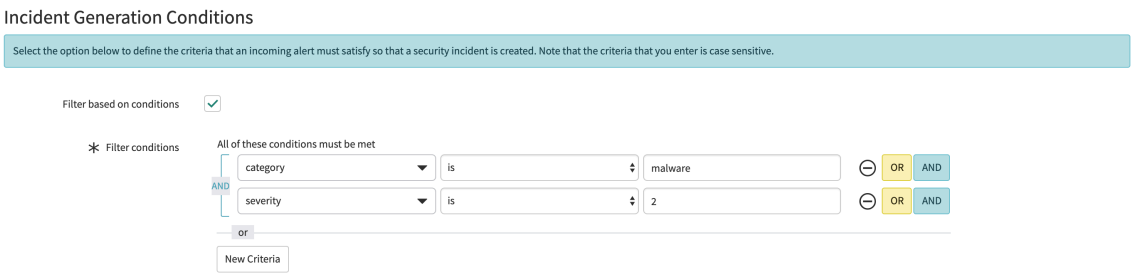
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Role até a seção Condições de geração de incidentes no formulário e selecione a opção Filtrar com base nas condições. O construtor de Condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

   As opções nas listas de seleção para o primeiro campo no construtor de Condições de filtro correspondem aos campos exibidos na seção Ingestão de amostra de alerta para o alerta que você ingeriu. Esses campos são dinâmicos e mudam dependendo do alerta que você ingere. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas e devem corresponder exatamente aos valores do alerta. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao locatário do Microsoft Azure e revisar os alertas para as palavras-chave.

2. Usando as listas de seleção e os campos do construtor de condições, defina filtros para a primeira linha.
3. Para adicionar mais condições, à direita dos campos, clique em **E** ou **OU**.
   - Se **AND**for selecionado, todas as condições deverão ser correspondidas.
   - Se **OU**for selecionado, qualquer uma das condições poderá ser correspondida.
4. Na segunda linha, defina uma segunda condição de filtro

   A imagem a seguir é um exemplo com duas condições que devem ser correspondidas antes que os incidentes de segurança sejam criados.



   Você definiu as condições de gatilho para que os incidentes de segurança sejam criados somente quando ambas as condições de filtragem inseridas forem correspondidas.

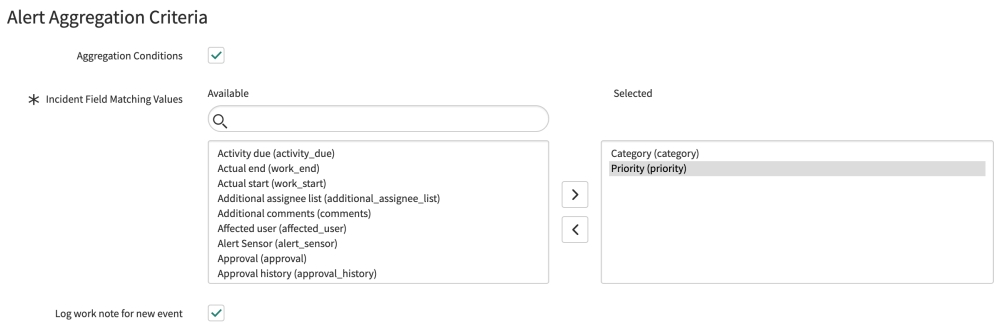
   Esse tipo de filtragem ajuda a isolar alertas de segurança e limita o número de incidentes de segurança que você cria. Se critérios de filtragem adicionais forem definidos, somente os alertas necessários serão ingeridos sem precisar mudar a consulta ou a configuração do alerta acionado.

Critérios de agregação de alertas para lidar com alertas semelhantes e evitar incidentes duplicados

Defina critérios adicionais de agregação de alertas que agregam um alerta de entrada a um incidente de segurança SIR existente em vez de criar incidentes semelhantes, potencialmente duplicados. Usando critérios de valor de correspondência de campo para cada perfil, essa capacidade de agregação adicional pode reduzir o número de incidentes de segurança ativos e sobrepostos, colocando todos os dados de alerta relacionados em um único incidente de segurança. Para definir os critérios, siga estas etapas abaixo:

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Role até a seção Critérios de agregação de alerta no formulário e selecione a opção Condições de agregação. As colunas Valores correspondentes do campo de incidente são exibidas. Esses nomes de campo são os campos no incidente de segurança que incluem todos os campos personalizados que estão configurados no incidente de segurança SIR.
2. Na lista Disponível, selecione os valores de campo que você deseja corresponder aos incidentes de segurança existentes na sua Now Platform e mova-os para a lista Selecionado. Todos os valores de campo selecionados devem ser correspondidos para anexar este alerta de entrada a um incidente de segurança existente. Isso inclui campos, como observáveis e itens de configuração, que podem ter vários valores de campo de alerta mapeados para eles. Todos os valores devem corresponder. Se apenas um subconjunto dos valores for correspondido, as condições de agregação de alerta não serão atendidas e um novo incidente de segurança será criado. Veja a captura de tela abaixo para mapeamento de campo de vários valores.



Se um novo alerta corresponder a todos os valores selecionados nas condições de campo de agregação na etapa de mapeamento, o alerta será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os alertas agregados adicionados em uma lista relacionada em um incidente de segurança. Todos os alertas agregados em um incidente de segurança são exibidos na lista relacionada Alertas agregados do Microsoft Graph. Esta lista detalha os carimbos de data/hora associados e os valores de campos agregados. Essas informações ajudam a entender por que os alertas são adicionados a incidentes de segurança existentes. Se esta guia não for exibida, role até o lado esquerdo do registro em Links relacionados e clique no link **Mostrar todas as listas** relacionadas.

3. (Opcional) Para registrar uma anotação de trabalho para um novo alerta que foi adicionado recentemente ao incidente de segurança, marque a caixa de seleção para habilitar esta opção. A anotação de trabalho registra que um novo alerta foi adicionado junto com um link para os detalhes do alerta e quaisquer outros detalhes que possam ter sido adicionados ao campo de anotação de trabalho na seção de mapeamento.

   Você mapeou com sucesso valores de um alerta para campos em um incidente de segurança SIR. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem. Você também anexou alertas ou eventos a incidentes de segurança SIR existentes.

4. Clique em **Continuar** para prosseguir com a configuração do perfil. A próxima etapa é visualizar os campos mapeados em um incidente de segurança SIR

Visualizar o incidente de segurança para a integração da API de segurança do Microsoft Graph

Depois de concluir a etapa de mapeamento, visualize os valores que você mapeou em um incidente de segurança Now Platform SIR. Esta etapa de visualização permite que

Tradução automática

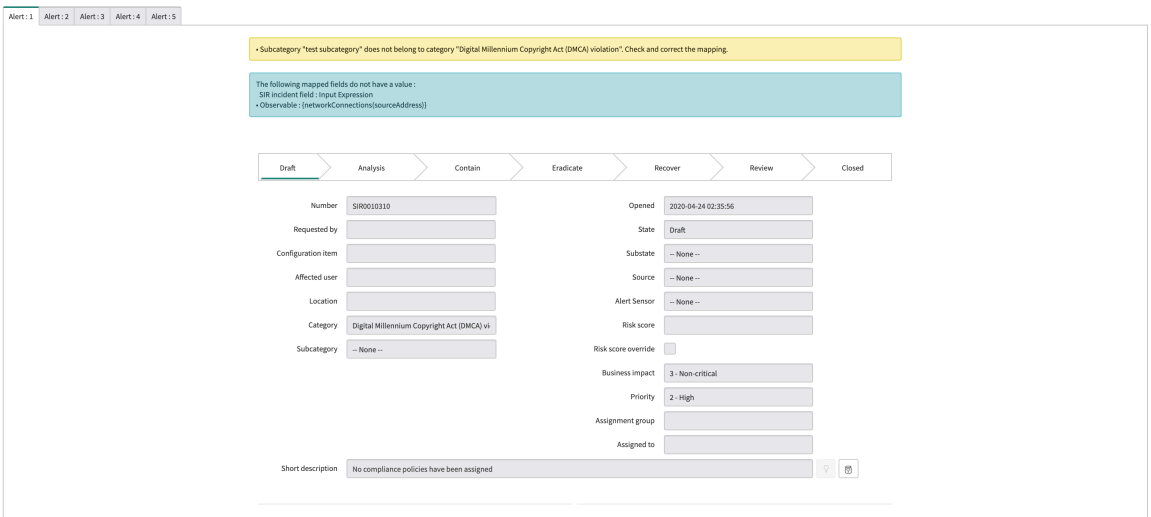
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

você verifique se mapeou todos os campos de alerta que deseja exibir no incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Como um usuário com a função sn_si.admin, visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou para preencher quaisquer dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. As visualizações de SIR incidentes de segurança não são salvas como incidentes reais no produto Security Incident Response.

Procedimento
1. Se a visualização do incidente de segurança não for exibida, clique em **Visualizar** na barra de andamento.
   Todos os alertas ingeridos e os mapeamentos de campo definidos na página Mapeamento são exibidos.
2. Clique em um ID de alerta para ver uma visualização do incidente de segurança.
   Esta exibição é somente leitura e um registro deste incidente de segurança não é salvo.
3. Revise o mapeamento de campo dos valores de alerta no incidente de segurança.



A imagem anterior é um exemplo de uma visualização com um erro de mapeamento das amostras que foram ingeridas.

4. Para resolver esse erro, clique em **Mapeamento** na barra de andamento.
5. Edite o mapeamento para corrigir valores incorretos ou preencha os dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir os erros descritos nas mensagens de erro.

O que Fazer Depois
Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campo no incidente de segurança, a próxima etapa é definir a programação.

Definir programação para integração da API de segurança do Microsoft Graph

Verifique as configurações padrão para recuperação de alerta ou modifique a programação conforme necessário. Esta etapa permite filtrar a recuperação do alerta com base em um intervalo de datas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Você também escolhe com que frequência pesquisará alertas futuros que correspondam à configuração do perfil de alerta. Para perfis de ingestão de alertas automatizados, antes de o perfil ser ativado, você verifica e modifica a programação e a recuperação do alerta. Esta etapa é necessária para perfis de alerta programados.

Como um usuário com a função sn_si.admin, você configura esses intervalos de pesquisa por perfil. O desempenho da integração de ingestão de alertas API de Segurança do Microsoft Graph é afetado pelos diferentes intervalos de pesquisa. Ao programar, talvez você prefira equilibrar a carga do sistema em relação à urgência do incidente. Um valor padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração com base na urgência do incidente e na carga antecipada em seu sistema.

Procedimento

1. Se a página Programação na barra de andamento não for exibida, selecione **Programação**.
2. Escolha um para programar como e quando os alertas são extraídos do locatário Microsoft Azure.
3. Clique em **Continuar** para navegar até a página Opções adicionais.

Automatizar atualizações de alerta e fechamento com base no status do incidente SIR

A integração de ingestão de alertas API de Segurança do Microsoft Graph tem uma interface bidirecional que permite que ambos os alertas criem incidentes de segurança, bem como a capacidade de atualizar os alertas depois que o incidente de segurança é criado e/ou encerrado com detalhes relevantes do incidente, como SIR incidente número, grupo de atribuição, SIR URL do incidente e assim por diante. Esta seção é a parte final da configuração do perfil que fornece recursos opcionais para atualizar os alertas.

Antes de Iniciar
Função necessária: sn_si.admin

Nota:
Os status de alerta inicial e de fechamento serão atualizados somente se esta funcionalidade for compatível com o provedor de serviços. Para obter detalhes, consulte a documentação API de Segurança do Microsoft Graph e a documentação do provedor de segurança.

Procedimento

1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais**.
2. Siga as instruções abaixo para concluir a configuração de atualização de alertas quando o incidente de segurança for criado.
3. Clique em **Concluir** para concluir a configuração e mover o perfil para o estado **Aguardando**.
   Uma caixa de diálogo de confirmação é exibida. Você concluiu com êxito a instalação e a configuração da integração. Ative este perfil para extrair alertas do locatário Microsoft Azure com base na sua programação. Um máximo de 1.000 incidentes de segurança podem ser criados em um período de 24 horas.

Definições de configuração de integração da API de segurança do Microsoft Graph

Use esta opção para modificar as propriedades do sistema padrão de integração de ingestão API de Segurança do Microsoft Graph.

Tradução automática

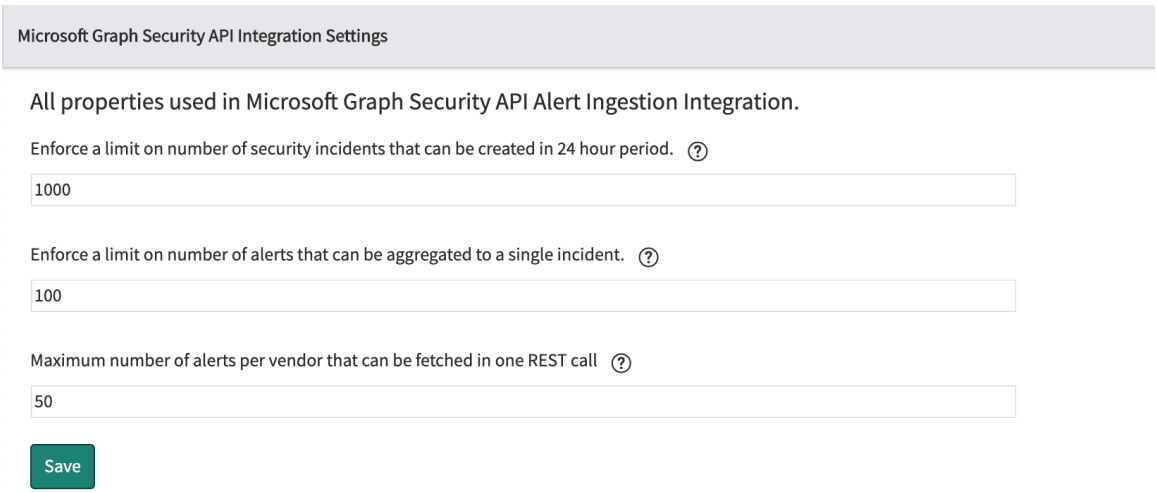
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Modifique as propriedades de configuração padrão para limitar o número de incidentes de segurança que podem ser criados durante um período de 24 horas ou o número de alertas que podem ser agregados em um incidente de segurança.

Para modificar as propriedades do sistema, faça login como um usuário com a função *sn_si.admin* e navegue até **Microsoft Graph Security API Integration** > **Configurações de integração da API de segurança do Microsoft Graph**.

As definições de configuração padrão são exibidas. Você pode modificar essas configurações, se necessário.



Todas as configurações de integração modificadas serão aplicadas durante o próximo intervalo de pesquisa, conforme definido no perfil.

Formulário do Security Incident Response após a ingestão do alerta

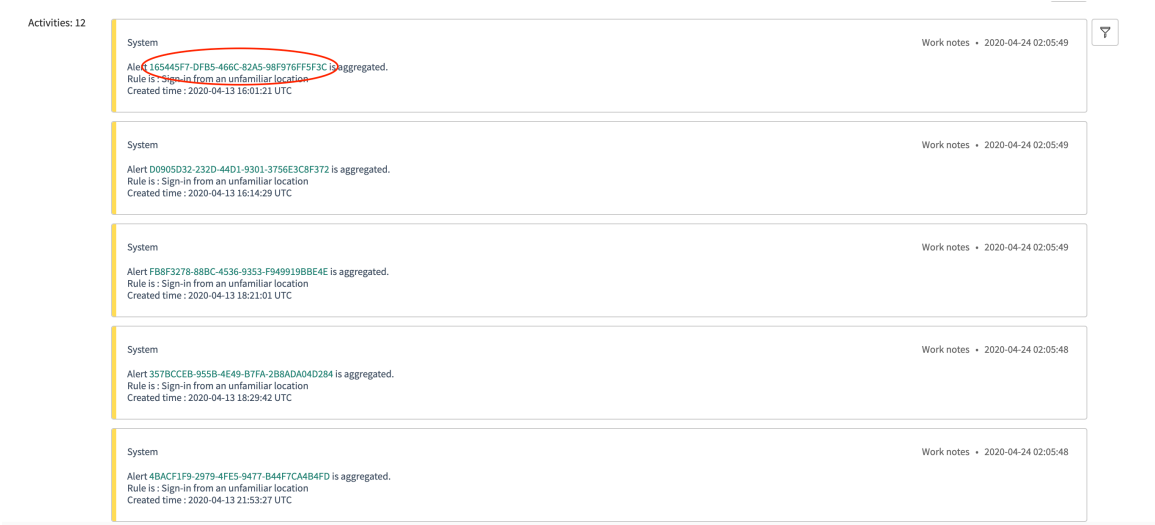
Depois que um alerta API de Segurança do Microsoft Graph tiver sido ingerido, um incidente de segurança será criado e as atualizações correspondentes serão feitas no registro do incidente de segurança.

Anotações de trabalho

Se você tiver selecionado a opção **Registrar anotação de trabalho em log para novo alerta** nos Critérios de agregação do alerta, conforme descrito em Mapeamento de alertas para campos de resposta a incidentes de segurança, uma anotação de trabalho será publicada quando o alerta for agregado.

Tradução automática

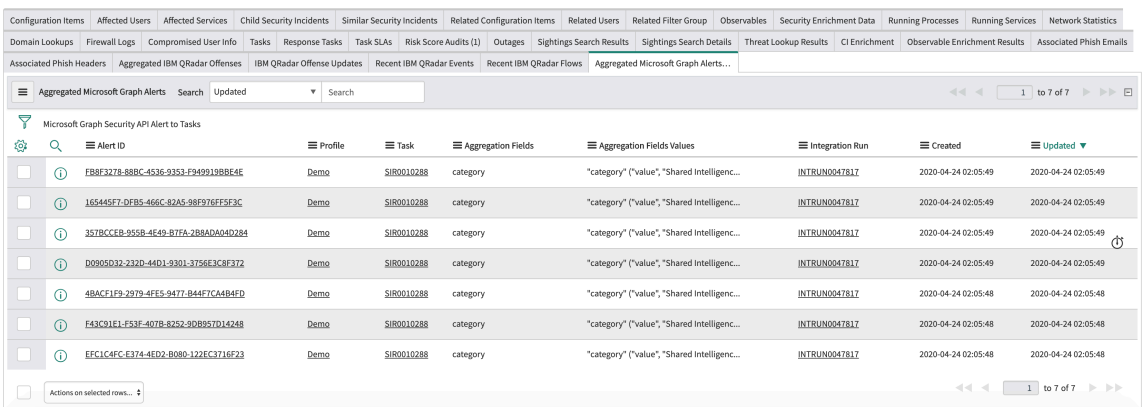
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Clique no link do alerta para navegar até o registro de importação de alerta interno que contém dados brutos de alerta.

Alertas agregados

Clicar **Listas relacionadas** > **Alertas de segurança do Microsoft Graph agregados** para exibir os alertas agregados ao incidente de segurança.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Criar incidente de segurança**: selecione um alerta na lista, clique no menu **Ações** e clique em **Criar incidente de segurança**. Esta opção cria um novo incidente de segurança para o alerta e este alerta é desagregado do incidente de segurança primário.
- **Excluir registro de alerta**: selecione um alerta na lista, clique no menu **Ações** e clique em **Excluir**. Esta opção exclui o registro de alerta.

Opcional: copiar um perfil de API de segurança do Microsoft Graph

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, convém copiar os perfis para economizar tempo.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Como um usuário com a função sn_si.admin, se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado está desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Procedimento

1. Navegar até **Todos** > **Microsoft Graph Security API Integration** > **Perfil da API de Segurança do Microsoft Graph**.
2. Na lista Perfis API de Segurança do Microsoft Graph exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Copiar**.
   O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo o mapeamento e a configuração de programação. O nome do perfil contém cópia. Embora o perfil original esteja habilitado (verdadeiro), a cópia está desabilitada neste ponto (falso). Você pode editar os valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil, conforme necessário.

   Você copiou com sucesso as configurações de um perfil existente para um novo perfil. Observe que o status da coluna **Ativa** está definido como falso, pois o perfil precisa ser ativado.

O que Fazer Depois

Você será solicitado a ativar (habilitar) o novo perfil depois de concluir as etapas de configuração.

Domain Separation e ingestão de alertas API de Segurança do Microsoft Graph

A separação de domínio é compatível com esta aplicação. A integração API de Segurança do Microsoft Graph ingere alertas dos provedores de segurança do Microsoft Graph e cria automaticamente incidentes de segurança. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Básico

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

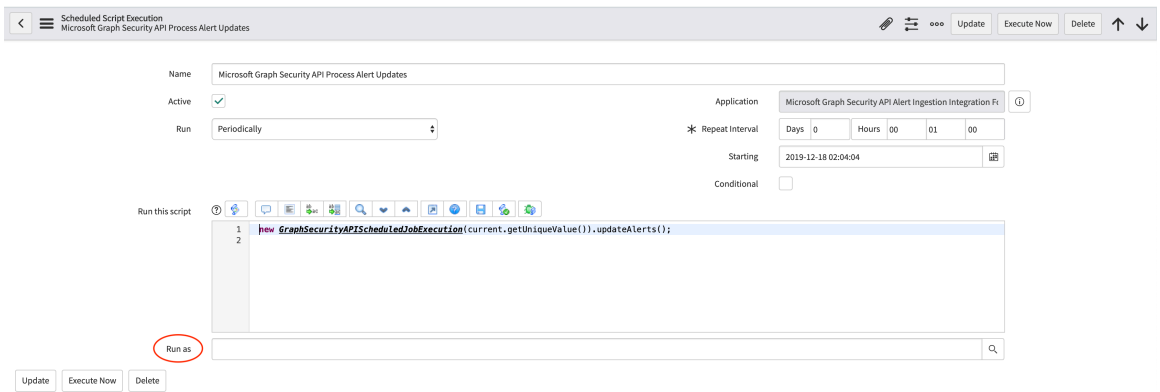
- Lógica de negócios: confirme se os dados vão para o domínio adequado para os casos de uso do provedor de serviço de aplicativo.
- O aplicativo oferece suporte à separação de domínio em tempo de execução. O Domain Separation inclui separação de domínio de interface do usuário, chaves de cache, relatórios, acúmulos e agregações.
- O proprietário da instância deve configurar o aplicativo para funcionar em vários locatários.

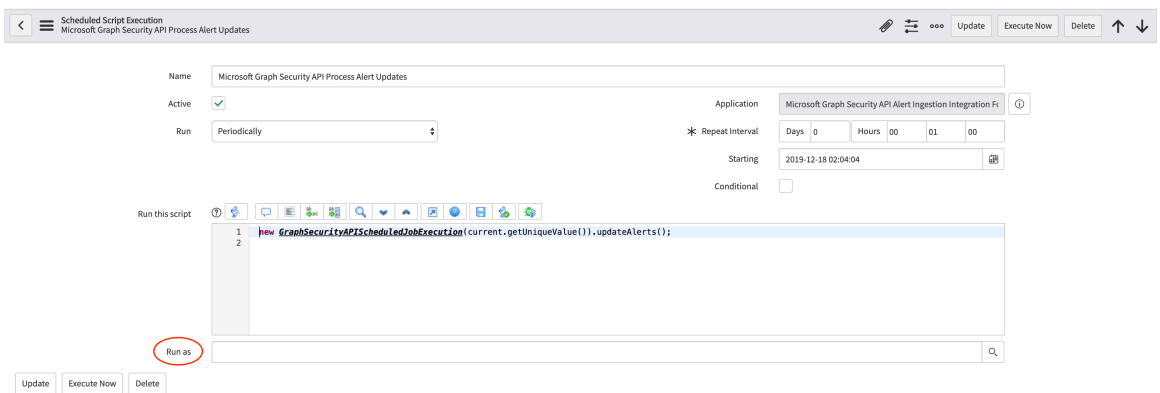
Exemplo de caso de uso: quando um SP (service provider, provedor de serviço) usa o bate-papo para responder à mensagem de um locatário-cliente, o cliente deve conseguir ver a resposta do SP.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como o Domain Separation funciona no API de Segurança do Microsoft Graph

Para obter a separação de domínio, replique os trabalhos programados API de Segurança do Microsoft Graph Processo de perfil e SIR Atualizações de alerta de processo e altere **Executar como** usuários. Por padrão, os usuários do sistema executam esses trabalhos programados. Altere **Executar como** para um usuário com a função sn_si.admin no respectivo domínio e execute o trabalho programado.





Tópicos relacionados

Domain Separation para provedores de serviço

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uso do Flow Designer e do Hub de integração na integração da API de segurança do Microsoft Graph

Usando a funcionalidade Flow Designer e Hub de integração, vários subfluxos e ações foram criados como parte da integração API de Segurança do Microsoft Graph.

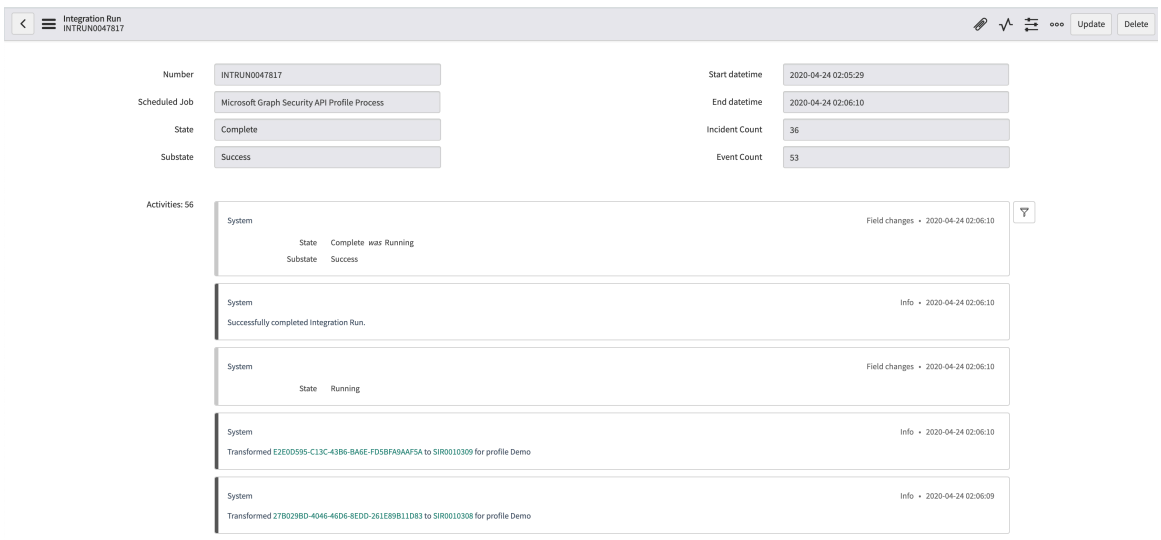
Os seguintes subfluxos estão disponíveis:

- API de Segurança do Microsoft Graph Validação de configuração: usada no bloco de configuração para validar as credenciais na configuração inicial.
- Chamada REST para API de Segurança do Microsoft Graph: isso é usado para todas as interações com a API de segurança do Microsoft Graph usando chamadas REST.
- Recuperar alertas de amostra: isso é usado na seção Mapeamento da configuração do perfil para buscar dados de amostra. Este subfluxo é acionado de forma assíncrona.

Solução de problemas da integração da API de segurança do Microsoft Graph

Esta seção aborda dicas importantes de solução de problemas e perguntas frequentes relacionadas à integração de ingestão de alertas API de Segurança do Microsoft Graph.

- **Execução de integração**: quando um trabalho programado começa a ser executado, um registro de execução de integração com logs, erros e avisos é exibido. O número de alertas extraídos e o número de incidentes criados em uma execução de trabalho programada também são exibidos. Usuários com a função sn_si.analyst podem ver se houve falha na extração de erros/perfis durante a execução da integração. Usuários com a função sn_si.analyst podem verificar a tabela sn_event_ingestion_integration_run em busca de erros ocorridos. Para solucionar problemas de integração, você deve primeiro verificar a execução da integração. Os erros são registrados como anotações de trabalho nos registros de execução de integração para cada execução de trabalho programada.



- **Perfil incompleto**: ao configurar o perfil, na seção Opções adicionais (Automatizar atualizações de alerta e fechamento com base no status do incidente SIR), você deve clicar no botão **Concluir** para garantir que o perfil seja movido para o estado Aguardando, indicando que está aguardando a ingestão.
- **Validar perfil**: para validar se a integração está funcionando corretamente, verifique os estados do perfil, a data da última extração do perfil, a tabela de importação de alertas, o alerta para os registros da tabela de tarefas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Problemas de SSL**: ao se conectar por meio de API de Segurança do Microsoft Graph, certifique-se de que a instância tenha um certificado de CA válido que não tenha expirado. Você pode importar o RSA ou seus próprios certificados para a plataforma e garantir que o nome comum do certificado corresponda ao nome do host. Consulte KB0778285 para obter detalhes.

Integração de Palo Alto Networks - AutoFocus

O sistema de base de integração Palo Alto Networks - AutoFocus inclui um fluxo de trabalho e uma série de atividades de fluxo de trabalho que você pode usar para integrar Palo Alto Networks - AutoFocus com sua instância.

Explorar Integrações do Security Incident Response	**Configurar** Ativar e configurar a integração Palo Alto Networks - AutoFocus
Usar • Security Operations Palo Alto Networks - Fluxo de trabalho de verificar e bloquear valor • Obter fluxo de trabalho de aprimoramento de informações da sessão do AutoFocus	**Desenvolver** • ServiceNow Security Operations diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Faça ou responda perguntas na comunidade do Security Operations • Pesquise artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Ativar e configurar a integração Palo Alto Networks - AutoFocus

O recurso Configuração de integração permite que você ative e configure rapidamente integrações de segurança de terceiros, incluindo Palo Alto Networks - AutoFocus. Antes de usar o Palo Alto Networks - AutoFocus, você deve baixá-lo do ServiceNow Store.

Antes de Iniciar

Função necessária: sn_si_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Baixe uma aplicação de ServiceNow Store pela primeira vez.
2. Quando a instalação estiver concluída, acesse o site de suporte da Palo Alto Networks e obtenha a chave de API.
3. Em sua instância, navegue até **Security Operations** > **Configuração de Integração**.
4. No cartão AutoFocus da Palo Alto Networks, clique em **Configurar**.
5. Insira (ou cole) a **chave de API** que você adquiriu no site de suporte da Palo Alto Networks.
6. Clique em **Enviar**.

Obter fluxo de trabalho de aprimoramento de informações da sessão do AutoFocus

Quando o fluxo de trabalho **Security Operations Palo Alto Networks - Obter aprimoramento de informações da sessão do AutoFocus** é executado, ele enfileira uma consulta de pesquisa com o AutoFocus para coletar informações sobre um IP de origem especificado. Se o AutoFocus tiver conhecimento sobre as sessões anteriores originadas desse endereço IP, um relatório no formato JSON será retornado.

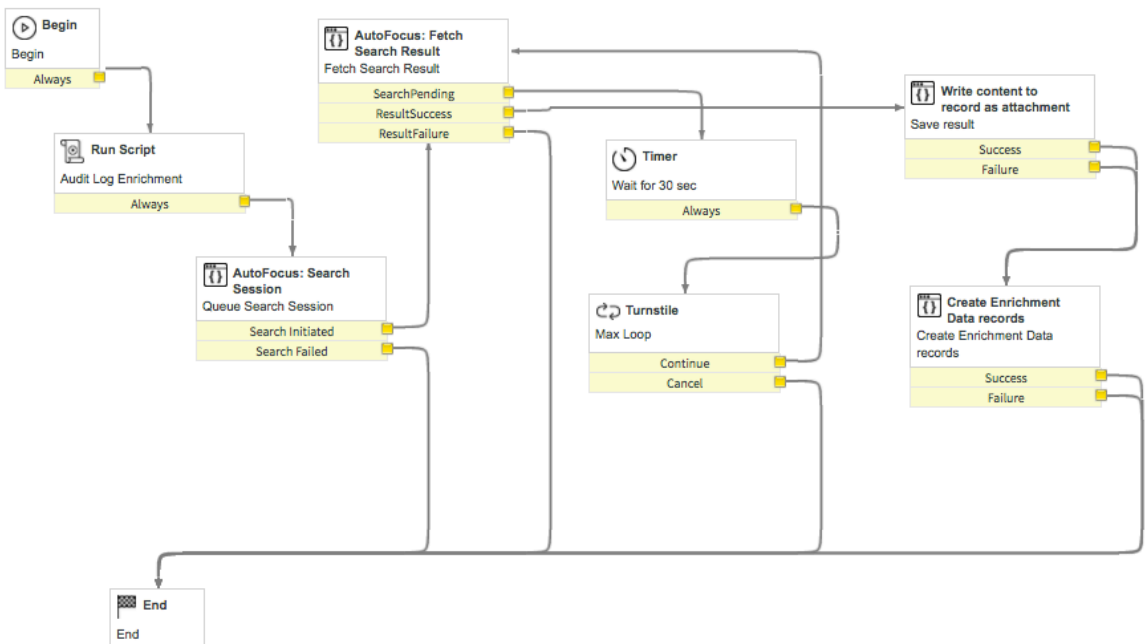
Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho **Security Operations Palo Alto Networks - Obter aprimoramento de informações da sessão do AutoFocus** é executado quando o campo **IP de origem** em um incidente de segurança é modificado e o registro é atualizado. O fluxo de trabalho busca o endereço IP e envia uma solicitação de consulta para o AutoFocus. Se o AutoFocus tiver identificado anteriormente sessões originadas do endereço IP, um relatório no formato JSON será retornado.

Security Operations Palo Alto Networks - Obter fluxo de trabalho de aprimoramento de dados do Wildfire



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar incidentes em aberto**.
2. Clique na guia **Indicadores de comprometimento** e preencha o campo **IP de origem**.
3. Clique em **Atualizar**.
   O AutoFocus verifica as informações do endereço IP e um arquivo de texto no formato JSON é anexado ao incidente de segurança.

   Atividades específicas para esta integração são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Atividade de sessão de pesquisa do AutoFocus

A atividade de fluxo de trabalho **Sessão de pesquisa do AutoFocus** carrega informações de um endereço IP atribuído a um incidente de segurança para o AutoFocus e o enfileira para uma consulta de pesquisa.

Variáveis de entrada

Nota:

Quando a atividade é executada, ela enfileira uma consulta de pesquisa com AutoFocus para coletar informações para um IP de origem especificado. Se o AutoFocus tiver identificado anteriormente sessões originadas desse endereço IP, um relatório no formato JSON será retornado.

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
searchSessionQuery [cadeia de caracteres]	A consulta de pesquisa para obter informações da sessão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
requestStatus [booliano]	Verdadeiro se uma consulta de pesquisa foi programada para execução no AutoFocus.
erro [cadeia de caracteres]	O erro, se houver, que ocorreu na atividade.
afcookie [cadeia de caracteres]	Um identificador da consulta de pesquisa do AutoFocus usado pelo Atividade Buscar resultados de pesquisa para recuperar os resultados da pesquisa.

Atividade Buscar resultados de pesquisa

A atividade de fluxo de trabalho **Buscar resultados** de pesquisa busca resultados de pesquisa identificados por um cookie para a consulta de pesquisa iniciada pela atividade de **Sessão de pesquisa** de foco automático.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
afcookie [cadeia de caracteres]	O cookie do AutoFocus para a solicitação de pesquisa gerada pelo Atividade de sessão de pesquisa do AutoFocus.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
searchPendente [Booliano]	Verdadeiro se a solicitação de pesquisa ainda estiver sendo processada no AutoFocus.
resultado [cadeia de caracteres]	Os dados dos resultados da pesquisa.
status [booliano]	Verdadeiro se a pesquisa for concluída e os resultados forem gerados com sucesso.
erro [cadeia de caracteres]	O erro, se houver, que ocorreu na atividade.

Gravar conteúdo para registro como atividade de anexo

Esta atividade grava o conteúdo passado de uma entrada e cria um anexo designado para um determinado registro.

A atividade **Gravar conteúdo para registro como anexo** pode ser usada com qualquer fluxo de trabalho para gravar conteúdo e anexá-lo a um registro.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
nome da tabela [cadeia de caracteres]	O nome da tabela para o registro. Este campo de entrada é obrigatório.
sysid [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de tarefa. Este campo de entrada é obrigatório.
carga	O conteúdo de texto sem formatação a ser gravado como anexo. Este campo de entrada é obrigatório.
nome do arquivo	O nome do arquivo do anexo.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	Indica se a atualização foi bem-sucedida.

Integração de Palo Alto Networks - Firewall

Para executar a integração Palo Alto Networks - Firewall, certifique-se de ter um MID Server configurado com credenciais SSH. Se um firewall ainda não estiver configurado, adicione um.

Explorar

Integrações do Security Incident Response

Configurar

- Ativar e configurar o Palo Alto Networks Firewall Integration
- Configurar credenciais SSH para o MID Server

Usar

Fluxo de trabalho de integração do Security Operations Palo Alto Networks inicializador de firewall

Desenvolver

- ServiceNow Security Operations diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação
- Localizar componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Faça ou responda perguntas na comunidade do Security Operations
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Configurar credenciais SSH para o MID Server

O Firewall da Palo Alto Networks envia chamadas de API para o MID Server. Dessa forma, certifique-se de que as credenciais SSH tenham sido criadas para o MID Server.

Antes de Iniciar

- O plug-in Orchestration deve ser ativado.

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Orquestração** > **Credenciais e Conexões** > **Credenciais**.
2. Clique em **Nova**.
3. Na tela do Interceptador, clique em **Credenciais SSH**.
4. Preencha os campos, conforme necessário.

Credenciais SSH

Campo	Descrição
Nome	Insira um nome para a credencial.
Ativo	Marque esta caixa de seleção para ativar esta credencial.
Aplica-se a	Selecione **Todos os MID servers** ou **MID servers específicos**.
MID Servers	Se você selecionou **MID Servers específicos**, clique no ícone de cadeado e selecione os MID Servers aos quais deseja aplicar essas credenciais.
Ordem	Selecione a ordem na qual as credenciais são testadas pelo servidor. Números menores são testados primeiro.
Nome de usuário	Insira o nome de usuário do usuário associado a essas credenciais, se houver.
Senha	Se você inseriu um **Nome de usuário**, insira a senha do usuário.
Marcador	Insira um marcador a ser usado para critérios de pesquisa. O campo **Marcador** deve conter o mesmo valor que o **Nome**.

Ativar e configurar o Palo Alto Networks Firewall Integration

O recurso Configuração de integração permite que você ative e configure rapidamente integrações de segurança de terceiros, incluindo Palo Alto Networks - Firewall. Antes de usar o Palo Alto Networks - Firewall, você deve baixá-lo do ServiceNow Store.

Antes de Iniciar

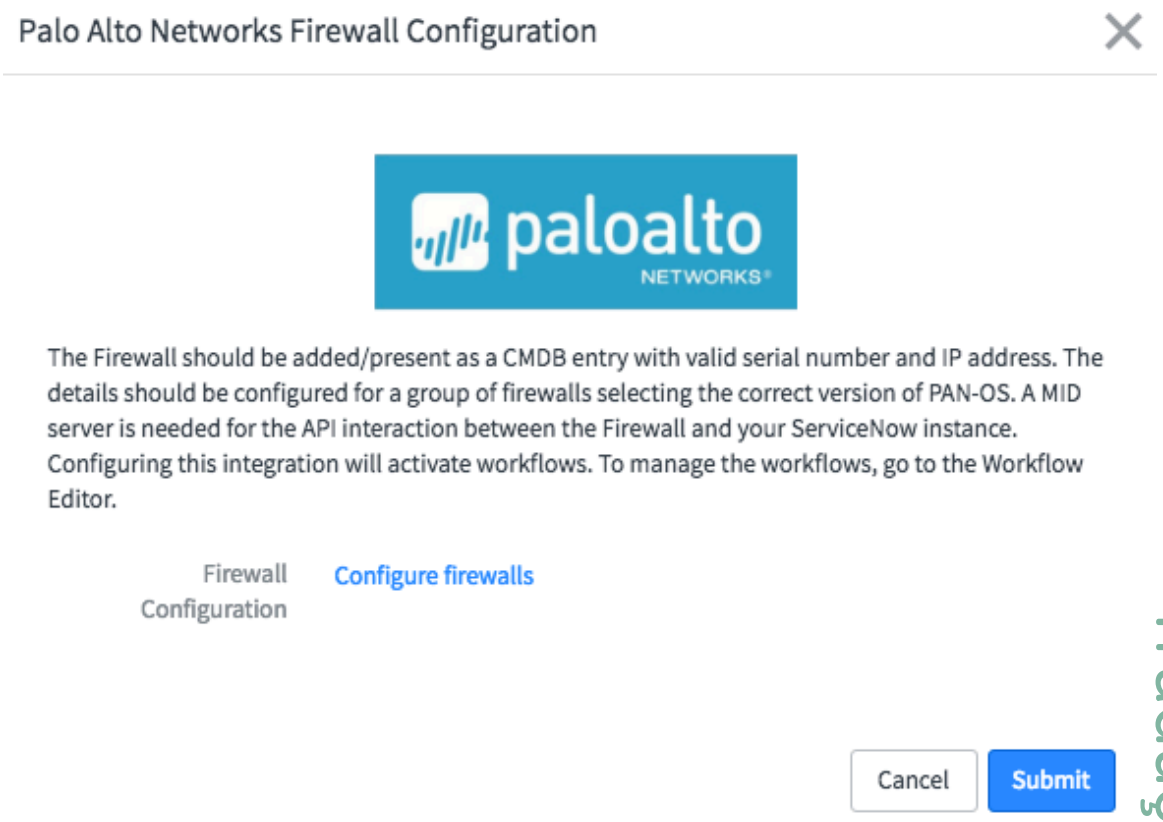
Função necessária: sn_si_admin

Procedimento

1. Antes de ativar e configurar a integração, acesse o painel do Firewall da Palo Alto Networks.
   Anote os nomes da lista dinâmica de IPs, da lista dinâmica de URLs ou da lista dinâmica de domínios que você está usando para o bloqueio de firewall.
2. Baixe a integração do ServiceNow Store.
3. Quando a instalação estiver concluída, navegue até **Security Operations** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
4. Na placa de firewall da Palo Alto Networks, clique em **Configurar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique **em Configurar firewalls**.
6. Na tela Configurações do firewall, clique em **Novo**.
7. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Firewalls	Clique no ícone de cadeado e selecione o firewall a ser configurado.
Versão do firewall	Selecione a versão do Firewall da Palo Alto Networks.**PAN-OS-7.1** é a versão recomendada. Selecionar versões anteriores pode retornar resultados inconsistentes.
Nome do usuário	Insira o nome de usuário a ser usado ao se conectar ao firewall por meio de endpoints REST.
Senha	Insira a senha do usuário de conexão.
Lista Dinâmica de IPs	Insira o nome da Lista Dinâmica Externa ou da Lista de Bloqueios Dinâmicos que você usa para endereços IP.
Lista Dinâmica de URLs	Insira o nome da Lista Dinâmica Externa ou da Lista de Bloqueios Dinâmicos que você usa para URLs.
Lista dinâmica de domínios	Insira o nome da Lista Dinâmica Externa ou da Lista de Bloqueios Dinâmicos que você usa para domínios.

8. Clique em **Enviar**.

Tradução automática

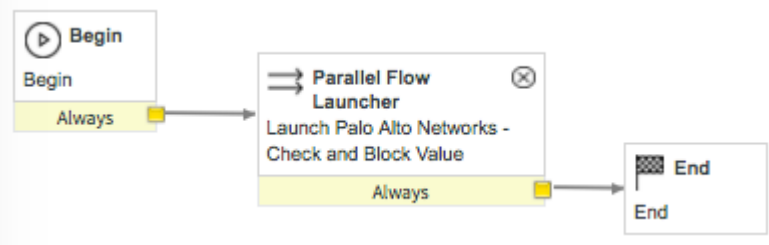
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de integração do Security Operations Palo Alto Networks inicializador de firewall

O fluxo de trabalho do**Security Operations Integration Palo Alto Networks Firewall Launcher** é a implementação do Palo Alto Networks Firewall iniciada pelo fluxo de trabalho do recurso **Security Operations Integration - Block Request**.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:Security Operations Palo Alto Networks - Fluxo de trabalho de verificar e bloquear valor.



Security Operations Palo Alto Networks - Fluxo de trabalho de verificar e bloquear valor

Conforme os incidentes de segurança são criados e triados para identificar possíveis ameaças, você pode usar o fluxo de trabalho **Security Operations Palo Alto Networks - Verificar e bloquear valor** para verificar e atualizar automaticamente endereços IP, URLs e domínios usando listas dinâmicas externas definidas em Palo Alto Networks - Firewall.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
O fluxo de trabalho **Security Operations Palo Alto Networks - Verificar e Bloquear Valor** é executado quando as Solicitações de Bloqueio de Firewall são enviadas. A solicitação de bloqueio especifica o firewall a ser usado, o tipo de observável a ser verificado e bloqueado (se necessário) e o valor do bloqueio. Ou seja, o endereço IP, a URL ou o domínio em questão.

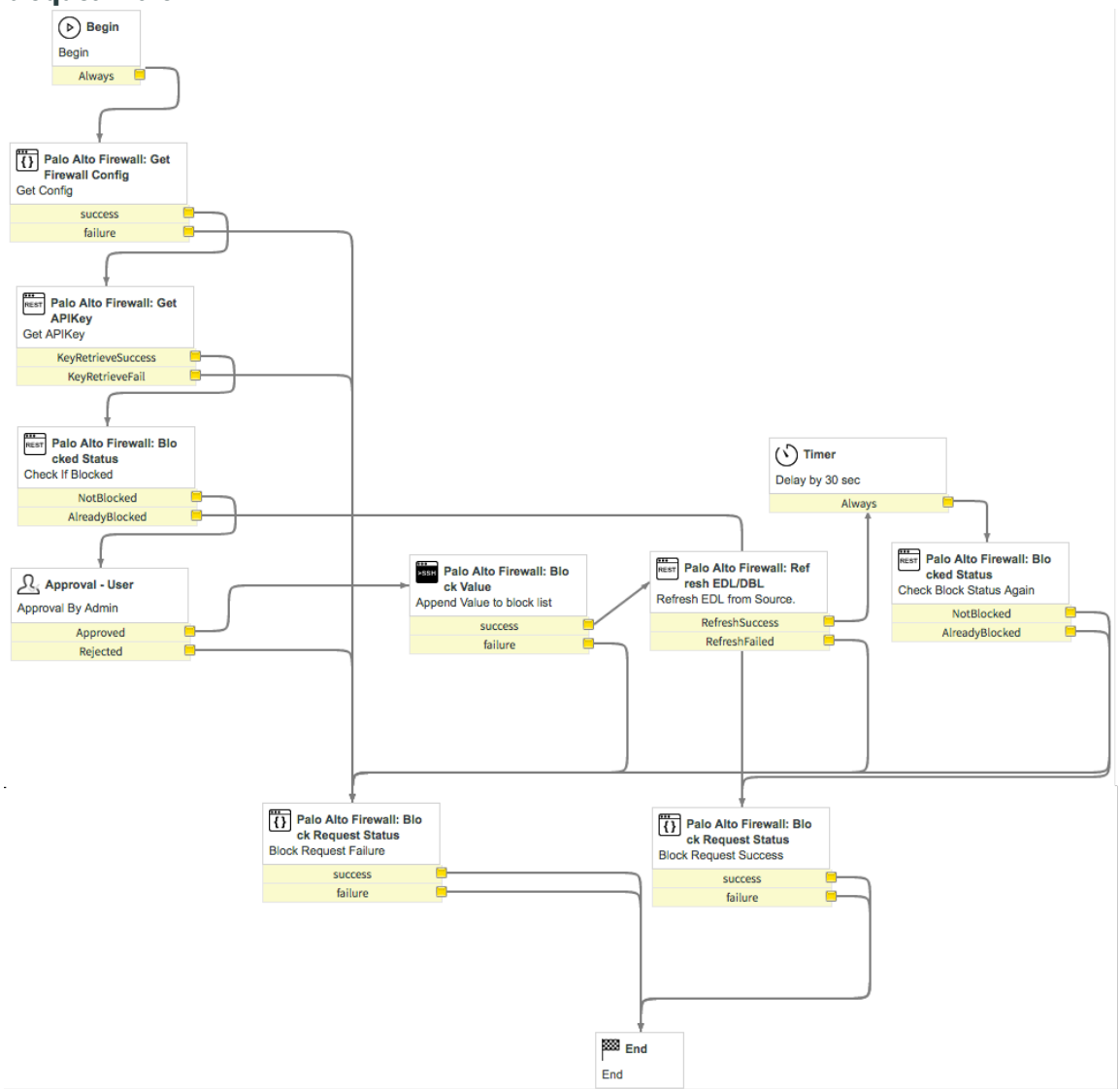
Durante a execução do fluxo de trabalho, os comandos definidos em **Palo Alto Networks Integration** > **Firewall** > **Comandos** são executados. Os comandos Mostrar tipo (por exemplo, Mostrar-IP-ExternalDynamicList) determinam se o valor existe no firewall. Os comandos de tipo de atualização (por exemplo, Atualizar-IP-ExternalDynamicList) adicionam valores que não existem no firewall à lista de bloqueios.

Depois que a atividade de Status bloqueado é executada, a aprovação de um administrador do sistema é necessária antes que o fluxo de trabalho possa prosseguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Security Operations Palo Alto Networks - Fluxo de trabalho de verificar e bloquear valor



Procedimento

1. Navegar até **Palo Alto Networks Integration** > **Firewall** > **Solicitações de bloqueio**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Firewall	Selecione o firewall a ser usado.
Tipo de bloco	Selecione o tipo de valor a ser verificado: ○ IP ○ URL ○ DOMÍNIO

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Valor do bloco	Insira o valor do tipo selecionado a ser verificado no firewall.

4. Clique em **Enviar**.

Firewall de Palo Alto - Atividade Bloquear status da solicitação

Esta atividade é chamada por outras atividades para definir o status da solicitação de bloqueio do Firewall como sucesso ou falha.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
firewallBlockRequestSysid [cadeia de caracteres]	O ID do sistema da solicitação de bloqueio do firewall. Esta variável de entrada é obrigatória.
status [cadeia de caracteres]	Indica se o trabalho de atualização foi executado: sucesso ou falha.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	Indica se o trabalho de atualização foi bem-sucedido ou não.

Firewall de Palo Alto - Atividade Bloquear valor

Depois que o fluxo de trabalho identifica um valor que não está no firewall, o registro é roteado para aprovação. Após a aprovação, esta atividade se conecta ao MID Server por meio de suas credenciais SSH e invoca um script que adiciona o valor à lista de bloqueios externos do firewall.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Nota:
Você deve inserir manualmente as variáveis de entrada para esta atividade e publicar o fluxo de trabalho. Se o fluxo de trabalho não for publicado, as variáveis de entrada não serão salvas para usuários que não sejam administradores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
toBeBlockedValue [cadeia de caracteres]	O valor a ser adicionado à EDL se ainda não estiver presente. Esta variável de entrada é obrigatória.
typeToBeBlocked [cadeia de caracteres]	O tipo de valor a ser bloqueado: IP, URL ou domínio. Esta variável de entrada é obrigatória.
targetHost [cadeia de caracteres]	O MID Server no qual o script é executado.
SSHCredentialTag [cadeia de caracteres]	O marcador de credencial SSH definido no MID Server.
scriptCommand [cadeia de caracteres]	O script AppendValueToList.sh usado para adicionar o valor à EDL. Requer o caminho completo para o MID Server.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	O resultado passado para a EDL.

Firewall Palo Alto - Atividade de status bloqueado

Esta atividade verifica se o valor (IP, URL ou domínio) está incluído em sua respectiva lista dinâmica externa/lista de bloqueios dinâmicos (EDL/DBL) no firewall. Os detalhes de EDL/DBL são obtidos do firewall usando um comando operacional e uma rotina é realizada para verificar se o valor está bloqueado no firewall.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade. Todas as entradas de variáveis de entrada listadas são obrigatórias.

Variáveis de entrada

Variável	Descrição
valueToBeChecked [cadeia de caracteres]	O valor na solicitação de bloqueio.
showEDLDetailsCommand [cadeia de caracteres]	O comando Lista dinâmica externa que está sendo usado para determinar se o valor existe no firewall.
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall usado.
FirewallApiKey [cadeia de caracteres]	A chave de API do firewall.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como dados gerados dinamicamente usando a mensagem da API Palo Alto Firewall Operational Command.

Variáveis de saída

Variável	Descrição
commandResultado [cadeia de caracteres]	Os resultados do firewall para o comando mostrar detalhes do EDL.
blockStatus [booliano]	Verdadeiro indica bloqueado. Falso indica não bloqueado.
commandResponse [cadeia de caracteres]	O status da resposta obtido do firewall para o comando mostrar detalhes do EDL.

Firewall de Palo Alto: obter atividade de chave de API

Esta atividade recupera a chave de API do firewall.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade. Todas as entradas de variáveis de entrada listadas são obrigatórias.

Variáveis de entrada

Variável	Descrição
Nome de usuário [string]	O nome de usuário do administrador do firewall.
Senha [cadeia de caracteres]	A senha do administrador do firewall.
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
APIKey [cadeia de caracteres]	A chave de API do firewall.

Firewall de Palo Alto: atividade Obter configuração de firewall

A atividade de fluxo de trabalho **Firewall de Palo Alto: Obter configuração de firewall** obtém todas as informações de configuração de firewall relacionadas do banco de dados e as disponibiliza para uso pela atividade subsequente.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
firewallSysid [cadeia de caracteres]	O ID do sistema do firewall. Esta variável de entrada é obrigatória.
typeOfValueToBeBlocked [cadeia de caracteres]	O tipo de valor a ser bloqueado no firewall: IP, URL ou domínio.
firewallIPAddress [cadeia de caracteres]	O endereço IP do firewall.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
ipEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para endereços IP.
urlEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para URLs.
domainEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para domínios.
firewallVersionSysId [cadeia de caracteres]	O ID do sistema para a versão do firewall.
refreshEDLCommand [cadeia de caracteres]	O comando a ser usado para atualizar a EDL da origem.
ShowEDLDetailsCommand [cadeia de caracteres]	O comando a ser usado para obter os detalhes da EDL.
status [booliano]	Verdadeiro indica sucesso. Falso indica falha.
erro [cadeia de caracteres]	O erro, se houver, que ocorreu na atividade.
endpoint [Criptografado]	O endpoint criptografado do banco de dados.

Tradução automática

Firewall Palo Alto - Atualizar atividade de EDL/DBL

Esta atividade executa um comando operacional no firewall para atualizar a lista dinâmica externa da origem configurada no firewall. A saída desta atividade indica se o trabalho de atualização foi enfileirado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade. Todas as entradas de variáveis de entrada listadas são obrigatórias.

Variáveis de entrada

Variável	Descrição
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall que está sendo atualizado.
FirewallApiKey [cadeia de caracteres]	A chave de API do firewall atualizada.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
FirewallCommand [cadeia de caracteres]	O comando operacional a ser executado para colocar o trabalho de atualização na fila.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
activity.Output.result [cadeia de caracteres]	Uma cadeia de caracteres de texto para indicar se o trabalho de atualização foi enfileirado para ser executado: sucesso ou falha.

Fluxo de trabalho Obter dados de log

Se Security Incident Response, Inteligência contra ameaçase Palo Alto Networks - Firewall estiverem ativados, o fluxo de trabalho **Security Operations Palo Alto Networks - Obter dados de log** será executado automaticamente quando o IP de origem dos observáveis em um incidente de segurança for alterado.

Antes de Iniciar

Função necessária: sn_si.analyst

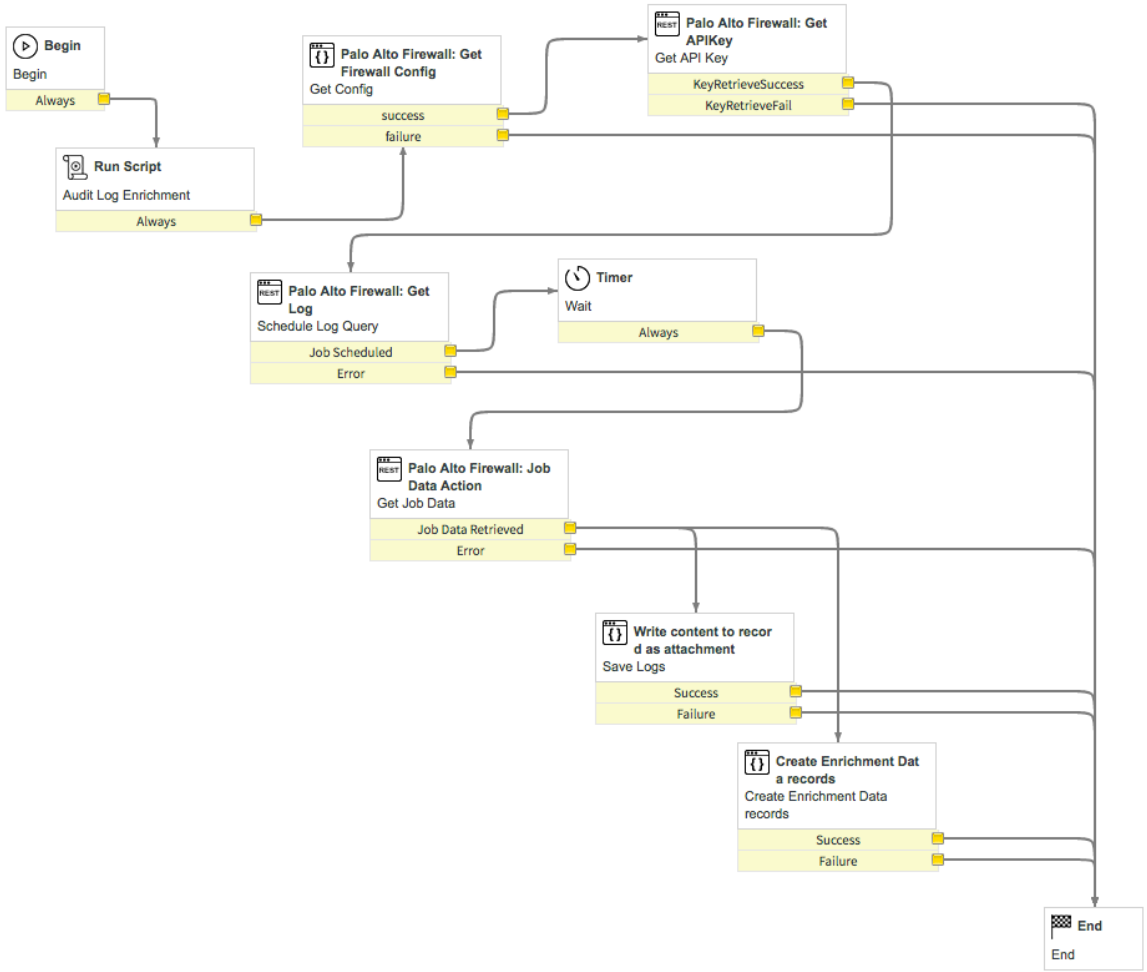
Por Que e Quando Desempenhar Esta Tarefa

Durante a execução do fluxo de trabalho, as informações de configuração do firewall são recuperadas do banco de dados e a chave de API é recuperada do firewall. A atividade Obter log enfileira uma consulta de pesquisa no firewall. Quando a consulta é executada, ela retorna um ID de trabalho que é usado para recuperar dados de logs de ameaça do firewall. Ele anexa os dados do log como um arquivo XML ao incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Security Operations Palo Alto Networks - Obter fluxo de trabalho de dados de log



Procedimento

1. Navegue até um incidente de segurança que contenha observáveis.
2. Clique na guia **Observáveis de incidente de segurança**.
3. Em **IP de origem**, adicione ou modifique o endereço IP.
4. Clique em **Atualizar**.
   O fluxo de trabalho **Security Operations Palo Alto Networks - Obter dados** de log é executado e os dados de log de ameaças aprimorados são anexados ao incidente de segurança. As informações também são analisadas e exibidas na seção **Logs de firewall** na guia **Dados** de aprimoramento.

Firewall de Palo Alto: obter atividade de chave de API

Esta atividade recupera a chave de API do firewall.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade. Todas as entradas de variáveis de entrada listadas são obrigatórias.

Variáveis de entrada

Variável	Descrição
Nome de usuário [string]	O nome de usuário do administrador do firewall.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
Senha [cadeia de caracteres]	A senha do administrador do firewall.
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
APIKey [cadeia de caracteres]	A chave de API do firewall.

Firewall de Palo Alto: atividade Obter configuração de firewall

A atividade de fluxo de trabalho **Firewall de Palo Alto: Obter configuração de firewall** obtém todas as informações de configuração de firewall relacionadas do banco de dados e as disponibiliza para uso pela atividade subsequente.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
firewallSysid [cadeia de caracteres]	O ID do sistema do firewall. Esta variável de entrada é obrigatória.
typeOfValueToBeBlocked [cadeia de caracteres]	O tipo de valor a ser bloqueado no firewall: IP, URL ou domínio.
firewallIPAddress [cadeia de caracteres]	O endereço IP do firewall.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
ipEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para endereços IP.
urlEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para URLs.
domainEDLName [cadeia de caracteres]	O nome da lista dinâmica externa para domínios.
firewallVersionSysId [cadeia de caracteres]	O ID do sistema para a versão do firewall.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
refreshEDLCommand [cadeia de caracteres]	O comando a ser usado para atualizar a EDL da origem.
ShowEDLDetailsCommand [cadeia de caracteres]	O comando a ser usado para obter os detalhes da EDL.
status [booliano]	Verdadeiro indica sucesso. Falso indica falha.
erro [cadeia de caracteres]	O erro, se houver, que ocorreu na atividade.
endpoint [Criptografado]	O endpoint criptografado do banco de dados.

Firewall Palo Alto - Obter atividade de log

A atividade de fluxo de trabalho **Firewall Palo Alto: Obter log** programa uma consulta no firewall para recuperar logs e retorna um JobID usado para recuperar os dados do log.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall. Esta variável de entrada é obrigatória.
FirewallApiKey [cadeia de caracteres]	A chave de acesso à API do firewall. Esta variável de entrada é obrigatória.
FirewallLogType [cadeia de caracteres]	O tipo de dados de log a serem recuperados (definido como ameaça). Esta variável de entrada é obrigatória.
FirewallLogFilterQuery [cadeia de caracteres]	A consulta a ser executada para pesquisar logs no firewall. Esta variável de entrada é obrigatória.
LogDirection [cadeia de caracteres]	Especifica se os logs são mostrados na ordem mais antiga primeiro (para trás) ou mais recente primeiro (para frente).
LogNumber [cadeia de caracteres]	Especifica o número de logs a serem recuperados.
LogSkipCount [cadeia de caracteres]	Especifica o número de logs a serem ignorados ao fazer uma recuperação de log.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
QueuedJobID [cadeia de caracteres]	O ID do trabalho retornado do firewall.
JobScheduled [cadeia de caracteres]	Especifica (sucesso ou falha) se o trabalho foi enviado para o firewall.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
erro [cadeia de caracteres]	Todos os erros retornados.

Firewall Palo Alto - Atividade de ação de dados do trabalho

Depois que a atividade **Firewall Palo Alto: Obter log** enfileira a consulta de pesquisa no firewall e o trabalho é executado, a atividade **Firewall Palo Alto: Ação de dados do trabalho** recupera os dados do log de ameaças do firewall.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade. Todos os campos de entrada são obrigatórios.

Variáveis de entrada

Variável	Descrição
FirewallIpAddress [cadeia de caracteres]	O endereço IP do firewall.
FirewallApiKey [cadeia de caracteres]	A chave de acesso à API do firewall.
JobID [cadeia de caracteres]	O ID do trabalho enfileirado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes. A saída consiste em dados da configuração do firewall, bem como em dados gerados dinamicamente.

Variáveis de saída

Variável	Descrição
commandStatus [cadeia de caracteres]	Especifica (sucesso ou falha) se os dados foram recuperados do firewall.
JobData [cadeia de caracteres]	Os dados coletados do firewall.
erro [cadeia de caracteres]	Todos os erros retornados.

Gravar conteúdo para registro como atividade de anexo

Esta atividade grava o conteúdo passado de uma entrada e cria um anexo designado para um determinado registro.

A atividade **Gravar conteúdo para registro como anexo** pode ser usada com qualquer fluxo de trabalho para gravar conteúdo e anexá-lo a um registro.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
nome da tabela [cadeia de caracteres]	O nome da tabela para o registro. Este campo de entrada é obrigatório.
sysid [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de tarefa. Este campo de entrada é obrigatório.
carga	O conteúdo de texto sem formatação a ser gravado como anexo. Este campo de entrada é obrigatório.
nome do arquivo	O nome do arquivo do anexo.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	Indica se a atualização foi bem-sucedida.

Integração de Palo Alto Networks - WildFire

Palo Alto Networks - WildFire é um aplicativo baseado em nuvem que interage com o firewall do sistema.

Explorar

Integrações do Security Incident Response

Configurar

Ativar Security Operations Palo Alto Networks - WildFire

Usar

Obter fluxo de trabalho de aprimoramento de dados do WildFire

Desenvolver

- ServiceNow Security Operations diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação
- Localizar componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Faça ou responda perguntas na comunidade do Security Operations

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Ativar Security Operations Palo Alto Networks - WildFire

Antes de usar a integração do Security Operations Palo Alto Networks - WildFire, você deve baixar a integração do ServiceNow Store.

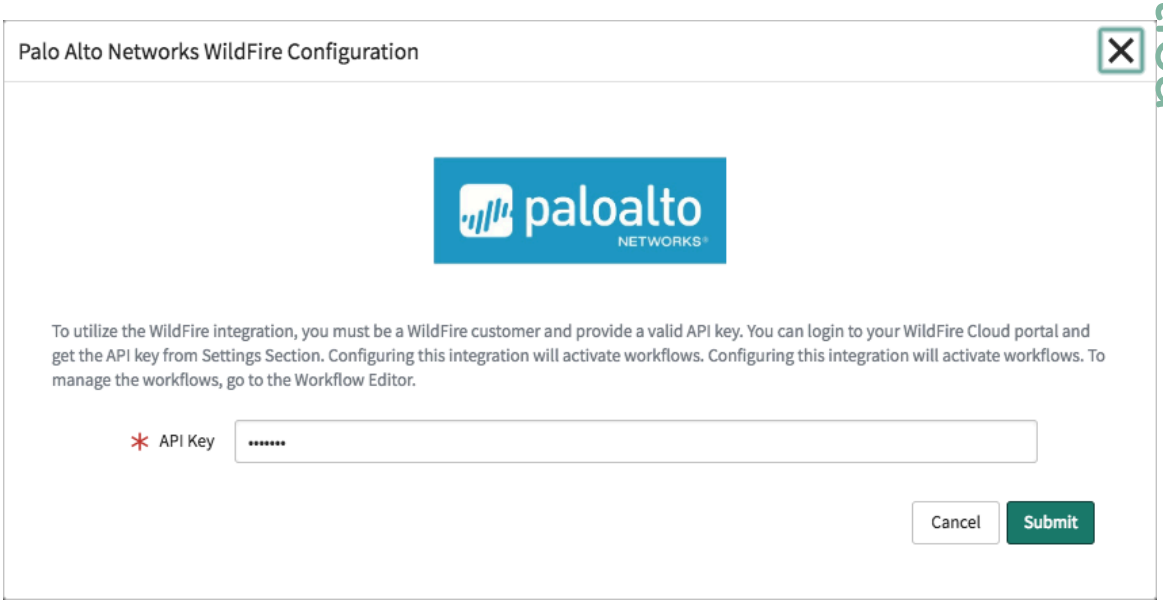
Antes de Iniciar

Função necessária: administrador

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Navegar até **Security Operations** > **Integrações** > **Configurações de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.

3. No cartão Carbon Black, clique em **Configurar**.



4. Insira a chave de API e clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O cartão de configuração de integração é exibido.

5. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Obter fluxo de trabalho de aprimoramento de dados do WildFire

Quando o fluxo de trabalho **Security Operations Palo Alto Networks - Obter aprimoramento de dados do WildFire** é executado, um arquivo hash é carregado no WildFire. Os dados são aprimorados e os relatórios são baixados para a instância para ajudar no processamento de possíveis ataques de malware.

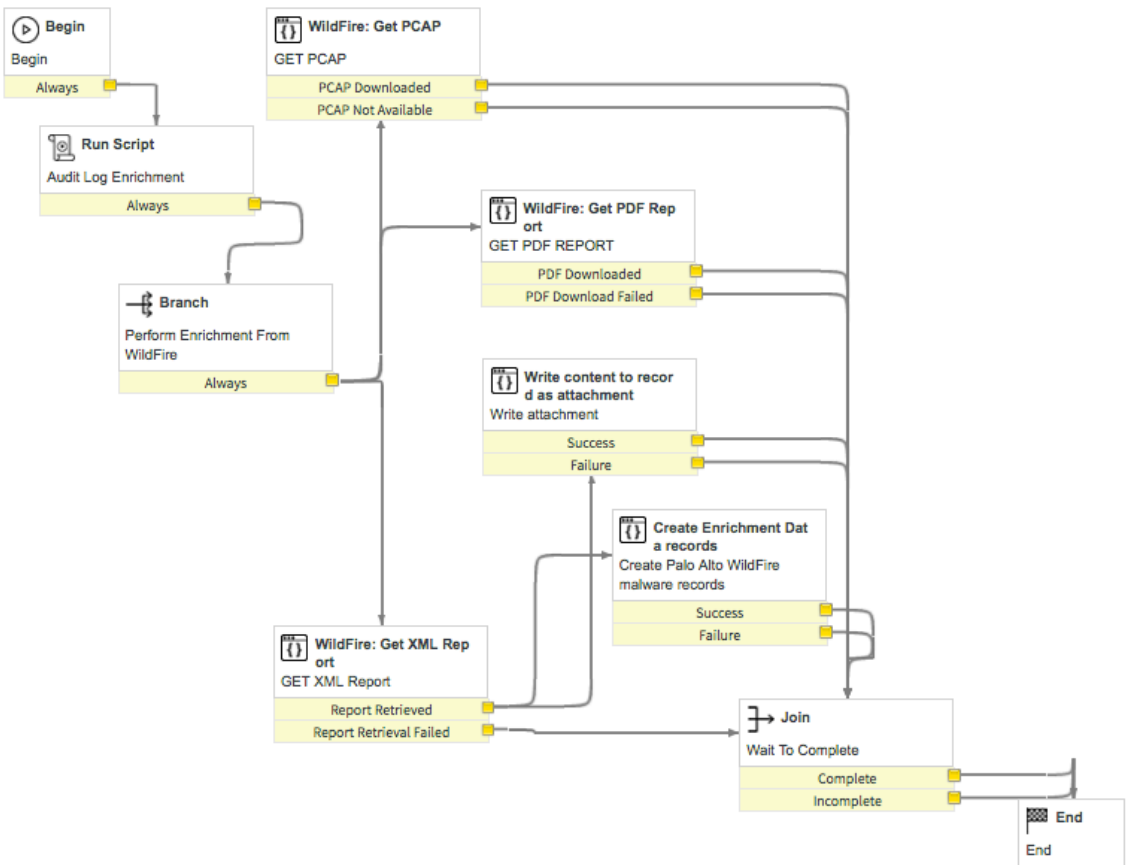
Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho **Security Operations Palo Alto Networks - Obter enriquecimento de dados do WildFire** é executado quando um incidente de segurança é criado a partir de um alerta recebido da aplicação Palo Alto Network Firewall. Um hash de malware da notificação por e-mail recebida do firewall é inserido na guia **IoC** do incidente de segurança e o registro é atualizado.

Security Operations Palo Alto Networks - Obter fluxo de trabalho de aprimoramento de dados do WildFire



Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar incidentes em aberto**.
2. Com base na notificação por e-mail recebida do Firewall, localize e abra o incidente de segurança que foi criado.

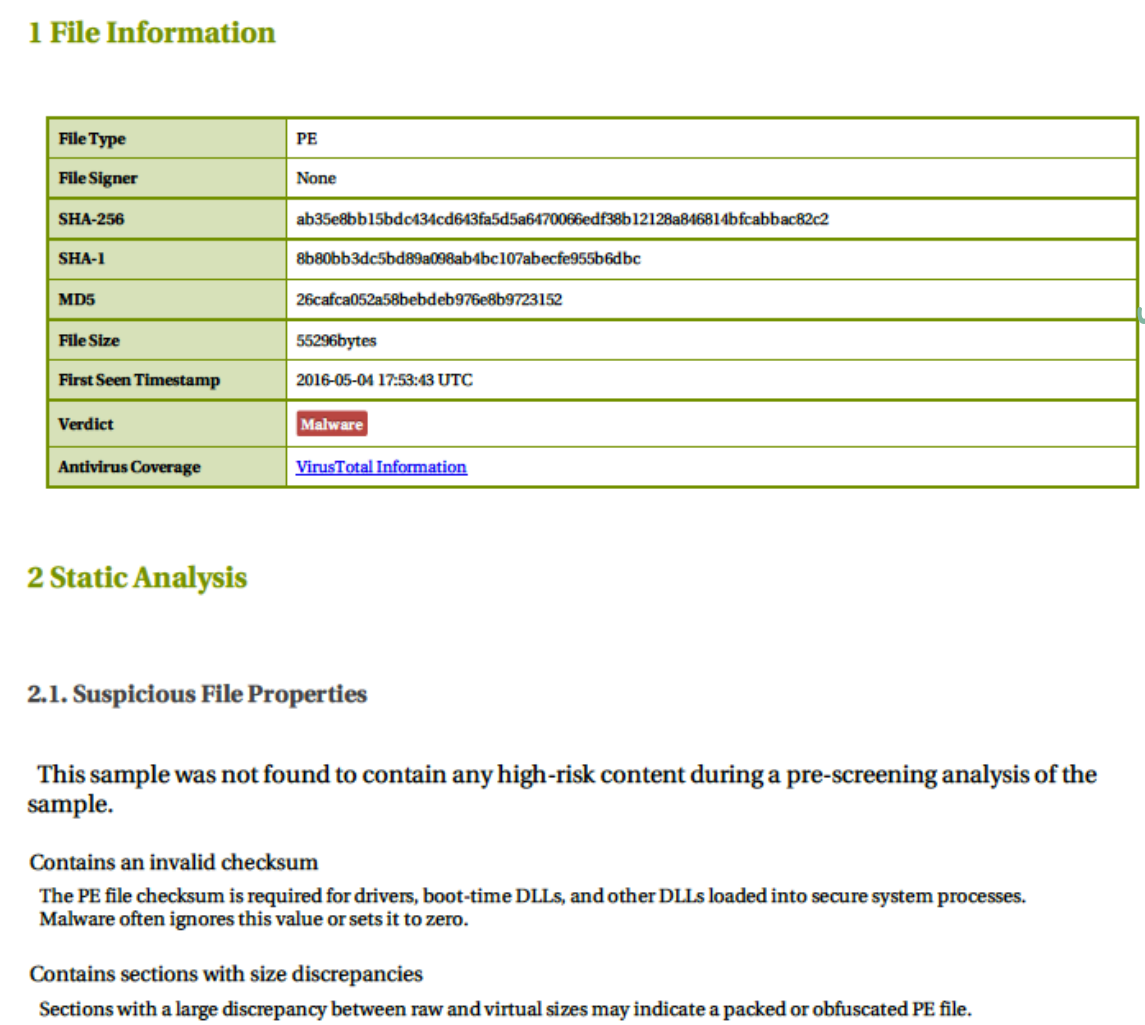
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique na guia **Indicadores de comprometimento** e preencha o **hash de malware** com o hash que você recebeu no alerta.
4. Clique em **Atualizar**.
   O fluxo de trabalho faz com que o arquivo hash seja carregado no WildFire, onde os dados são enriquecidos. Relatórios nos formatos PDF e XML são anexados ao registro (incidente de segurança ou IoC) em sua instância para ajudar no processamento de possíveis ataques de malware.

Nota:
Se os dados aprimorados incluírem informações de captura de pacote, as informações do PCAP também serão baixadas. Os dados de PCAP capturam quais ações o arquivo estava executando. Por exemplo, ele pode relatar quais servidores o arquivo estava contatando. Para exibir arquivos PCAP, você precisa de um analisador de pacotes, como o Wireshark .

PDF de amostra gerado pelo Wildfire



1 File Information

File Type	PE
File Signer	None
SHA-256	ab35e8bb15bdc434cd643fa5d5a6470066edf38b12128a846814bfcabbac82c2
SHA-1	8b80bb3dc5bd89a098ab4bc107abecfe955b6dbc
MD5	26cafca052a58bebdeb976e8b9723152
File Size	55296bytes
First Seen Timestamp	2016-05-04 17:53:43 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains an invalid checksum

The PE file checksum is required for drivers, boot-time DLLs, and other DLLs loaded into secure system processes. Malware often ignores this value or sets it to zero.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

Tradução automática

WildFire - Obter atividade de PCAP

A atividade de fluxo de trabalho **WildFire: Obter PCAP** obtém as informações de captura de pacote (PCAP) geradas durante a análise de um hash de arquivo especificado no WildFire. O resultado desta atividade é anexado a um registro específico, conforme identificado por **TableName** e **RecordId**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
FileSHA256Hash [cadeia de caracteres]	O hash do arquivo recebido da aplicação Palo Alto Network Firewall.
TableName [cadeia de caracteres]	A tabela afetada.
RecordId [cadeia de caracteres]	O incidente de segurança ou IoC que está sendo atualizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
commandStatus [booliano]	Verdadeiro se um resultado for obtido e anexado com sucesso.
errorMessage	O erro, se houver, que ocorreu na atividade.

WildFire - obter atividade de relatório em PDF

A atividade de fluxo de trabalho **WildFire: Obter relatório em PDF** obtém o relatório gerado durante a análise de um hash de arquivo especificado no WildFire em formato PDF. O resultado desta atividade é anexado a um registro específico, conforme identificado por **TableName** e **RecordId**.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
TableName [cadeia de caracteres]	A tabela afetada.
FileSHA256Hash [cadeia de caracteres]	O hash do arquivo recebido da aplicação Palo Alto Network Firewall.
RecordId [cadeia de caracteres]	O incidente de segurança ou IoC que está sendo atualizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
commandStatus [booliano]	Verdadeiro se um resultado for obtido e anexado com sucesso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
errorMessage	O erro, se houver, que ocorreu na atividade.

WildFire - Atividade de obtenção de relatório XML

A atividade de fluxo de trabalho **WildFire: Obter relatório XML** obtém o relatório gerado durante a análise de um hash de arquivo especificado no WildFire em formato XML. O resultado desta atividade é anexado a um registro específico, conforme identificado por **TableName** e **RecordId**.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
TableName [cadeia de caracteres]	A tabela afetada.
FileSHA256Hash [cadeia de caracteres]	O hash do arquivo recebido da aplicação Palo Alto Network Firewall.
RecordId [cadeia de caracteres]	O incidente de segurança ou IoC que está sendo atualizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
commandStatus [booliano]	Verdadeiro se um resultado for obtido e anexado com sucesso.
errorMessage	O erro, se houver, que ocorreu na atividade.

Gravar conteúdo para registro como atividade de anexo

Esta atividade grava o conteúdo passado de uma entrada e cria um anexo designado para um determinado registro.

A atividade **Gravar conteúdo para registro como anexo** pode ser usada com qualquer fluxo de trabalho para gravar conteúdo e anexá-lo a um registro.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
nome da tabela [cadeia de caracteres]	O nome da tabela para o registro. Este campo de entrada é obrigatório.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
sysid [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de tarefa. Este campo de entrada é obrigatório.
carga	O conteúdo de texto sem formatação a ser gravado como anexo. Este campo de entrada é obrigatório.
nome do arquivo	O nome do arquivo do anexo.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	Indica se a atualização foi bem-sucedida.

Integração de Palo Alto Networks Next-Generation Firewall

Depois de instalado e configurado, o analista de incidentes de segurança usa essa integração para bloquear endereços IP mal-intencionados, URLs e domínios usando recursos de Lista dinâmica externa (EDL) com os produtos ServiceNow Security Incident Response (SIR). O analista de incidentes de segurança cria entradas para uma EDL a partir de observáveis determinados como mal-intencionados em ServiceNow SIR incidentes de segurança.

Uma EDL é um arquivo de texto hospedado em um servidor Web externo. Para esta integração, este servidor Web é sua instância Now Platform, que permite que o Palo Alto Networks Next-Generation Firewall importe objetos que estão incluídos na lista, endereços IP, URLs e domínios e aplique a política.

Para impor a política nas entradas da EDL, a lista é referenciada em uma regra de política ou perfil. Conforme as entradas da EDL são modificadas, o firewall importa dinamicamente a lista no intervalo configurado e impõe a política sem uma mudança de configuração ou uma confirmação no firewall. Para esta integração, Now Platform criou uma tabela contendo entradas EDL que são recuperadas por Palo Alto Networks Next-Generation Firewalls autorizados nos intervalos de recuperação configurados.

A integração inclui os seguintes recursos:

- Flexibilidade para criar várias EDLs que se aplicam a diferentes políticas de negação ou permissão de firewall.
- Relatórios detalhados sobre os tipos de sites que estão sendo bloqueados (phishing, malware e sites permitidos listados).
- Marcação de Now Platform incidentes de segurança com entradas de EDL pelo tipo de observável (URL, domínio, endereço IP).
- Configurar períodos de expiração de EDL para manter o tamanho da lista de EDL expirando ou removendo automaticamente entradas mais antigas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Pesquisar, excluir ou migrar entradas de EDL entre listas de EDL.
- Vincular entradas de EDL a registros observáveis e incidentes de segurança que incluem resultados de inteligência contra ameaças e detalhes sobre o motivo pelo qual uma entrada está bloqueada.

A integração requer que os plug-ins (com.snc.security_incident) e (com.snc.secops.orchestration) do produto Security Incident Response estejam ativados.

Esta integração é compatível somente com Palo Alto Networks (PAN-OS 8.x). Versões anteriores não são compatíveis.

Esta integração é compatível com as versões Kingston, London, Madrid e New York da Now Platform®.

Nota:
Os tópicos a seguir são numerados. Para uma instalação, configuração e verificação dos resultados esperados sem problemas, siga os tópicos na ordem em que são apresentados.

Criar um perfil de certificado para o Palo Alto Networks Next-Generation Firewall

A integração requer um perfil de certificado para validar e autenticar a conexão segura entre o servidor Now Platform® e o servidor Palo Alto Networks Next-Generation Firewall.

Antes de Iniciar
Função necessária: Palo Alto Networks Next-Generation Firewall Administrador

Por Que e Quando Desempenhar Esta Tarefa
Um Palo Alto Networks Next-Generation Firewall autentica em uma instância Now Platform®, recupera entradas EDL da tabela de banco de dados e incorpora as entradas nas regras de política de firewall correspondentes. Esta recuperação requer a função de conta de usuário da API na instância Now Platform®, que é usada pelo administrador de firewall do PAN para acessar a API Now Platform®.

O administrador Palo Alto Networks Next-Generation Firewall cria um perfil de certificado em Palo Alto Networks. Este certificado valida e autentica a conexão segura entre o servidor [Now Platform® e o servidor de firewall Palo Alto Networks.

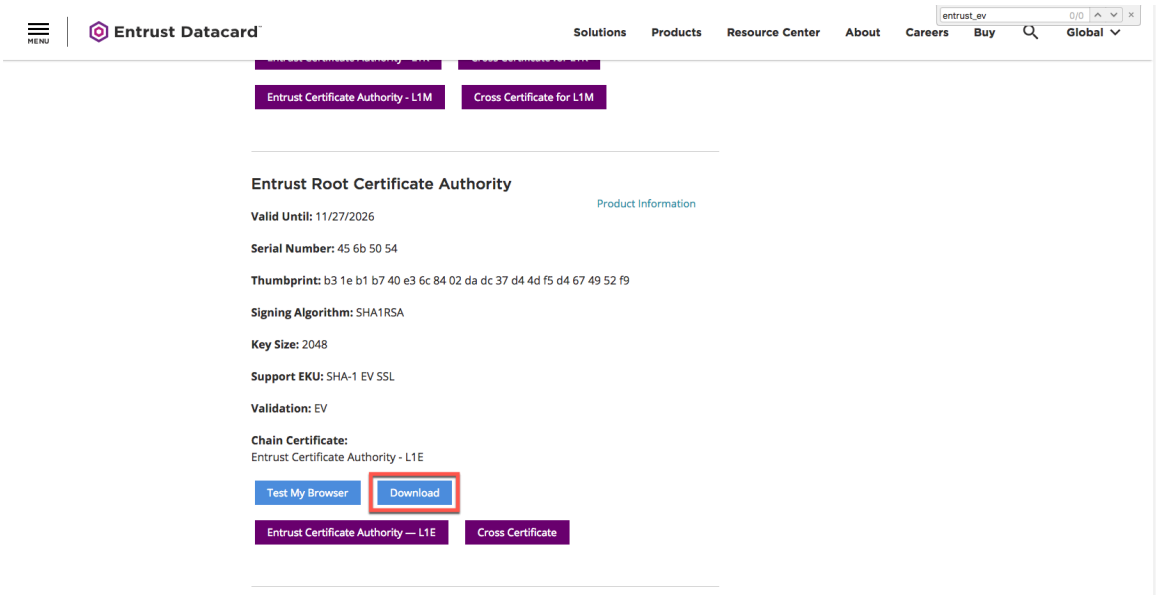
Now Platform® usa Entrust como uma autoridade de certificação e o perfil de certificado necessário é criado usando o certificado entrust_ev_ca.cer. Este certificado está disponível para download no site do cartão EntrustData ™. Para garantir que você obtenha as versões mais recentes, baixe esses certificados diretamente do site da Entrust.

Procedimento

1. Navegue até Certificados raiz Download .
2. No site da Entrust, role até o **certificado Entrust Root Certificate Authority**, conforme mostrado na figura a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique **em Download**.
   O nome do arquivo baixado é **entrust_ev_ca.cer**.
4. Consulte a documentação Palo Alto Networks para saber como configurar o perfil de certificado depois de baixá-lo.
   Os requisitos podem ser encontrados no site Palo Alto Networks.

Tópicos relacionados

"Configurar um perfil de certificado" no Guia do administrador do PAN-OS 10.0

Configurar e instalar Palo Alto Networks Next-Generation Firewall

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação sem problemas.

Antes de Iniciar

Função necessária: (admin)

Configuração de tarefa	Descrição
Verifique se você tem as funções Now Platform e Security Incident Response atribuídas.	As seguintes funções são necessárias: • O administrador do sistema (admin) instala o app e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração e cria, ativa e remove EDLs. Esta função também atribui a função sn_si.analyst. • O (administrador) atribui a função de conta de API Now Platform® (sn_sec_panfw.api_account_access), que é usada exclusivamente para inserir as credenciais necessárias para autenticação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	em Palo Alto Networks para que os firewalls possam recuperar EDLs do Now Platform®. • (sn_si.analyst) ou Analista do Security Operations Center (SOC), cria entradas de EDL e trabalha com incidentes de segurança.
Verifique se você está usando Palo Alto Networks Next-Generation Firewall versão-OS 9.x e 10.x.	Esta integração é compatível somente com Palo Alto Networks Next-Generation Firewall OS 9.0 e posterior.
Configure perfis EDL, regras de política de segurança e perfis de certificado em Palo Alto Networks conforme recomendado na documentação Palo Alto Networks.	Consulte Palo Alto Networks a documentação geral e os requisitos no: site de documentação da Paloalto Networks .
Verifique se você baixou e configurou o certificado Entrust™ Root Certificate Authority.	A integração requer este certificado para validar e autenticar a conexão segura entre o servidor Now Platform e o servidor Palo Alto Networks Next-Generation Firewall. Para obter mais informações sobre como configurar o certificado, consulte "Configurar um perfil de certificado" no Guia do administrador do PAN-OS 10.0 . Para fazer o download, consulte Criar um perfil de certificado para o Palo Alto Networks Next-Generation Firewall e Download de certificados raiz .
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Requisitos da versão Madrid e posteriores Para a versão Madrid e versões posteriores da família, o plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras aplicações Security Operations necessárias para a integração. Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Orquestração de suporte de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.
Se sua organização tiver Now Platform® processos de gestão de mudanças e aprovação para exclusão de e-mail, verifique se a capacidade de envio/recebimento de e-mail está habilitada.	Para verificar se a capacidade de envio/recebimento de e-mail está habilitada na sua instância Now Platform®, navegue até **Propriedades do e-mail** > **Administração** > **Propriedades do E-mail**. Em Configuração de e-mail de saída, verifique se **Envio** de e- **mail** e Recebimento de e-mail estão selecionados.

Procedimento

Se você não instalou a aplicação para a integração, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.

Criar a função de conta de API para Palo Alto Networks Next-Generation Firewall

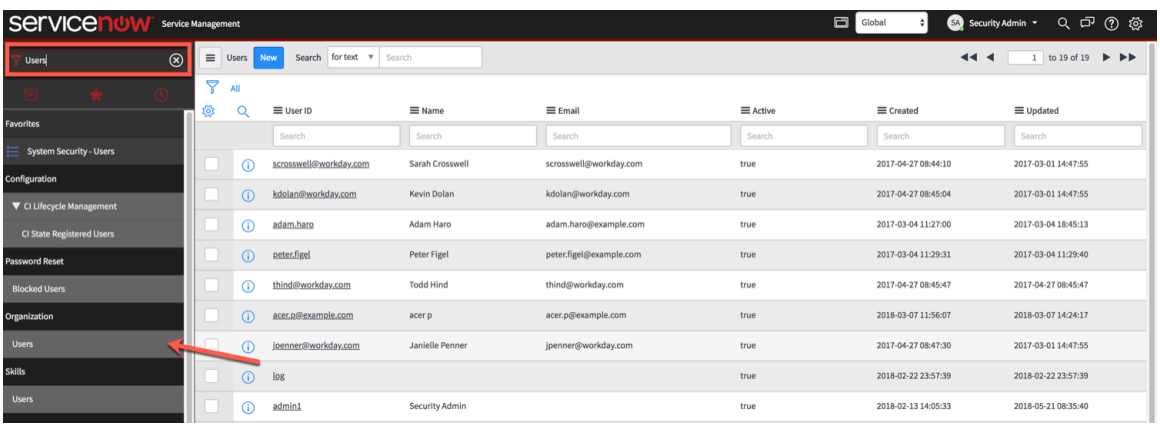
Uma função de conta de API é necessária em sua instância Now Platform® para esta integração. O nome de usuário e a senha associados a esta conta são criados no Now Platform® e inseridos no Palo Alto Networks para que o Palo Alto Networks Next-Generation Firewall seja autenticado com o Now Platform® ao recuperar entradas EDL.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
O administrador Now Platform® cria uma função de conta de API (sn_sec_panfw.api_account_access). Esta conta é usada exclusivamente para inserir as credenciais necessárias para autenticação em Palo Alto Networks para que os firewalls possam recuperar EDLs do Now Platform®. Esta conta é uma conta de usuário de API separada e exclusiva na instância Now Platform® e atribuída ao administrador Palo Alto Networks Next-Generation Firewall.

Procedimento

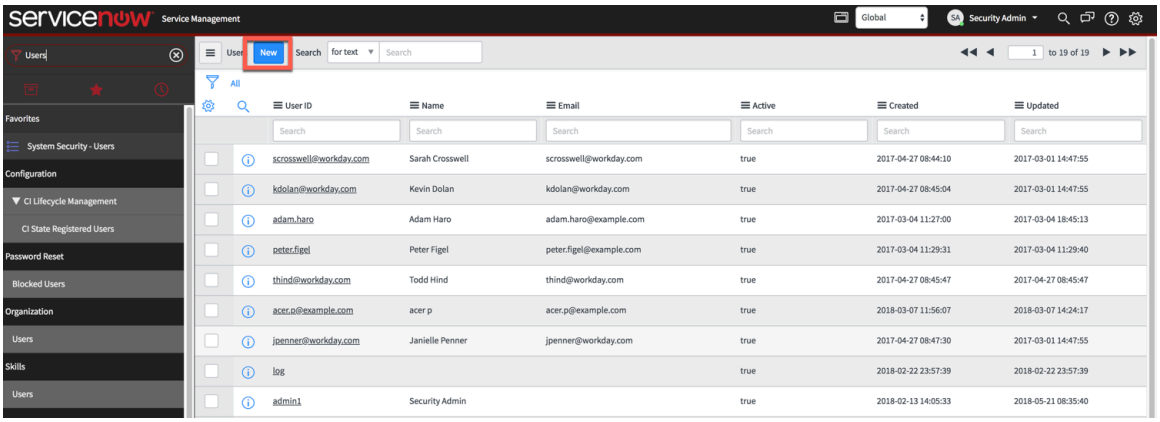
1. Navegar até **Todos** > **Organização** > **Usuários**.
2. Clique no módulo **Usuários**.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na lista Usuários exibida, clique em **Novo**.



Um novo formulário de usuário será exibido.

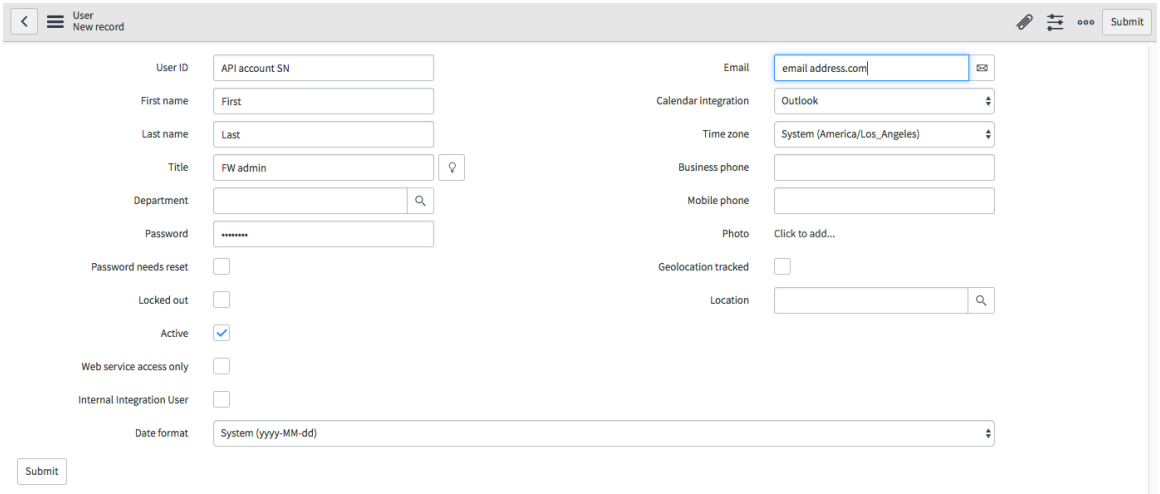
4. Preencha o formulário.

Nota:
Os valores do título do ID do usuário e do endereço de e-mail mostrados na tabela e na figura a seguir são valores de exemplo.

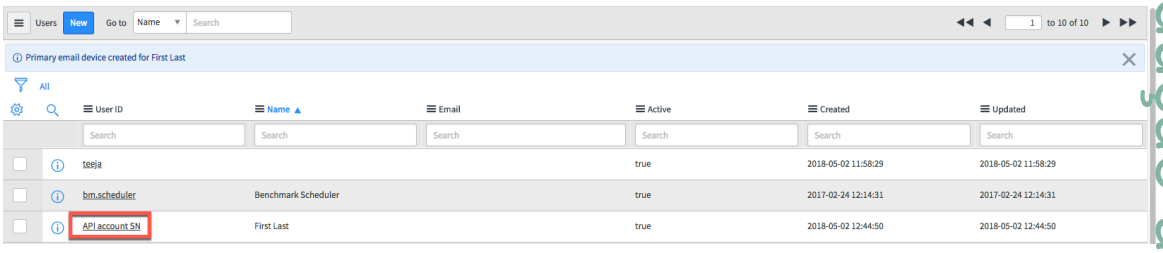
Campo	Descrição
ID do usuário	ID do usuário exclusivo para a função na sua instância Now Platform®. Este ID de usuário é inserido no campo **Nome** de usuário na seção **Autenticação de cliente** da caixa de diálogo Listas dinâmicas externas no site Palo Alto Networks. Um exemplo é a conta de API SN.
Nome	Pessoa que você está atribuindo.
Sobrenome	Pessoa que você está atribuindo.
Título	Cargo, por exemplo, administrador de FW.
Senha	Senha exclusiva criada para esta função. Esta senha é inserida no campo **Senha** na seção **Autenticação de cliente** da caixa de diálogo Listas dinâmicas externas no site Palo Alto Networks.
E-mail	Endereço de e-mail exclusivo.

Tradução automática

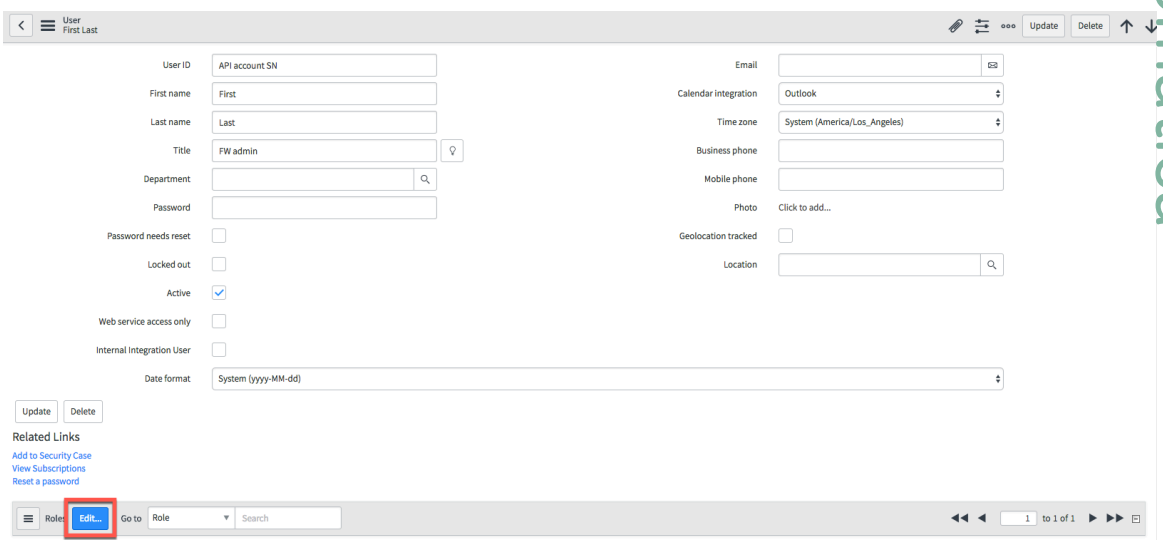
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Enviar**.
   Depois de enviado, você pode atribuir a função.
6. Na lista Usuários na coluna **ID** do usuário, clique no nome do ID do usuário que você inseriu, por exemplo, SN da conta da API.



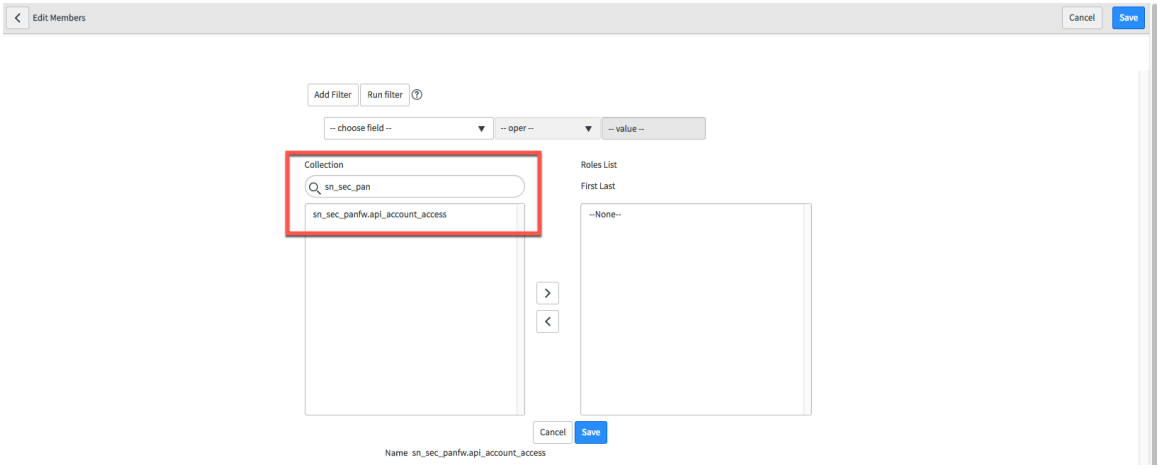
7. No registro aberto na seção Funções, clique em **Editar**.



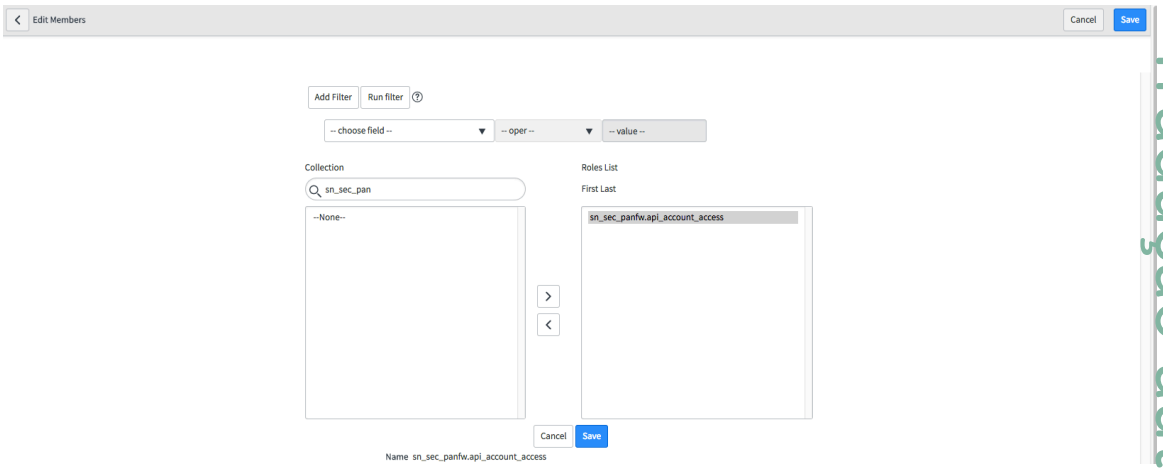
8. No formulário **Editar membros**exibido, insira `sn_sec_panfw.api_account_access` no campo **Coleção**.
   Abaixo do campo **Coleção**, a função é exibida na coluna.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



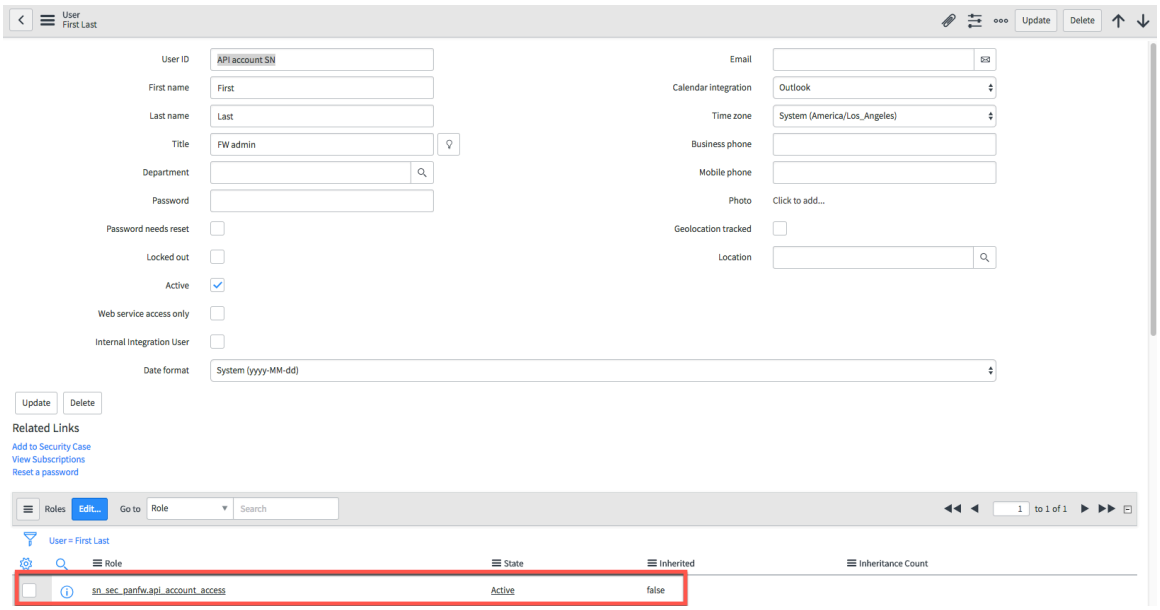
9. Na coluna **Coleção**, selecione e mova `sn_sec_panfw.api_account_access` para a **Lista de funções**.



10. Clique em **Salvar**.
11. Navegue até **Usuários**e, na coluna **Usuário** da lista, clique no nome do ID que você criou para a função (SN da conta da API).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O registro do usuário é exibido. Este registro verifica se a conta do usuário foi atribuída. O **Estado** está ativo e a função não é herdada.

Listas dinâmicas externas compatíveis para Palo Alto Networks Next-Generation Firewall

A integração ServiceNow Palo Alto Networks Next-Generation Firewall oferece suporte a listas dinâmicas externas (EDLs) que aceitam IP, URL e observáveis de domínio.

EDLs e observáveis compatíveis

Uma *lista dinâmica externa* é um arquivo de texto hospedado em um *servidor Web*externo, que para esta integração é a instância Now Platform. O Palo Alto Networks Next-Generation Firewall pode importar objetos - endereços IP, URLs, domínios - incluídos na lista e impor a política. Para impor a política nas entradas da EDL, a lista é referenciada em uma regra de política ou perfil.

Esta integração oferece suporte a três tipos de EDLs:

- IP (inclui um único endereço IP, bem como blocos CIDR (intervalos) de endereços).
- URL
- Domínio

A tabela a seguir lista as descrições dos observáveis compatíveis com esta integração e formatos de exemplo para cada tipo.

Observáveis compatíveis e formatos de exemplo

Observável	Formatos de exemplo	Descrição
Endereço IP	• 95.153.103.54 (IPv4) • (IPv6): 2001:00B8:130F:FE03:0000:0900:0830F:130B	Representa um endereço de interface único e distinto. A integração oferece suporte aos formatos IPv4, IPv6 e CIDR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Observáveis compatíveis e formatos de exemplo

Observável	Formatos de exemplo	Descrição
		O suporte para observáveis de endereço IP inclui intervalos CIDR (Roteamento entre domínios sem classe), por exemplo, 95.153.100.0/22. Observação: uma mensagem de erro é exibida quando você tenta anexar um único endereço IP a uma EDL que você já bloqueou como parte de um intervalo CIDR. Por exemplo, o endereço único 95.153.103.54 faz parte do intervalo CIDR representado por 95.153.100.0/22 (95.153.100.0-95.153.103.255).
URL	• www.exemplo.com • www.example.com/article.html • example.com • *.exemplo.com	Caracteres curinga são compatíveis. O Now Platform reformata as entradas de URL para conformidade com os requisitos de formato Palo Alto Networks EDL.
Domínio	• www.exemplo.com • example.com • mail.exemplo.com	Caracteres curinga não são compatíveis.

Para obter mais informações sobre como formatar diretrizes e EDLs, consulte "Diretrizes de formatação para uma lista dinâmica externa" no Guia do administrador do PAN-OS 10.0 no site Palo Alto Networks.

Criar uma EDL para o firewall de última geração da Palo Alto Networks

Crie uma lista dinâmica externa (EDL) na sua instância Now Platform. Depois de aprovado e ativado, você pode criar entradas para EDLs a partir de observáveis determinados como mal-intencionados em Now Platform Security Incident Response (SIR) incidentes e solicitar aprovação para bloqueá-los.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Crie a EDL na sua instância Now Platform para que o firewall possa importar objetos (endereços IP, URLs, domínios) incluídos na lista e aplicar a política. Para impor a política nas entradas da EDL, a lista é referenciada em uma regra de política ou perfil.

Os números na seção a seguir são mostrados com os **formulários** com guia desmarcados em Configurações do sistema. Para obter mais informações sobre como selecionar e limpar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

formulários com guias, consulte a seção "Exibir formulários com guias" em Configuring the form layout .

Procedimento

1. Após a conclusão da instalação da aplicação, navegue até **Integrações** > **Configurações de Integração**.
2. Localize o bloco Palo Alto Networks Next-Generation Firewall e clique em **Configurar**.

3. Clique **em Criar nova lista de EDL**.

4. No formulário, preencha os campos.

Palo Alto Networks Formulário Lista dinâmica externa do firewall

Campo	Descrição
Nome	Palo Alto Networks Nome da lista dinâmica do firewall.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Inclua o tipo de observável (URL, IP, domínio) neste campo para que o analista de segurança possa reconhecer facilmente a intenção da EDL pelo nome. O nome também deve indicar claramente para qual política de firewall esses objetos EDL estão mapeados. Alguns exemplos de nomes de EDL são IP de malware de saída ou URL de phishing de saída.
Ativo	Essa caixa de seleção está desmarcada por padrão para indicar que a EDL está inativa. Quando inativa, a EDL não pode receber entradas adicionais. Quando a caixa de seleção está marcada, a EDL é ativada e fica disponível para entradas da EDL.
Marcador de exibição	A caixa de seleção é marcada por padrão para marcar automaticamente o observável e o registro de incidente de segurança associado se o observável estiver bloqueado em uma EDL. Quando selecionados, o tipo de marcador e o marcador EDL para campos de observáveis ficam disponíveis no formulário. **Nota:** Um nome de marcador é criado por padrão a partir do valor inserido no campo **Nome** com um prefixo *EDL-*, por exemplo, EDL-Malware OutBound IP. Você pode mudar o nome e a cor do marcador. Consulte: (Opcional) Editar o nome do marcador de segurança para Palo Alto Networks Next-Generation Firewall. O nome do marcador é exibido no campo Marcador da EDL para observáveis depois que a EDL é salva. Quando a caixa de seleção está desmarcada, nenhum marcador é criado e o tipo de marcador e o marcador EDL para os campos de observáveis não estão disponíveis no formulário.
Tipo de observável	Selecione um tipo de observável que esta EDL aceita na lista de seleção: IP (incluindo CIDR), URL ou domínio.
Tipo de marcador	Marcadores que estão disponíveis na lista de seleção. Uma lista de bloqueios é uma lista de observáveis que você deseja que o Palo Alto Networks Next-Generation Firewall bloqueie.

Tradução automática

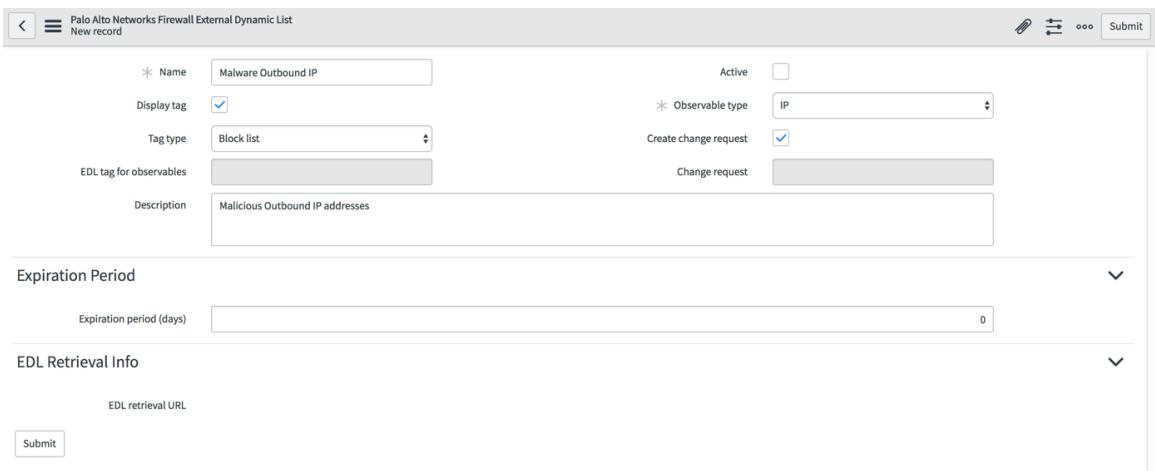
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Uma lista de permissões é uma lista de observáveis que você deseja que o Palo Alto Networks Next-Generation Firewall permita. Por padrão, a cor do marcador da lista de bloqueios é preta e a cor do marcador da lista de permissões é cinza. Você pode mudar a cor. Consulte: (Opcional) Editar o nome do marcador de segurança para Palo Alto Networks Next-Generation Firewall.
Criar solicitação de mudança	Esta caixa de seleção é marcada por padrão para criar automaticamente uma solicitação de mudança e tarefas de mudança em sua instância Now Platform, que são anexadas ao registro EDL. A solicitação de mudança é usada para configurar o URL de recuperação da lista EDL no servidor Palo Alto Networks Next-Generation Firewall. Esta opção será recomendada se o administrador do firewall também estiver usando o Now Platform para políticas de firewall ou mudanças de regra. Se você criar uma solicitação, depois que ela for fechada, a lista de EDL será ativada automaticamente. Desmarque a caixa de seleção para ativar manualmente a EDL depois de receber um aviso por e-mail do administrador do firewall de que a configuração em Palo Alto Networks foi concluída. Quando a caixa de seleção de Criar solicitação de mudança está desmarcada, o campo Solicitação de mudança fica indisponível.
Marcador de EDL para observáveis	Este campo será exibido somente se a caixa de seleção Exibir marcador estiver marcada. O campo é preenchido automaticamente depois que a EDL é salva com um valor padrão do campo Nome. Para obter mais informações sobre como mudar o nome e a cor do marcador padrão, consulte (Opcional) Editar o nome do marcador de segurança para Palo Alto Networks Next-Generation Firewall
Solicitação de mudança	Quando a caixa de seleção Criar solicitação de mudança está marcada, o número da solicitação de mudança é exibido na instância Now Platform depois que a EDL é salva.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

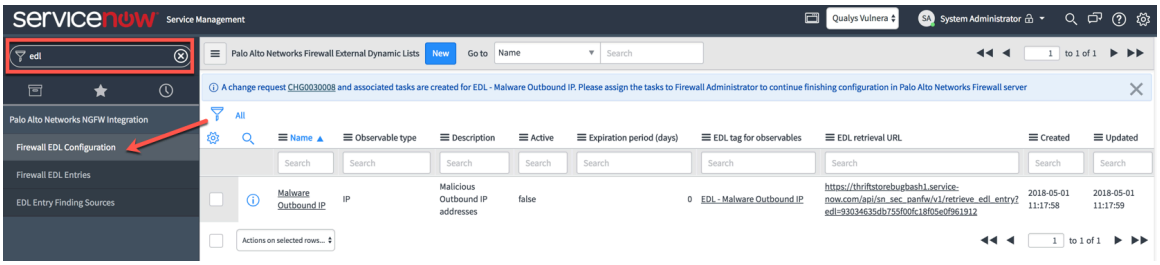
Campo	Descrição
	Quando a caixa de seleção Criar solicitação de mudança está desmarcada, este campo não é exibido.
Descrição	Descrição da lista dinâmica do firewall da Palo Alto Networks. O nome geralmente contém os tipos de sites e observáveis que você esperaria estar nesta EDL e você pode usar este campo para obter mais detalhes.
Período de expiração (dias)	Período de expiração da EDL. 0 (o padrão) indica que a entrada EDL nunca expira. Se você alterar este valor, esta entrada ficará ativa para o número de dias inseridos. Você pode inserir um valor mínimo de 1 e não há valor máximo. Por exemplo, se você inserir 30 dias às 14h01 de 1º de maio, a EDL expirará às 14h01 de 31 de maio. Todas as entradas nesta EDL herdam este valor por padrão, a menos que você substitua o valor na entrada individual.



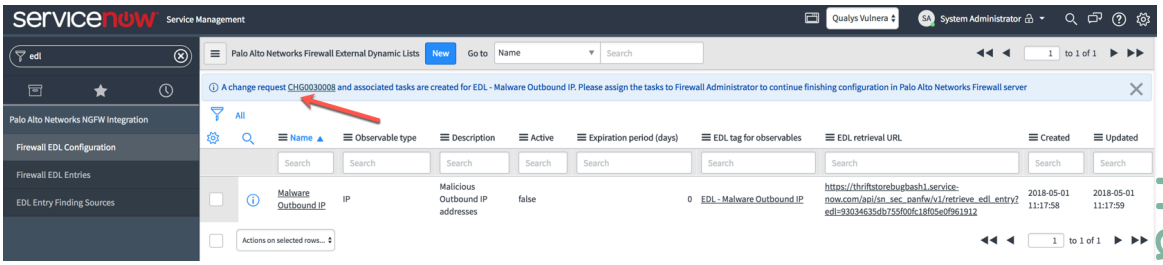
Tradução automática

5. Clique em **Enviar**.
6. Se a lista de Listas dinâmicas externas do Firewall da Palo Alto Networks não for exibida, navegue até **Integração de NGFW com a Palo Alto Networks** > **Configuração de EDL do Firewall** e clique em **Configuração de EDL do firewall**.

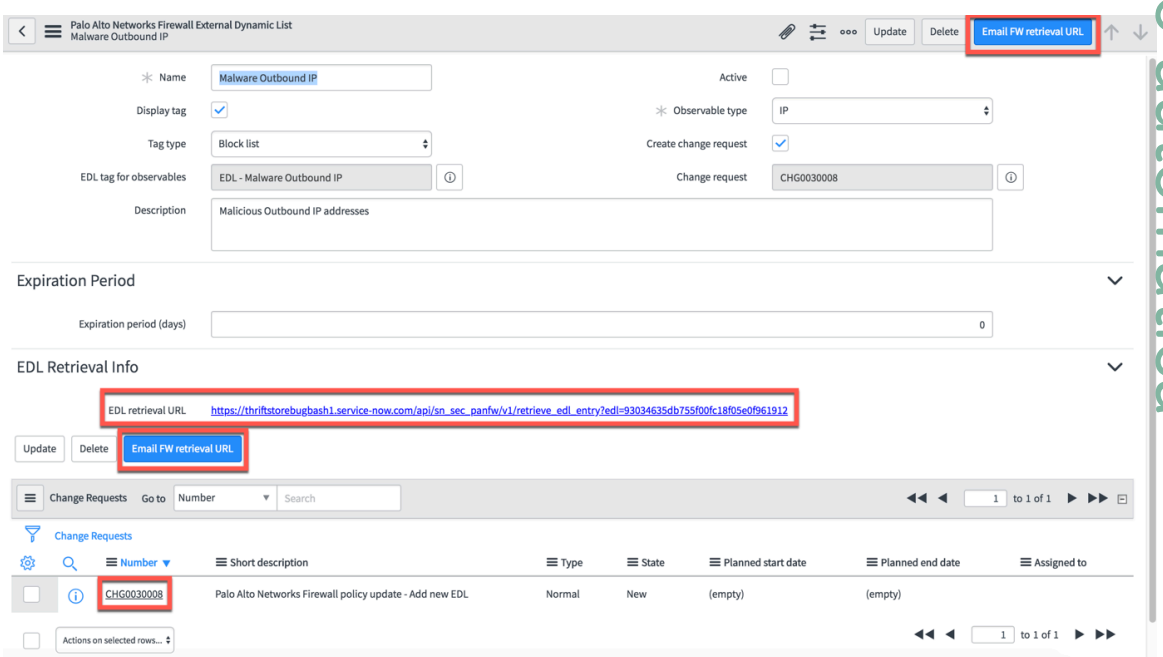
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A nova EDL é exibida. O status da EDL ainda está inativo (falso), o que significa que a EDL não está disponível para aceitar entradas. Se **Criar solicitação de mudança** tiver sido configurada, uma mensagem será exibida indicando que uma solicitação de mudança e tarefas foram criadas na sua instância Now Platform.



7. Na coluna **Nome**, clique em um item para abrir o registro.
   O registro EDL é exibido. Este exemplo mostra um EDL de IP de saída de malware. Os campos, opções e links a seguir são exibidos no novo registro após o envio e descritos na tabela a seguir.



URL de recuperação e links de solicitação de mudança no registro EDL

Opção	Descrição
URL de recuperação do firmware do e-mail	Envia por e-mail um aviso de que o link da EDL está disponível para configuração para o administrador de firewall Palo Alto Networks.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
URL de recuperação da EDL	Este URL é colocado no campo **Origem** na caixa de diálogo de autenticação Listas dinâmicas externas na guia **Criar lista** no site Palo Alto Networks. O link da URL que o administrador de firewall Palo Alto Networks usa para configuração no firewall Palo Alto Networks é gerado e exibido automaticamente. **Nota:** Se você tiver as Configurações do sistema definidas como **Formulários com**guia , este link será exibido na guia **Informações de recuperação de EDL** na parte inferior do registro.
Now Platform solicitação de mudança	Um link para o registro de solicitação de mudança é exibido na seção Solicitações de mudança quando configurado, e o número da solicitação é exibido no campo Solicitação de mudança.
Atualizar	Modifique os dados e atualize os campos editáveis.
Excluir	Exclua o registro.

8. Crie e adicione mais EDLs conforme necessário.
   As EDLs são exibidas na lista Palo Alto Networks Listas dinâmicas externas.

O que Fazer Depois

Ative uma EDL manualmente ou com uma solicitação de mudança Now Platform.

Ativar uma EDL para Palo Alto Networks Next-Generation Firewall

Depois que a Lista dinâmica externa (EDL) tiver sido criada em seu Now Platform® e o URL estiver disponível, o administrador de firewall Palo Alto Networks configura a EDL no Palo Alto Networks Next-Generation Firewall. O URL de recuperação é usado pelo administrador de firewall Palo Alto Networks para configurar a EDL no servidor Palo Alto Networks Next-Generation Firewall. Antes de aceitar entradas de EDL, a EDL deve ser configurada em Palo Alto Networks e ativada em Now Platform®.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

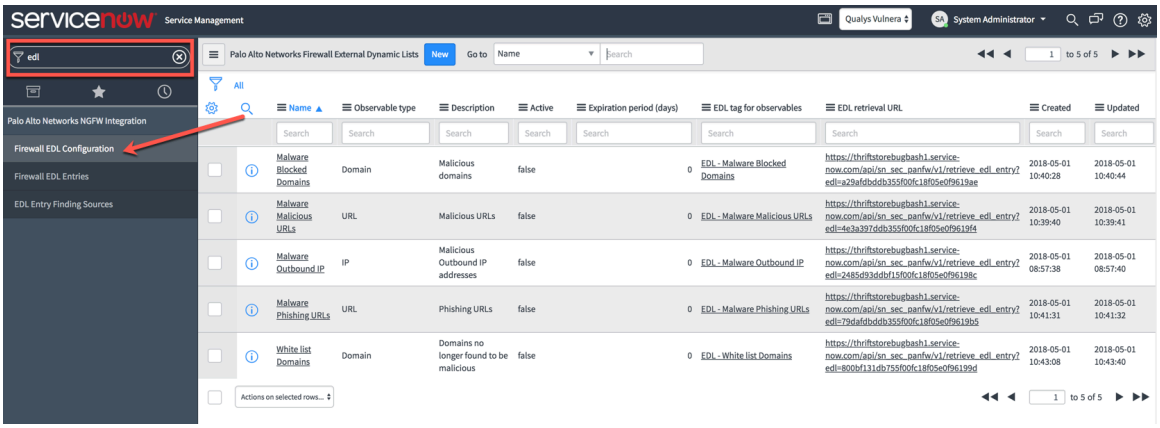
Depois que a EDL for configurada, como administrador de incidentes de segurança, você poderá ativar a EDL manualmente ou a EDL será ativada automaticamente após a conclusão de uma Now Platform® Solicitação de Mudança. A EDL deve ser aprovada e movida do estado inativo para o estado ativo antes de aceitar entradas da EDL.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

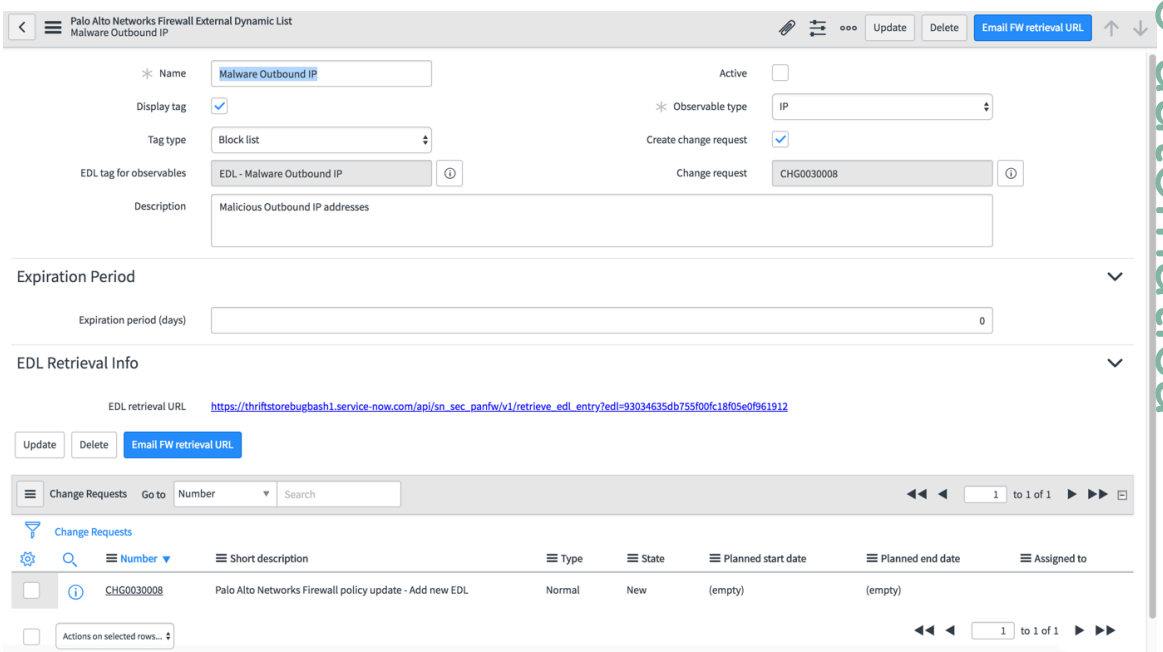
Procedimento

1. Navegar até **Todos** > **Integração de NGFW com a Palo Alto Networks** > **Configuração de EDL do Firewall** e selecione o módulo **Configuração de EDL do Firewall**.



2. Na lista Listas dinâmicas do firewall da Palo Alto Networks exibida, selecione sua nova EDL na coluna Nome.

3. No registro exibido, observe os botões de **URL de recuperação de FW de e-mail**, o link de URL de recuperação de EDL ativo e, se configurado, a solicitação de mudança Now Platform® na seção Solicitações de mudança.
   Certifique-se de que a caixa de seleção **Ativo** esteja desmarcada.

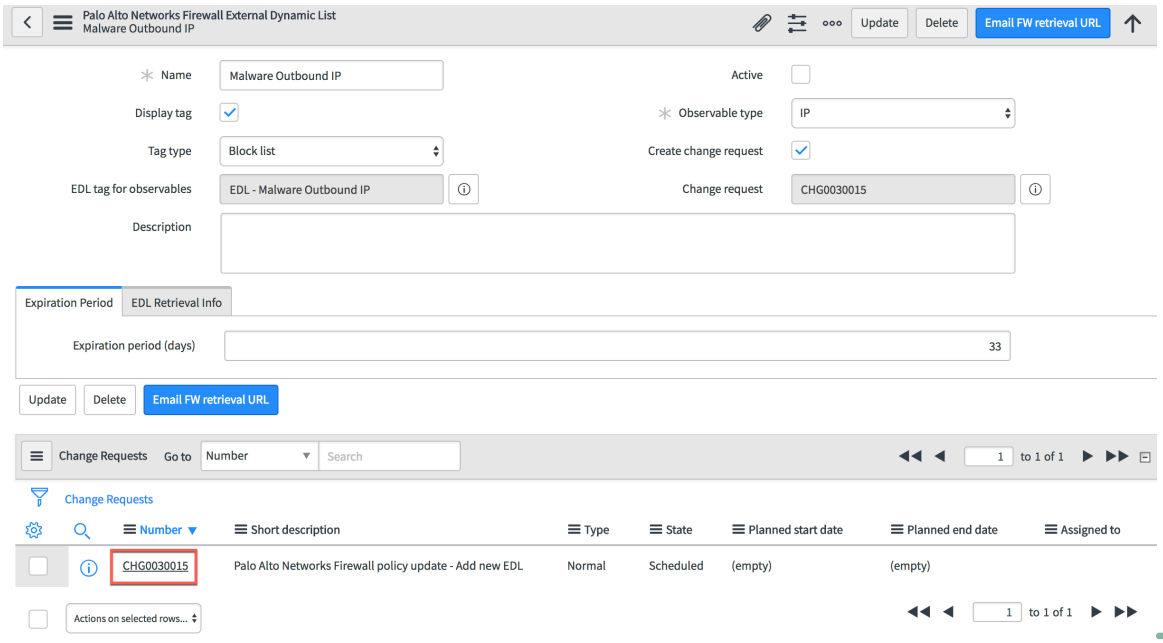


Nota:
Com os **formulários com** guia desmarcados nas configurações do sistema, o URL de recuperação de EDL aparece na seção **Informações de recuperação** de EDL, conforme mostrado na figura anterior.

A figura a seguir mostra as **informações de recuperação de EDL** exibidas como uma guia com os **formulários** com guia selecionados nas configurações do sistema. Clique na guia **Informações de recuperação de EDL** para exibir o URL de recuperação. O link para a solicitação de mudança (**CH0030015**) também é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Para concluir a configuração e mover o EDL de inativo para ativo, você deve escolher uma das opções a seguir para notificar o administrador do firewall de que o URL de recuperação está disponível.
   Depois de notificar o administrador do firewall de que o URL de recuperação está disponível e de confirmar que a EDL foi configurada em Palo Alto Networks, como administrador de incidentes de segurança, a próxima etapa é ativar a EDL. Você ativa a EDL manualmente ou, se configurado, usa o formulário de solicitação de mudança Now Platform para ativar a EDL.

Tópicos relacionados

Configurar uma EDL em Palo Alto Networks Next-Generation Firewall

Ativar uma EDL manualmente para Palo Alto Networks Next-Generation Firewall

Se o administrador de firewall da Palo Alto Networks não estiver usando o Now Platforme você for notificado diretamente de que o Palo Alto Networks Next-Generation Firewall está configurado, você poderá ativar a Lista dinâmica externa (EDL) manualmente.

Antes de Iniciar

Em Palo Alto Networks, atribua um objeto EDL, uma política e o URL de origem à EDL que você criou. Para obter mais informações sobre como configurar o EDL para Palo Alto Networks Next-Generation Firewall em Palo Alto Networks, consulte Configurar uma EDL em Palo Alto Networks Next-Generation Firewall.

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

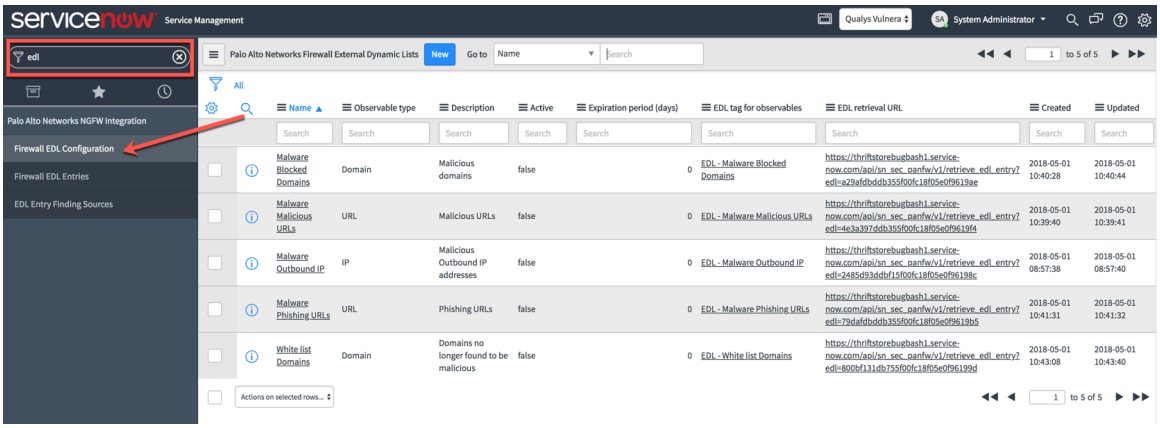
Como administrador de incidentes de segurança Now Platform, você será notificado pelo administrador de firewall Palo Alto Networks quando a configuração do EDL for concluída no Palo Alto Networks Next-Generation Firewall.

Tradução automática

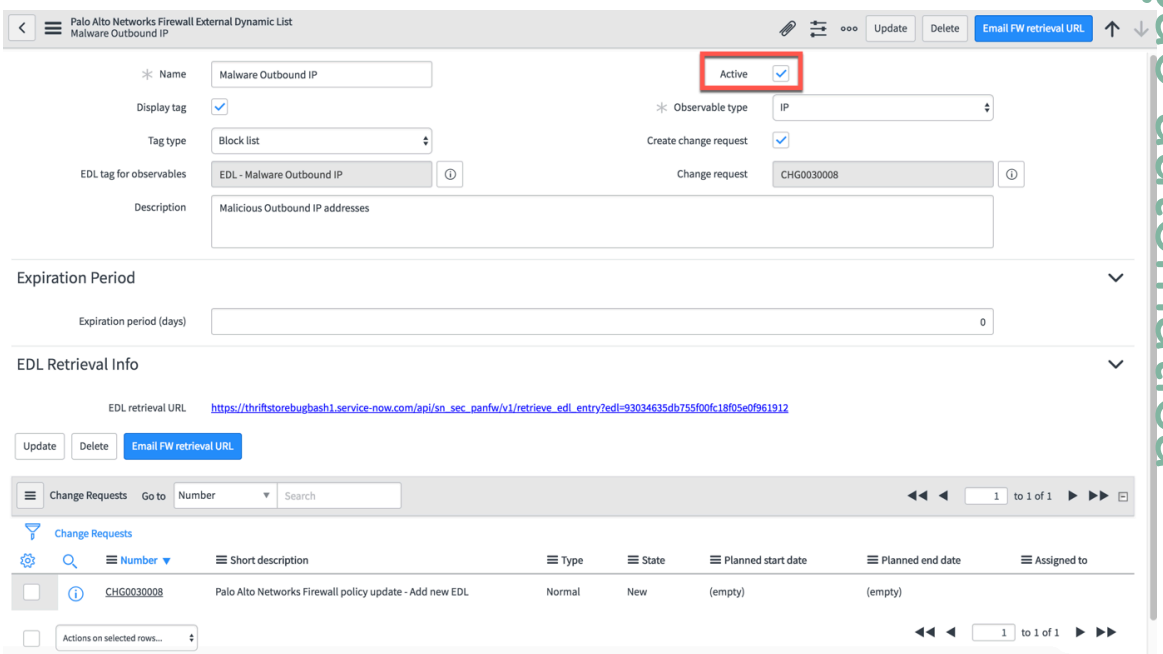
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Integração de NGFW com a Palo Alto Networks** > **Configuração de EDL do Firewall**.



2. Selecione o módulo **Configuração de EDL do Firewall**.
3. Na lista Listas dinâmicas externas do Firewall da Palo Alto Networks, clique em um item na coluna **Nome** para abri-lo.
4. No registro que é aberto, marque a caixa de seleção **Ativo**.

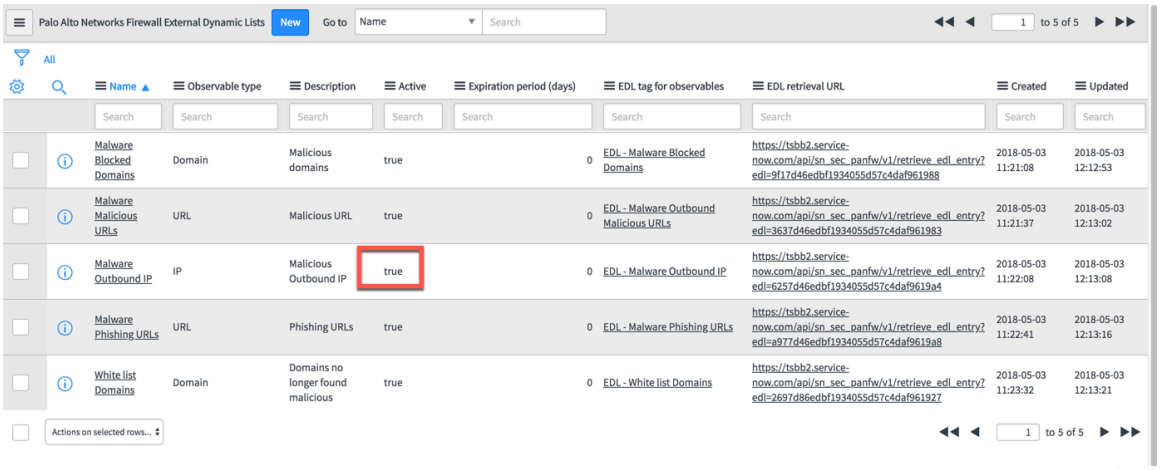


5. Clique em **Atualizar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na coluna **Ativa** da lista Listas dinâmicas externas do Firewall da Palo Alto Networks, verdadeiro é exibido para o estado da EDL.



Resultado

A EDL está ativada e pronta para receber entradas da EDL

O que Fazer Depois

Envie entradas de EDL de um incidente de segurança ou da lista de bloqueios.

Configurar uma EDL em Palo Alto Networks Next-Generation Firewall

O administrador de firewall Palo Alto Networks configura um EDL para o Palo Alto Networks Next-Generation Firewall depois de notificado que o URL de recuperação está disponível no Now Platform. Antes que a EDL possa aceitar entradas de EDL, ela deve ser configurada em Palo Alto Networkse ativada em Now Platform®.

Antes de Iniciar

Função necessária: Palo Alto Networks administrador de firewall

Por Que e Quando Desempenhar Esta Tarefa

O administrador Palo Alto Networks Next-Generation Firewall cria um objeto EDL e atribui a URL (Recuperação) de origem e a política à EDL. Essas tarefas são realizadas em Palo Alto Networks antes que a EDL seja ativada em Now Platform.

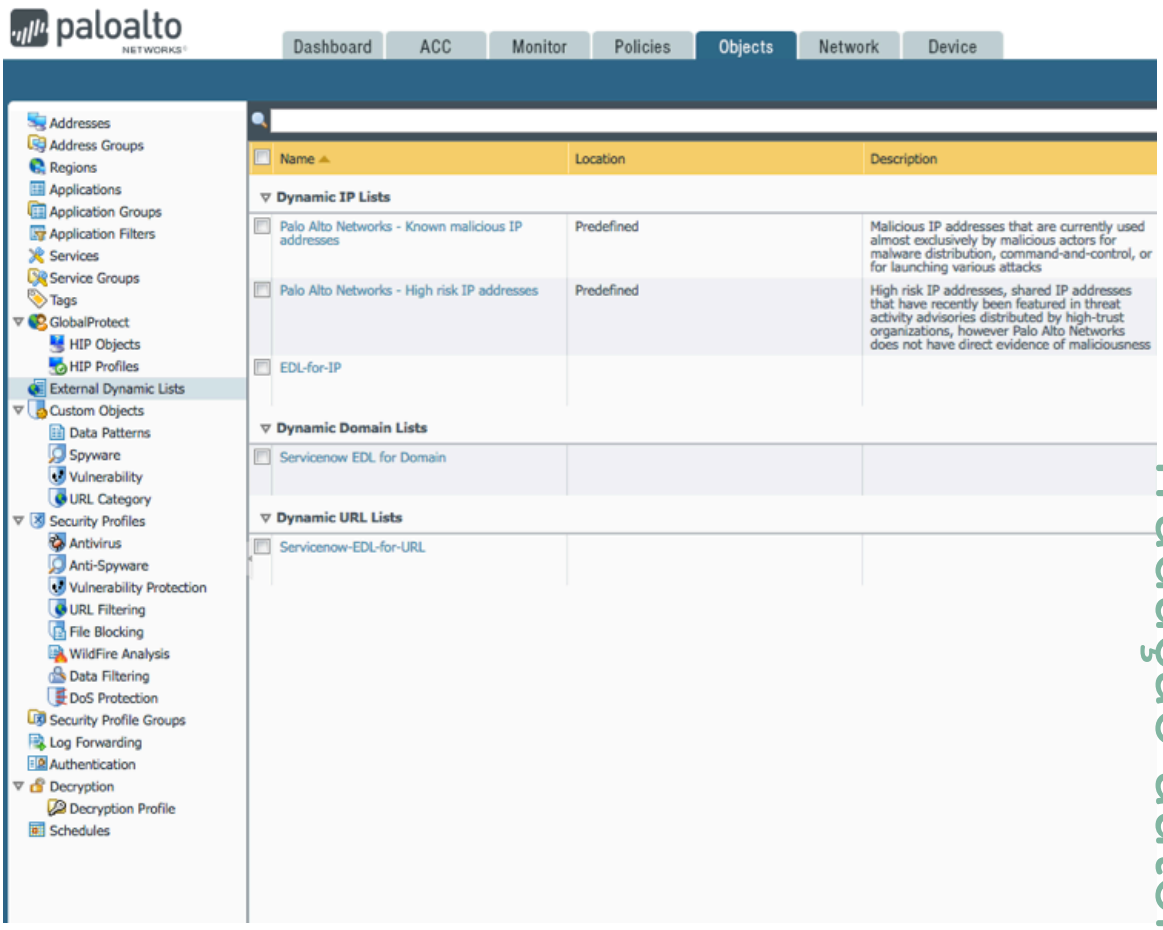
As imagens na seção a seguir são usadas com permissão e são PRIVILEGIADAS e PROPRIETÁRIAS.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

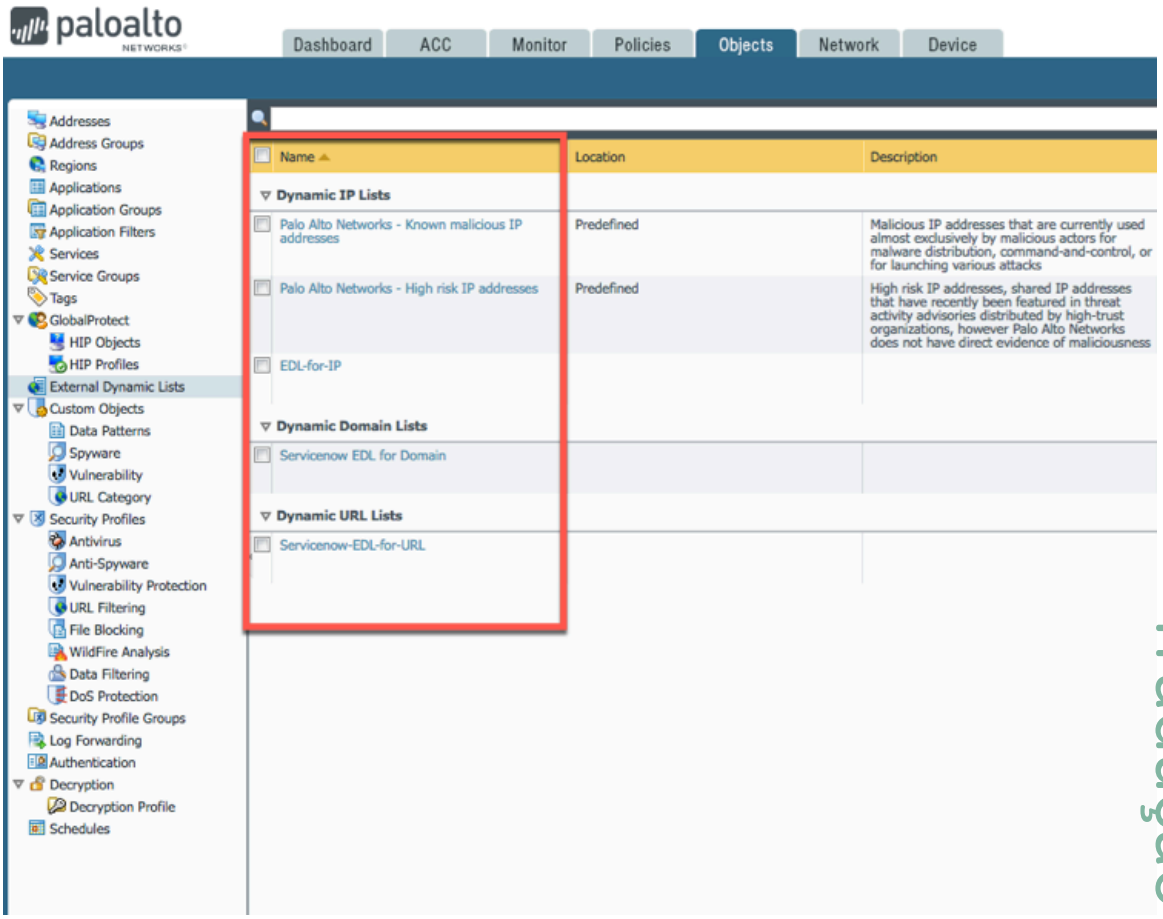
1. Se você não configurou a EDL para o firewall, navegue até **Listas dinâmicas externas** > **Objetos** em Palo Alto Networks.



2. Na coluna **Nome**, selecione o ServiceNow EDL que você deseja configurar na lista, por exemplo, **EDL da ServiceNow para URL**.

Tradução automática

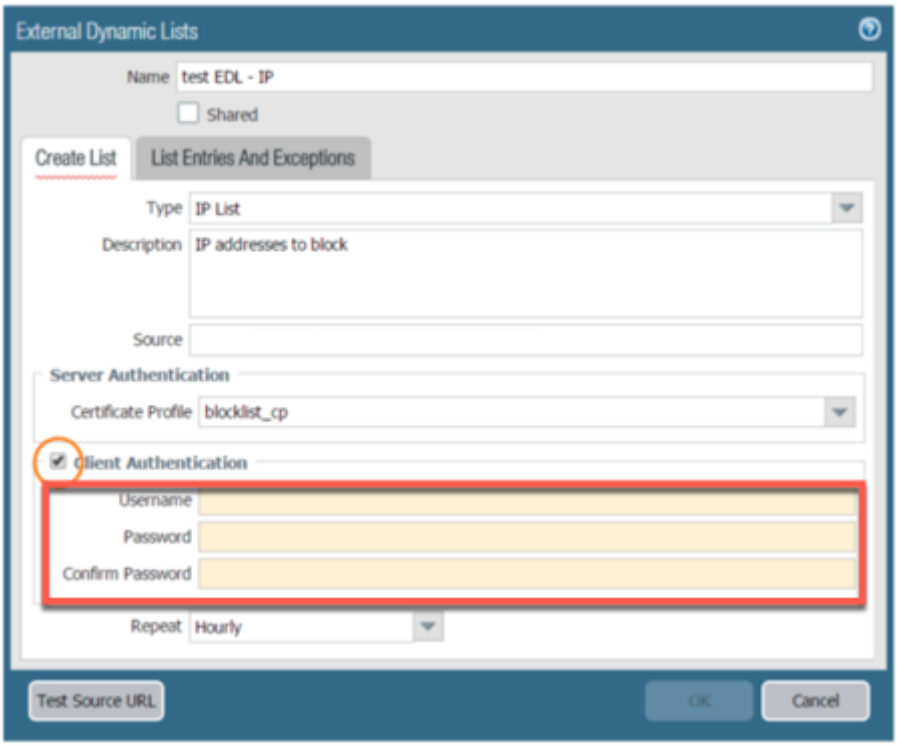
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



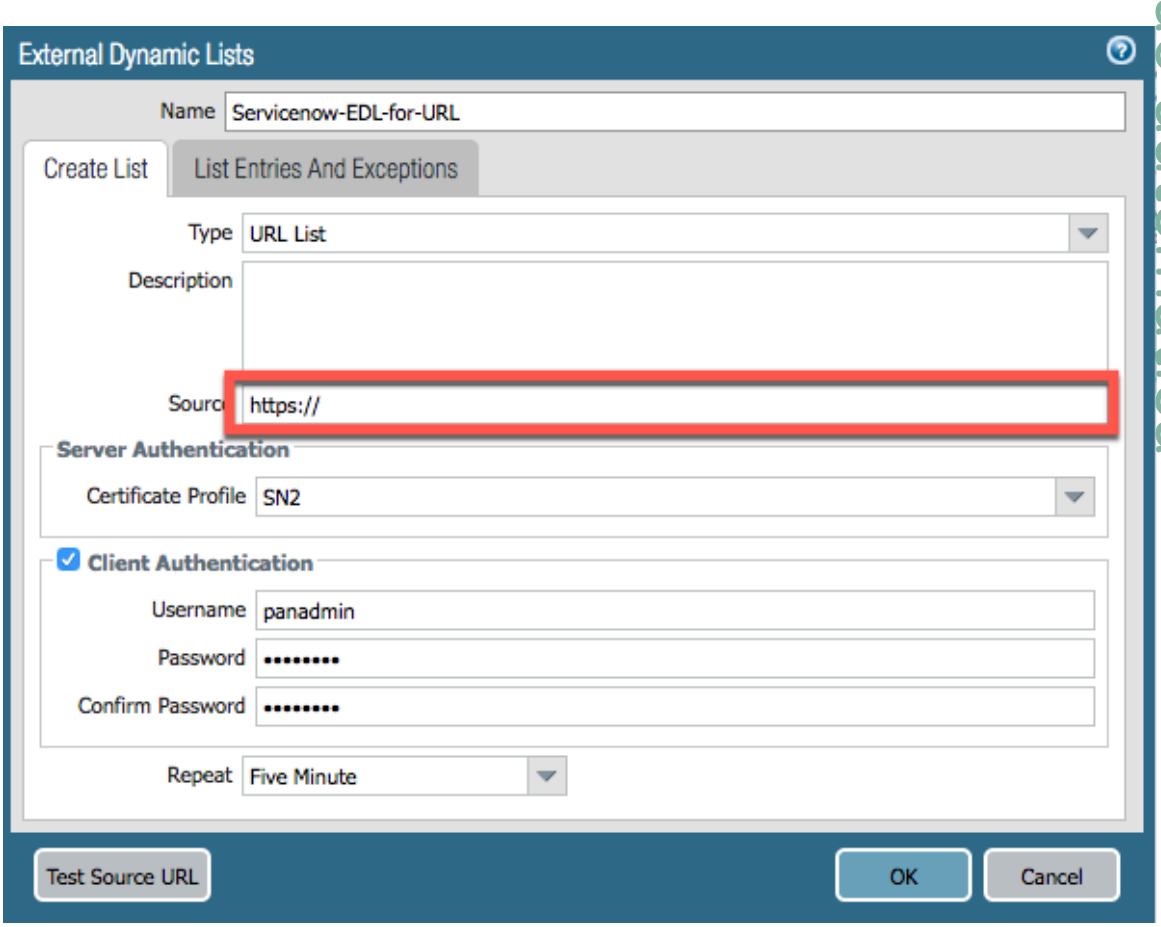
3. Na caixa de diálogo Listas dinâmicas externas, insira o Nome de usuário e a Senha para autenticar com Now Platform®.
Essas credenciais são o nome de usuário e a senha que você criou para a função da conta da API (sn_sec_panfw.api_account_access) na sua instância ServiceNow.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No campo Origem, insira o URL que foi gerado na lista EDL na sua instância ServiceNow.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione um Perfil de certificado na lista de seleção, SN2, por exemplo.
6. Clique em OK.

Ativar uma EDL para Palo Alto Networks Next-Generation Firewall com uma solicitação de mudança

Se configurado, o formulário de solicitação de mudança ServiceNow será usado para ativar a lista dinâmica externa (EDL). Esta opção será recomendada se o administrador do firewall também estiver usando o Now Platform para políticas de firewall ou mudanças de regra. A EDL é ativada automaticamente e fica pronta para receber entradas de EDL após o fechamento da solicitação de mudança Now Platform.

Antes de Iniciar

Nota:
Os números na seção a seguir são mostrados com os **formulários** com guia selecionados em Configurações do sistema. Para obter mais informações sobre como selecionar e limpar formulários com guias, consulte a seção intitulada Exibir formulários com guias em Como configurar o layout do formulário no site de documentação do produto da ServiceNow .

Função necessária: sn_si.admin para aprovar a solicitação de mudança e as tarefas de mudança

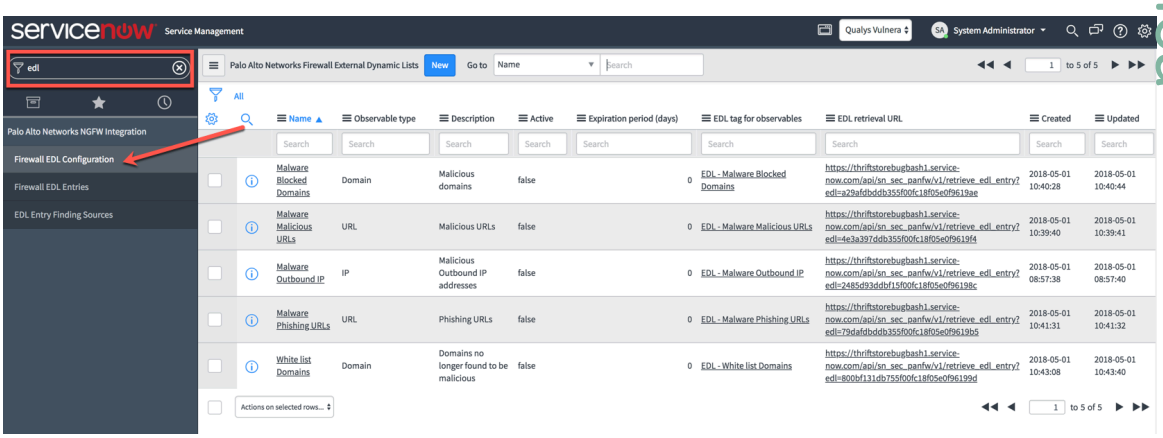
Palo Alto Networks Administrador de firewall para concluir tarefas de configuração no Palo Alto Networks

Por Que e Quando Desempenhar Esta Tarefa

Se configurado, monitore sua solicitação de mudança Now Platform e atribua todas as tarefas necessárias para configurar o Palo Alto Networks Next-Generation Firewall. Depois que essas tarefas forem concluídas, feche a solicitação de mudança Now Platform para ativar a EDL automaticamente.

Procedimento

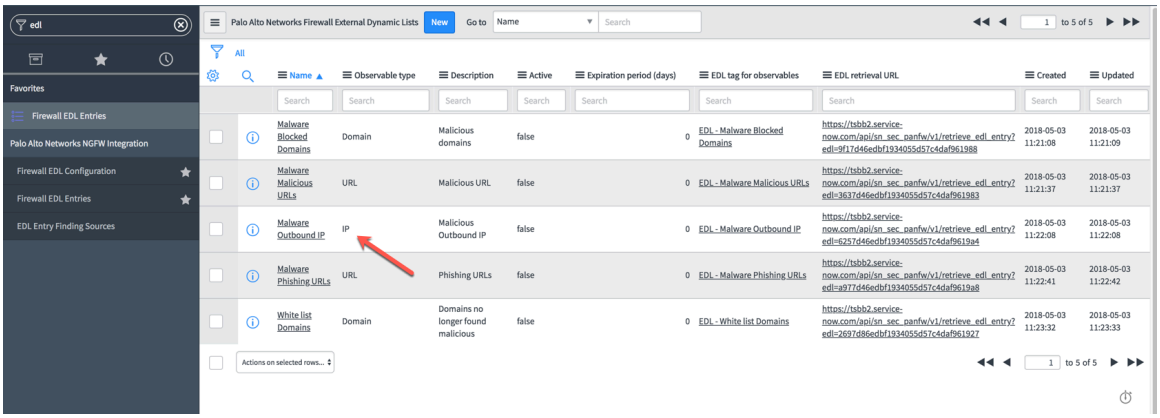
1. Navegar até **Todos** > **Integração de NGFW com a Palo Alto Networks** > **Configuração de EDL do Firewall**.



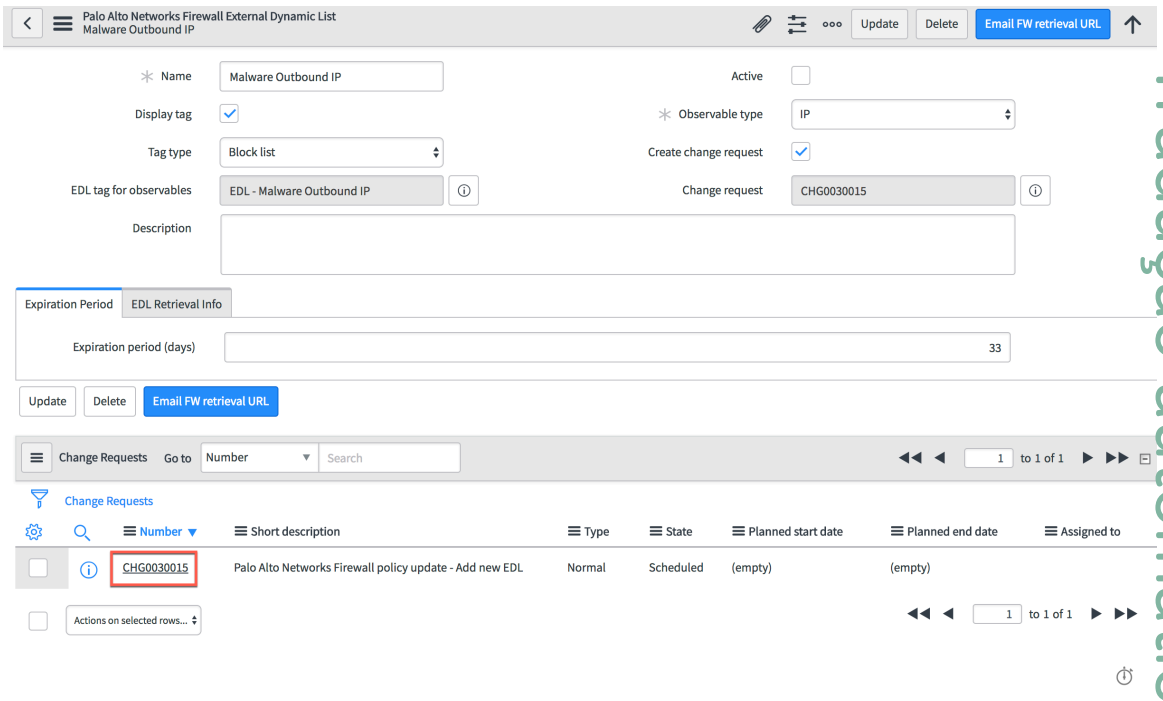
2. Selecione o módulo EDL e clique em um EDL na coluna **Nome**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



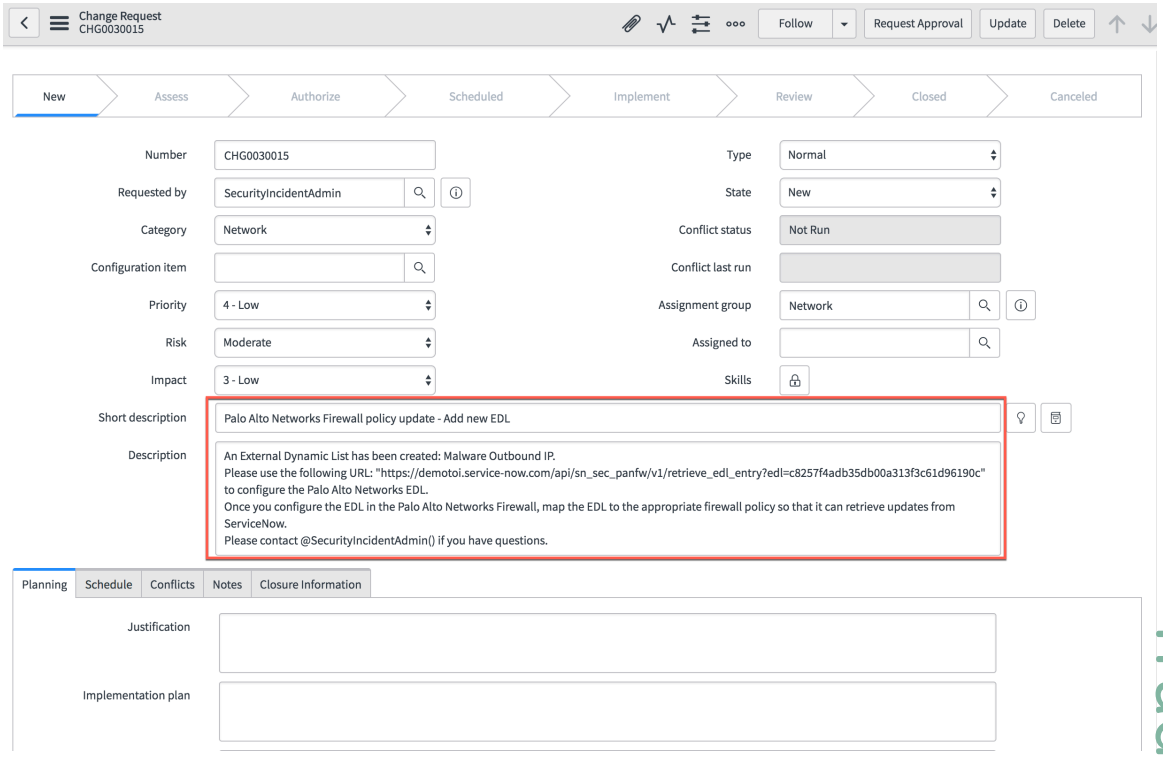
3. No registro EDL aberto, clique no número da solicitação de mudança na lista relacionada Solicitações de mudança.



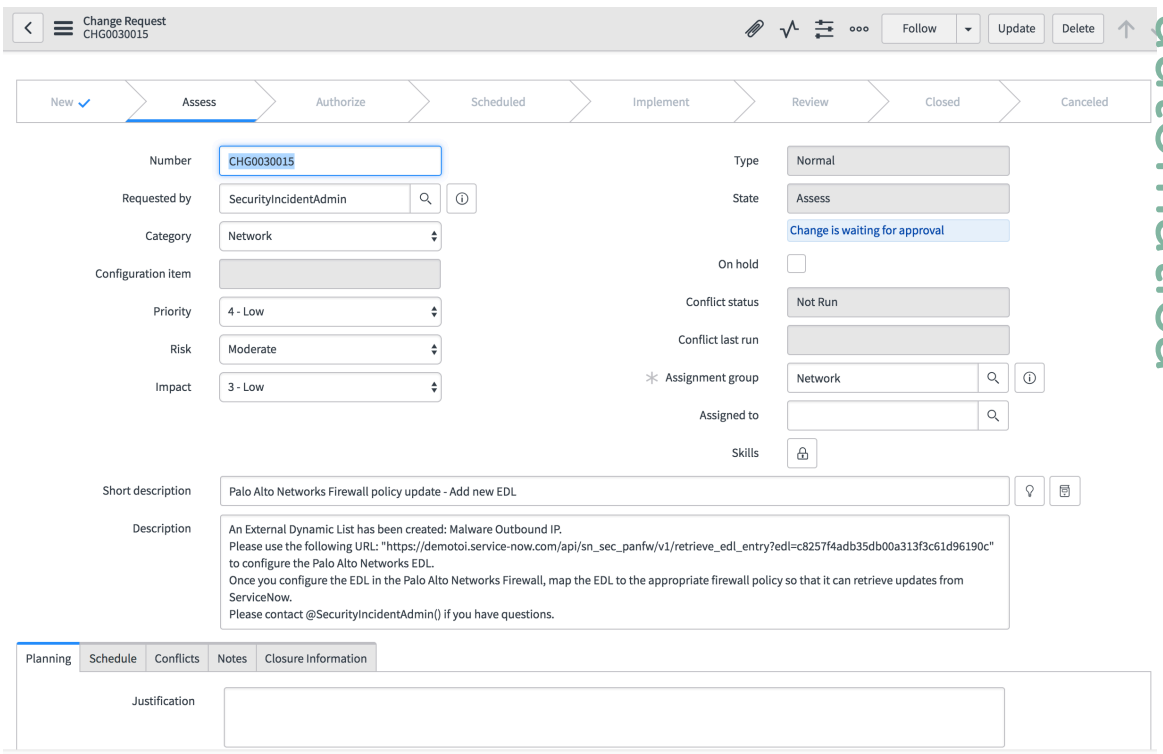
O registro de solicitação de mudança é exibido. O campo **Descrição** lista o URL de recuperação usado para configurar a Palo Alto Networks EDL. Detalhes sobre como mapear a EDL para a política Palo Alto Networks Next-Generation Firewall apropriada também estão incluídos. No campo **Descrição resumida**, um comentário indica que há uma solicitação para adicionar uma nova EDL.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No canto superior direito do registro, clique em **Solicitar aprovação**.
O Estado muda para Avaliar e uma mensagem é exibida informando que a solicitação de mudança está aguardando aprovação.

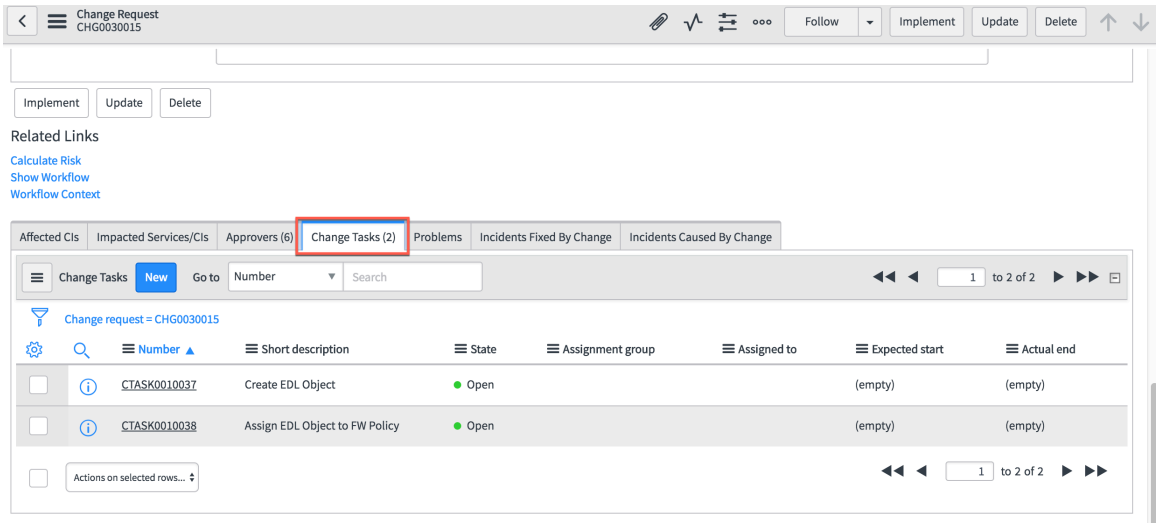


5. Para concluir a solicitação de mudança e ativar a EDL, siga as etapas para atribuir as tarefas e fechar a solicitação de mudança.

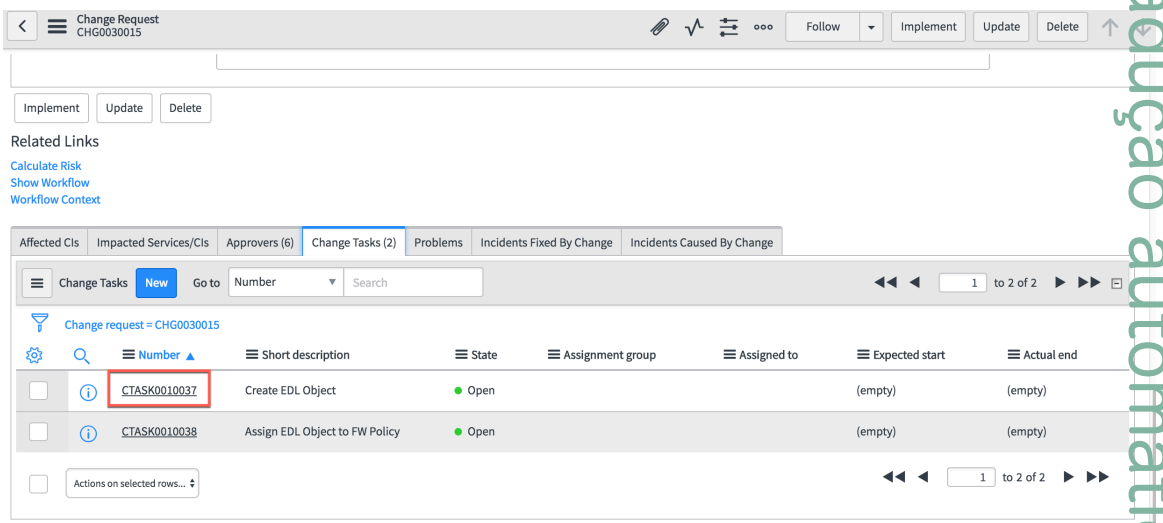
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Se não for exibido, abra a solicitação de mudança e selecione a guia **Tarefas de mudança**.



b. Clique na tarefa associada à criação do objeto EDL para abri-lo.

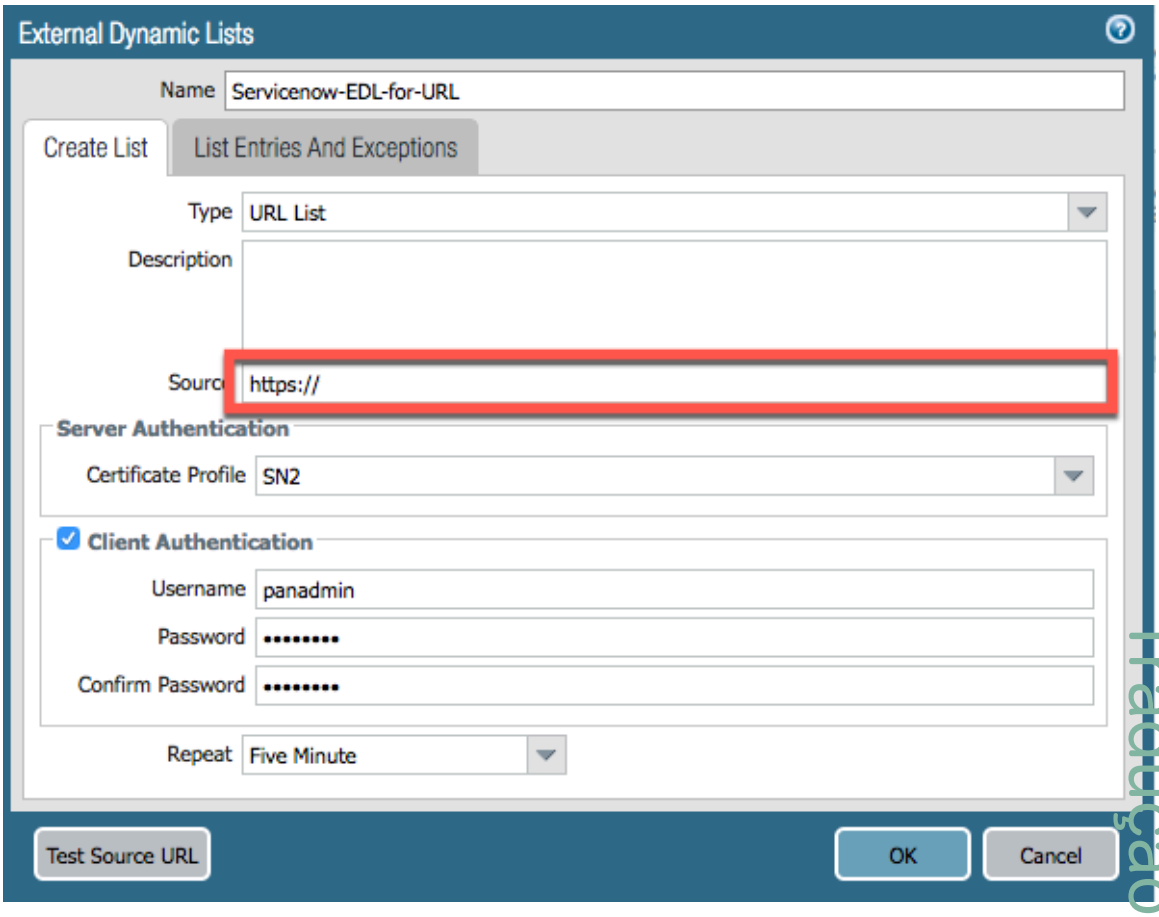


c. No registro exibido, atribua a tarefa ao administrador de firewall Palo Alto Networks e clique em **Atualizar**.
O administrador do firewall é notificado e cria o objeto EDL no Palo Alto Networks Next-Generation Firewall.

Para criar o objeto EDL, o URL de recuperação Now Platform é copiado em Palo Alto Networks em **Listas dinâmicas externas** > **Criar listas** > **Origem**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

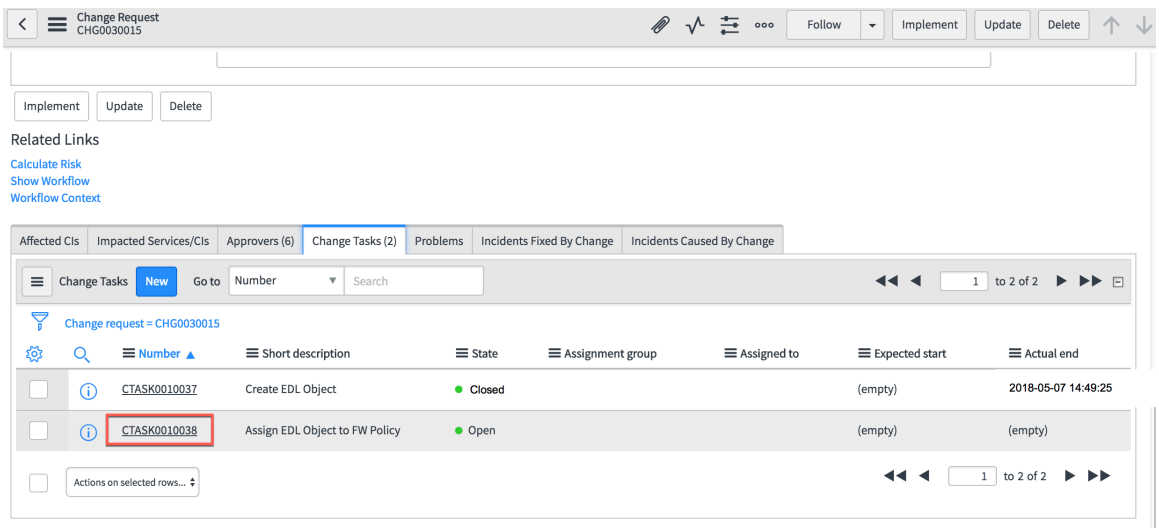


A imagem é usada com permissão e é PRIVILEGIADA e PROPRIETÁRIA.

d. Depois de verificar que o objeto EDL foi criado em Palo Alto Networks, no Now Platform, navegue até a solicitação de mudança associada à criação do objeto EDL e clique em **Fechar tarefa**.

No registro da tarefa para este exemplo, CTASK0010037 foi encerrado para esta tarefa.

e. Navegue até a guia Tarefas de mudança e clique na tarefa para atribuir uma política de firewall ao objeto EDL.



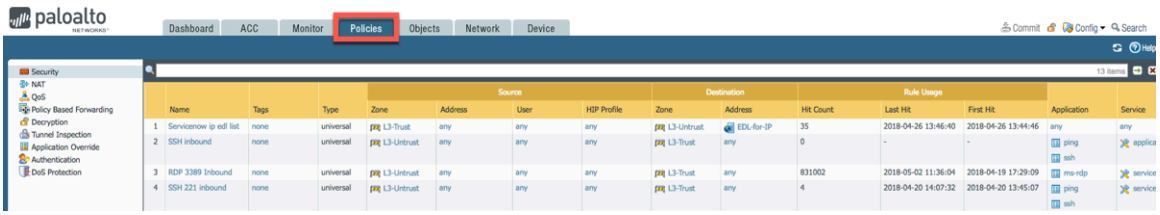
O status de CTASK0010037 é Encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

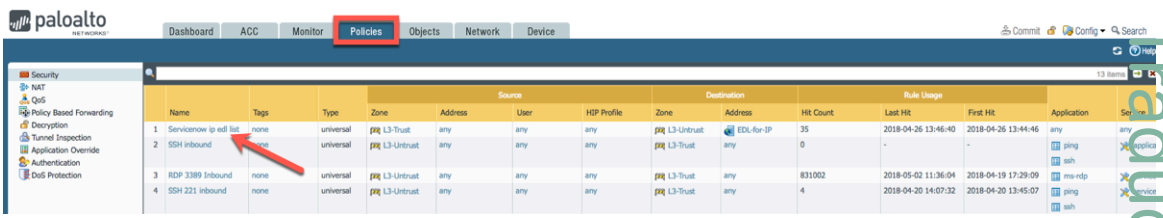
f. Abra o registro e atribua a próxima tarefa.

Depois que a tarefa tiver sido atribuída, em Palo Alto Networks, o administrador do firewall navegará até a guia **Políticas** para atribuir a política.



A imagem é usada com permissão e é PRIVILEGIADA e PROPRIETÁRIA.

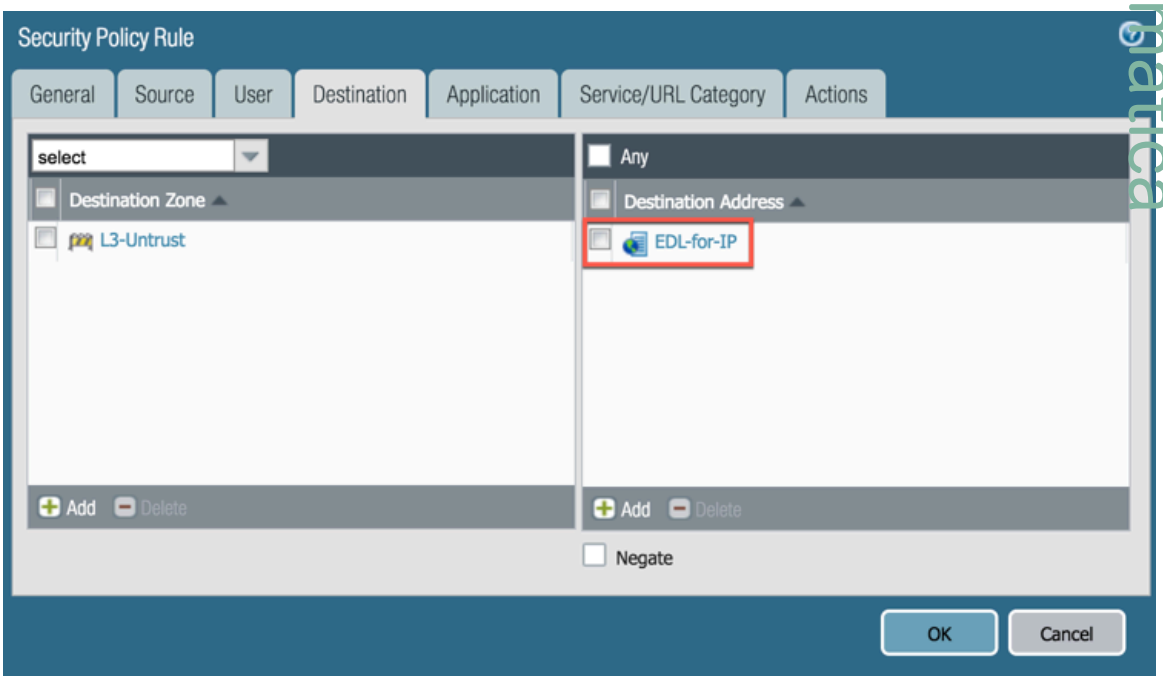
g. Na coluna **Nome**, localize e clique na regra de política de segurança à qual você deseja adicionar a EDL, por exemplo, **ServiceNow ip edl list**.



A imagem é usada com permissão e é PRIVILEGIADA e PROPRIETÁRIA.

h. Na caixa de diálogo Regra de política de segurança, selecione a guia **Destino** para adicionar uma EDL no campo **Endereço de destino**.

i. Para exibir todas as EDLs disponíveis, clique no ícone **Adicionar**.



A imagem é usada com permissão e é PRIVILEGIADA e PROPRIETÁRIA.

Tradução automática

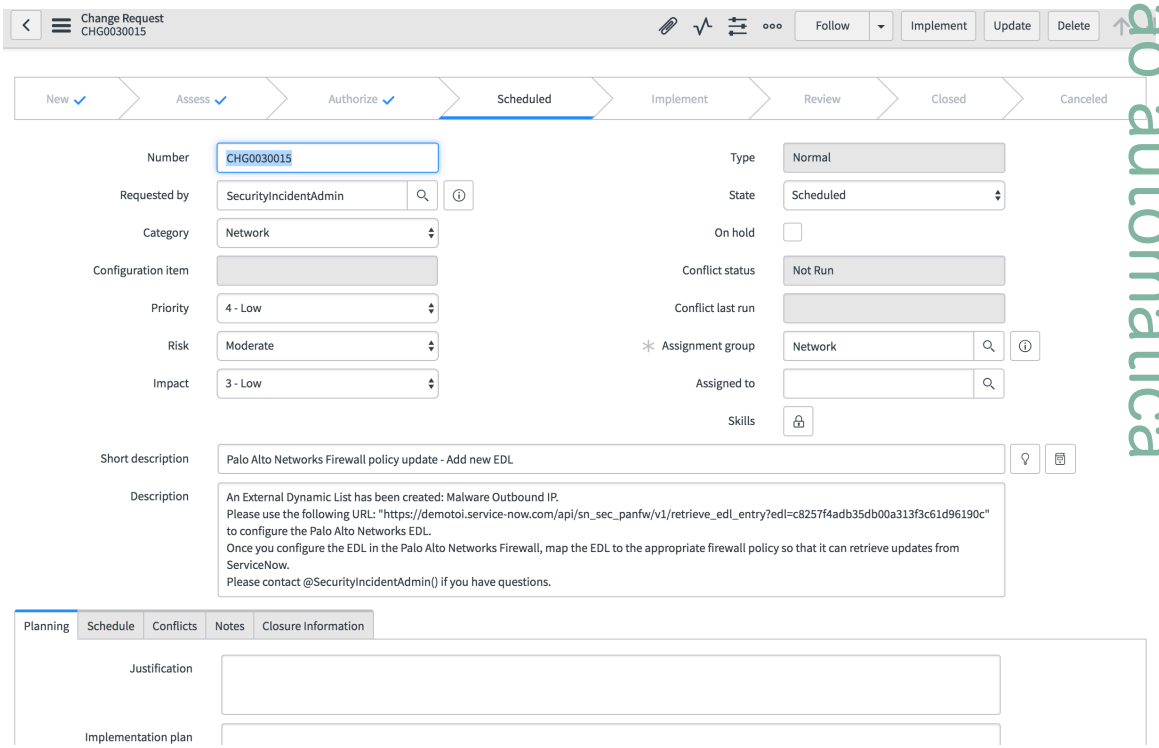
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

j. Clique em **OK**.

k. Depois de verificar que o objeto EDL foi atribuído a uma política de segurança, no Now Platform, navegue até a solicitação de mudança, abra a tarefa associada à atribuição do objeto EDL e clique em **Fechar tarefa**.
Depois que as duas tarefas forem encerradas, a solicitação de mudança estará pronta para aprovação.

l. No registro de solicitação de mudança, clique na lista relacionada **Aprovadores** e selecione um item na coluna **Estado** para abrir a solicitação usada para criar a EDL.

m. No formulário de solicitação de aprovação em aberto, clique em **Aprovar**.
O estado da solicitação de mudança muda para Programado.



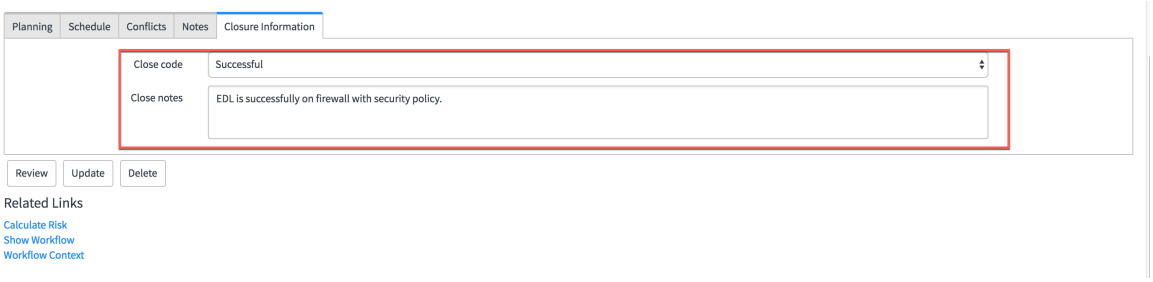
n. Clique em **Implementar**.

o. Clique na guia relacionada **Informações de fechamento** e insira anotações para fechar a solicitação.

Uma entrada neste campo é necessária para fechar a solicitação de mudança.

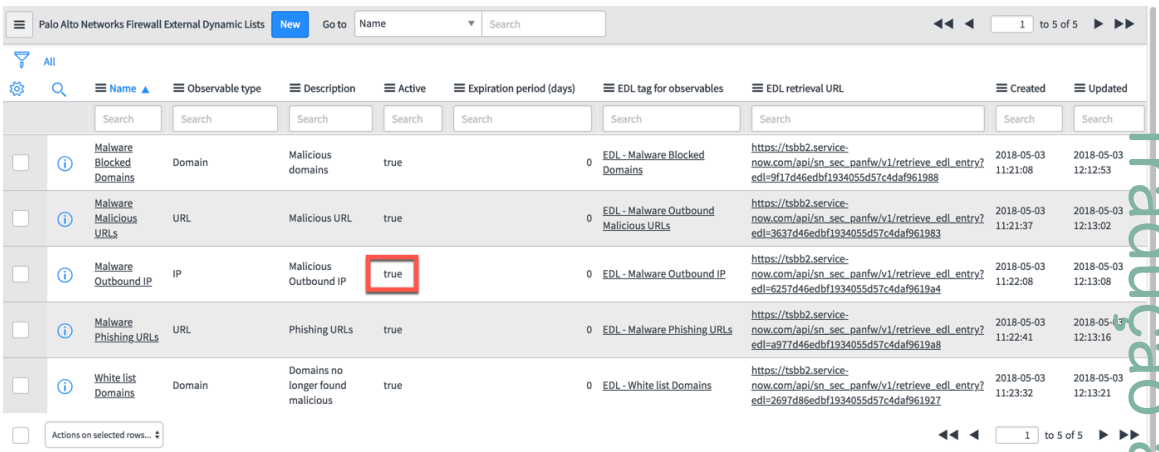
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

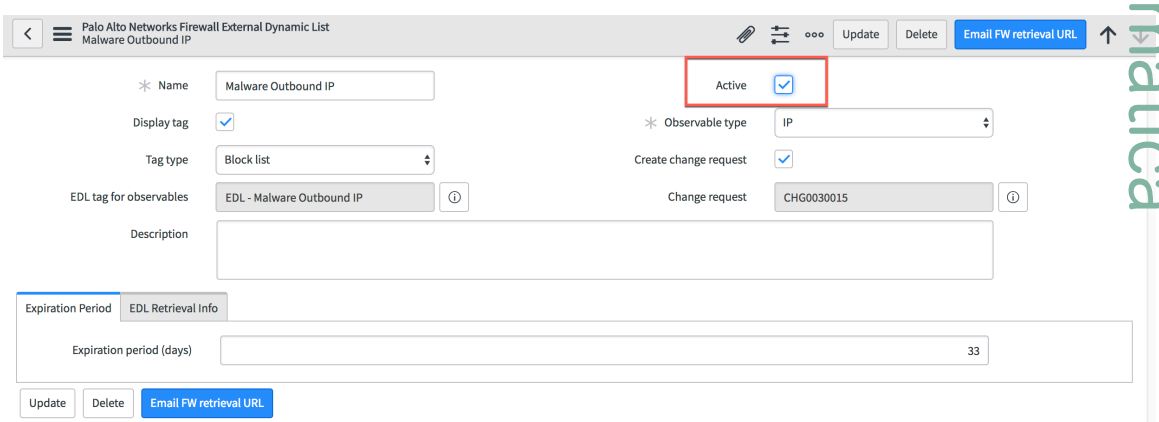


Depois que a solicitação de mudança é fechada, a EDL é ativada automaticamente. Se você não verificou se a EDL está ativada, navegue até **Integração de NGFW com a Palo Alto Networks** > **Configuração de EDL do Firewall**.

Na coluna Ativo na lista, observe que o status da EDL é (verdadeiro).



Na coluna Nome, clique no nome EDL e, no registro aberto, observe que a caixa de seleção **Ativa** também está marcada.



A EDL agora está pronta para aceitar entradas da EDL.

O que Fazer Depois

Envie entradas de EDL de um incidente de segurança ou da lista de bloqueios.

Enviar entradas de EDL de um registro de incidente de segurança para Palo Alto Networks Next-Generation Firewall

Os observáveis anexados a um registro de incidente de segurança são enviados para aprovação como entradas de Lista dinâmica externa (EDL) para EDLs. Um processo de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

aprovação para entradas de EDL faz parte do fluxo de trabalho pré-configurado. O firewall importa entradas de EDL - endereços IP, URLs, domínios - que estão incluídas nas listas de EDL e impõe a política.

Antes de Iniciar

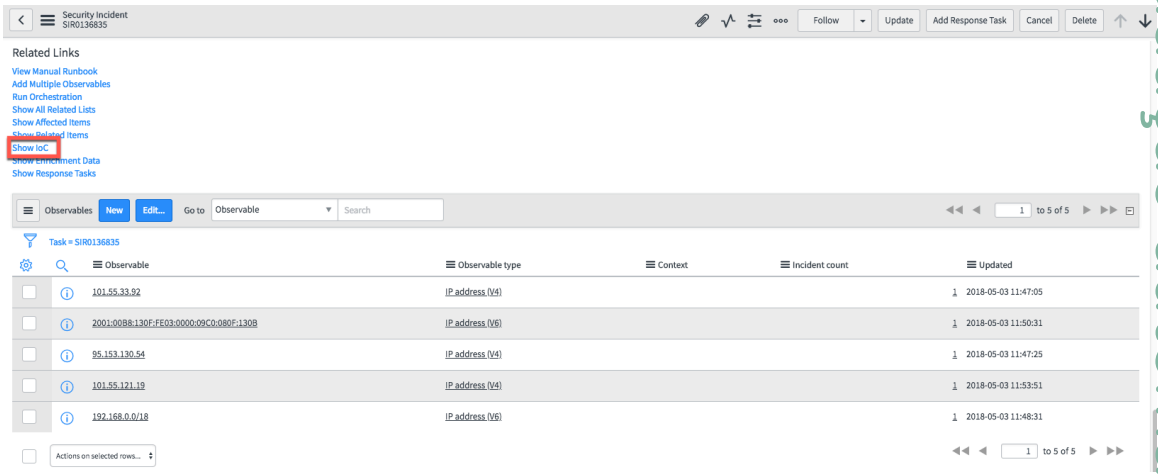
Função necessária: sn_si.analyst para enviar entradas de EDL. Para aprovar entradas EDL: a aprovação é atribuída a sn_si.admin por padrão, mas essa autoridade pode ser atribuída conforme exigido pela sua organização.

Por Que e Quando Desempenhar Esta Tarefa

Usuários com a função sn_si.analyst enviam entradas de EDL solicitando um bloco em observáveis anexados a um registro de incidente de segurança. Depois de enviada, uma entrada de EDL com um status Pendente é gerada e enviada para aprovação. O exemplo a seguir mostra uma solicitação de bloqueio para um observável de URL.

Procedimento

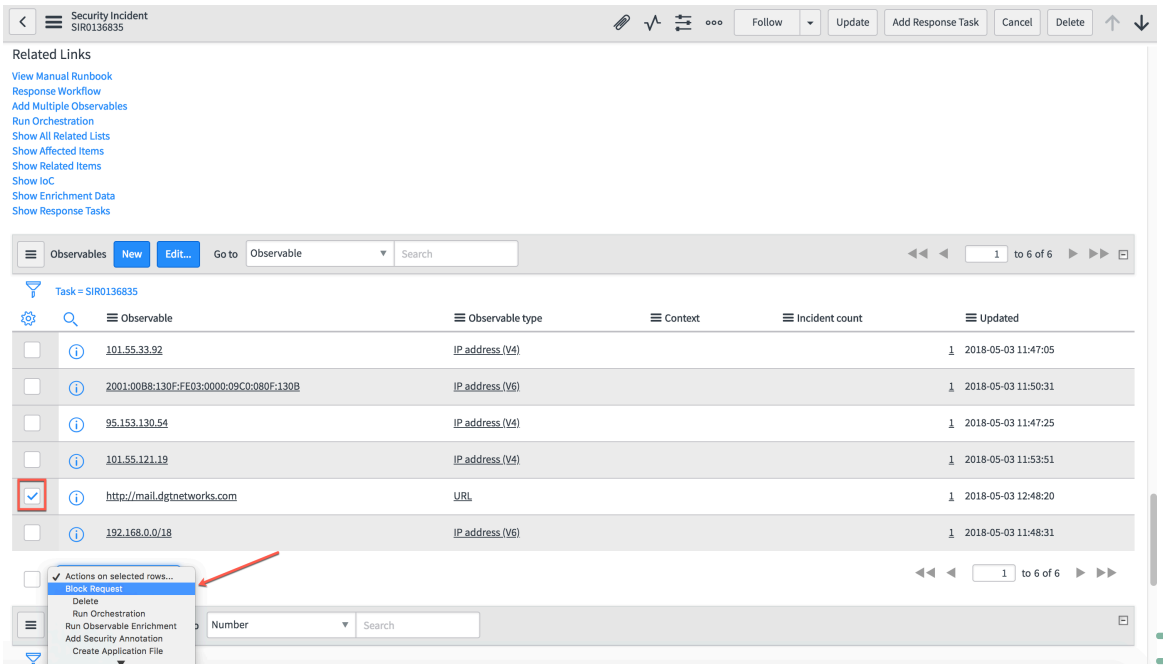
1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar Todos os Incidentes**e clique em um registro de incidente de segurança para abri-lo.
2. Clique no link relacionado **Mostrar IoC**.



3. Na lista relacionada Observáveis, selecione os observáveis que você deseja bloquear e, na lista **Ações nas linhas selecionadas**, selecione **Solicitação de bloqueio**.

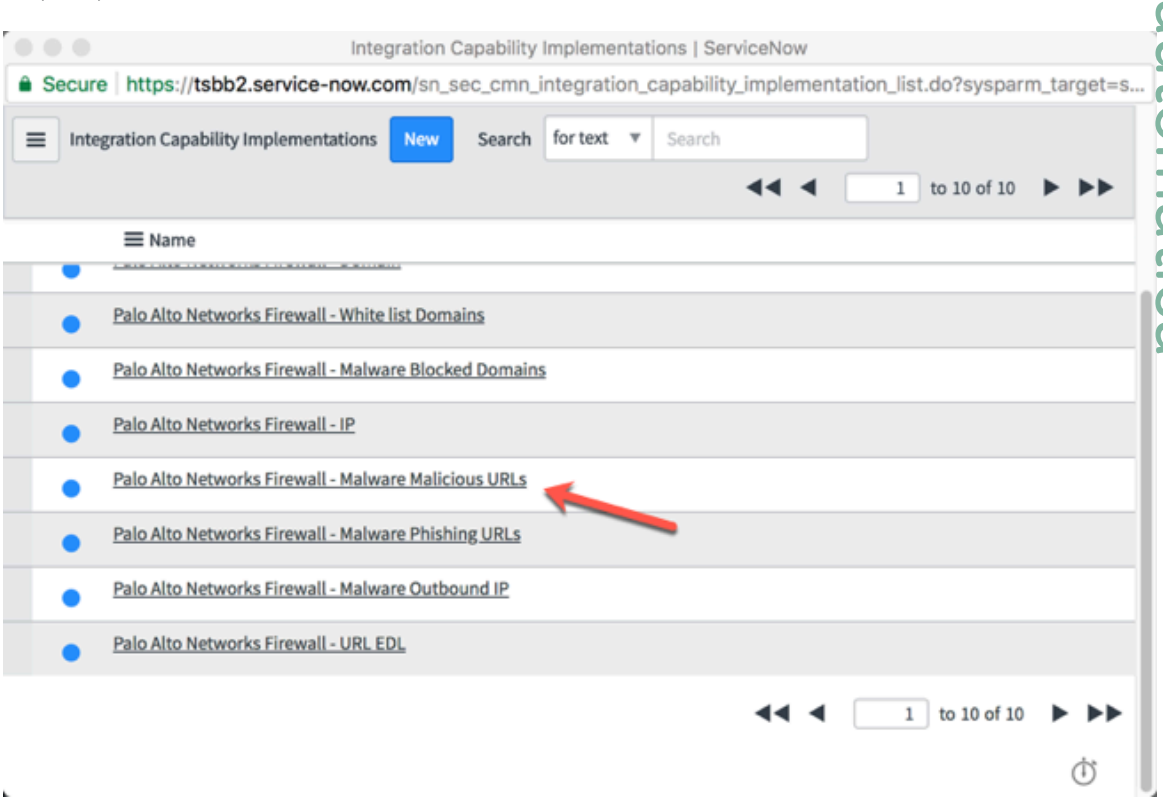
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Na caixa de diálogo exibida, clique no ícone de pesquisa (ícone de).
5. Na lista exibida, selecione a EDL à qual você deseja anexar esta entrada.

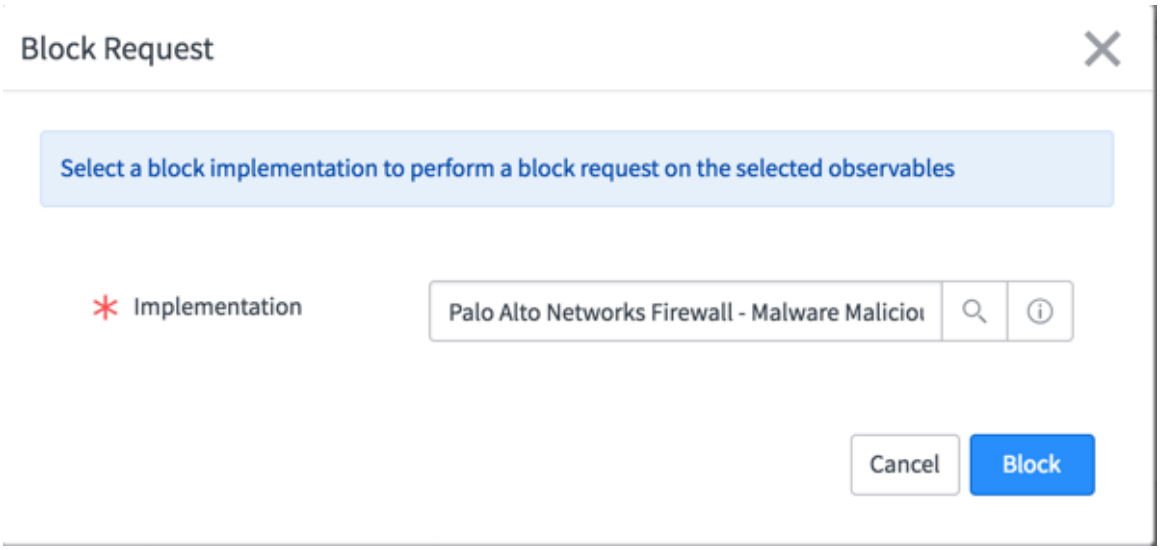
Nota:
Para este exemplo, o tipo de observável de entrada (URL) deve corresponder ao tipo de observável EDL (URL).



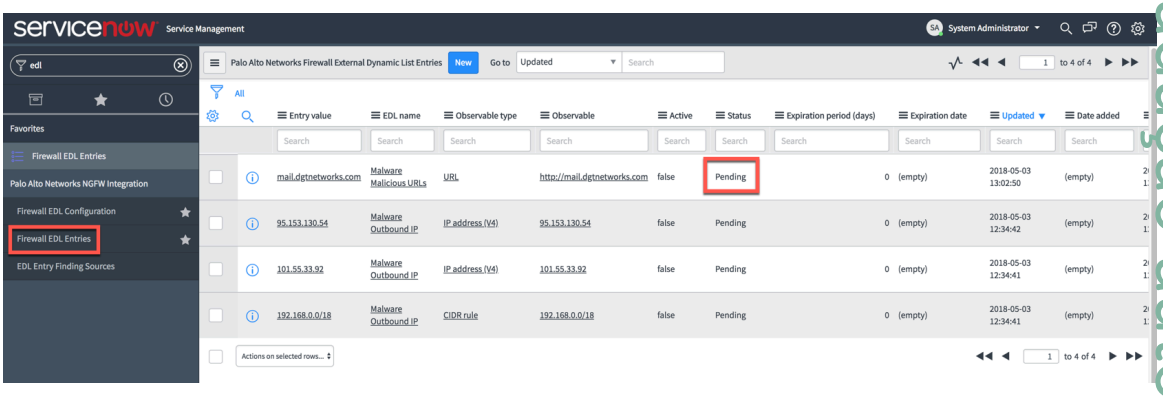
6. Na caixa de diálogo Solicitação de bloqueio com o nome da EDL exibido no campo **Implementação**, clique em **Bloquear**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

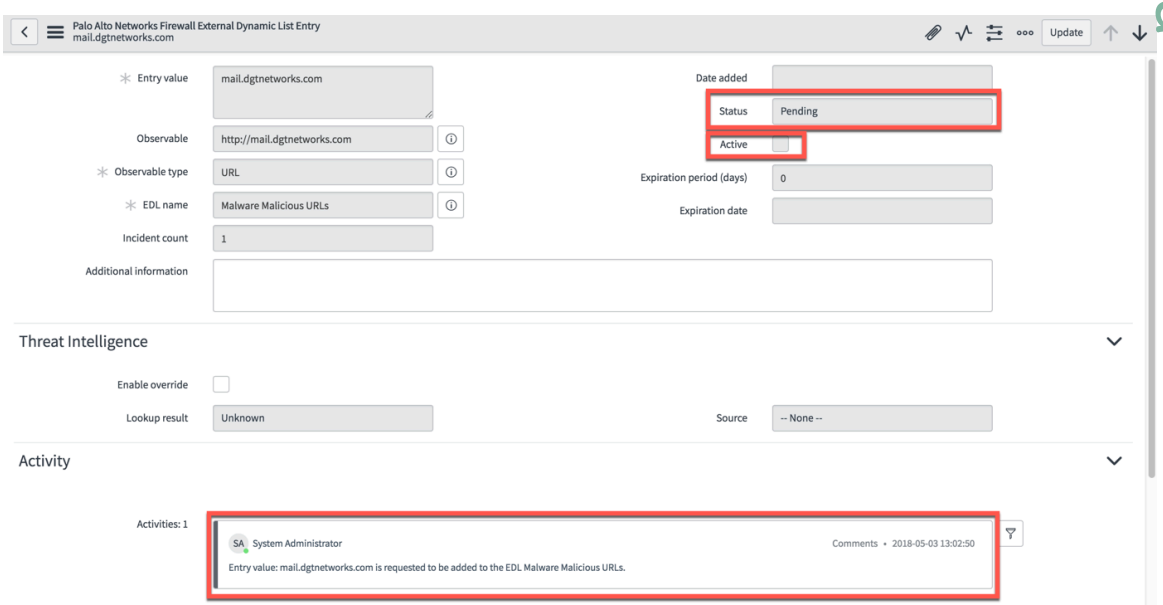


7. Navegar até **Integração de NGFW com a Palo Alto Networks** > **Entradas de EDL do Firewall** e clique em **Entradas de EDL do firewall**.



8. Na lista de Entradas da Lista Dinâmica Externa do Firewall da Palo Alto Networks, clique no seu observável na coluna **Valor de entrada** para abrir o registro.

   Para este exemplo, o registro de **mail.dgtnetworks.com** é exibido.

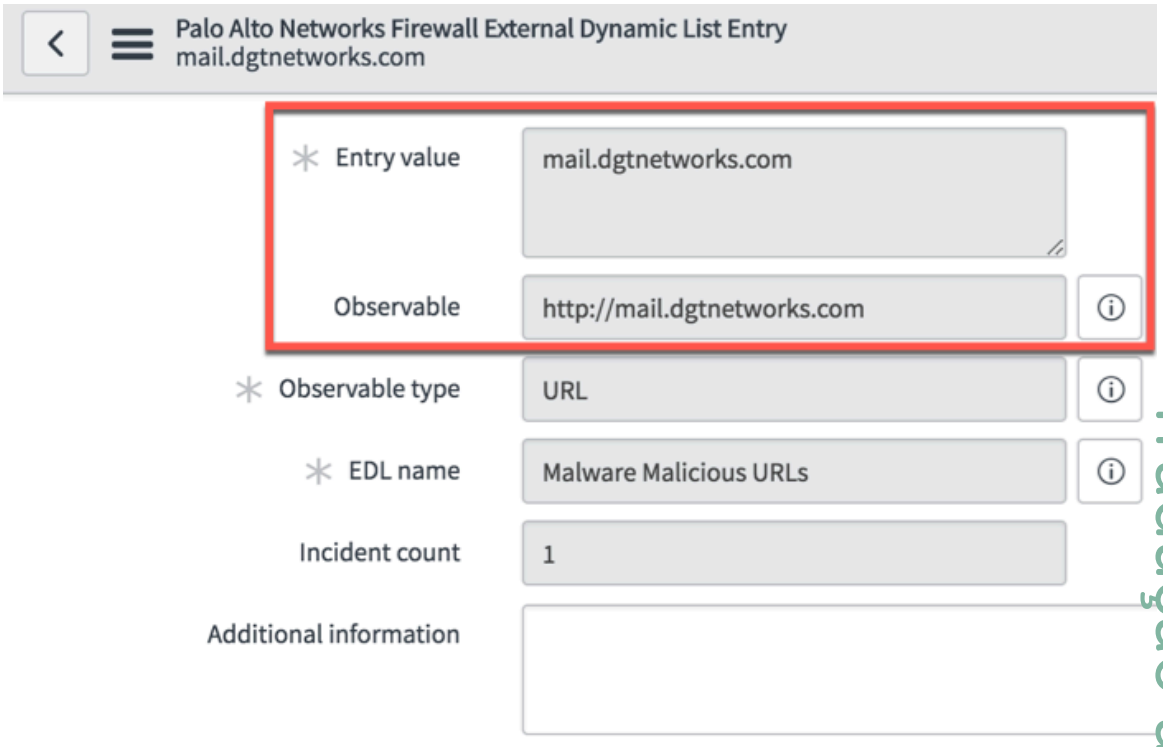


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O status é Pendente, a caixa de seleção Ativo está desmarcada e as anotações de trabalho mostram que há uma solicitação para adicionar o observável. Esta solicitação de entrada de EDL está pronta para aprovação.

Os campos Valor de entrada e Observável mostram formatos diferentes para o observável de URL.



O ícone ao lado do campo Observável é um link para a tabela Now Platform® Observável.

O valor no campo Observável (http://mail.dgtnetworks.com) é vinculado à tabela Observável e corresponde ao formato que foi trazido do evento de acionamento de incidente Security Incident Response.

O Now Platform® pode modificar automaticamente as entradas da EDL para que sejam compatíveis com o formato de URL da EDL Palo Alto Networks.

Neste exemplo, o observável foi criado com o protocolo http:// (http://mail.dgtnetworks.com) e este formato é exibido no campo Observável. O protocolo http:// é removido automaticamente do observável pelo Now Platform®, portanto, é compatível com Palo Alto Networks e pode ser recuperado. Como resultado, mail.dgtnetworks.com é exibido no campo Valor de entrada.

O que Fazer Depois

Aprovar entradas de EDL.

Tópicos relacionados

Exceções de entrada de EDL para Palo Alto Networks Next-Generation Firewall

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Enviar entradas de EDL da lista de bloqueios para Palo Alto Networks Next-Generation Firewall

Para observáveis determinados como mal-intencionados e não associados a um incidente de segurança Now Platform específico, envie entradas de Lista dinâmica externa (EDL) da lista de bloqueios.

Antes de Iniciar

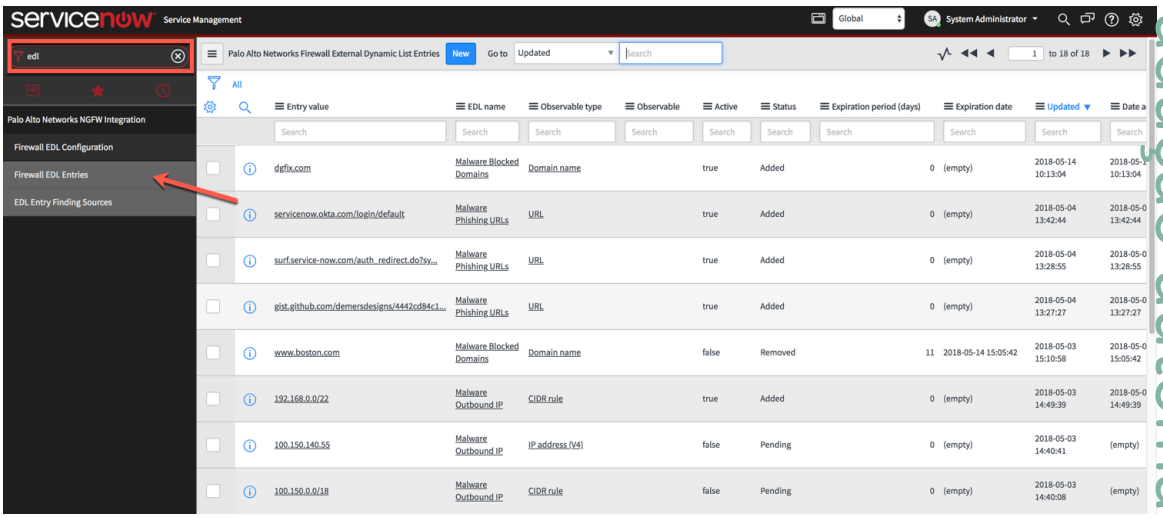
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Quando você quiser bloquear um observável que você determinou que é malicioso ou permitir que um observável que você determinou não seja malicioso e o observável não esteja associado a um registro de incidente de segurança Now Platform específico, envie entradas de EDL diretamente da lista de bloqueios. Exemplos desses tipos de entradas EDL podem ser URLs ou domínios para sites específicos.

Procedimento

1. Navegar até **Todos** > **Integração de NGFW com a Palo Alto Networks** > **Entradas de EDL do Firewall**.



2. Clique no módulo **Entradas de EDL do Firewall**.
3. Na lista de Entradas da Lista Dinâmica Externa do Firewall da Palo Alto Networks, clique em **Novo**.
4. No novo registro exibido, no campo **Valor de entrada**, insira um valor para o seu observável.
   Os dois resultados possíveis desta entrada:

   Os campos restantes no formulário são preenchidos automaticamente.

   Um observável correspondente é encontrado e uma mensagem é exibida informando que existe um observável correspondente. Selecione a EDL à qual você deseja anexar esta entrada e clique em **Enviar**. Selecione a EDL à qual você deseja anexar esta entrada antes de definir o período de expiração.

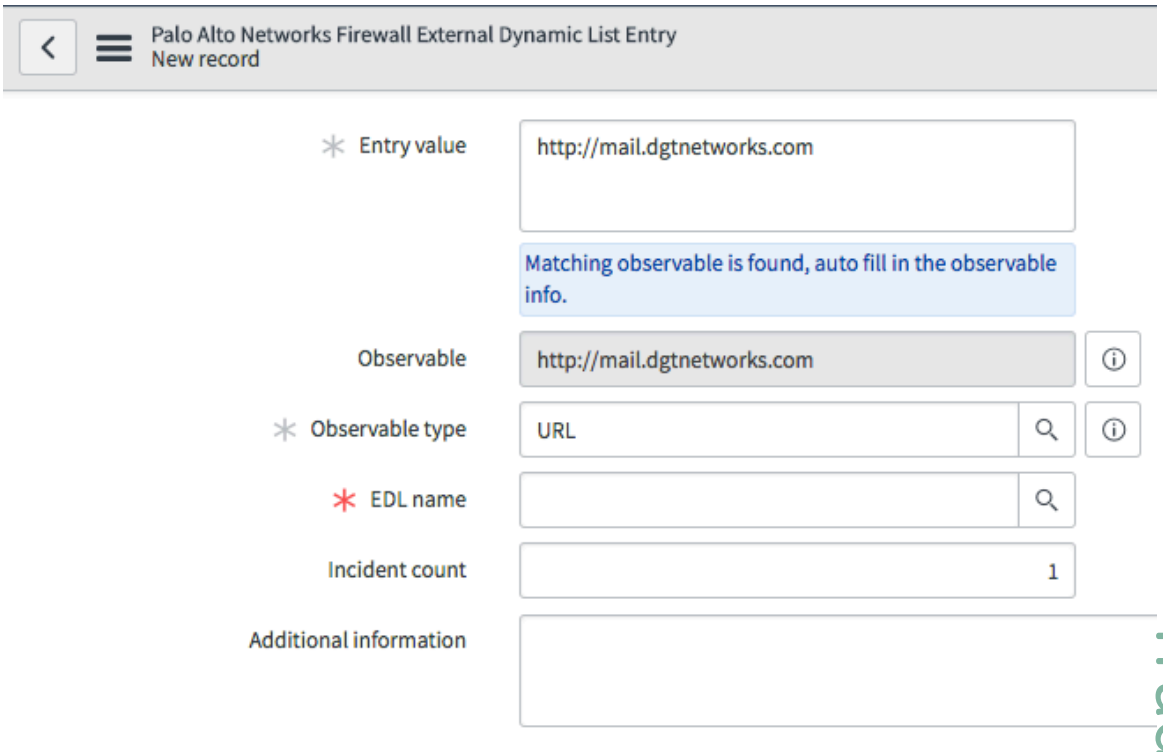
   Uma mensagem será exibida instruindo você a preencher o formulário.

   Um observável correspondente não foi encontrado e você deve preencher o formulário. Depois de concluir, selecione a EDL à qual você deseja anexar o observável e clique em **Enviar**. Um registro observável é criado.

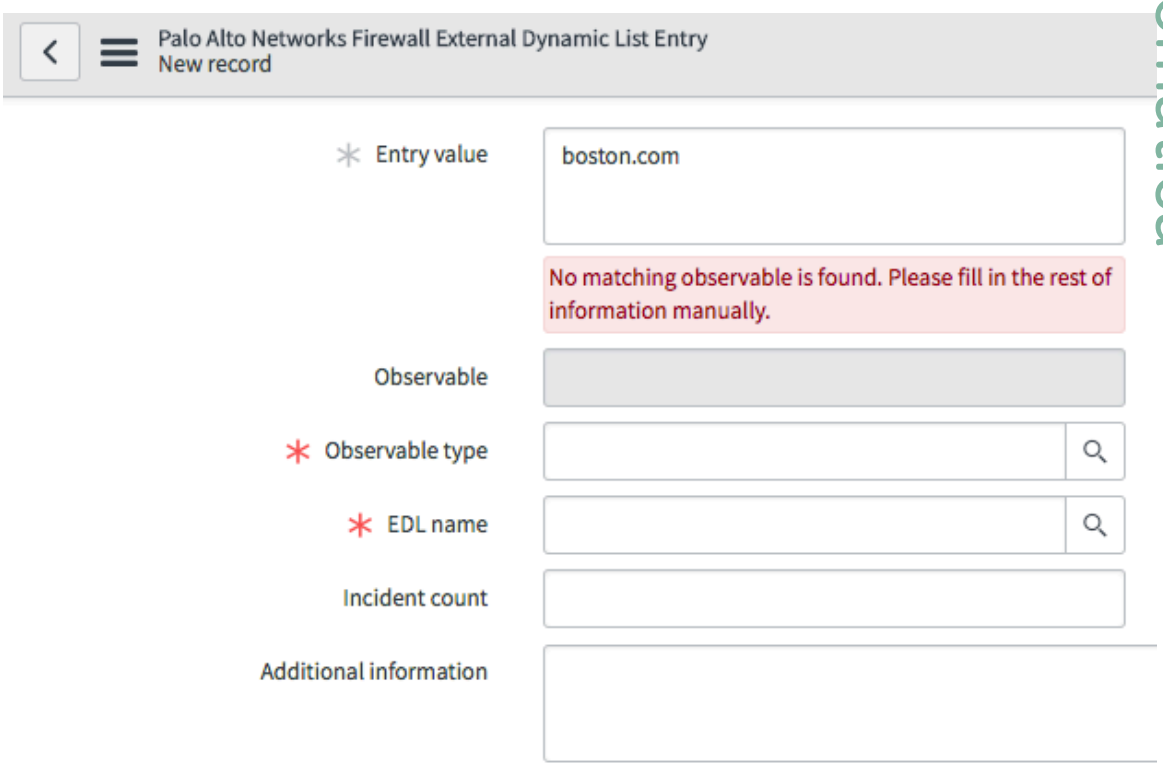
   A figura a seguir mostra um exemplo de um observável de domínio existente e como os campos são preenchidos automaticamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



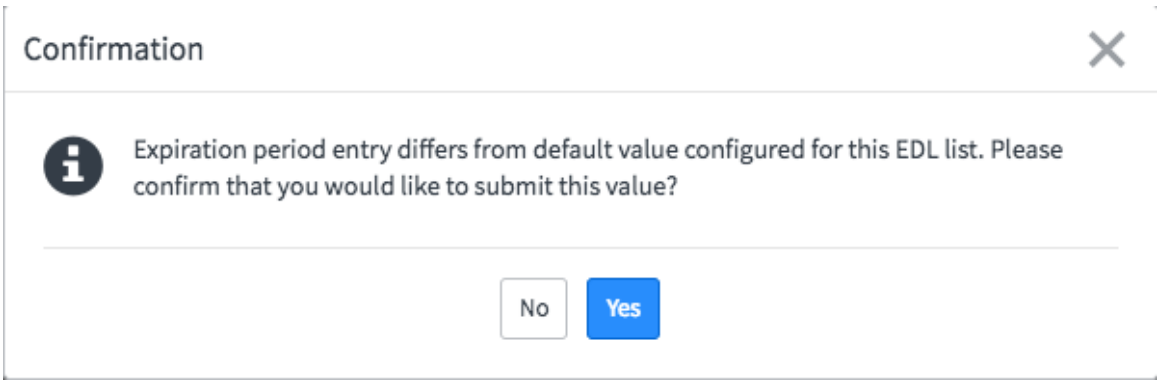
5. Clique no ícone de pesquisa para selecionar a EDL à qual você deseja anexar a entrada.
6. Clique em **Enviar**.
   Se você tiver a aprovação por e-mail configurada em seu fluxo de trabalho, uma solicitação de e-mail de aprovação será enviada.
7. Se for exibida uma mensagem solicitando que você preencha o restante das informações manualmente, preencha os campos.



Tradução automática

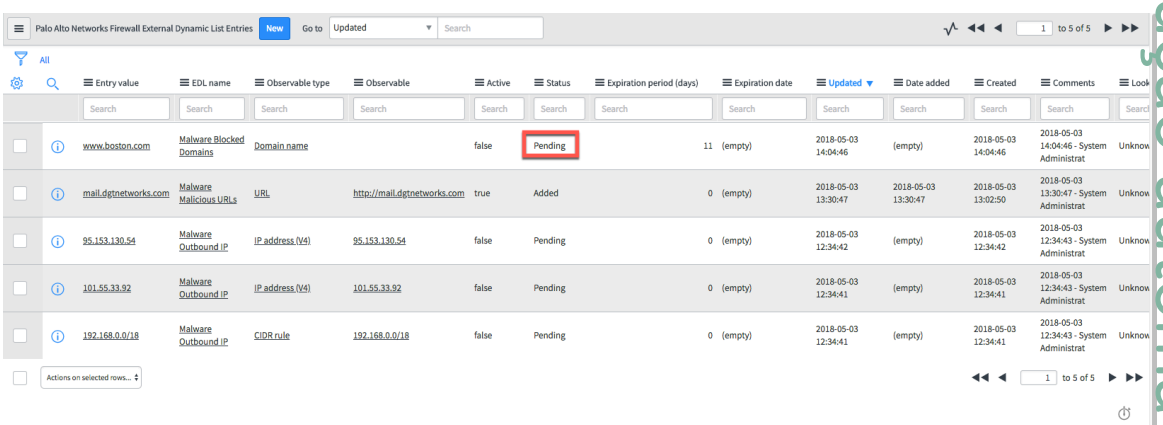
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Clique em **Enviar**.
   Se você alterou o período de expiração padrão da entrada da EDL, uma caixa de diálogo de confirmação de aviso será exibida indicando que o período é diferente da EDL selecionada.



9. Escolha uma opção para configurar o período de expiração.

10. Se não for exibido, navegue até a **lista Entradas da Lista Dinâmica Externa do Firewall da Palo Alto Networks** e observe que o status da entrada é Pendente.



A entrada está pronta para aprovação.

O que Fazer Depois

Aprovar entradas de EDL.

Tópicos relacionados

Exceções de entrada de EDL para Palo Alto Networks Next-Generation Firewall

Aprovar entradas de EDL para Palo Alto Networks Next-Generation Firewall

Um processo de aprovação para entradas da Lista dinâmica externa (EDL) faz parte do fluxo de trabalho pré-configurado. Você aprova as entradas de EDL antes que as entradas sejam ativadas em EDLs. Depois que você aprova a entrada EDL, o firewall recupera a entrada e seu observável é bloqueado a partir desse ponto.

Antes de Iniciar

Função necessária: a aprovação de entradas de EDL é atribuída a sn_si.admin por padrão, mas essa autoridade pode ser atribuída conforme exigido pela sua organização. No exemplo a seguir, o administrador Now Platform tem autoridade de aprovação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

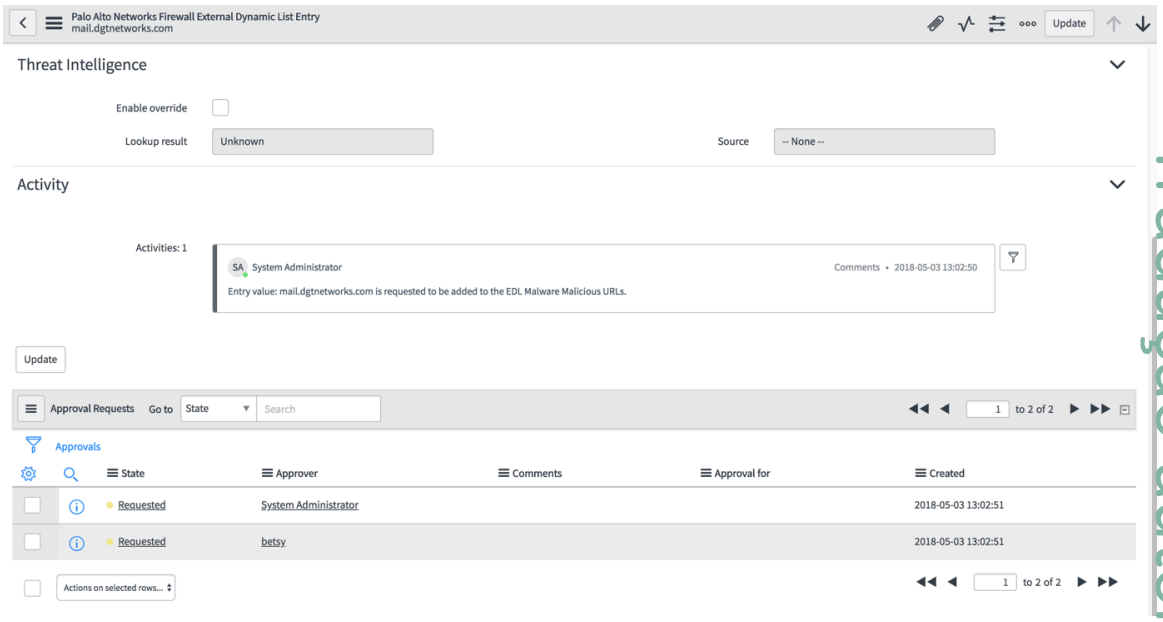
Por Que e Quando Desempenhar Esta Tarefa

Quando o processo de aprovação está habilitado, uma entrada de EDL não é ativada ou desativada na EDL até que seja aprovada.

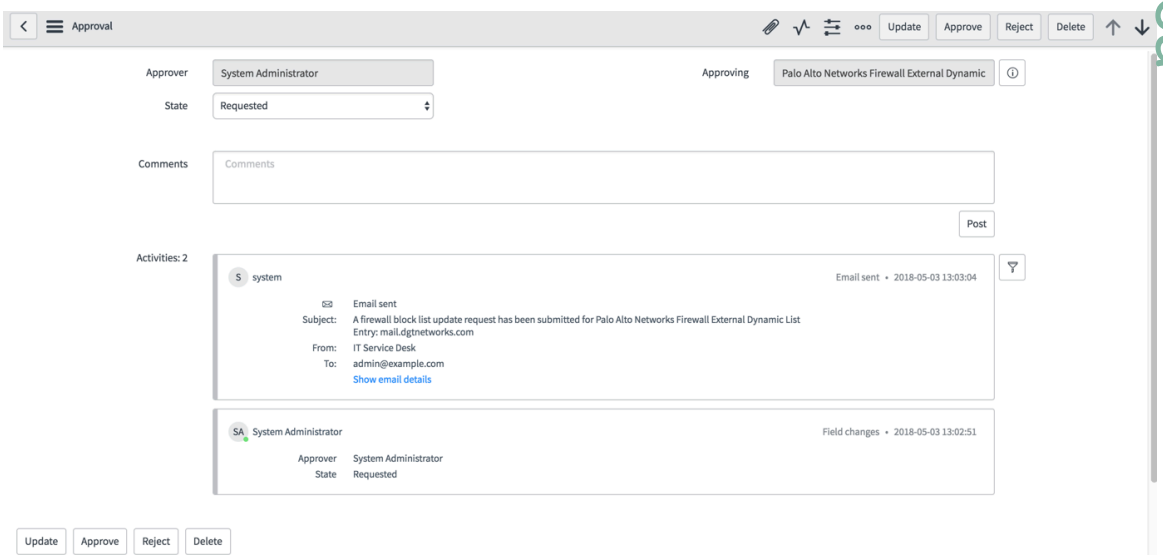
Procedimento

1. Navegar até **Todos** > **Integração de NGFW com a Palo Alto Networks** > **Entradas de EDL do Firewall** e abra o registro EDL.
2. No registro EDL, role até a seção Solicitações de aprovação.

> **Nota:**
> Se você tiver Formulários com guia selecionados em Configurações do sistema, a seção aparecerá como uma guia no registro.



3. Em Solicitações de aprovação, clique em um item na coluna **Estado** para abri-lo.
   O registro de aprovação é exibido.



4. Escolha uma opção para aprovar a entrada da EDL.

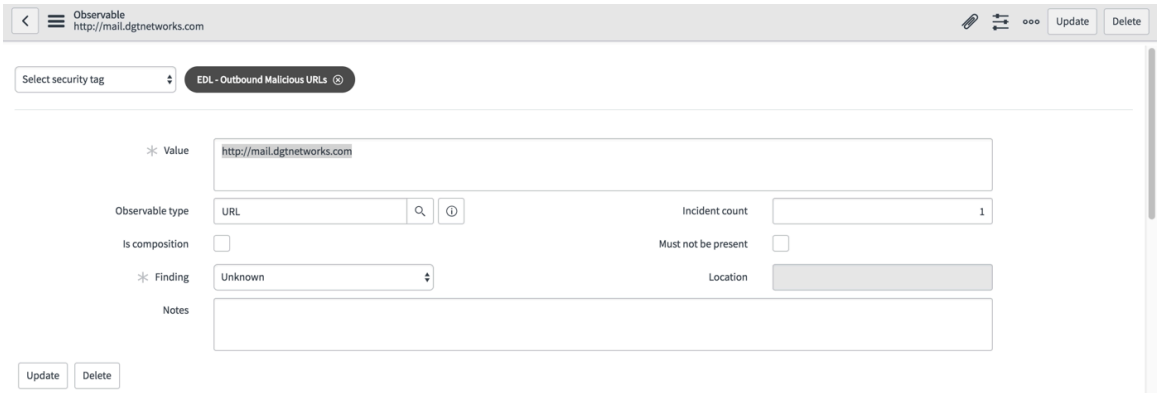
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O marcador de segurança também é exibido no registro observável.



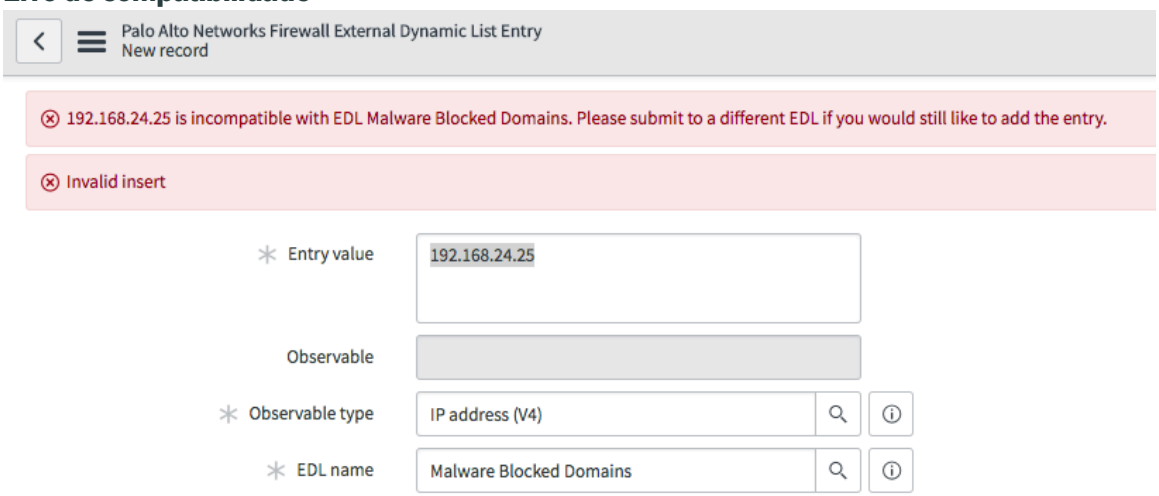
Exceções de entrada de EDL para Palo Alto Networks Next-Generation Firewall

Há restrições para adicionar entradas de Lista dinâmica externa (EDL) a EDLs. Se houver conflitos duplicados, de compatibilidade ou de CIDR (roteamento entre domínios sem classe) ao tentar adicionar entradas de EDL a EDLs, serão exibidas mensagens de erro que ajudarão a resolver esses erros.

Exceção de compatibilidade

Cada EDL aceita somente entradas compatíveis com seu tipo de observável. Se você criar um domínio EDL e tentar anexar um endereço IP observável a ele, uma mensagem de erro incompatível será exibida. Por exemplo, uma EDL de domínio só pode aceitar observáveis de domínio, conforme ilustrado na figura a seguir.

Erro de compatibilidade



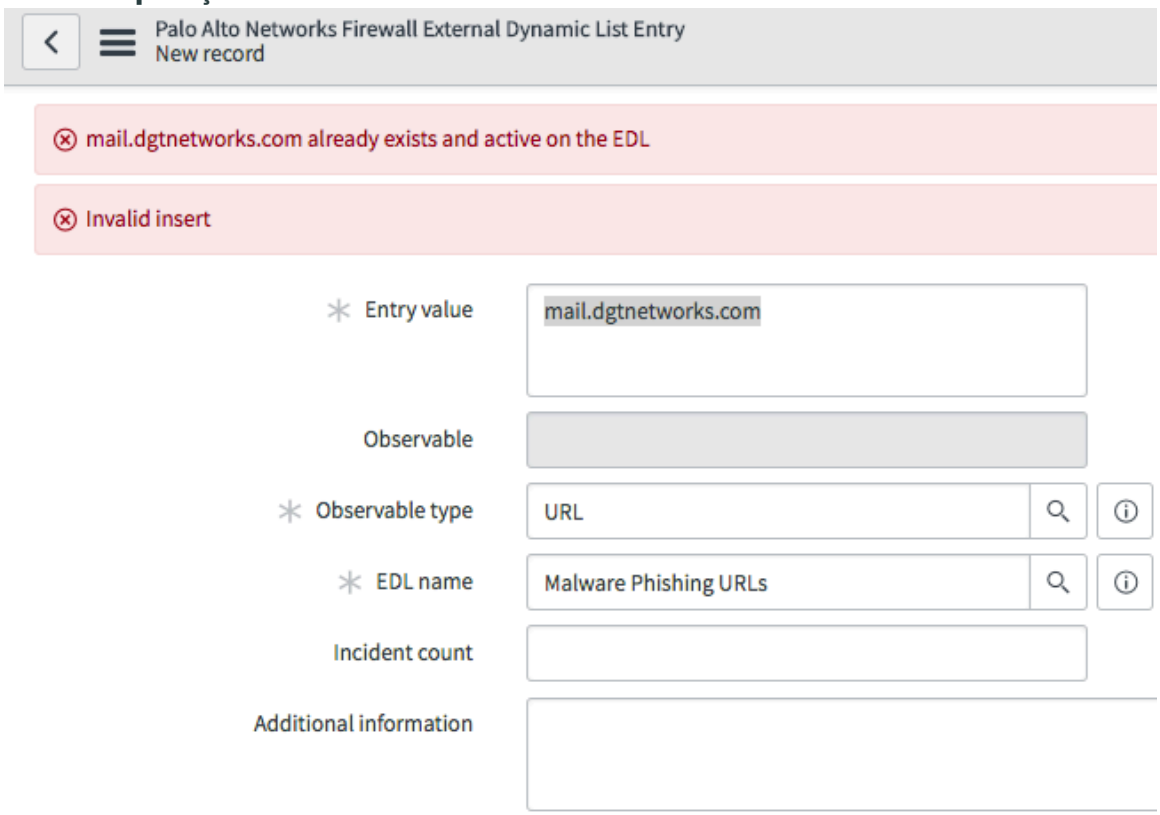
Exceção de duplicação

Um observável não pode ser ativado em várias EDLs do mesmo tipo de observável. Se um observável de URL já estiver ativado em uma EDL de URL e você tentar ativar o mesmo observável em uma EDL de URL de phishing, será exibida uma mensagem de erro de duplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Erro de duplicação



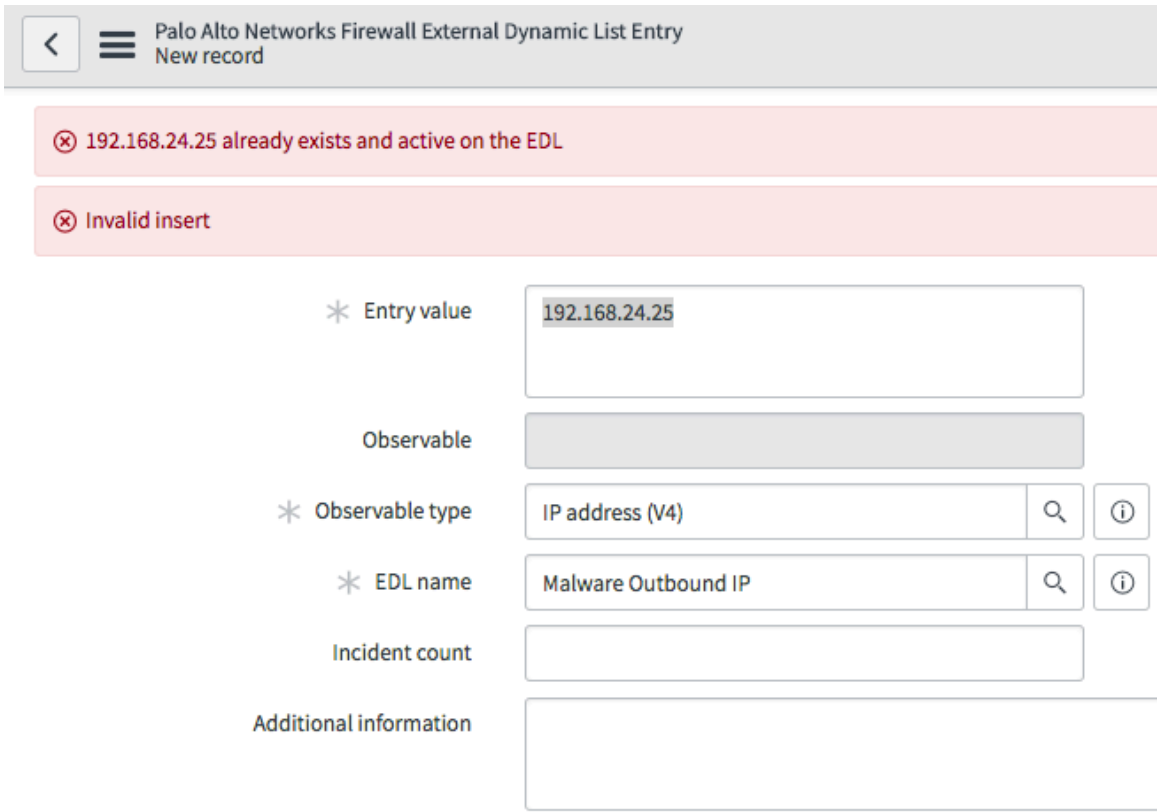
Exceção de CIDR (roteamento entre domínios sem classe)

Se você tentar anexar um único endereço IP a uma EDL e esse endereço IP já fizer parte de um observável CIDR em uma EDL, será exibido um erro de conflito de CIDR. Este erro indica que o único endereço IP já está incluído na EDL como parte do observável CIDR. Por exemplo, 192.168.24.25 faz parte do bloco CIDR 192.168.0.0/22.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conflito de CIDR



(Opcional) Editar o nome do marcador de segurança para Palo Alto Networks Next-Generation Firewall

Se a caixa de seleção **Exibir marcador** estiver marcada ao criar o registro de lista dinâmica externa (EDL), você poderá editar os nomes dos marcadores e as cores dos marcadores de segurança. Os marcadores de segurança ajudam a rastrear observáveis que já estão bloqueados.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

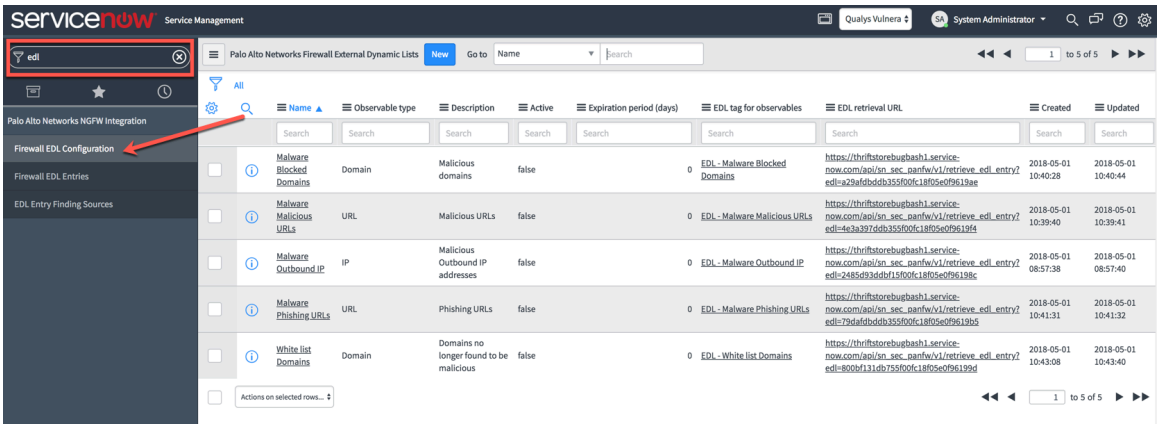
Os marcadores de segurança ajudam a identificar rapidamente quais incidentes de segurança têm observáveis em uma lista de bloqueios. Os marcadores também ajudam a identificar se um observável já está bloqueado ou se foi removido de uma EDL. Por padrão, a cor do marcador de segurança é preta para entradas da lista de bloqueios e cinza para entradas da lista de permissões. Você pode mudar os nomes e as cores dos marcadores para ajudá-lo a reconhecer determinados marcadores com mais facilidade.

Tradução automática

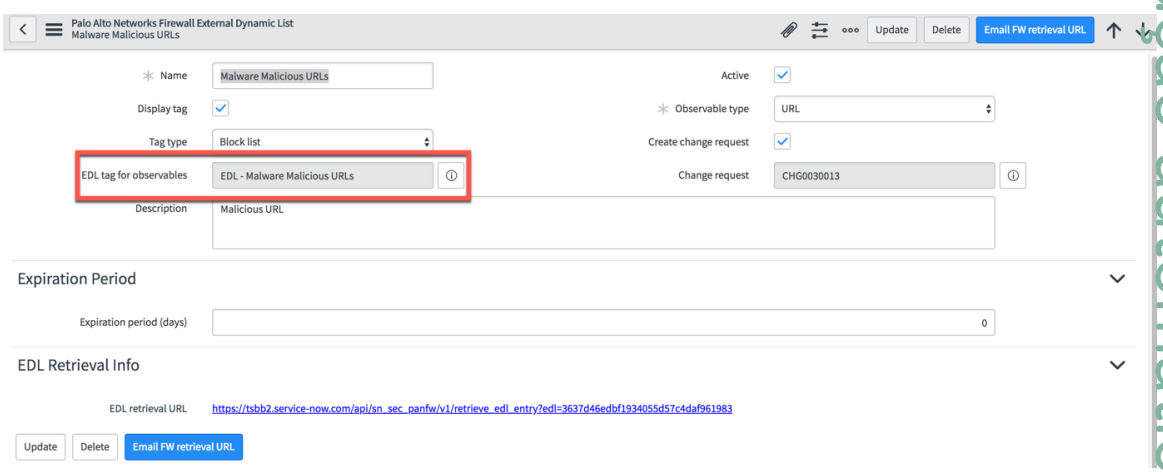
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

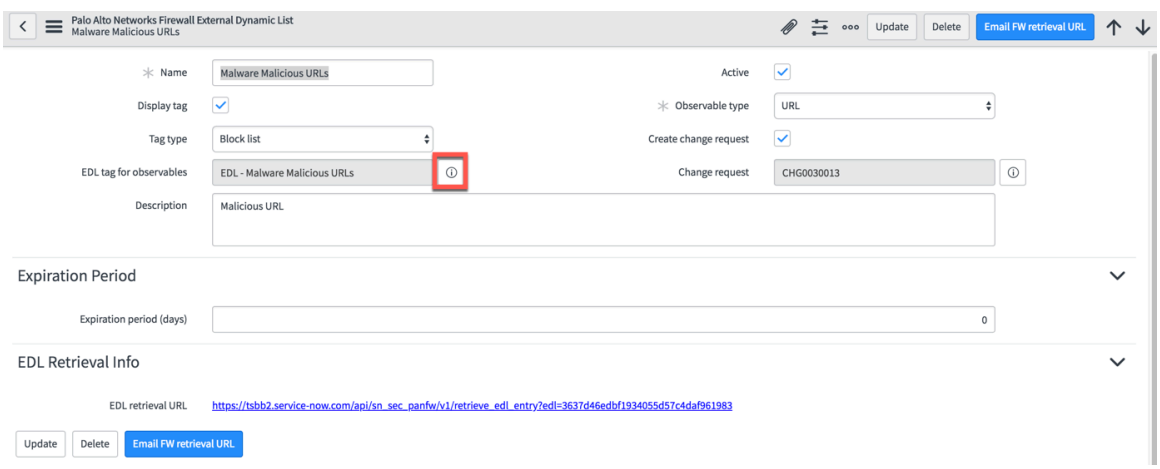
1. Navegar até **Todos** > **Integração de NGFW com a Palo Alto Networks** > **Configuração de EDL do Firewall**.



2. Clique em um item na coluna **Nome** para abri-lo
   O registro EDL é exibido. Por padrão, o nome do marcador de segurança é o mesmo valor inserido no campo **Nome** da EDL ao criá-la. Por padrão, o nome também inclui um prefixo *EDL*, por exemplo, EDL - URLs maliciosos de malware.



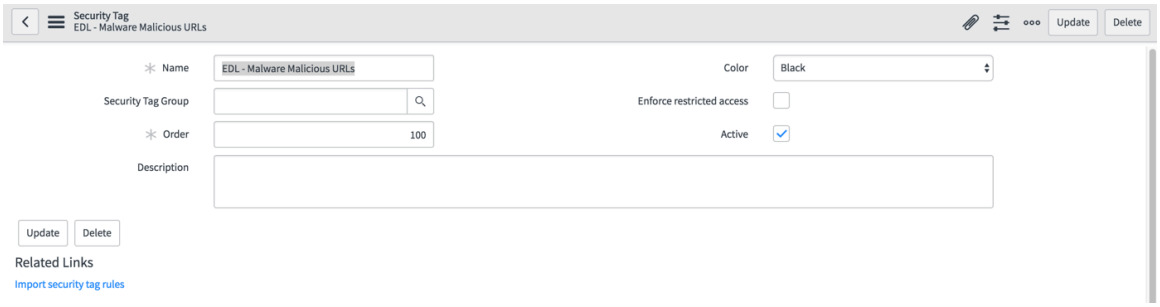
3. Clique no ícone de informações (ícone ⓘ) ao lado do **marcador EDL para observáveis** e, em seguida, em **Abrir registro**.



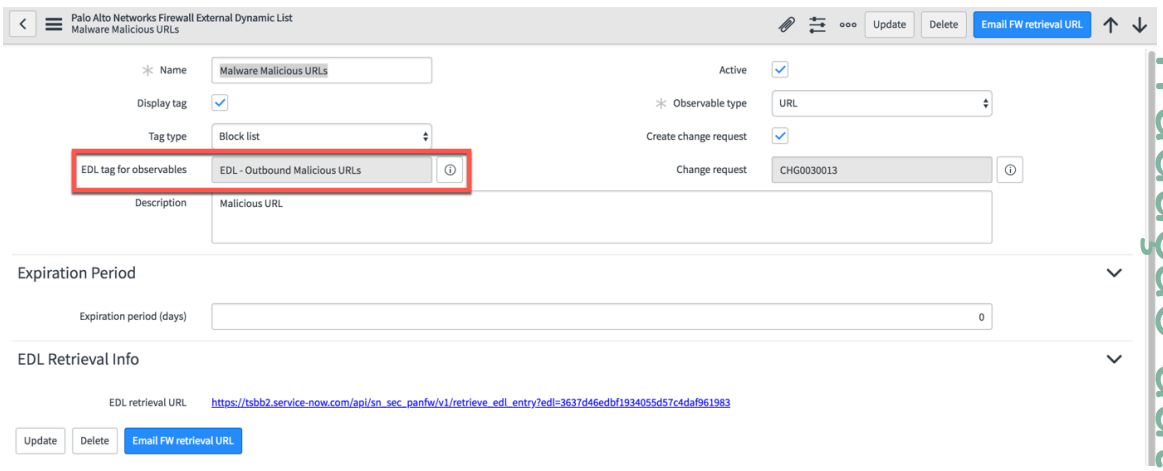
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

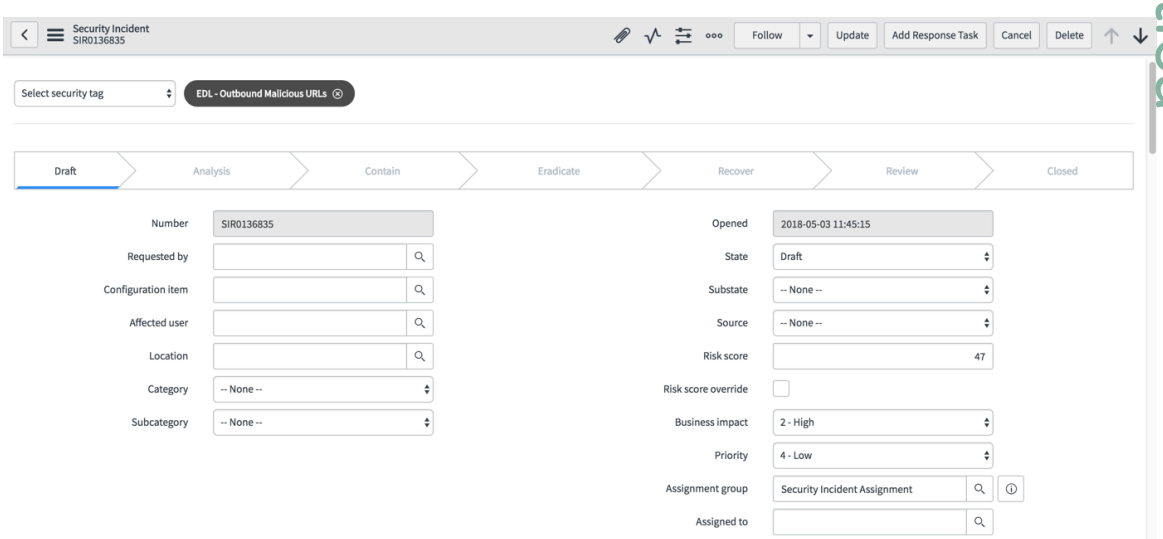
O formulário de marcador de segurança é exibido.



4. No campo **Nome**, modifique o nome do marcador de segurança e clique em **Atualizar**.
   O registro EDL atualizado é exibido com o nome do marcador modificado. No exemplo a seguir, Saída foi adicionada ao nome do marcador. Mantenha o prefixo EDL no novo nome do marcador para ajudar a identificar se o marcador está associado à integração Palo Alto Networks Next-Generation Firewall.



Os marcadores de segurança são exibidos para cada tipo de observável (IP, URL, domínio) no registro de Incidente de segurança e no registro de Observável sempre que esse observável é adicionado a uma EDL.



Se um observável já tiver sido adicionado a uma EDL e um marcador de segurança for exibido em um incidente de segurança para este observável, o marcador de segurança EDL também será exibido automaticamente em todos os registros de incidente de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

segurança subsequentes que forem criados. Essa duplicação informa que o observável já está em uma lista de bloqueios. Você não precisa adicionar este observável e bloqueá-lo novamente.

Quando um observável não está mais bloqueado, um marcador de segurança não é exibido no registro do incidente de segurança ou no registro do observável. Nesta instância, nenhum marcador de segurança indica que a data de expiração do observável pode ter passado ou que o observável foi desabilitado de uma EDL.

Desinstalar Palo Alto Networks Next-Generation Firewall

Se você quiser desinstalar Palo Alto Networks Next-Generation Firewall da sua instância Now Platform e remover todos os resquícios da integração, consulte o site de documentação ServiceNow para obter instruções sobre como desinstalar aplicações.

Antes de Iniciar

Função necessária: administrador do sistema (admin)

Consulte Desinstalar aplicações no site de documentação do produto da ServiceNow .

Integração de PhishTank

PhishTank O é um sistema de verificação de phishing baseado na comunidade para o qual os usuários enviam ameaças suspeitas e outros usuários no sistema votam para determinar se as ameaças de phishing são legítimas. Quando integrados ao produto Now Platform Security Operations, os resultados de inteligência contra ameaças fornecem aos analistas informações adicionais sobre incidentes de segurança relacionados a phishing ou investigações.

A integração PhishTank realiza pesquisas em possíveis URLs de sites de phishing.

O fluxo de trabalho verifica se há novos observáveis conforme eles chegam em incidentes de segurança. Se os observáveis forem de um tipo reconhecido pela integração da API, os observáveis serão avaliados. Os observáveis determinados como maliciosos são marcados.

Esta integração é compatível com as versões Kingston, London, Madrid e New York da Now Platform®.

Instalar e configurar PhishTank

Antes de executar a integração na sua instância, conclua as etapas de instalação e configuração para que a aplicação PhishTank se integre corretamente com Now Platform Security Operations.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Tarefas de configuração	Descrição
Verifique se você atribuiu as funções Now Platform necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador do sistema (admin) instala o app e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	a configuração e verifica os resultados esperados. Esta função também tem acesso ao módulo Security Operations.
Obtenha uma chave de API.	Visite o site PhishTank para obter informações sobre chaves de API e para criar uma conta: site PhishTank .
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Requisitos da versão Madrid e posterior Para a versão Madrid e versões posteriores da família, o plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras aplicações Security Operations necessárias para a integração. Verifique se as aplicações Security Operations a seguir estão instaladas e ativadas em ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Orquestração de suporte de segurança Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

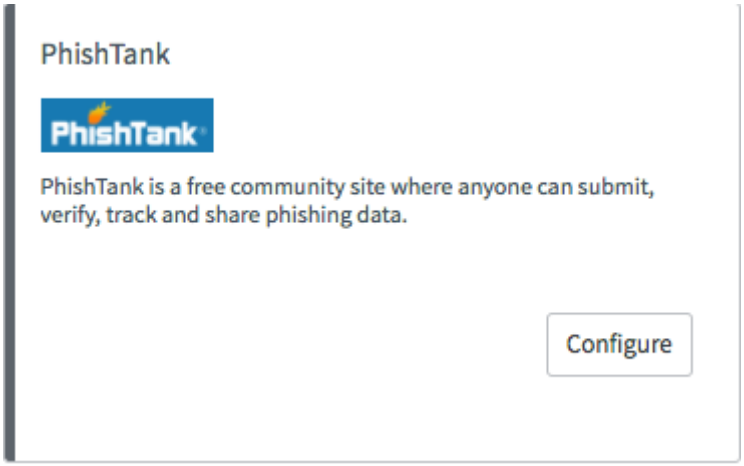
Função necessária: administrador

Procedimento

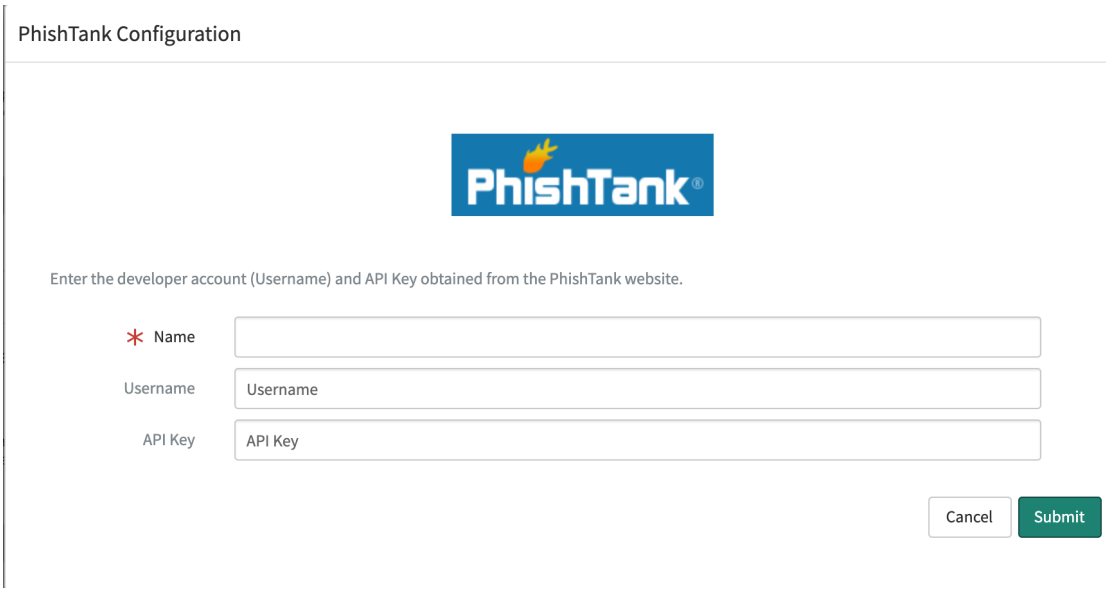
1. Se você não instalou a aplicação para a integração, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.
2. Após a conclusão da instalação, navegue até **Integrações** > **Configurações de integrações** e localize o bloco PhishTank.
3. Clique em **Configurar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Na caixa de diálogo **Configuração do PhishTank**, insira o Nome da configuração, o Nome de usuário (conta de desenvolvedor criada no PhishTank) e a chave de API que você obteve no site PhishTank e clique em **Enviar**.



5. Verifique a configuração bem-sucedida.
A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida.

Trouble?

Se uma mensagem de erro for exibida durante a configuração, a chave de API PhishTank pode ser inválida.

Verificar resultados esperados para PhishTank

Os observáveis são gerados automaticamente por um incidente de segurança e verificados pela aplicação. Os resultados da pesquisa são exibidos na guia Resultados da pesquisa de ameaças na parte inferior do registro do incidente de segurança.

Antes de Iniciar

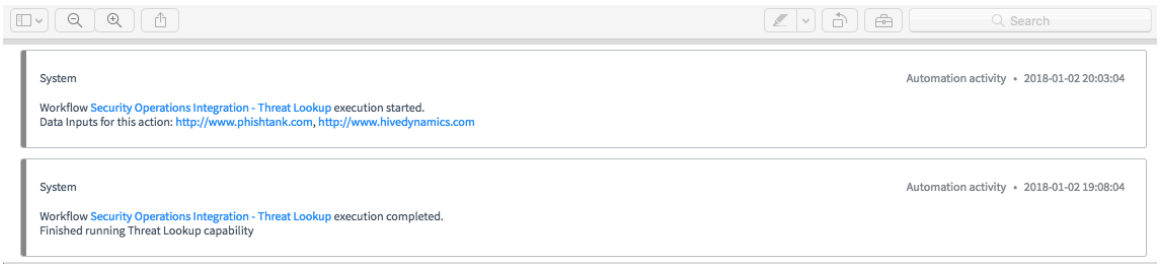
Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o formulário de incidente de segurança com o qual você está trabalhando e verifique se a pesquisa foi executada com sucesso.

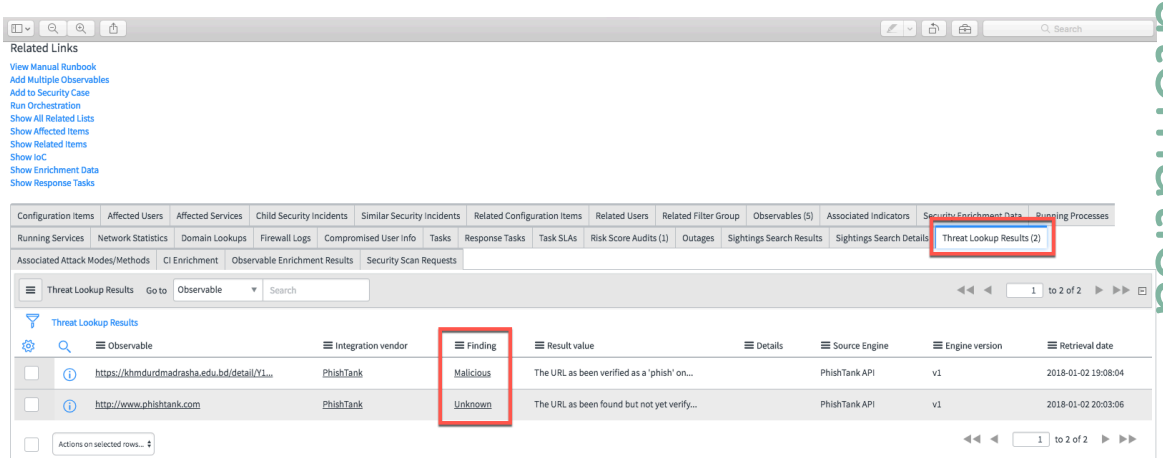


   Depois que a aplicação é configurada, o fluxo de trabalho é iniciado automaticamente após a criação do incidente. O status de execução e conclusão da pesquisa é exibido nas anotações de trabalho no registro do incidente de segurança.

2. Revise as anotações de trabalho para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

3. Navegue até a parte inferior do incidente de segurança e clique no link relacionado **Mostrar todas as listas** relacionadas.

   Nota:
   As imagens nas etapas a seguir são mostradas com a configuração **Formulários** com guia ativa nas Configurações do sistema. Se os formulários com guias não forem exibidos, no canto superior direito do quadro da faixa, clique no ícone de engrenagem Configurações. Na caixa de diálogo **Configurações do sistema** exibida, clique em **Formulários** e verifique se **Formulários com guia** e **Com o formulário** estão selecionados.



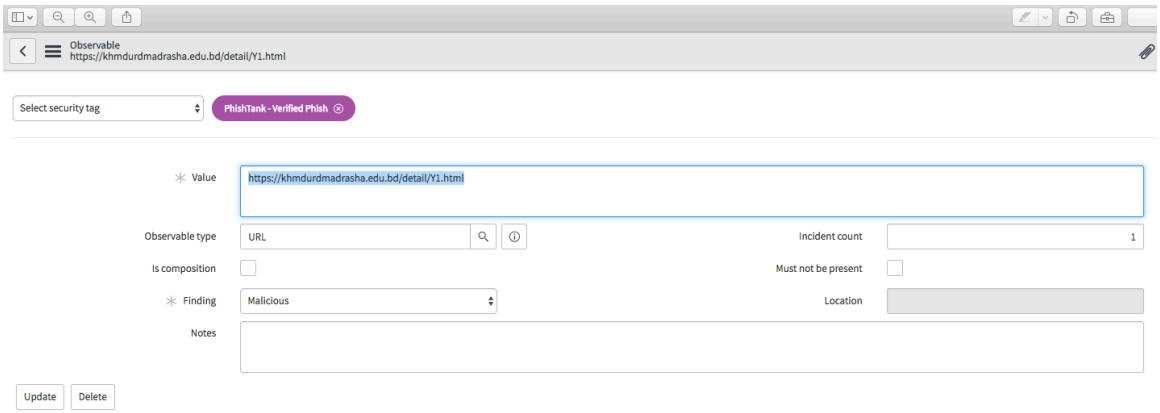
   A guia **Resultados da pesquisa de ameaças** na parte inferior do registro do incidente de segurança exibe os resultados da pesquisa.

   A coluna **Descoberta** exibe Desconhecido para registros não determinados como mal-intencionados. Para resultados correspondentes a mal-intencionado, Mal -intencionado é exibido na coluna **Descoberta**.

4. Na coluna **Observável**, clique em um observável para abrir um registro e exibir mais informações.

Tradução automática

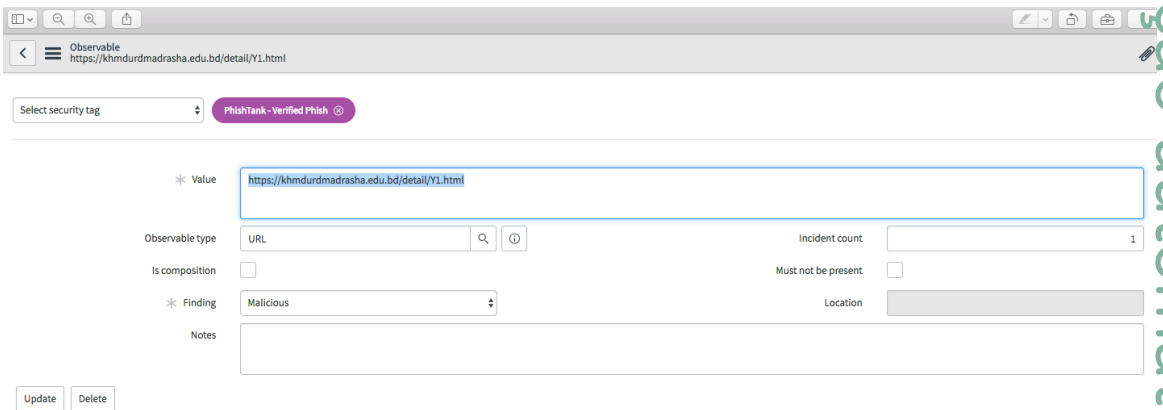
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



No registro observável, para pesquisas correspondentes a mal-intencionados, Mal -intencionado é exibido no campo **Descoberta**. O observável é marcado com a origem Inteligência contra ameaças que o considerou mal-intencionado, neste caso, a aplicação PhishTank.

5. Para exibir dados brutos, navegue de volta para o incidente de segurança e clique no ícone de informações azul ao lado de um observável.

6. Na janela exibida, clique em **Abrir registro**.



O link criado pela API e o campo **Descoberta** exibido com os resultados.

Tradução automática

Trouble?

Se você não vir resultados na guia **Resultados da pesquisa de ameaças**, verifique se o observável é um tipo compatível para pesquisa pela integração.

(Opcional) Anexar manualmente um observável para PhishTank

Você pode anexar manualmente observáveis a um incidente de segurança. Você anexa observáveis manualmente quando deseja executar pesquisas de ameaça em observáveis que não estão anexados a um incidente de segurança no gatilho de evento inicial. Além disso, você pode executar esta tarefa quando quiser mais informações sobre um observável relacionado.

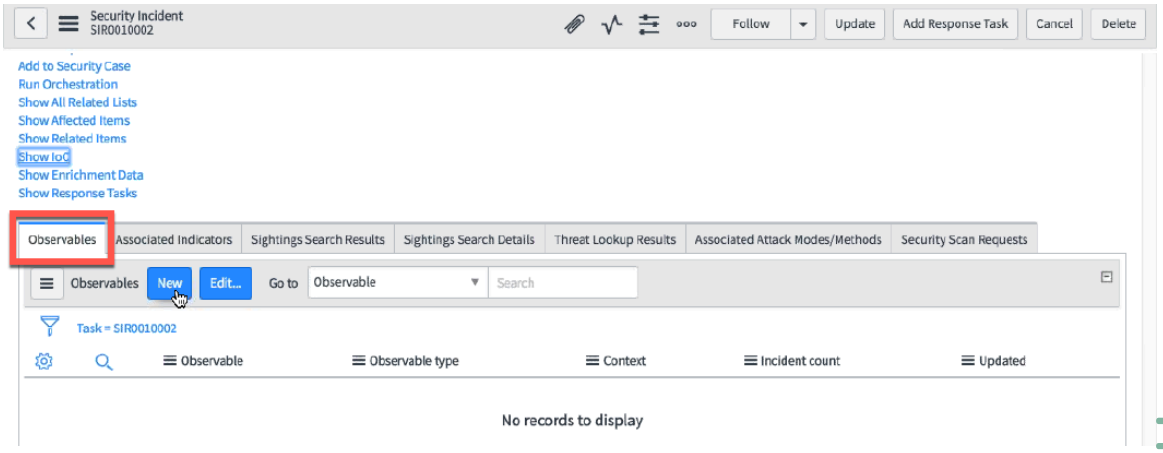
Antes de Iniciar

Função necessária: sn_si.analyst

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

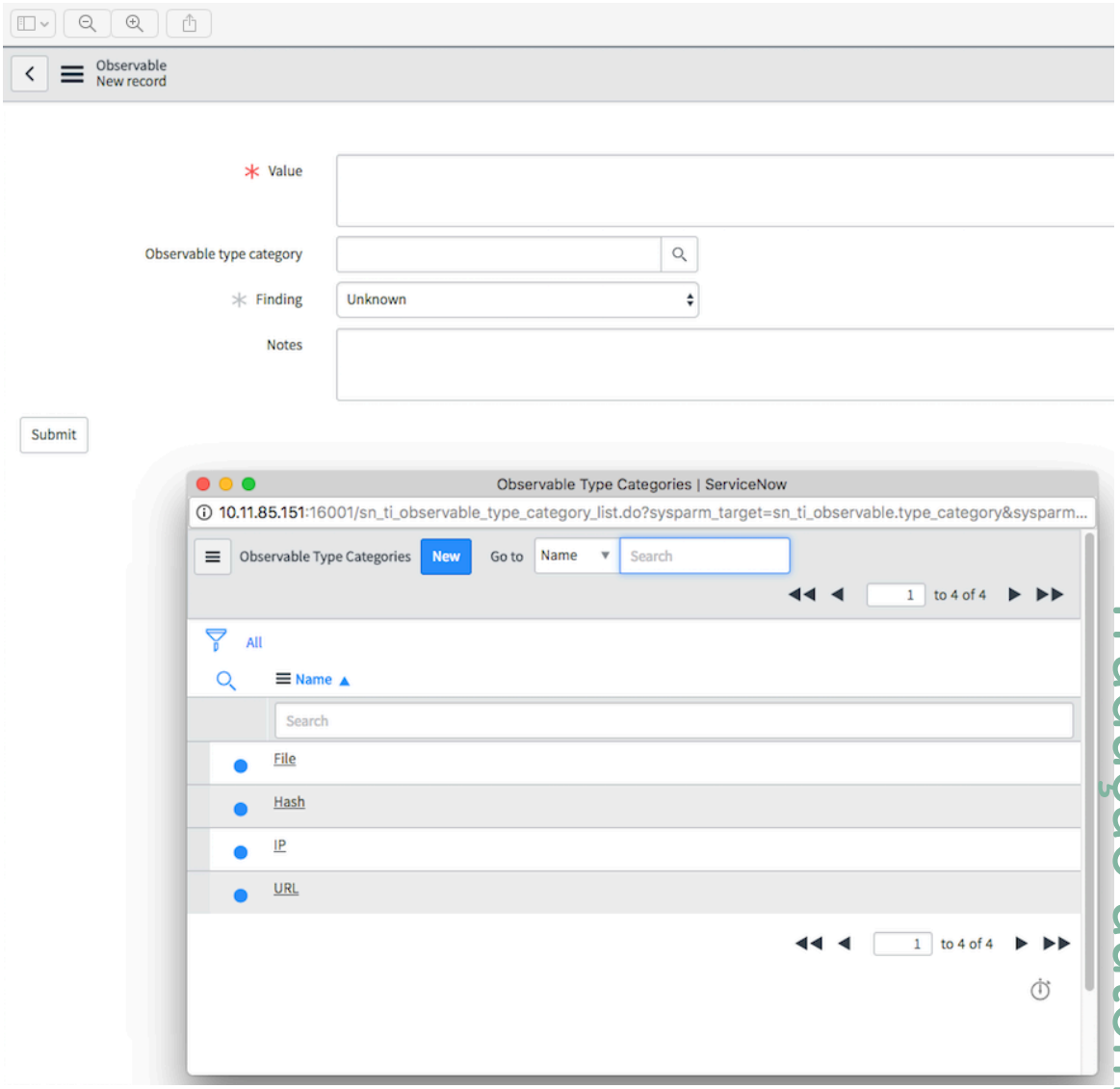
1. Navegue até o seu incidente de segurança em aberto.
2. No registro de incidente de segurança aberto, clique no link **Mostrar IoC**em **Links relacionados** para exibir a guia **Observáveis**.



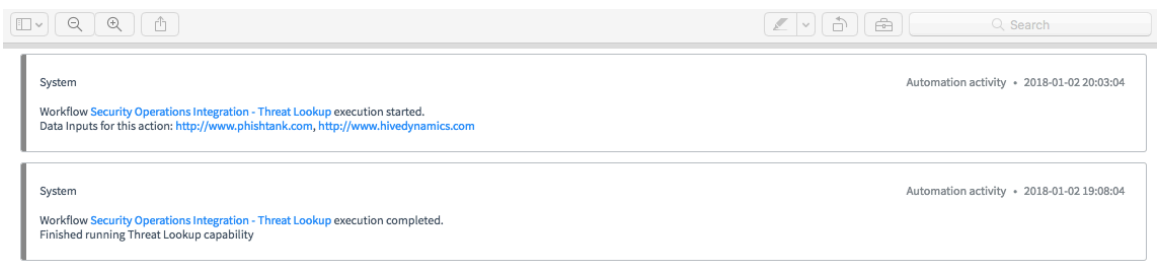
3. Clique em **Nova**.
   O formulário Observável é exibido.
4. No campo **Valor**, insira um URL.
5. Clique no ícone de pesquisa e, na caixa de diálogo **Categorias de tipo de observável**, clique em **URL** na lista para preencher o campo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



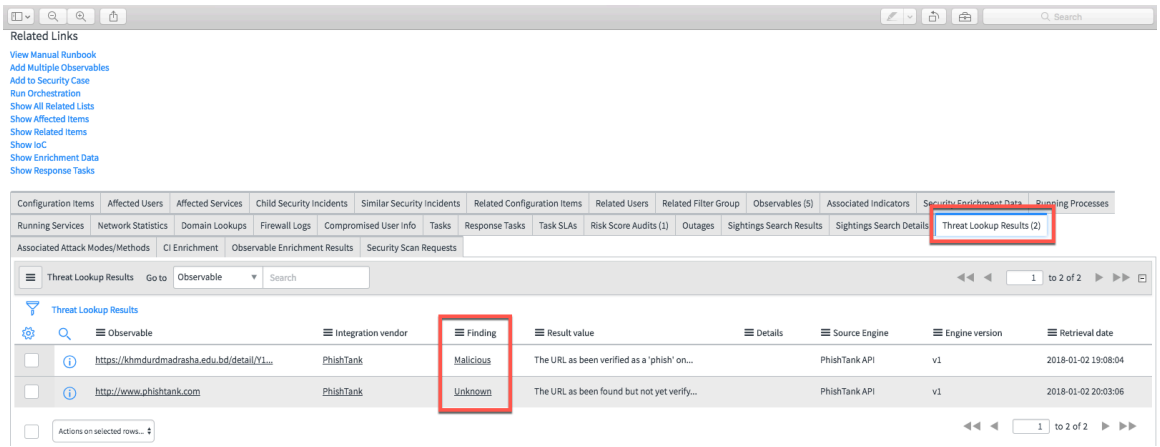
6. Clique em **Enviar**.
   O fluxo de trabalho é iniciado e verifica o novo observável. O status de execução e conclusão é exibido na seção de anotações de trabalho no registro de Incidente de segurança.
7. Navegue até o seu incidente de segurança e revise as anotações de trabalho.



8. Clique no link relacionado **Mostrar todas as listas** relacionadas na parte inferior do incidente de segurança.
9. Clique na guia **Resultados da pesquisa de ameaças** para exibir os resultados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



10. Na coluna **Observável**, clique no ícone de informações azul ao lado de um determinado observável para obter mais informações e dados brutos.

11. Na caixa de diálogo exibida, clique em **Abrir registro**.

Trouble?
Revise as anotações de trabalho para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

Integração de Reverse Whois

Reverse Whois é um serviço que realiza pesquisas em nomes de domínio registrados por indivíduos ou organizações.

Execute pesquisas de domínio usando termos de pesquisa em observáveis que você anexa a um incidente de segurança. A API Reverse Whois pesquisa registros de domínio com base nos termos de pesquisa inseridos e retorna todos os registros que correspondem a esses termos.

Às vezes, os analistas usam essa integração junto com a integração Whois para pesquisa de incidentes de segurança. A integração Whois fornece informações de aprimoramento adicionais com base nas pesquisas de domínio da integração Reverse Whois.

Esta integração é compatível com as versões Kingston, London, Madrid e New York da Now Platform®.

Instalar e configurar Reverse Whois

Antes de executar a integração na sua instância, conclua as etapas de instalação e configuração para que a aplicação Reverse Whois se integre corretamente ao produto Security Operations.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções obrigatórias da ServiceNow.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador do sistema (admin) instala o app e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração. O administrador de incidentes de segurança também atribui a função de Analista de incidentes de segurança (sn_si.analyst). • O Analista de incidentes de segurança (sn_si.analyst) executa pesquisas de domínio com Reverse Whois e analisa e trabalha com incidentes de segurança.
Obtenha uma chave de API.	Visite o site da API WhoisXML para obter informações sobre chaves de API e para criar uma conta: site da API WhoisXML . A configuração requer que você insira as chaves de API.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Requisitos da versão Madrid e posterior Para a versão Madrid e versões posteriores da família, o plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras aplicações Security Operations necessárias para a integração. Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Orquestração de suporte de segurança Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte Obter direito para um

Tradução automática

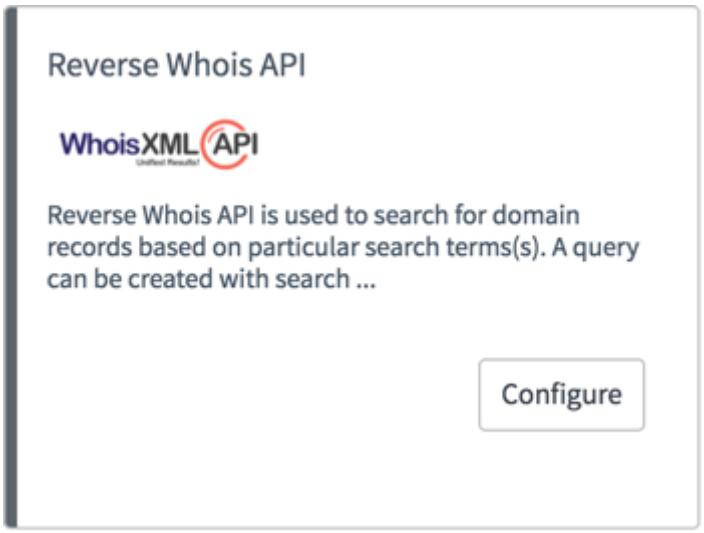
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

Função necessária: administrador

Procedimento

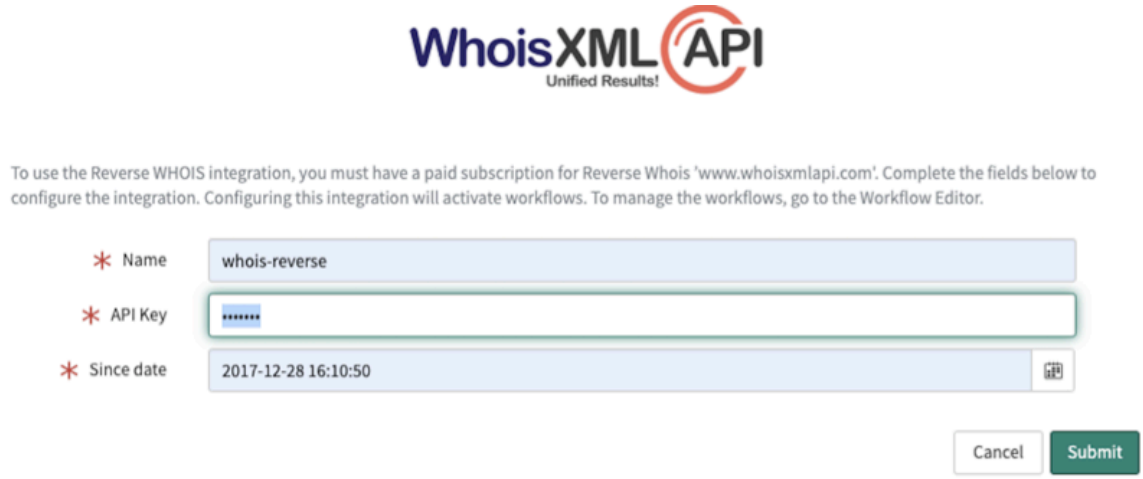
1. Se você já instalou e configurou a aplicação Reverse Whois, siga estas etapas:
   a. Exclua a configuração existente.
   b. Instale e crie uma nova configuração usando a chave de API que você obteve.
2. Se você não instalou a aplicação para a integração, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.
3. Após a conclusão da instalação, navegue até **Integrações** > **Configurações de integrações** e localize o bloco de API Reverse Whois.
4. Clique em **Configurar**.



5. Na caixa de diálogo **Reverter configuração da API Whois**, insira a chave de API que você obteve no site da Whois XML API.
6. Escolha uma opção na tabela a seguir para filtrar pesquisas de domínio para seus termos de pesquisa. Essas definições de configuração permanecem salvas até que você as altere e se apliquem a todas as Reverse Whois pesquisas de API.

Tradução automática

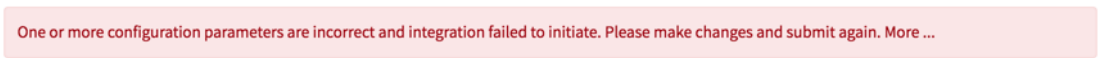
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



7. Clique em **Enviar**.
   A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida.

Trouble?
Se uma mensagem de erro for exibida, a chave de API pode ser inválida.

Mensagem de erro



(Opcional) Instalar e configurar Whois

Instale o plug-in Whois para fornecer informações de aprimoramento adicionais em suas pesquisas de domínio da API Reverse Whois. Esta pesquisa fornece dados de aprimoramento adicionais no domínio, como a data de registro, o nome do registrador e o país de origem.

Antes de Iniciar

1. Se você não solicitou o direito da aplicação, consulte Obter direito para um produto ou aplicação Security Operations para a aplicação Whois na ServiceNow Store.
2. Obtenha credenciais para a chave de API Whois no site do produto: site da API WHOIS .

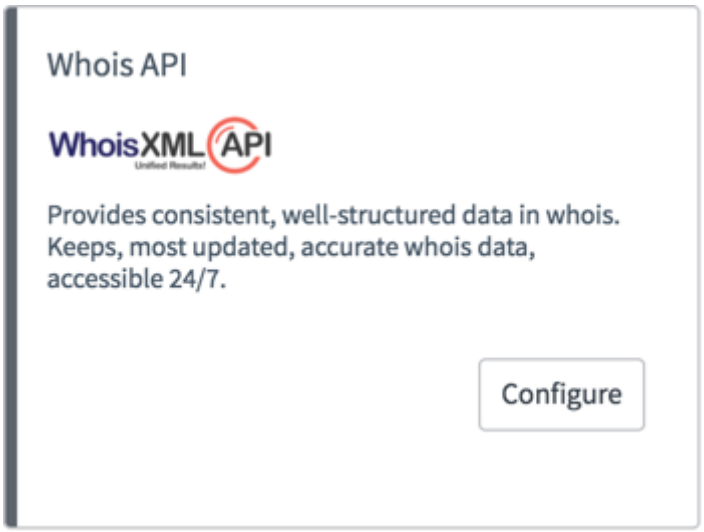
Função necessária: administrador

Procedimento

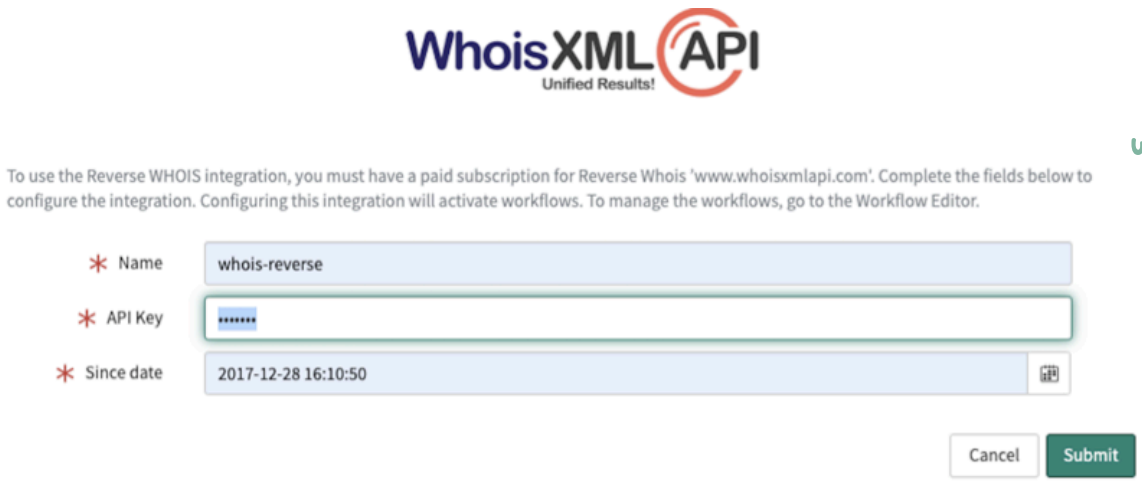
1. Se você não instalou o aplicativo, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.
2. Após a conclusão da instalação, navegue até **Integrações** > **Configurações de integrações** e localize o bloco de API Whois.
3. Clique em **Configurar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



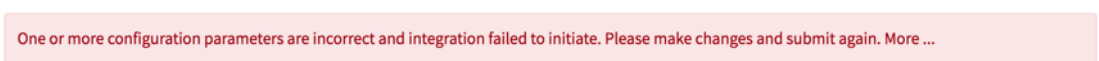
4. Na caixa de diálogo **Configuração da API Whois**, insira a chave de API que você obteve no site do produto.



5. Clique em **Enviar**.
   A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida. Agora você pode executar pesquisas de aprimoramento nos domínios retornados da integração Reverse Whois.

Trouble?
Se uma mensagem de erro for exibida, a chave de API pode ser inválida.

Solução de problemas



Iniciar a pesquisa para Reverse Whois

Inicie pesquisas de domínio usando termos de pesquisa em observáveis que você anexa manualmente a um registro de incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.analyst

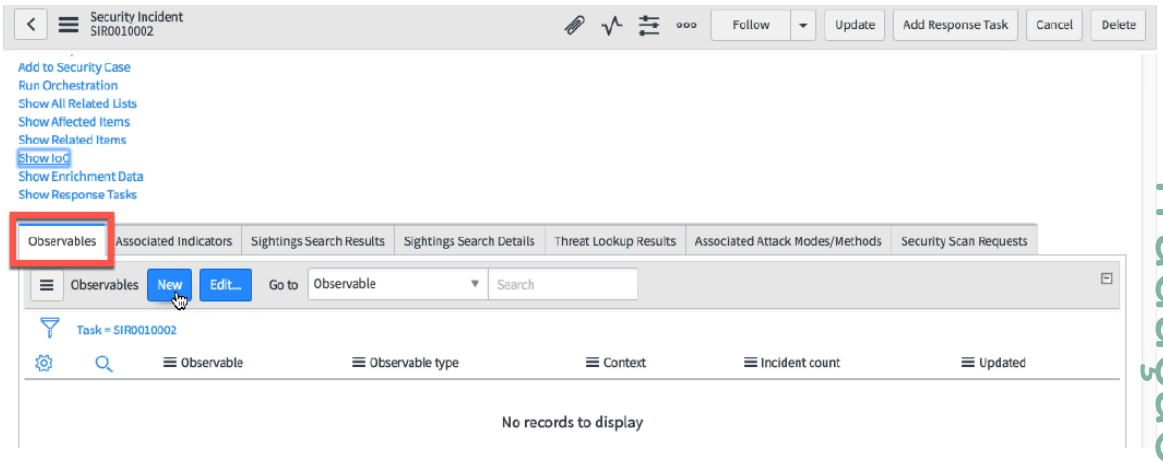
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se não estiver aberto, navegue até **Incidente de segurança** > **Incidentes** > **Mostrar Todos os Incidentes** e abra o incidente de segurança com o qual você está trabalhando.
2. Na parte inferior do registro, clique no link relacionado **Mostrar IoC** para exibir a guia Observáveis.

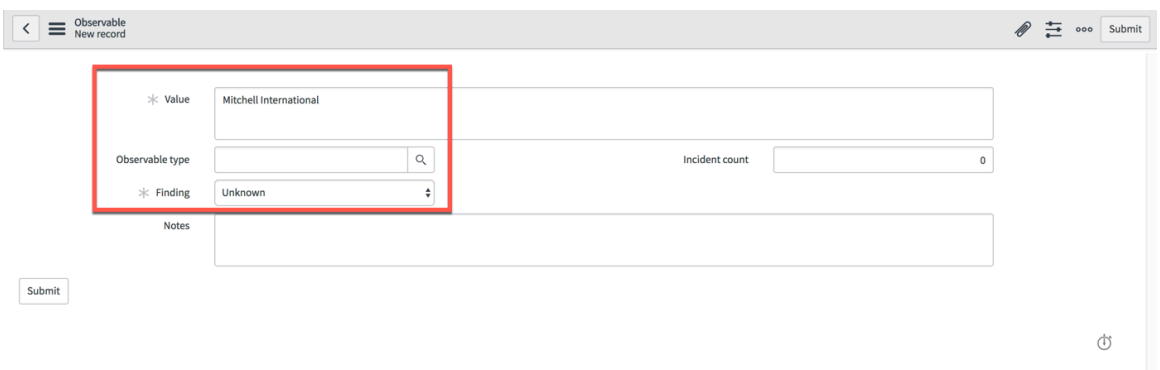
Nota:
As imagens nas etapas a seguir são mostradas com a configuração **Formulários** com guia ativa nas Configurações do sistema. Se você não vir as guias no incidente de segurança, no canto superior direito do quadro da faixa, clique no ícone de engrenagem **Configurações**. Na caixa de diálogo **Configurações do sistema** exibida, clique em **Formulários** e verifique se **Formulários com guia** e **Com o formulário** estão selecionados.



3. Na guia Observáveis, clique em **Novo**.
4. Preencha os campos.

Campos obrigatórios no novo registro

Campo	Descrição
Valor	Termo de pesquisa exclusivo para um domínio.
Tipo de observável	Este campo é limpo automaticamente.
Descoberta	Este campo é definido automaticamente como **Desconhecido**.



5. Clique em **Enviar**.
Você retornará ao registro de incidente de segurança e o fluxo de trabalho iniciará a pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Verifique os resultados da pesquisa no incidente de segurança. Consulte Verificar resultados esperados para Reverse Whois.

Verificar resultados esperados para Reverse Whois

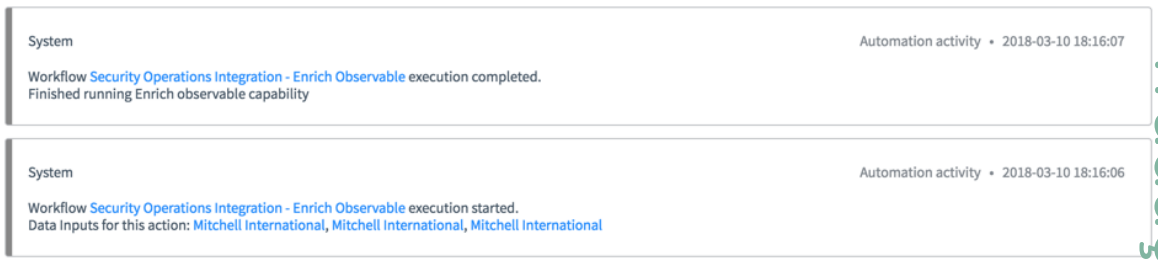
Os resultados do aprimoramento são exibidos na guia **Domínios ReverseWhois** na parte inferior do registro do incidente de segurança. Localize os resultados da pesquisa para verificar se a pesquisa foi executada com sucesso.

Antes de Iniciar

Função necessária: sn_si.analyst

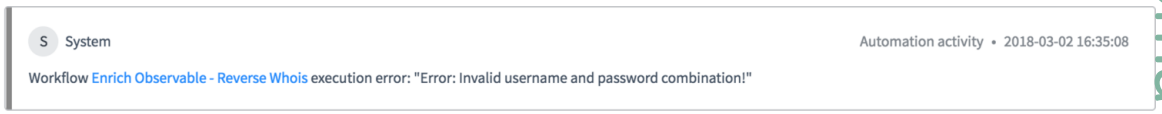
Procedimento

1. Se ainda não estiver aberto, navegue até **Incidentes de segurança** > **Incidentes** > **Mostrar Todos os Incidentes** e localize o incidente de segurança com o qual você está trabalhando.



   Depois que a aplicação é configurada e um observável é anexado, o fluxo de trabalho é iniciado automaticamente. As anotações de trabalho no registro do incidente de segurança exibem o status de execução e conclusão da pesquisa.

2. Se você não puder verificar se a pesquisa foi executada com sucesso, revise as anotações de trabalho para obter mais informações sobre como prosseguir.

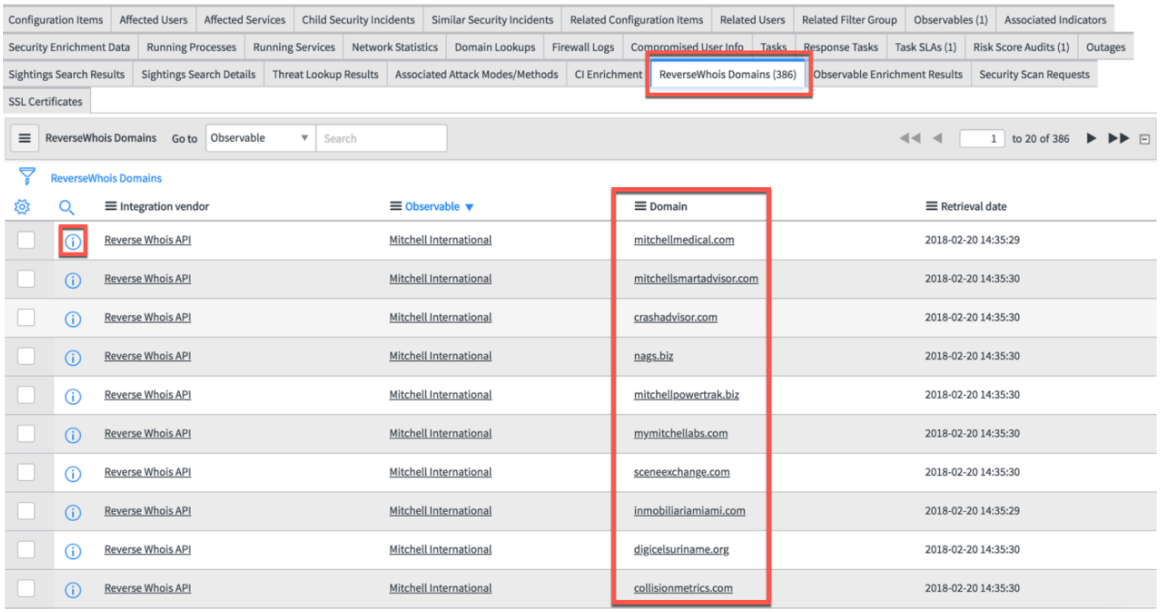


3. Navegue até a parte inferior do incidente de segurança e clique no link relacionado **Mostrar todas as listas** relacionadas.

   Nota:
   Para os resultados de pesquisa filtrados mostrados na figura a seguir, as definições de configuração no bloco de configuração da API Reverse Whois foram salvas com **1991-06-01** inserido no campo **Desde a data**.

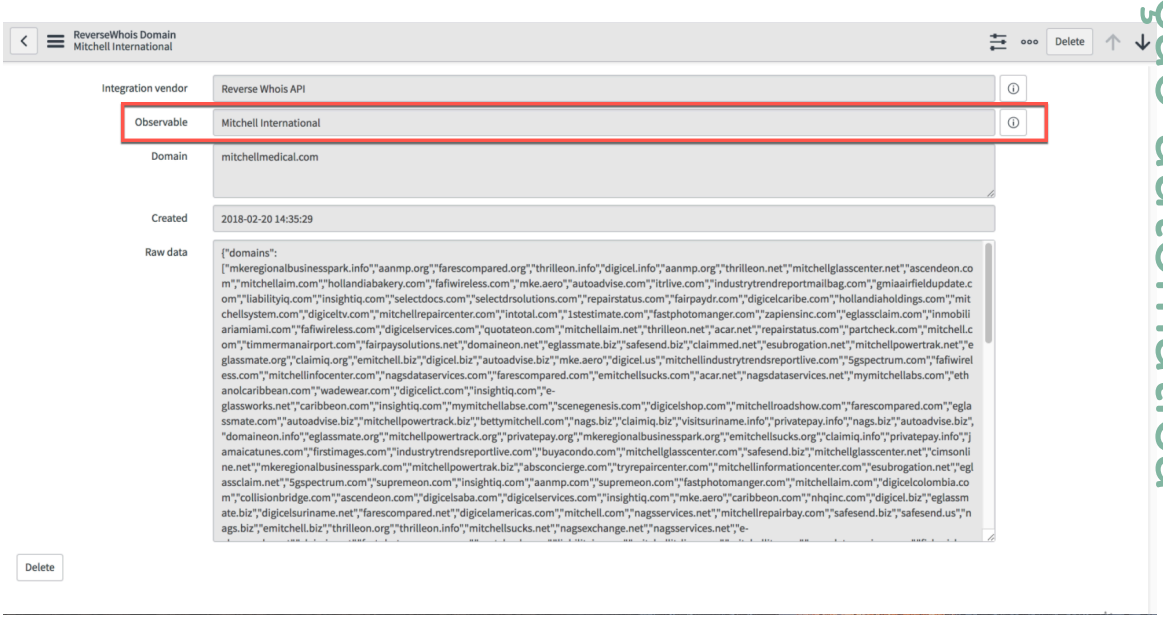
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Os resultados do aprimoramento são exibidos na guia **Domínios do ReverseWhois**. Os domínios ativos para este observável são exibidos na coluna **Domínio**.

4. Clique no ícone de informações azul ao lado de um item e clique em **Abrir registro** na caixa de diálogo exibida.

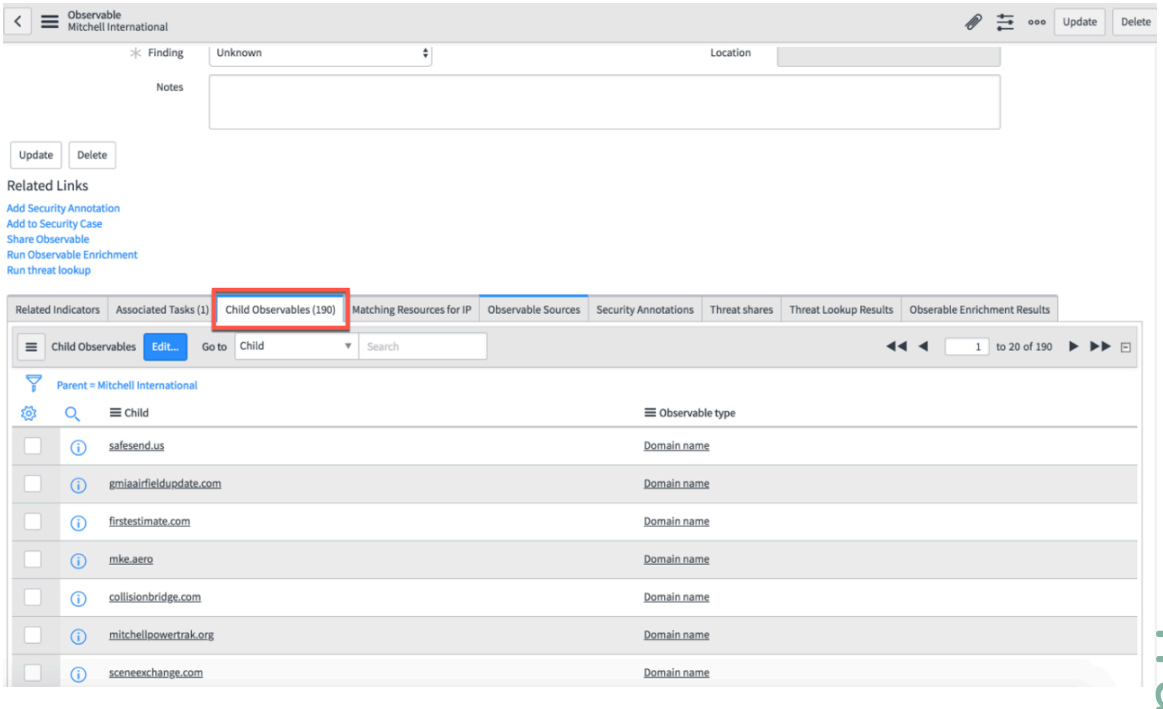


O registro é exibido com detalhes de aprimoramento, incluindo os dados brutos.

5. Navegue de volta para o incidente de segurança e, com a guia **ReverseWhois Domains** selecionada, clique em um observável na coluna **Observável** para abrir um registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Os observáveis secundários são exibidos na guia **Observáveis** secundários no registro do observável. Os observáveis secundários serão gerados somente se a aplicação Reverse Whois tiver retornado domínios.

Trouble?

Se a pesquisa não for concluída com sucesso, verifique se os termos de pesquisa inseridos são compatíveis com a integração. Revise as anotações de trabalho para obter mais informações.

O que Fazer Depois

Para obter mais dados de aprimoramento nos resultados da pesquisa de domínio, você pode executar a integração Whois para realizar pesquisas de aprimoramento nos observáveis secundários retornados pela integração Reverse Whois. Esses dados de aprimoramento nos observáveis secundários incluem informações sobre data de registro, nome do registrador e país de origem.

(Opcional) Execute a pesquisa de aprimoramento e verifique os resultados esperados para Whois

Execute a integração Whois para realizar pesquisas de aprimoramento nos domínios retornados da integração Reverse Whois.

Antes de Iniciar

Verifique se você instalou e configurou os plug-ins Reverse Whois e Whois. Execute essas etapas somente depois de executar a pesquisa de domínio com o plug-in Reverse Whois com sucesso.

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

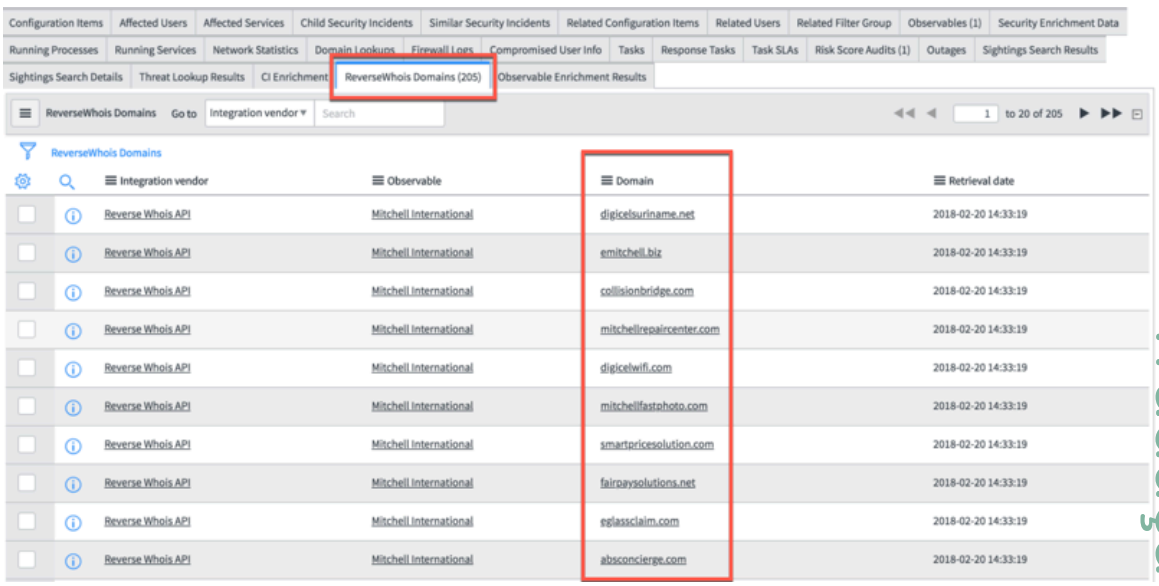
Os resultados são exibidos na guia **Resultados** de aprimoramento do observável no registro do observável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

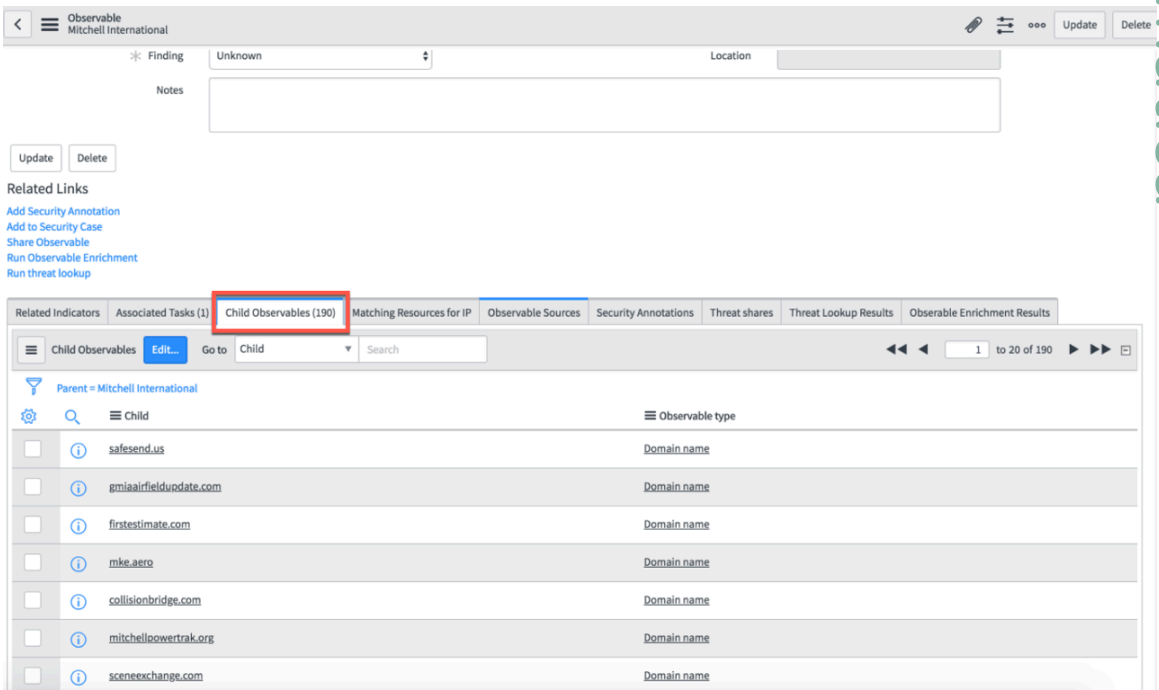
Procedimento

1. Navegar até **Todos** > **Incidentes de segurança** > **Incidentes** > **Mostrar Todos os Incidentes** e localize o incidente de segurança com o qual você está trabalhando que executou a pesquisa de domínio com sucesso.
2. Abra o registro e clique no link relacionado **Mostrar todas as listas** relacionadas.
3. Selecione a guia **Reverter domínios Whois** na parte inferior do registro.



Na coluna **Domínios**, a lista de domínios retornados é exibida.

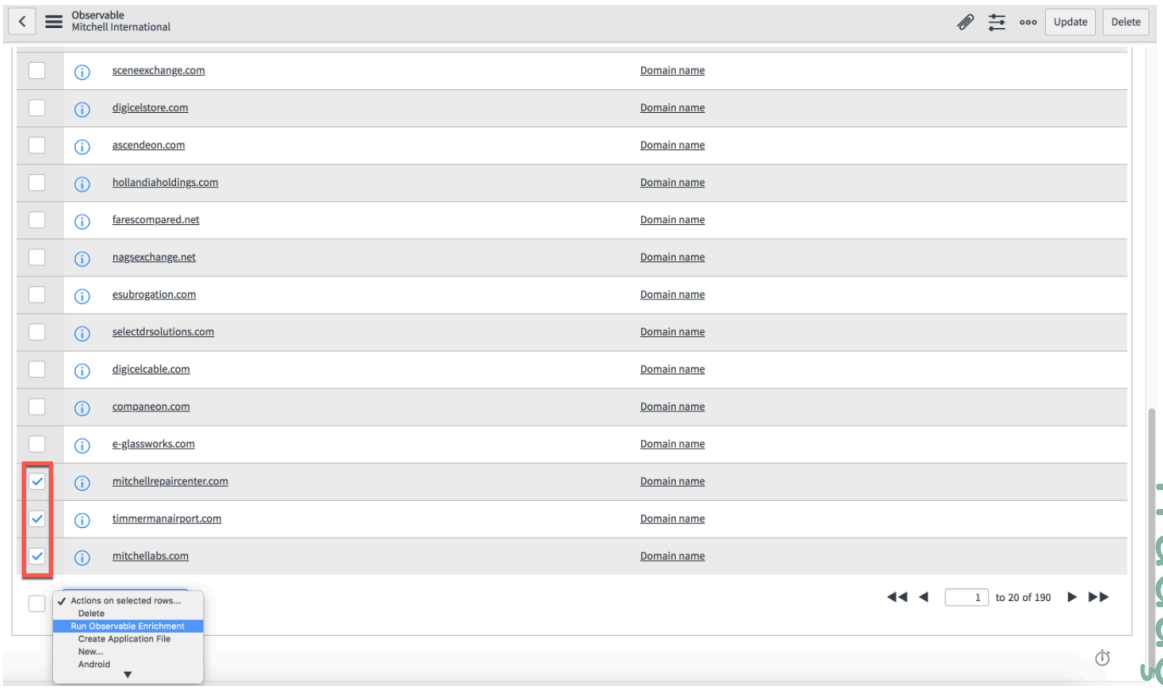
4. Na coluna **Observável**, clique em um observável.
   Na guia **Observáveis secundários**, os observáveis secundários são exibidos. Os observáveis secundários serão gerados somente se a verificação inicial do observável pela aplicação Reverse Whois retornar domínios.



Tradução automática

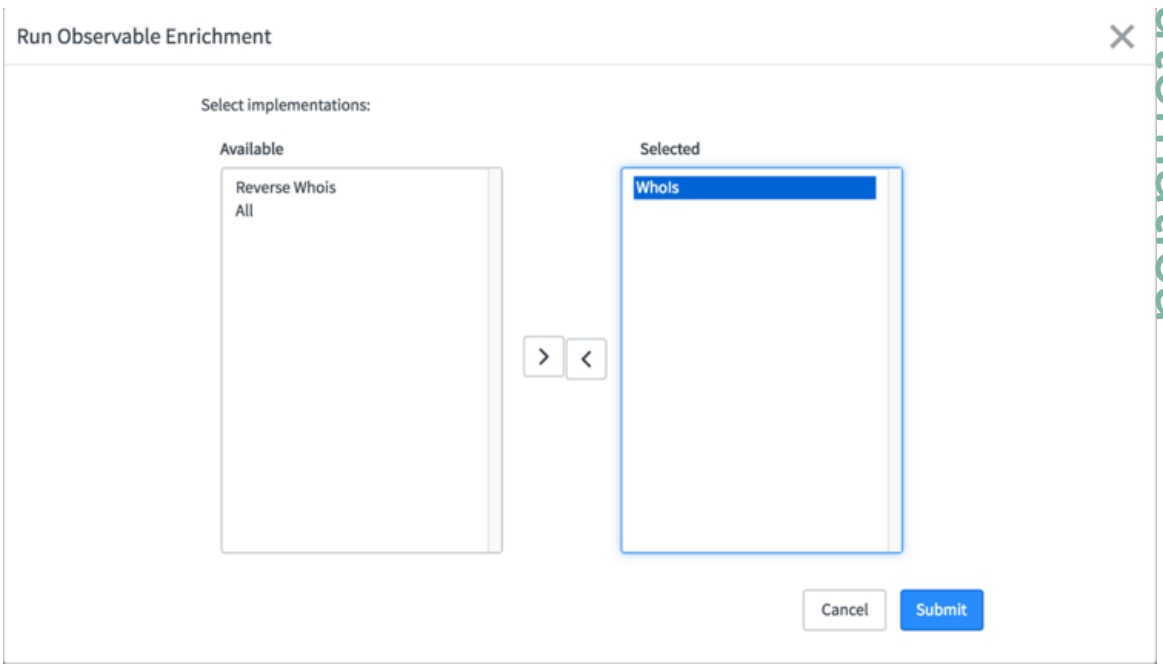
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione os observáveis secundários nos quais você deseja executar o aprimoramento do observável e, na lista de seleção **Ação nas linhas selecionadas**, selecione **Executar aprimoramento do observável**.



A caixa de diálogo **Executar aprimoramento de observável** é exibida.

6. Mova a integração Whois de **Disponível** para **Selecionado** e clique em **Enviar**.

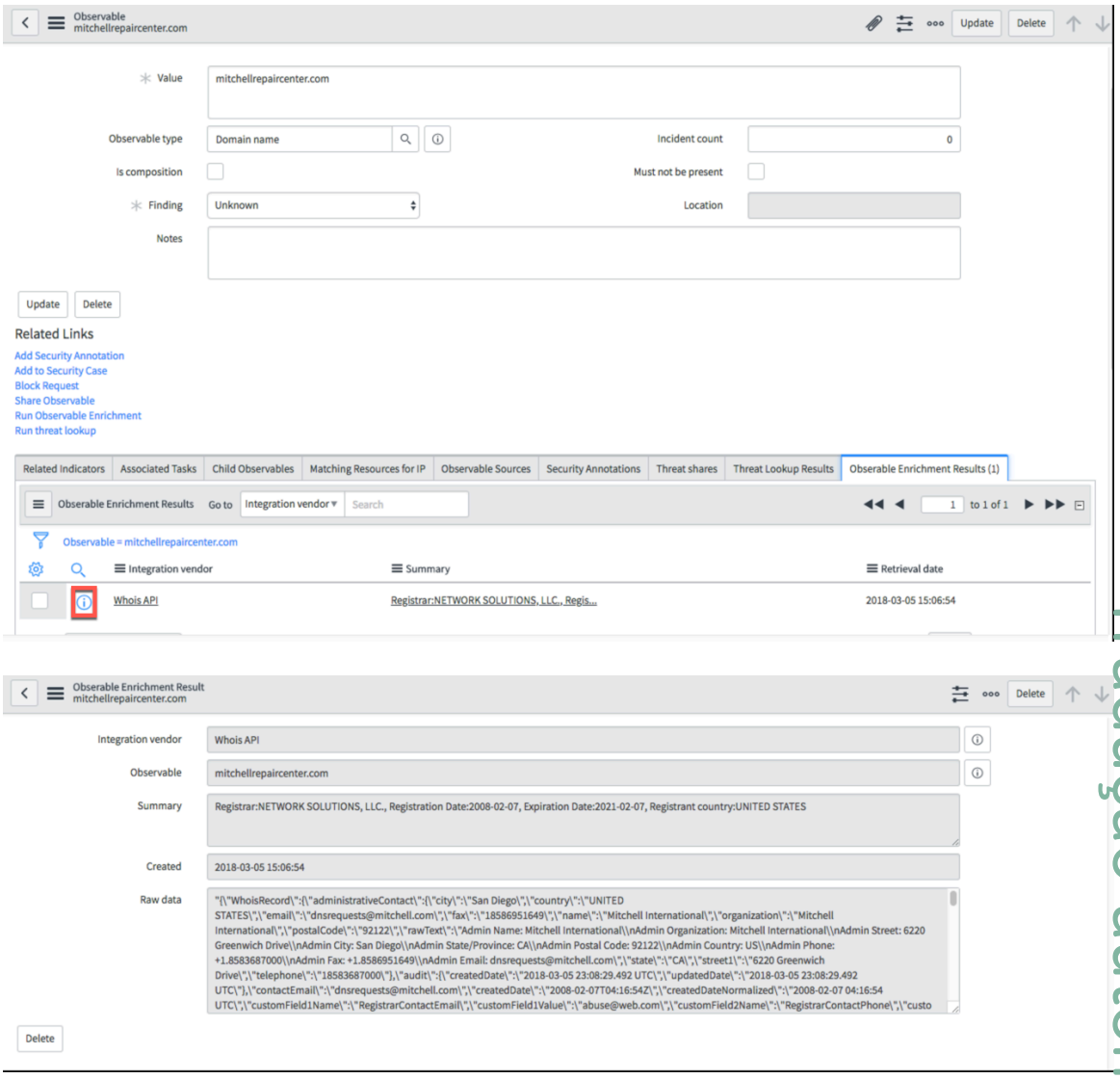


Os resultados são exibidos na guia **Resultados** de aprimoramento do observável do registro do observável.

7. Clique no ícone de informações azul e em **Abrir registro** na caixa de diálogo exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Mais informações e dados brutos relacionados à pesquisa de domínio original são exibidos, como a data de registro, o nome do registrador e o país de origem.

Trouble?
Se você não conseguir localizar observáveis secundários ou resultados de aprimoramento, verifique se a integração Reverse Whois foi executada com sucesso e retornou domínios. Além disso, consulte as anotações de trabalho no registro para obter mais informações.

Tópicos relacionados

Instalar e configurar Reverse Whois

Verificar resultados esperados para Reverse Whois

IntegraçãoRISKIQ e WHOISIQ

Com a integração das APIs RISKIQ e WHOISIQ com o produto Now Platform® Security Operations, os analistas de segurança recebem dados de aprimoramento adicionais e informações sobre a validade dos sites.

A RISKIQ API de Certificados SSL executa pesquisas em Certificados SSL, que incluem detalhes sobre a autoridade de certificação de emissão, as organizações que solicitam

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

certificados, os certificados de entidade para os quais os certificados são emitidos e o domínio. As pesquisas de certificado SSL são realizadas automaticamente quando os incidentes de segurança são criados.

A API RISKIQ WHOISIQ executa pesquisas em outros tipos de observáveis, como domínio, e-mail, nameserver, organização, endereço e número de telefone. Os observáveis de URL e domínio são enriquecidos automaticamente quando os incidentes de segurança são criados.

A integração requer os produtos Security Incident Response e Inteligência contra ameaças.

Esta integração é compatível com Rome ou versões posteriores do Now Platform®.

Observáveis compatíveis para RISKIQ e RISKIQ WHOISIQ

A API RISKIQ oferece suporte a pesquisas automáticas de certificado SSL no endereço IP, hash de arquivo, número de série do certificado, domínio e observáveis de URL. Os observáveis de URL e domínio são enriquecidos automaticamente com a API WHOISIQ. Para aprimoramento de observável em outros tipos de observáveis com a API WHOISIQ, crie observáveis e execute pesquisas manualmente na tabela Observáveis.

Observáveis compatíveis

A tabela a seguir lista o tipo de APIs usadas nesta integração e os observáveis compatíveis com cada API. A tabela também indica se uma pesquisa ocorre automaticamente quando os incidentes de segurança são criados ou se a pesquisa é executada manualmente a partir da tabela Observáveis.

Pesquisa e observáveis compatíveis

API	Observáveis compatíveis	Pesquisa (automatizada ou manual)
RISKIQ API do certificado SSL	• Endereço IP • Hash de arquivo (impressão digital do certificado). Consulte a figura a seguir para obter um exemplo de um hash de arquivo. • Número de série do certificado ou número de série. Esta cadeia de caracteres é um ID exclusivo da entidade. Consulte a figura a seguir para obter um exemplo de um número de série de certificado. • Domínio (`www.site.com` ou `site.com`)	Pesquisa automatizada quando os incidentes são criados. Os resultados são exibidos na guia **Certificados SSL** do registro do incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa e observáveis compatíveis

API	Observáveis compatíveis	Pesquisa (automatizada ou manual)
	• URL **Nota:** verificações automáticas são executadas para o formato URL usando o protocolo https://, por exemplo, https://example.com/index.html	
RISKIQ WHOISIQ API	• Domínio • URL	Pesquisa automatizada quando os incidentes são criados. Os resultados são exibidos na guia **Resultados de aprimoramento do observável** no registro do incidente de segurança.
RISKIQ WHOISIQ API	• Endereço de e-mail • Nome da organização • Número de telefone • Endereço para correspondência	A pesquisa manual é executada na tabela Observáveis. Os resultados são exibidos na guia **Resultados** de aprimoramento do observável no registro do observável.

Exemplo de um hash de arquivo e número de série de certificado

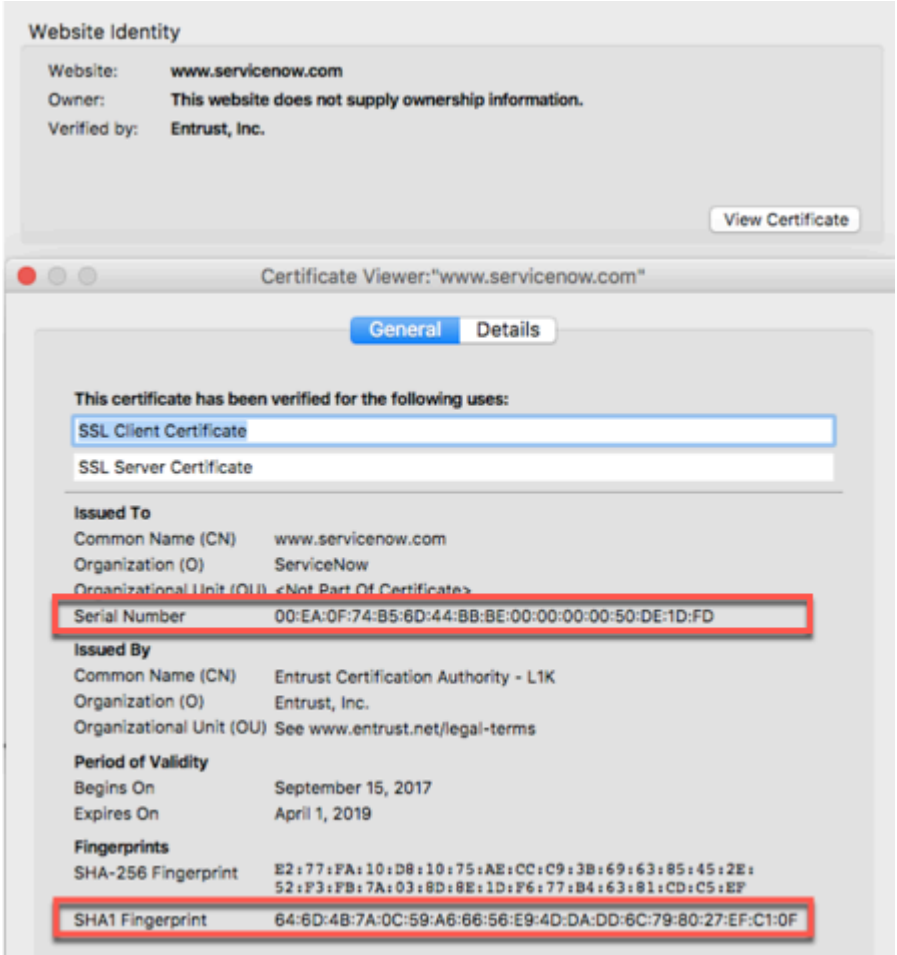
Esta figura mostra um exemplo do hash do arquivo e do número de série do certificado observáveis usados para as pesquisas de certificado SSL para esta integração.
O hash do arquivo se refere a uma impressão digital SHA-1. Este valor é exibido na sua instância Now Platform sem os separadores de dois pontos. Por exemplo, 646D4B7A0C59A66656E94DDADD6C798027EFC10F.

O número de série do certificado observável se refere ao ID exclusivo ou ao número de série da entidade. Este valor também é exibido sem os separadores de dois pontos. Por exemplo, 00EA0F74B56D44BBBE0000000050DE1DFD.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Hash do arquivo e número de série do certificado



Instalar e configurar RISKIQ e WHOISIQ

Antes de executar a integração em sua instância, conclua as etapas de instalação e configuração para que as aplicações RISKIQ e WHOISIQ se integrem corretamente ao Now Platform Security Operations.

Antes de Iniciar

Função necessária: admin, RISKIQ e WHOISIQ admin.

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções necessárias.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador do sistema (admin) instala o app e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração e verifica os resultados esperados. Esta função também tem acesso ao módulo Security Operations e

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

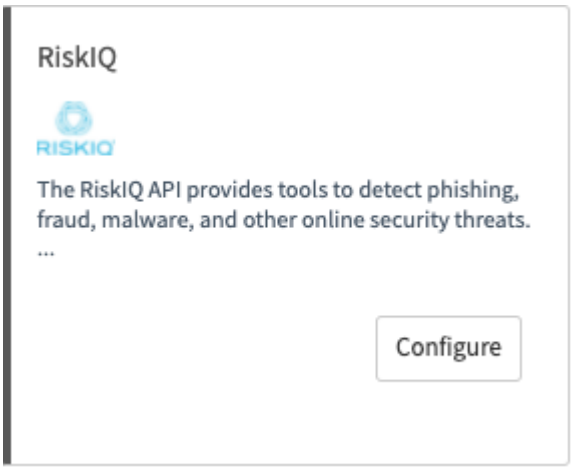
Configuração de tarefa	Descrição
	atribui a função de Analista de incidentes de segurança (sn_si.analyst). • O Analista de incidentes de segurança (sn_si.analyst) trabalha com registros de incidentes de segurança.
Obtenha um nome de usuário e uma chave de API.	Visite o site para obter informações sobre a chave de API e como criar uma conta: site do RISKIQ . A configuração requer que você insira a chave de API.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Requisitos da versão Madrid e posterior Para a versão Madrid e versões posteriores da família, o plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras aplicações Security Operations necessárias para a integração. Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Orquestração de suporte de segurança Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

Procedimento

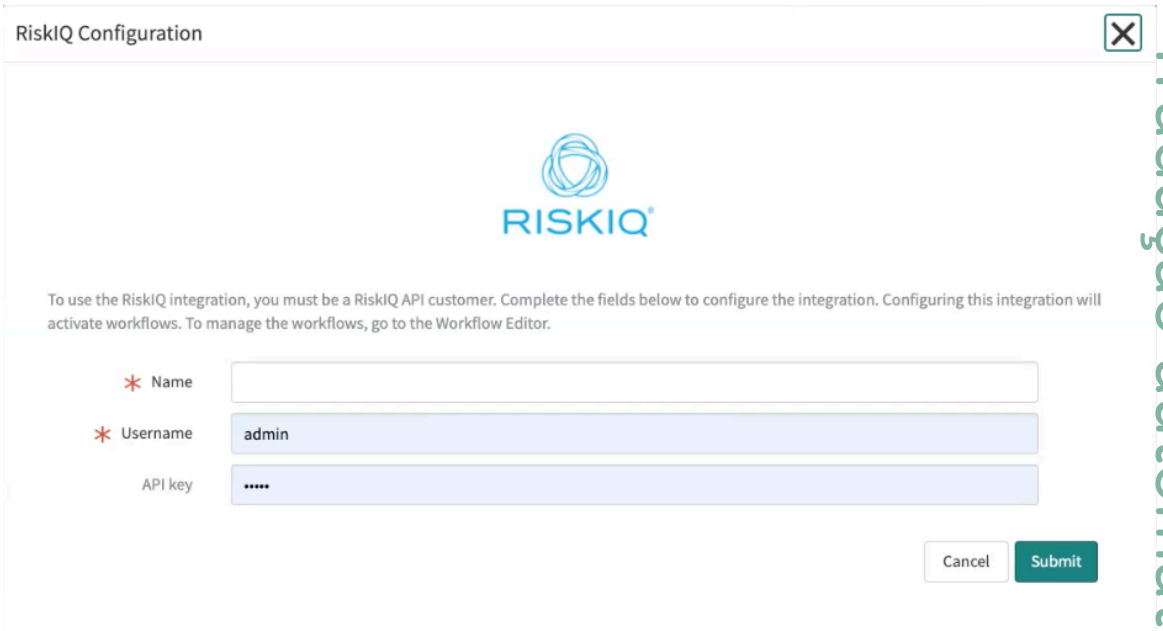
1. Se você não instalou a aplicação para a integração, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.
2. Quando a instalação for concluída, navegue até **Security Operations** > **Integrações** > **Configurações de integrações** e localize o bloco de API.
3. Clique em **Configurar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Na caixa de diálogo Configuração RiskIQ exibida, insira o Nome de **usuário** e **a chave de API**.



5. Clique em **Enviar**.
6. Verifique a configuração bem-sucedida.
   Quando a configuração é concluída com sucesso, a página Integrações de segurança com os blocos de integração é exibida.

Trouble?
Se uma mensagem de erro for exibida, o nome de usuário ou a chave de API podem ser inválidos. Verifique se o nome de usuário e a chave de API estão corretos:

Solução de problemas

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verifique os resultados esperados para pesquisas de certificado SSL RISKIQ

Quando um incidente de segurança gera observáveis para URLs, domínios, endereços IP, hashes de arquivo de certificado (impressão digital SHA-1) e números de série de certificado, os analistas de incidentes de segurança usam os resultados da pesquisa de certificado SSL para verificar se os sites têm certificados que foram emitidos por um confiável autoridade de certificação (CA) pública.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Para observáveis compatíveis, o Now Platform verifica a ocorrência mais recente de URLs, domínios, endereços IP, hashes de arquivo de certificado (impressão digital SHA-1) e números de série de certificados. Estes são os resultados possíveis da verificação:

Uma correspondência exata foi encontrada

Um emissor válido de um certificado SSL está listado no registro de incidente de segurança.

Nenhum resultado de certificação encontrado

Nenhum resultado é listado no registro de incidente de segurança.

Uma correspondência exata foi encontrada para um certificado autoassinado ou gerado internamente

Os resultados de um certificado SSL gerado internamente são exibidos no registro de Incidente de segurança.

Não foi encontrada uma correspondência exata para um certificado SSL primário

Um valor de pesquisa retorna várias entradas e um certificado primário não pode ser identificado. Uma mensagem de resumo é exibida no registro do Incidente de segurança.

Procedimento

1. Para exibir os observáveis e verificar os resultados da pesquisa, abra o registro de incidente de segurança com o qual você está trabalhando e localize as anotações de trabalho.

Example

Para ilustrar exemplos dos possíveis resultados de pesquisa para esta integração, suponha que um incidente de segurança tenha sido gerado com os seguintes observáveis:

- comunidade.servicenow.com
- invalidsubdomain.servicenow.com
- mail.dgnetworks.com
- servicenow.com

Observáveis e localização dos resultados da pesquisa

Observável (exemplo)	Resultados da varredura	Descrição e local
comunidade.servicenow.com	Certificado encontrado com um hash SHA1.	Uma correspondência exata é encontrada e um emissor válido de um certificado SSL é listado. Os resultados da correspondência exata são exibidos na guia **Certificados SSL** no registro do incidente de segurança.

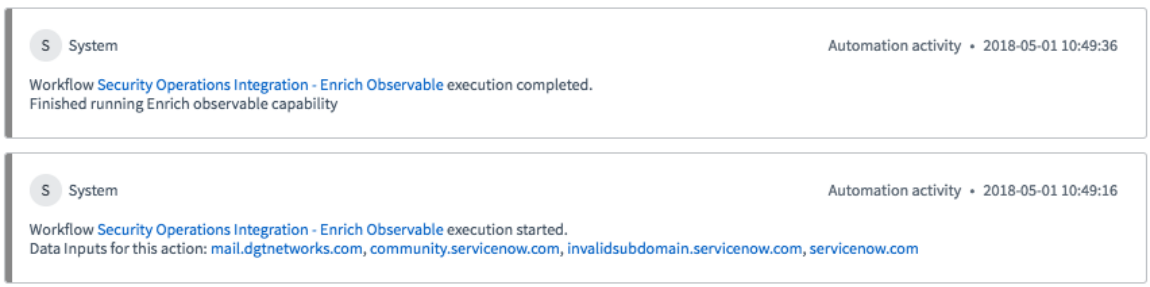
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Observável (exemplo)	Resultados da varredura	Descrição e local
invalidsubdomain.servicenow.com	Nenhum certificado encontrado.	Um resumo que indica que nenhum resultado de certificado foi encontrado é exibido na guia **Resultados de aprimoramento do observável** no registro do incidente de segurança.
mail.dgnetworks.com	Certificado encontrado com hash SHA1.	Uma correspondência exata é listada para um certificado autoassinado ou gerado internamente. Os resultados são exibidos na guia **Certificados SSL** no registro do incidente de segurança.
servicenow.com	A pesquisa retornou 138 certificados e não foi possível identificar um único certificado primário.	Uma correspondência exata não foi encontrada para um certificado SSL primário porque um valor de pesquisa retorna vários certificados. Um resumo que indica que nenhum certificado primário foi encontrado é exibido na guia **Resultados de aprimoramento do observável** no registro do incidente de segurança.

Depois que a aplicação é configurada, o fluxo de trabalho é iniciado automaticamente. O status de pesquisa e os observáveis são exibidos nas anotações de trabalho.

2. Verifique se a pesquisa foi executada com sucesso.



Trouble?
Se você não puder exibir os resultados esperados, verifique se o observável é compatível com a pesquisa de certificado SSL para a integração.

Tópicos relacionados

Observáveis compatíveis para RISKIQ e RISKIQ WHOISIQ

RISKIQ Pesquisas de certificado SSL que retornam uma correspondência exata

RISKIQ Os resultados da pesquisa de certificado SSL para uma correspondência exata são exibidos na guia **Certificados SSL** no registro do incidente de segurança. Uma correspondência exata fornece um nome de autoridade de certificação válido, o que ajuda um analista de incidente de segurança a determinar a validade de um site.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example: Correspondência exata para um certificado SSL válido

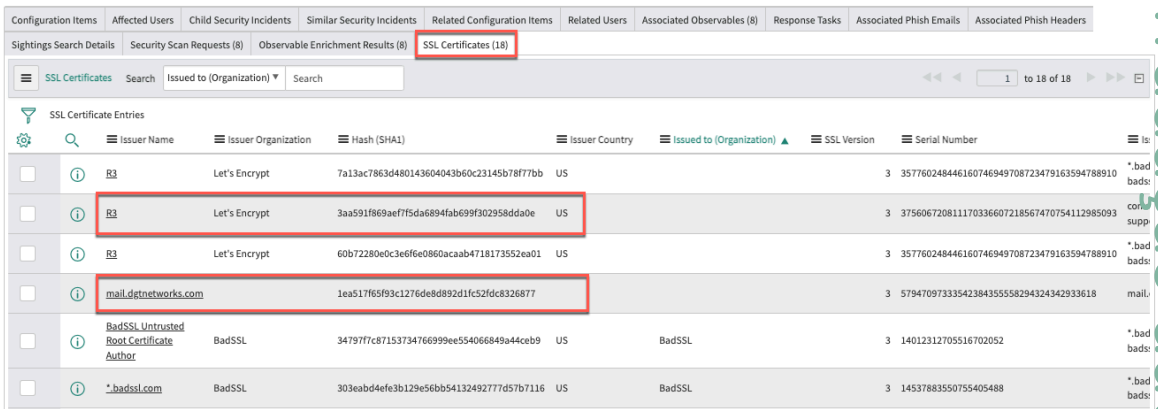
O exemplo a seguir mostra um emissor válido de um certificado SSL de uma correspondência exata nos resultados da pesquisa. Siga as etapas para exibir os resultados e os dados brutos.

Nota:
As imagens nos exemplos a seguir são mostradas com a configuração **Formulários** com guia ativa nas Configurações do sistema. Se sua tela não corresponder à exibição mostrada abaixo, siga as etapas para definir formulários com guias.

1. No canto superior direito do quadro da faixa, clique no ícone Configurações.
2. Na caixa de diálogo **Configurações do sistema** exibida, clique em **Formulários** e verifique se **Formulários com guia** e **Com o formulário** estão selecionados.

1. No registro do incidente de segurança, clique na guia **Certificados SSL**.

Guia Certificados SSL



Informações sobre o nome do emissor do certificado, a organização do emissor e para quem o certificado foi emitido (organização) são exibidas junto com outros dados.

18 itens são exibidos na coluna **Nome do emissor**. O segundo item (R3) fornece um nome de autoridade de certificação válido (Let's Encrypt) na coluna **Organização do emissor**.

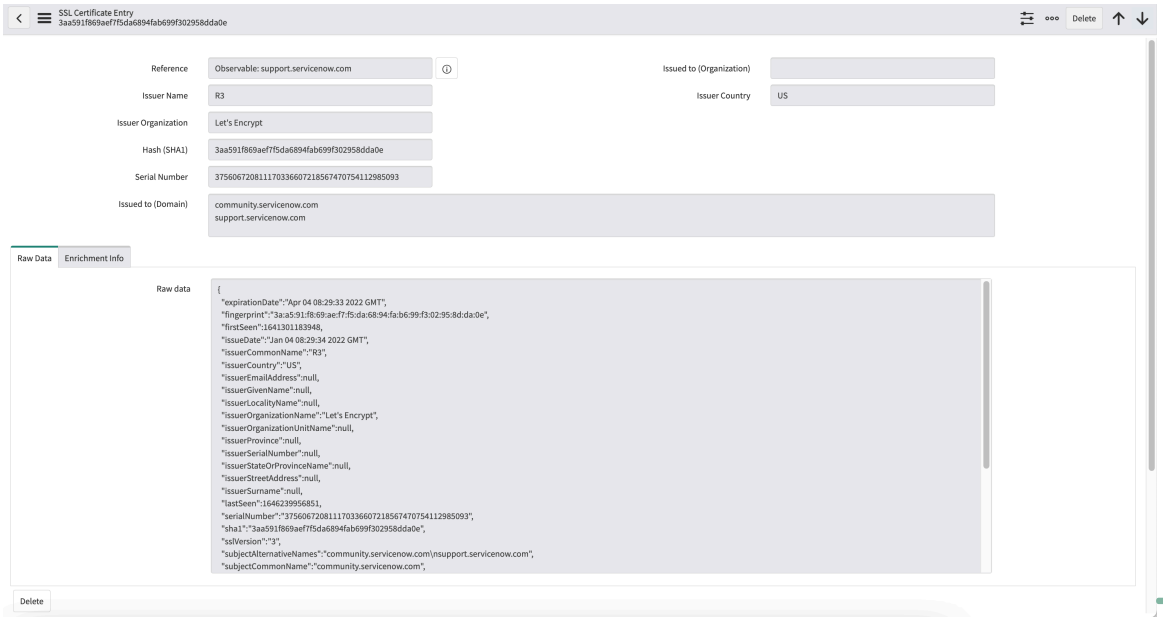
Nenhuma informação nas colunas **Organização do emissor** e **Emitido para** é exibida para o segundo item (mail.dgtnetworks.com).

2. Clique no segundo item na coluna **Nome do emissor**, que é (**R3**) para abrir o registro de entrada. Como alternativa, clique no ícone de informações ao lado do item seguido por **Abrir registro**.
3. Selecione a guia **Dados brutos**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Dados brutos



O registro de entrada de certificado SSL inclui o observável na guia **Dados brutos** na coluna **Nome da entidade**, bem como outros dados.

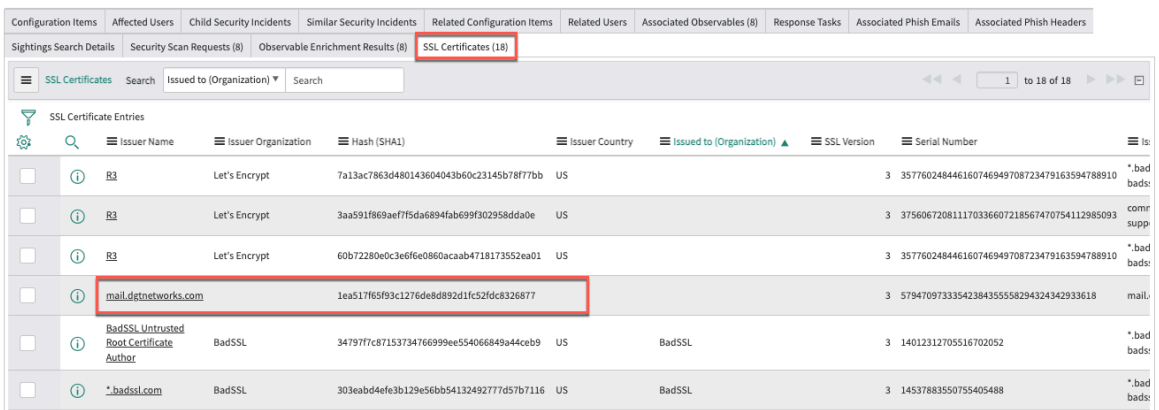
Observe que na coluna **Categoria**, o Assuntoe o Emissor correspondem a entidades reconhecíveis na coluna **Nome da entidade**. O emissor deste certificado provavelmente é válido e de uma autoridade de certificação pública confiável. Observe também que o Assuntoe o Emissor são entidades diferentes. Essas entidades separadas indicam que o certificado não é um certificado assinado internamente de uma autoridade de certificação desconhecida.

Example: Correspondência exata para um certificado SSL autoassinado

O exemplo a seguir mostra os resultados de um certificado SSL autoassinado da pesquisa. Siga as etapas para exibir os resultados e os dados brutos.

1. Navegue de volta para o registro do incidente de segurança. Na coluna **Nome do emissor**, clique no outro item (**mail.dgtnetworks.com**).

Guia Certificados SSL

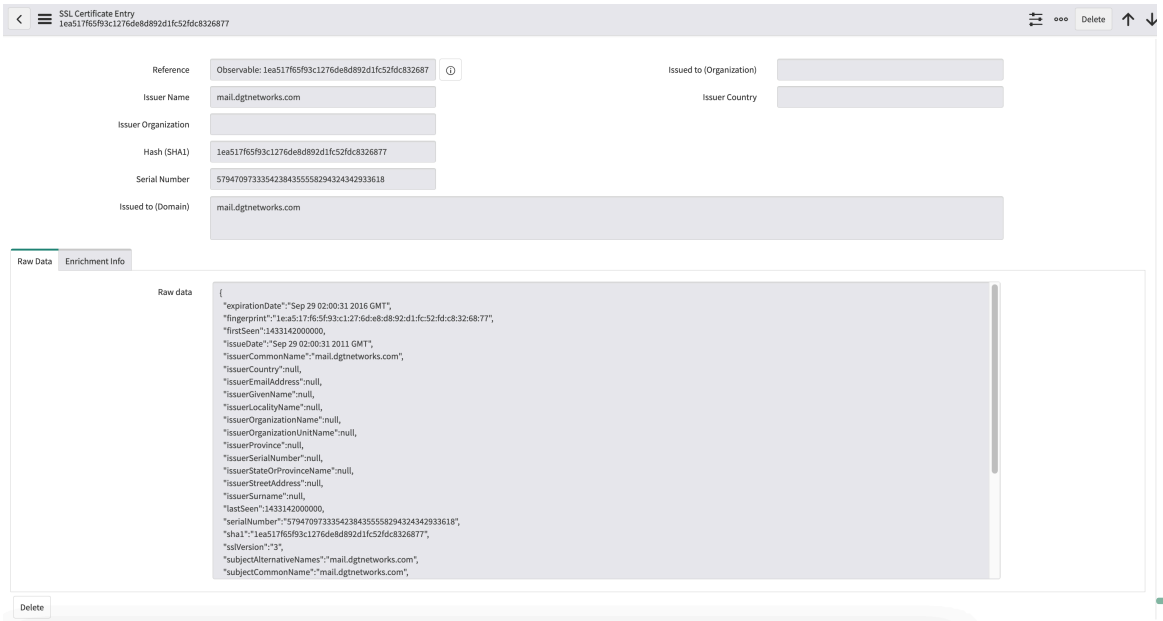


2. No registro aberto, selecione a guia **Dados brutos**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Dados brutos



A coluna **Categoria** indica que o Emissor (mail.dgtnetworks.com e dgtsbs.DGTNetworks.local) não são autoridades de certificação públicas confiáveis. Observe também que o Emissor e o Assunto são a mesma entidade (dgtsbs.DGTNetworks.local) e cada um contém o nome do observável (dgtsbs). Este certificado é possivelmente um certificado autoassinado. Certificados autoassinados podem justificar uma investigação mais aprofundada, já que esses certificados não são emitidos por uma autoridade de certificação conhecida.

RISKIQ Pesquisas de certificado SSL que retornam vários certificados ou nenhum certificado

Um analista de incidente de segurança pode usar vários resultados de certificado SSL para determinar se um site faz parte de uma entidade comum reconhecível. Nenhum resultado de certificado SSL pode indicar que sites com nomes obscuros ou suspeitos não têm certificados confiáveis. Os resultados da pesquisa de observáveis que não retornam certificados SSL ou que retornam vários certificados SSL são exibidos na guia Resultados de aprimoramento de observável no registro de incidente de segurança.

Example: Nenhum resultado de certificado SSL ou vários resultados de certificado SSL

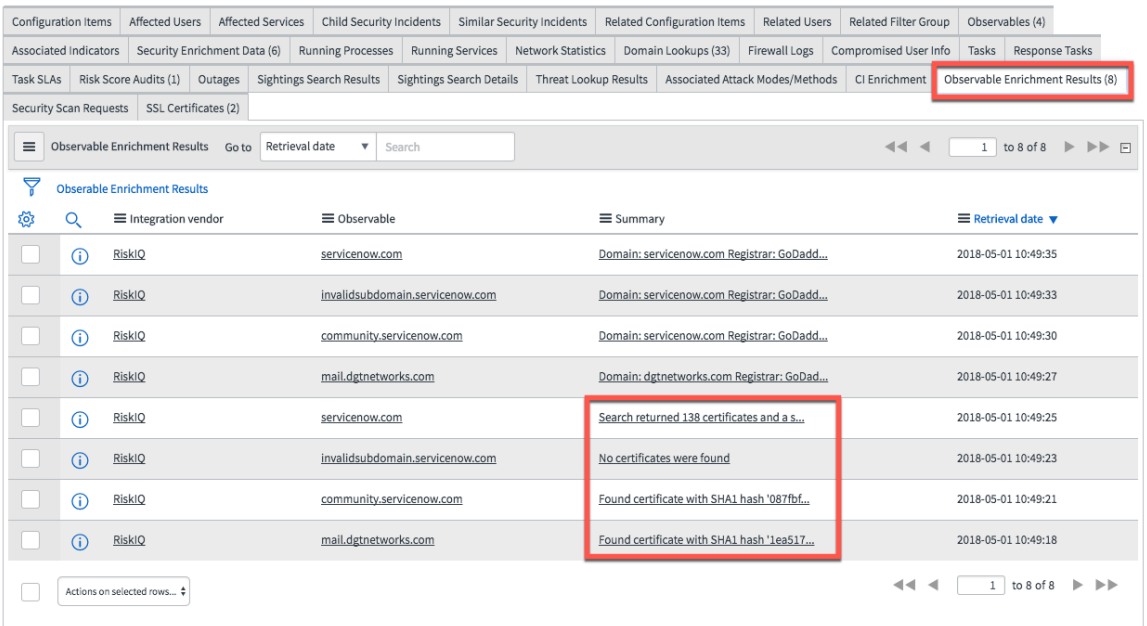
Siga as etapas para exibir os resultados dos observáveis que não retornam certificados SSL ou que retornam vários certificados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. No registro de incidente de segurança, clique na guia **Resultados de aprimoramento do observável**.

Guia Resultados de aprimoramento de observável

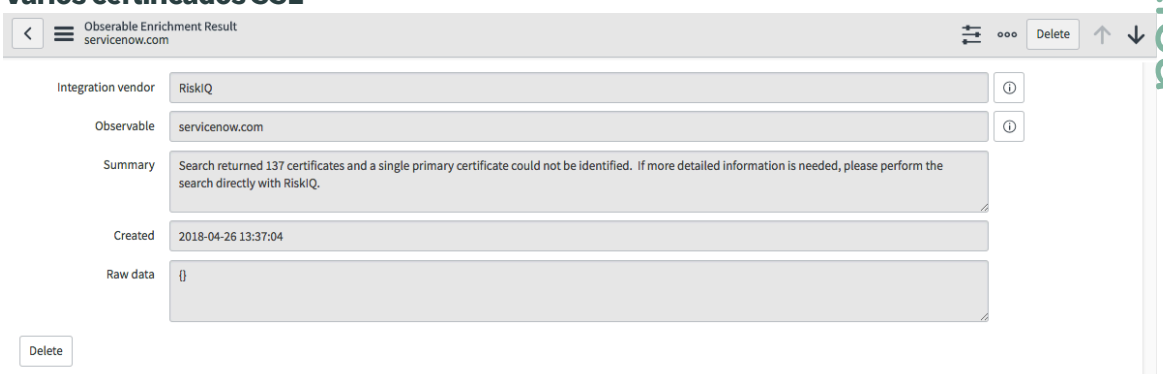


Os resultados de aprimoramento observáveis para a pesquisa RISKIQ e WHOISIQ são exibidos.

Na coluna **Observável**, servicenow.com corresponde à mensagem A pesquisa retornou 138 certificados na coluna **Resumo**. Da mesma forma, invalidsubdomain.servicenow.com corresponde a Nenhum certificado encontrado na coluna **Resumo**. Esses resumos indicam que vários certificados SSL foram encontrados e que nenhuma correspondência exata para os certificados SSL foi encontrada, respectivamente.

2. Na coluna **Observável**, clique em **servicenow.com**.

Vários certificados SSL



A mensagem de resumo exibida no registro indica que vários resultados de certificados SSL foram retornados para servicenow.come um certificado SSL primário não pôde ser correspondido. Essa mensagem geralmente é retornada em pesquisas que incluem nomes de domínio comuns, como servicenow.com.

Se você precisar de mais informações sobre um domínio comum, poderá executar a pesquisa diretamente com a API RISKIQ.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Navegue de volta para a guia **Resultados** de aprimoramento do observável e, na coluna **Observável**, clique em **invalidsubdomain.servicenow.com**.

Nenhum certificado SSL

Nota:

- Se nenhum certificado SSL for encontrado para o observável atual, o campo Resumo exibirá a mensagem Nenhum certificado encontrado.
- Se nenhum certificado SSL ativo for encontrado para o observável atual, o campo Resumo exibirá a mensagem Nenhum certificado ativo encontrado.

Verifique os resultados esperados para pesquisas de URL WHOISIQ

Quando um incidente de segurança gera observáveis para URLs ou domínios, a API WHOISIQ executa o aprimoramento do observável automaticamente após a criação do incidente de segurança. Os resultados da pesquisa são exibidos nas guias **Resultados de aprimoramento do observável** e **Certificados SSL** no registro do incidente de segurança.

Antes de Iniciar

Nota:
As imagens nas etapas a seguir são mostradas com a configuração **Formulários** com guia ativa nas Configurações do sistema.

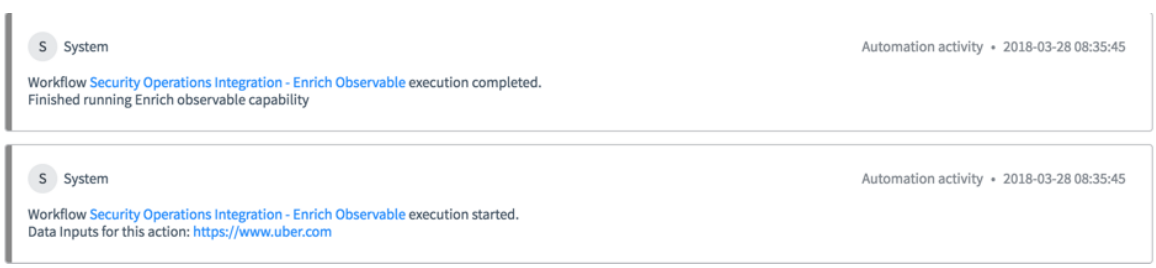
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Os resultados de aprimoramento do observável são exibidos na guia **Resultados** de aprimoramento do observável na parte inferior do registro do incidente de segurança. Para observáveis compatíveis, uma pesquisa de certificado SSL também é executada e os resultados são exibidos na**guia Certificados SSL**.

Procedimento

1. Abra o registro de incidente de segurança com o qual você está trabalhando e verifique se a pesquisa foi executada com sucesso nas anotações de trabalho.

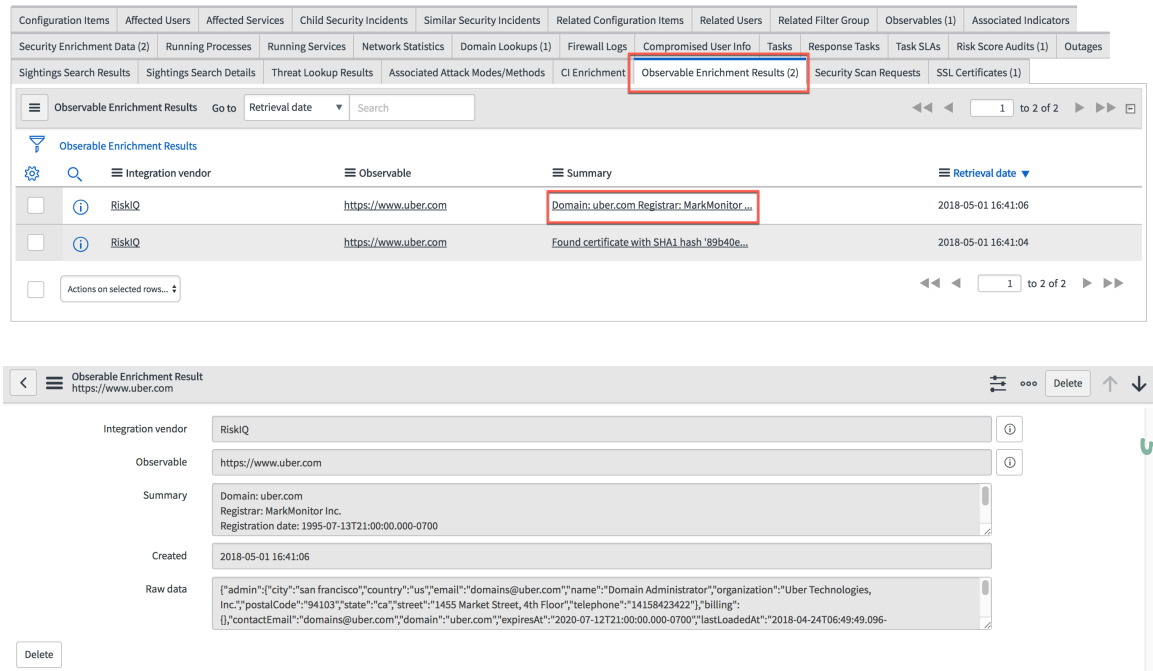


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

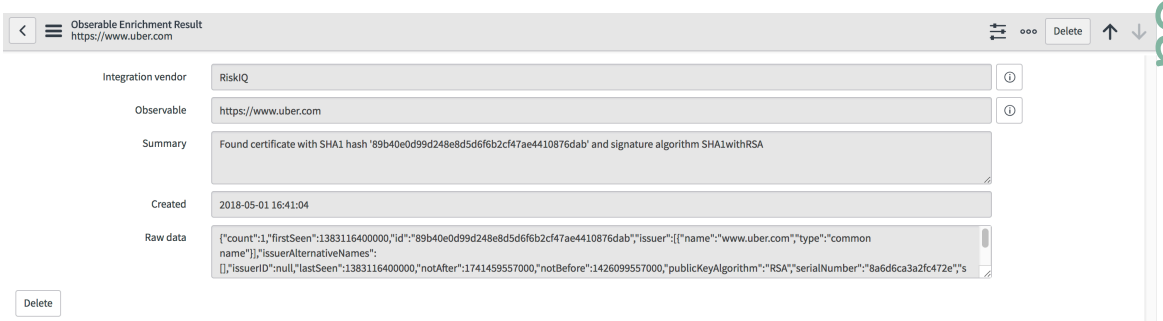
Depois que a aplicação estiver configurada, o fluxo de trabalho será iniciado automaticamente após a criação do incidente. O status de execução e conclusão da pesquisa é exibido nas anotações de trabalho no registro de Incidente de segurança.

2. Se você não puder verificar se a pesquisa foi executada com sucesso, revise as anotações de trabalho para obter mais informações sobre como prosseguir.
3. No incidente de segurança aberto, clique no link relacionado **Mostrar todas as listas** relacionadas.
4. Clique na guia **Resultados de aprimoramento do observável** para selecioná-la.
5. Na coluna **Resumo**, clique no primeiro item, **Domínio: uber.com Registrador: Markmonitor...**.



O registro exibido contém informações sobre o domínio.

6. Navegue de volta para a guia **Resultados de aprimoramento do observável** e, na coluna **Resumo**, clique no segundo item, **Certificado encontrado com hash SHA1...**.

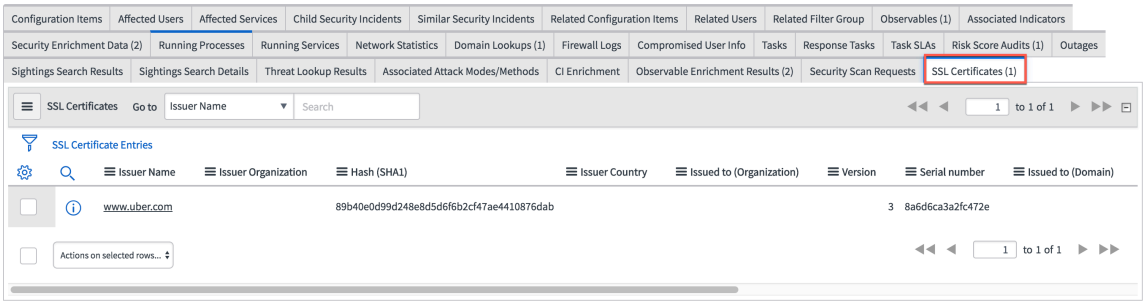


Este registro indica que um certificado SSL foi encontrado com um hash de arquivo.

7. Navegue de volta para o registro do incidente de segurança e clique na guia **Certificados SSL**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Os resultados do Certificado SSL para o hash do arquivo também são exibidos aqui.

Trouble?

Se você não puder exibir os resultados esperados, revise as anotações de trabalho. Além disso, verifique se o observável é compatível com a pesquisa pela integração.

Tópicos relacionados

Observáveis compatíveis para RISKIQ e RISKIQ WHOISIQ

Criar um observável para pesquisas manuais WHOISIQ

Os analistas de incidentes de segurança usam informações do aprimoramento observável com a API WHOISIQ para saber mais sobre os endereços de e-mail, nomes e números de telefone das organizações.

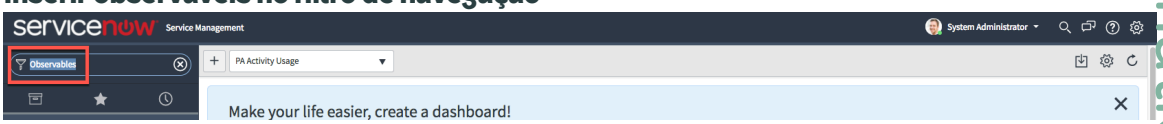
Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

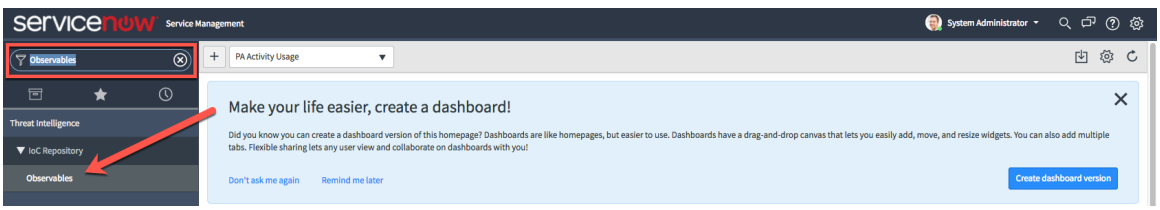
1. Navegar até **Todos** > **Repositório LOC** > **Observáveis**.

Inserir observáveis no filtro de navegação



No painel de navegação, o módulo Observáveis é exibido.

Módulo de observáveis

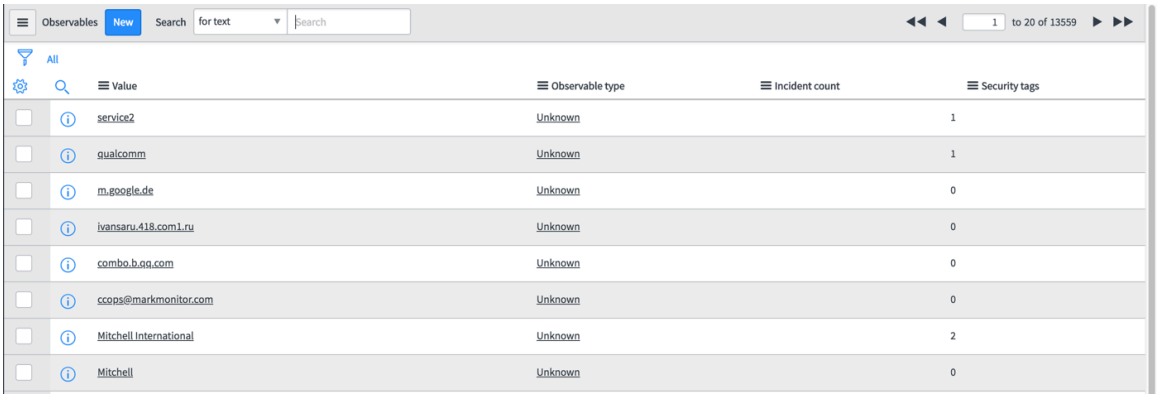


2. Clique no módulo **Observáveis** para exibir a lista de Observáveis.

Tradução automática

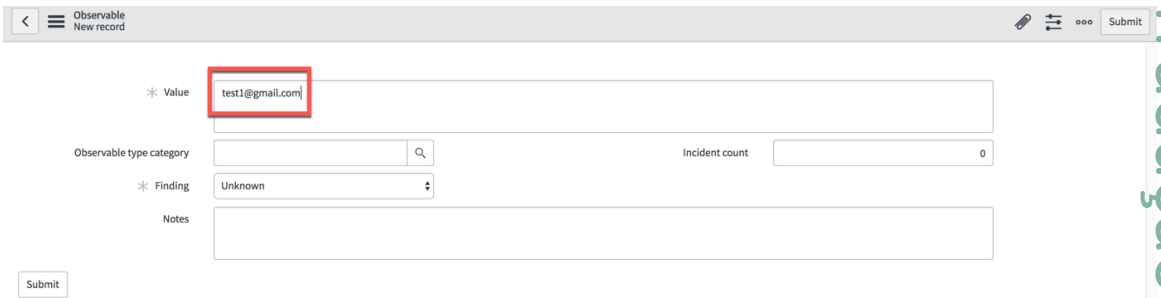
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista de observáveis



3. Clique em **Novo** para criar um novo observável.
4. No formulário Observável, preencha os campos.

Criar um novo observável



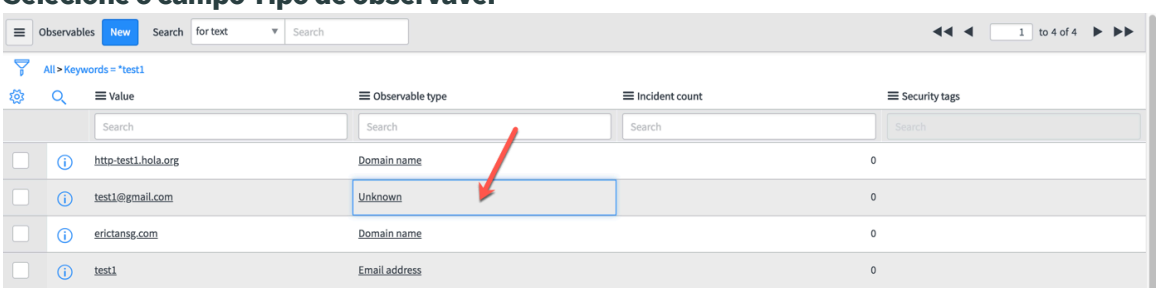
5. Clique em **Enviar**.
   Você retornará à lista Observáveis. Na coluna **Valor**, seu novo observável é exibido.

> **Nota:**
> Se você não conseguir localizar seu observável na parte da lista exibida, use a funcionalidade de pesquisa para localizá-lo.

6. Edite o campo **Tipo de observável** para mudar o tipo de **Desconhecido** para Endereço de **e-mail** para corresponder ao seu observável.

   a. Na coluna **Tipo de observável**, clique uma vez à direita do texto **Desconhecido** para selecioná-lo.

Selecione o campo Tipo de observável



   O campo selecionado é contornado em azul.

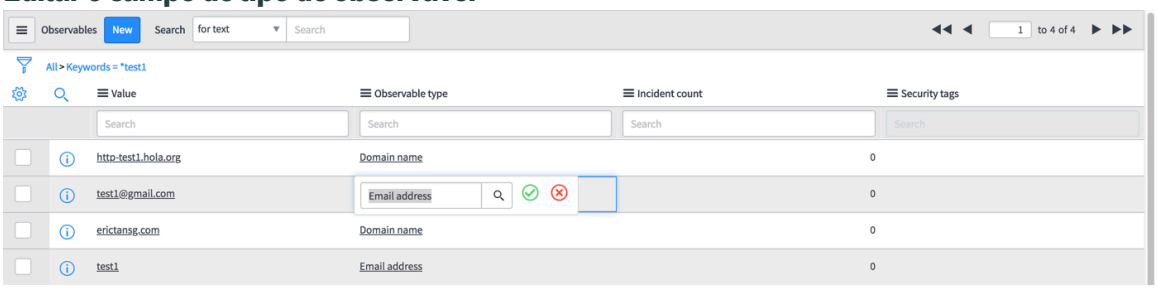
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

b. Com o campo contornado em azul, clique duas vezes em qualquer lugar dentro do campo realçado para abrir o editor.

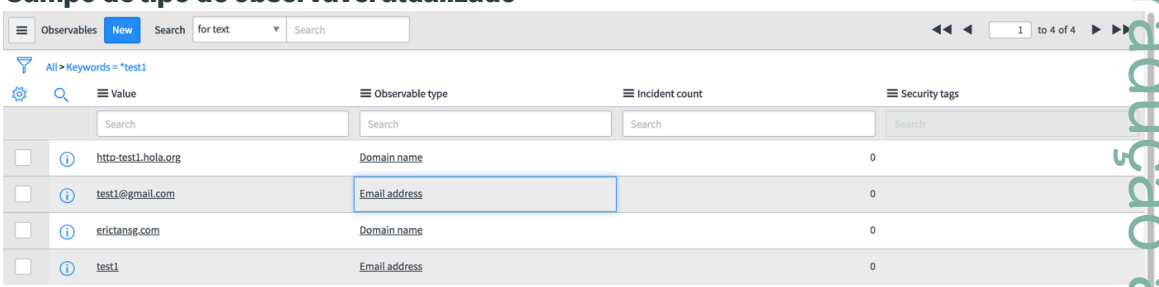
c. No campo exibido, insira o tipo de observável (Endereço de e-mail) e clique na marca de seleção verde para salvar o valor.

Editar o campo de tipo de observável



Na coluna **Tipo de observável** na lista, Endereço de e-mail é exibido para o novo observável.

Campo de tipo de observável atualizado



O que Fazer Depois

Se você tiver criado e editado um observável para pesquisa, execute a pesquisa de aprimoramento do observável do registro do observável com a API WHOISIQ.

Verificar resultados esperados para pesquisas manuais WHOISIQ

Execute uma pesquisa manual em um observável quando ele não gerar automaticamente um incidente de segurança. Para pesquisas de aprimoramento observáveis usando a API WHOISIQ para endereços de e-mail, nomes de organizações, números de telefone ou endereços de correspondência, inicie a pesquisa manualmente na tabela Observáveis.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

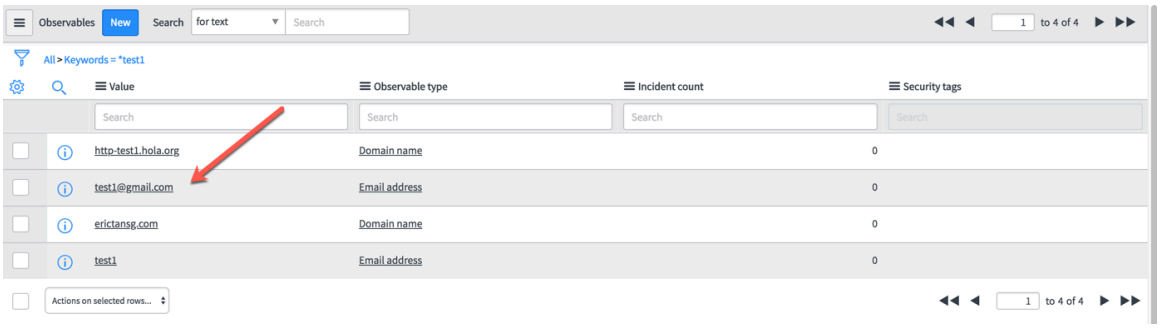
Crie um observável para uma pesquisa manual usando a API WHOISIQ. Para obter mais informações sobre como criar e editar um observável, consulte Criar um observável para pesquisas manuais WHOISIQ.

Procedimento

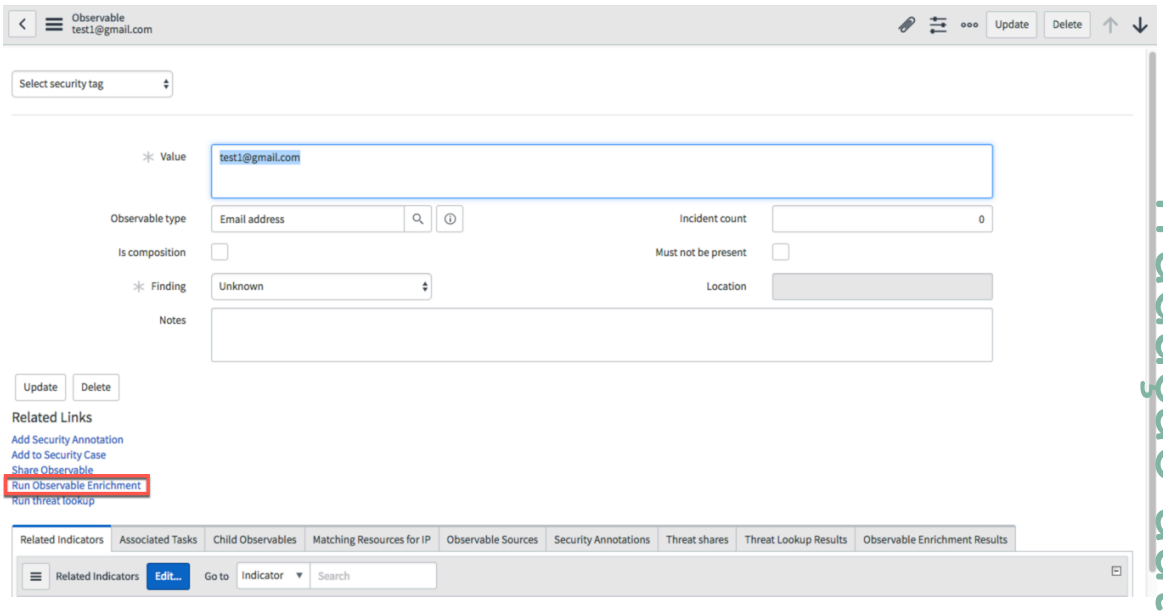
1. Navegar até **Todos** > **Repositório LOC** > **Observáveis** e localize o observável na lista com a qual você está trabalhando.
2. Clique no seu observável na coluna **Valor** para abrir o registro.

Tradução automática

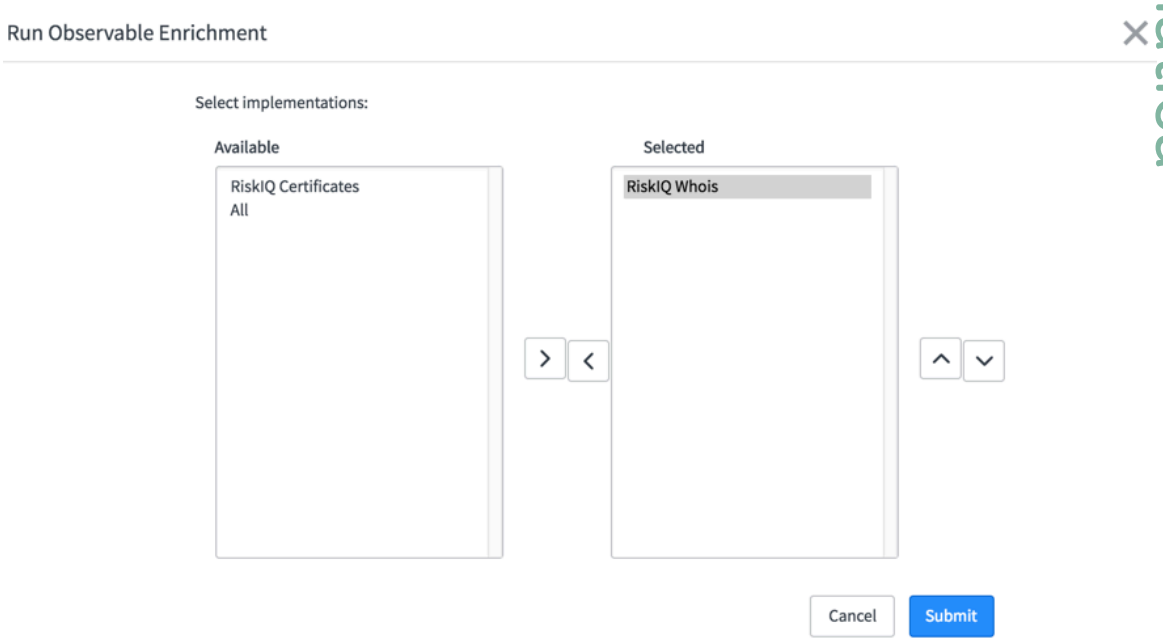
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique no link relacionado **Executar aprimoramento de observável** para executar a pesquisa.



4. Na janela **Executar aprimoramento de observável**, mova **RiskIQ Whois** para a lista Selecionado.

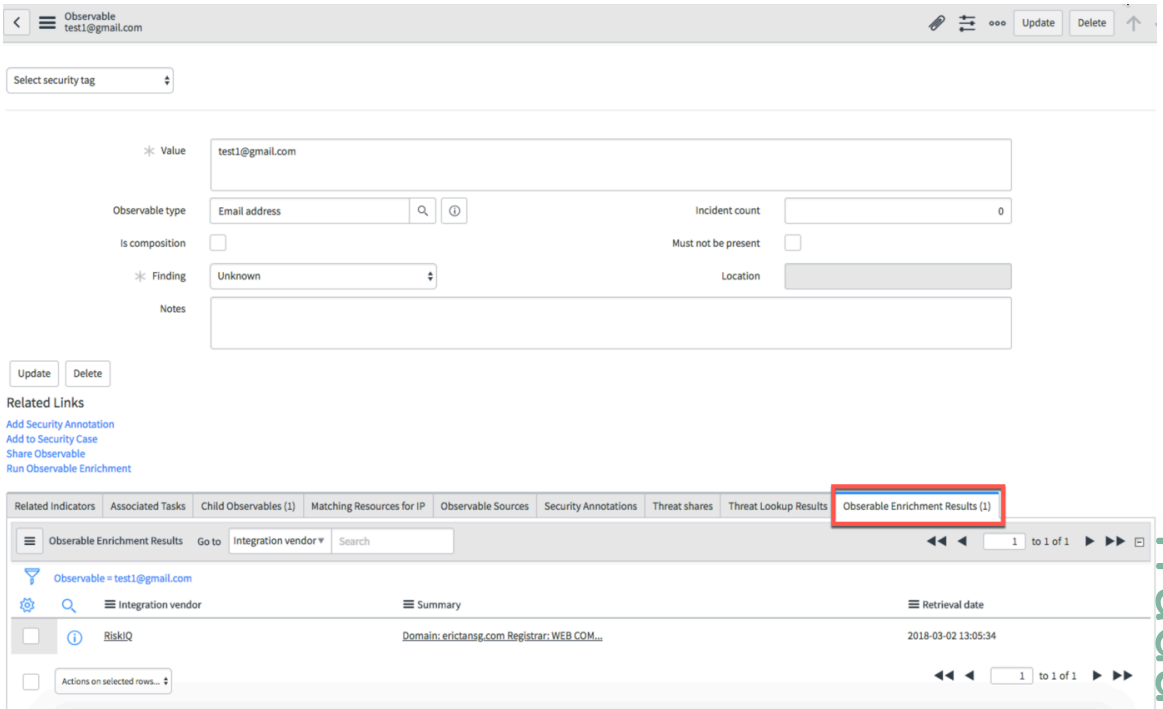


5. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os resultados da pesquisa são exibidos na guia **Resultados** de aprimoramento do observável no registro do observável.



Trouble?
Se nenhum resultado for retornado para o observável, uma mensagem será exibida na coluna **Resumo**. Se você não vir resultados, verifique se o observável é compatível com a API.

Tópicos relacionados

Observáveis compatíveis para RISKIQ e RISKIQ WHOISIQ

Integração de Shodan

Shodan é um mecanismo de pesquisa que analisa as informações da faixa de serviço de dispositivos conectados em todo o mundo. As faixas de serviço incluem informações sobre um sistema de computador, como nome do host, tipo de dispositivo, sistema operacional, localização geográfica e ISP conectado. Quando integrado ao produto Now Platform Security Operations, essas informações de faixa de serviço fornecem aos analistas dados de aprimoramento adicionais e informações para incidentes de segurança ou investigações.

A integração requer os plug-ins Security Incident Response e Inteligência contra ameaças.

A integração Shodan executa o aprimoramento nos seguintes observáveis:

- Endereços IP
- URLs
- Hashes de arquivo

A aplicação verifica se há novos observáveis a cada cinco minutos. Se os observáveis forem de um tipo reconhecido pela integração Shodan, os observáveis serão aprimorados.

Esta integração é compatível com as versões Kingston, London, Madrid e New York da Now Platform®.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instalar e configurar Shodan

Antes de executar a integração na sua instância, conclua as etapas de instalação e configuração para que a aplicação Shodan se integre corretamente com Now Platform Security Operations.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Tarefas de configuração	Descrição
Verifique se você atribuiu as funções Now Platform necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • O administrador do sistema (admin) instala o app e atribui a função de administrador de incidentes de segurança (sn_si.admin). • O administrador de incidentes de segurança (sn_si.admin) supervisiona a configuração e verifica os resultados esperados. Esta função também tem acesso ao módulo Security Operations.
Obtenha a chave de API Shodan.	Crie uma conta e obtenha a chave de API no site Shodan : site do Shodan .
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Para a versão Madrid e versões posteriores da família, o plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras aplicações Security Operations necessárias para a integração. Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas. **1.** Security Incident Response **2.** Security Integration Framework **3.** Security Support Common **4.** Orquestração de suporte de segurança Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte Obter direito para um

Tradução automática

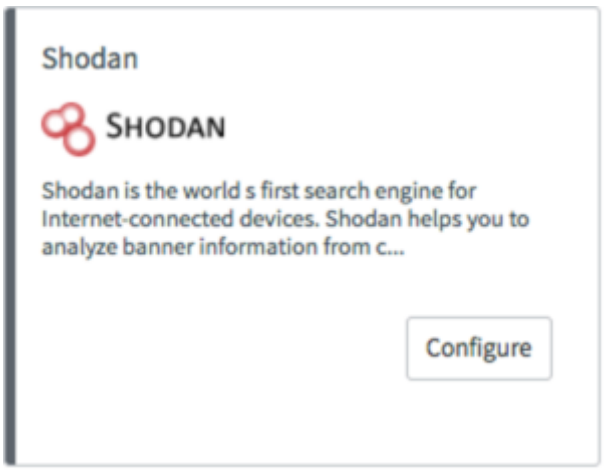
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

Função necessária: administrador

Procedimento

1. Se você não instalou a aplicação para a integração, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.
2. Após a conclusão da instalação, navegue até **Integrações** > **Configurações de integrações** e localize o bloco Shodan.



3. Clique em **Configurar**.
4. Na caixa de diálogo **Configuração do Shodan**, insira a chave de API que você obteve no site Shodan e clique em **Enviar**.

5. Verifique a configuração bem-sucedida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida.

Trouble?

Se uma mensagem de erro for exibida durante a configuração, a chave de API Shodan pode ser inválida.

Verificar resultados esperados para Shodan

Os observáveis são gerados automaticamente por um incidente de segurança e verificados pela aplicação. Os resultados de aprimoramento são exibidos nas guias **Resultados de aprimoramento do observável** e **Faixas de rede**.

Antes de Iniciar

Função necessária: sn_si.analyst.

Procedimento

1. Abra o incidente de segurança com o qual você está trabalhando e verifique se a pesquisa foi executada com sucesso.

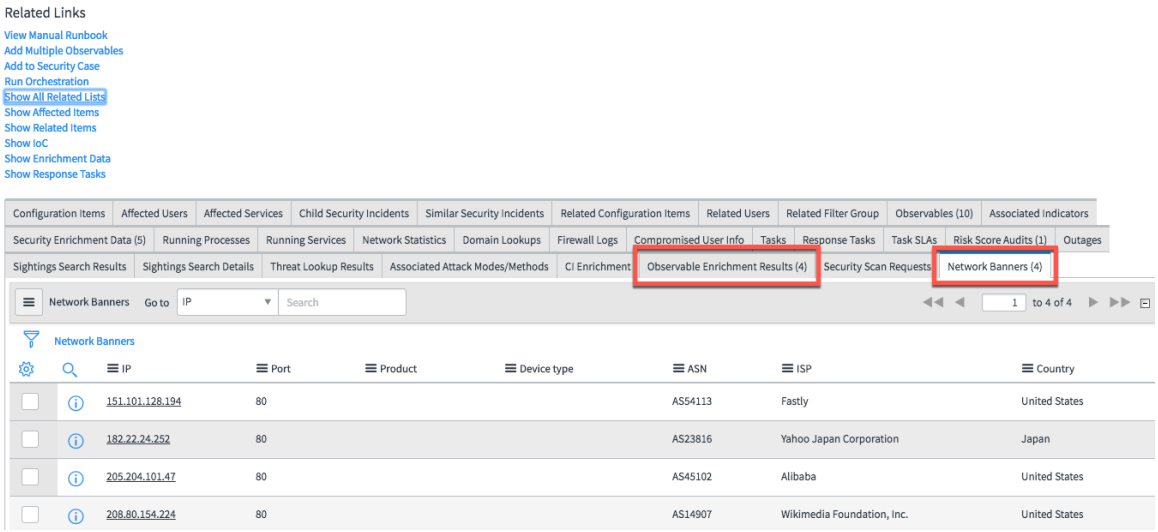
   Depois que a aplicação estiver configurada, o fluxo de trabalho será iniciado automaticamente após a criação do incidente. O status de execução e conclusão da pesquisa é exibido nas anotações de trabalho no incidente de segurança.

2. Revise as anotações de trabalho para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.
3. Navegue até a parte inferior do incidente de segurança e clique no link **Mostrar todas as listas** relacionadas em **Links relacionados**.

> **Nota:**
> As imagens nas etapas a seguir são mostradas com a configuração **Formulários** com guia ativa nas Configurações do sistema. Se os formulários com guias não forem exibidos, no canto superior direito do quadro da faixa, clique no ícone de engrenagem Configurações. Na caixa de diálogo **Configurações do sistema** exibida, clique em **Formulários** e verifique se **Formulários com guia** e **Com o formulário** estão selecionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Os resultados são exibidos nas guias **Resultados de aprimoramento do observável** e **Faixas de rede** na parte inferior do incidente de segurança.

4. Com a guia **Faixas de rede** selecionada, clique no ícone de informações azul ao lado de um observável.

5. Na caixa de diálogo exibida, clique em **Abrir registro** para exibir os dados brutos e mais detalhes.

Trouble?
Se você não vir resultados nas guias **Resultados de aprimoramento do observável** e **Faixas de rede**, verifique se o observável é um tipo compatível para pesquisa pela integração.

(Opcional) Anexar manualmente um observável para Shodan

Você pode anexar manualmente observáveis a um incidente de segurança. Você anexa observáveis manualmente quando deseja executar pesquisas de ameaça em observáveis que não estão anexados a um incidente de segurança no gatilho de evento inicial. Além disso, você pode executar esta tarefa quando quiser mais informações sobre um observável relacionado.

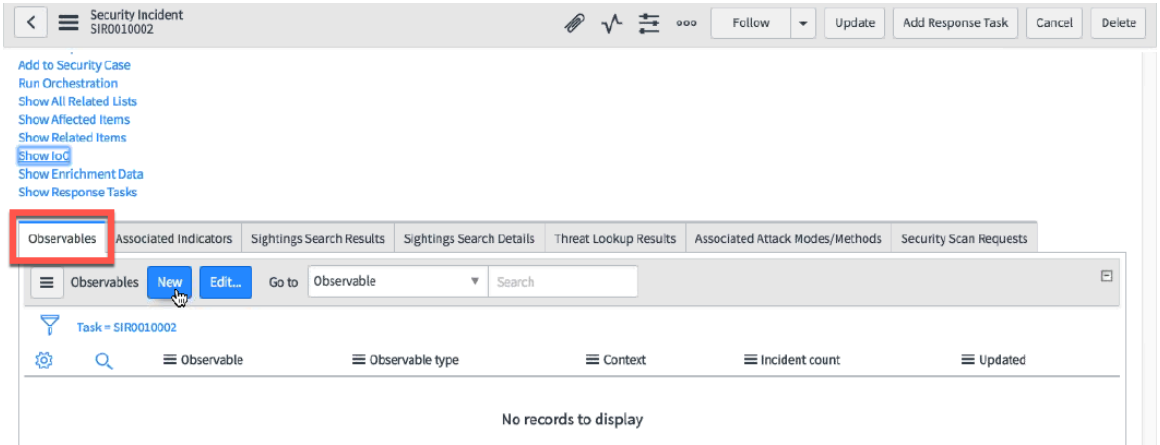
Antes de Iniciar
Função necessária: sn_si.analyst

Procedimento

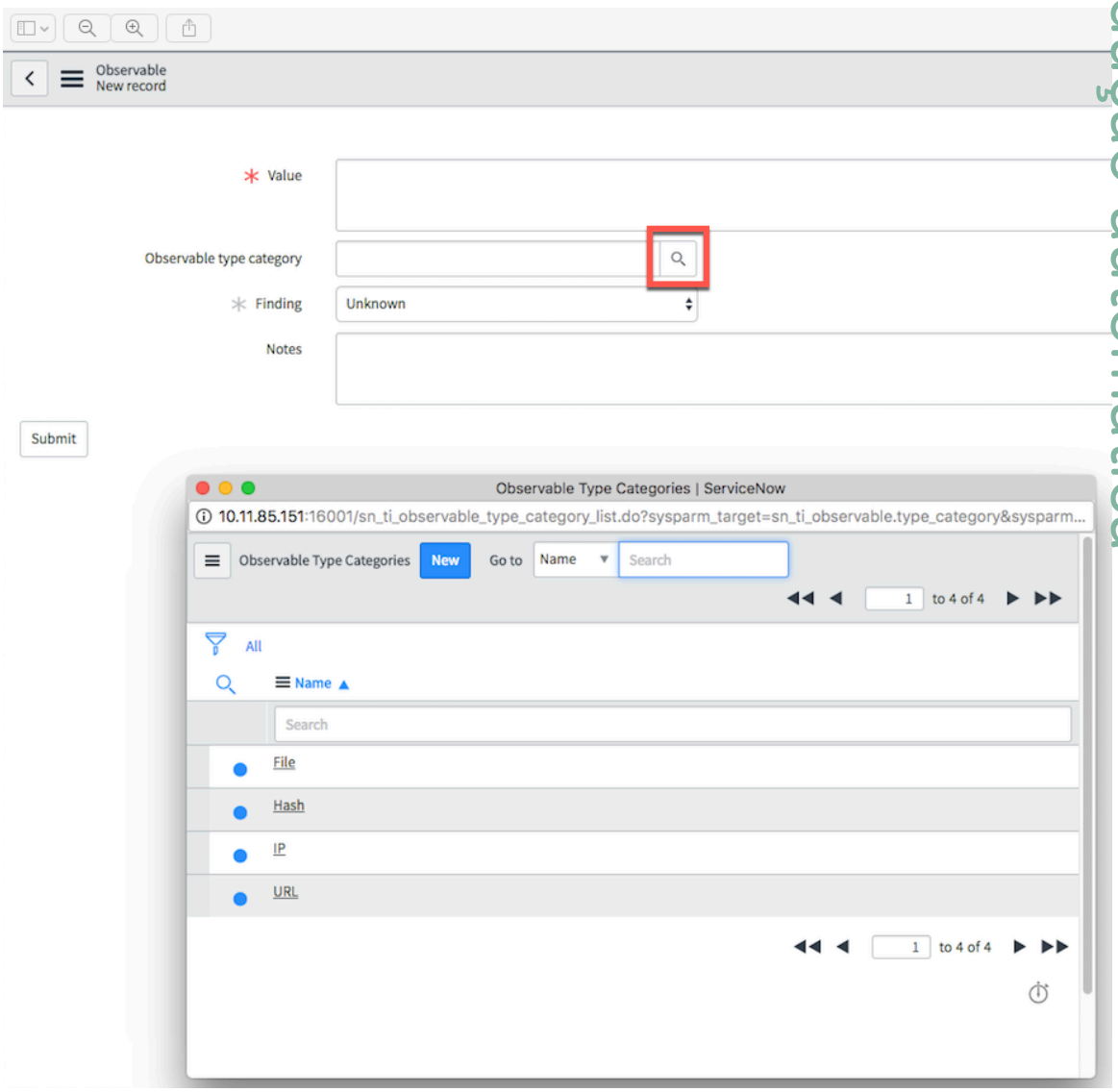
1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar Todos os Incidentes** e abra um incidente de segurança ao qual você deseja anexar o observável.
2. Na parte inferior do registro, clique no link **Mostrar IoC**em **Links relacionados**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Na guia **Observáveis**, clique em **Novo**.
   O formulário Observável é exibido.
4. No campo **Valor**, insira um observável (endereço IP, hash de arquivo ou URL).
5. Clique no ícone de pesquisa e, na caixa de diálogo **Categorias de tipo de observável**, clique no tipo de observável desejado na lista para preencher o campo.

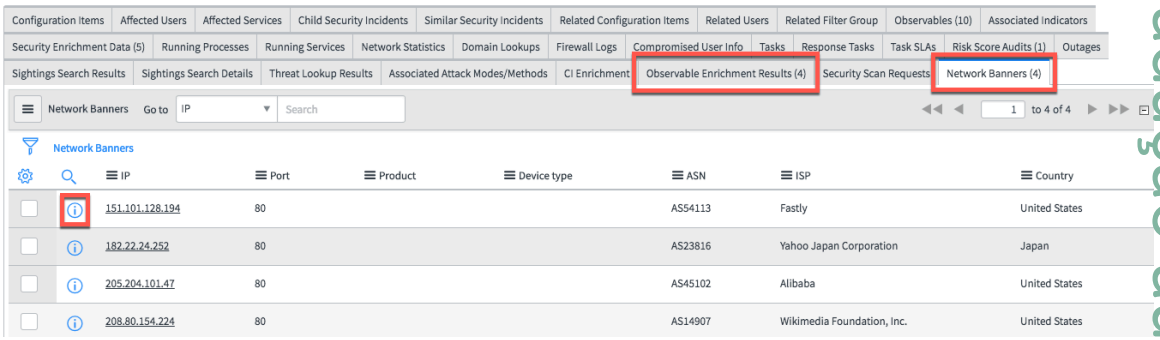


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Enviar**.
   O fluxo de trabalho é iniciado e verifica o novo observável. O status de execução e conclusão é exibido na seção de anotações de trabalho no registro do incidente de segurança.
7. Navegue até o seu incidente de segurança e revise as anotações de trabalho.

8. Na parte inferior do registro, clique no link relacionado **Mostrar todas as listas** relacionadas.
9. Clique nas guias **Resultados de aprimoramento do observável** ou **Faixas de rede** para obter os resultados e clique no ícone de informações azul ao lado de um observável para obter mais informações sobre um item específico.



10. Na caixa de diálogo exibida, clique em **Abrir registro** para exibir os dados brutos e mais detalhes.
11. **Opcional:** Clique no ícone de configurações azul próximo ao ícone de pesquisa para personalizar a saída e a ordem da coluna.
12. Em **Personalizar colunas da lista**, selecione as configurações disponíveis, mova-as para a coluna **Selecionado** e clique em **OK**.

Trouble?
Revise as **anotações de trabalho** para obter mais informações e como prosseguir se você não puder verificar se a pesquisa foi executada com sucesso.

Secureworks CTP Integração de ingestão de tíquete

A integração de ingestão de tíquete Secureworks Counter Threat Platform permite que você busque automaticamente Secureworks CTP tíquetes, converta-os em incidentes de segurança e execute ações de resposta automatizadas.

Os principais recursos desta integração incluem:

- Ingestão automática de tíquetes selecionados (incluindo anexos) com base em uma programação predefinida.
- Mapeamento de campos de tíquete e evento para campos Security Incident Response.
- Visualização de incidentes de segurança mapeados para os campos de tíquete.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Filtragem e agregação de tíquetes.
- Recuperação sob demanda de eventos associados a um tíquete.
- Acompanhamento periódico das principais atualizações dos tíquetes.
- Automatizando atualizações e fechamentos de tíquete com base no status do incidente SIR
- Atualização de tíquete mestre.
- Sincronização de logs de trabalho do Secureworks com Security Incident Response anotações de trabalho.

Configure sua instância [Now Platform para a integração de ingestão de tíquete Secureworks CTP

A seção a seguir lista as tarefas de configuração que você deve concluir em sua instância Now Platform antes de instalar a aplicação do ServiceNow Store.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração sem problemas.

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform e Security Incident Response.	As funções a seguir são necessárias para a instalação, configuração e uso da integração na sua instância Now Platform. • Um usuário com a função de administrador Now Platform (admin) instala a aplicação a partir do ServiceNow Store e atribui a função de administrador SIR (sn_si.admin). • Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no Now Platform: ◦ Nomeia, cria e edita perfis. ◦ Seleciona e mapeia campos de tíquete Secureworks CTP para os campos de incidente de segurança. ◦ Visualiza os detalhes do incidente de segurança para precisão antes de finalizar a configuração. ◦ Programa a ingestão de tíquetes em andamento. ◦ Habilita atualizações de tíquete quando um incidente SIR SIR é criado e encerrado. ◦ Atribui a função de analista de incidente de segurança (sn_si.analyst). ◦ Usuários com o sn_si.analyst trabalham com incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de tarefa	Descrição
	Para obter mais informações sobre funções e atribuição de funções a usuários, consulte Managing roles
Verifique se você está usando as seguintes versões: • API de tíquete do Secureworks 4.0 • API de evento do Secureworks 1.0 • API de aprimoramento do Secureworks 1.0	Se você tiver acesso ao portal Secureworks CTP, terá acesso à API necessária para esta integração. Não há nenhuma outra configuração especial necessária para a API.
Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas antes de instalar a aplicação para a integração.	Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas. 1. Security Incident Response 2. Ingestão de evento e alerta para Security Operations (necessário para integrações de SIEM): este aplicativo requer: ◦ com.glide.hub.integration.runtime => ServiceNow IntegrationHub Runtime ◦ com.glide.hub.action_step.rest => Etapa de ação do ServiceNow IntegrationHub - REST **Nota:** Os componentes do Integration Hub são instalados junto com o plug-in Event and Alert Ingestion. Se eles não estiverem instalados, entre em contato com o Suporte ao cliente para obter assistência. Para obter mais informações sobre como instalar as aplicações principais Security Operations, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

Instalar e configurar a aplicação ServiceNow para a integração de ingestão de tíquete do Secureworks CTP

Antes de executar a integração na sua instância Now Platform, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente aos produtos Security Incident Response e Security Operations na sua instância Now Platform.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se você não instalou a aplicação de tíquete [Secureworks CTP de ServiceNow Store para a integração, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.
2. Depois de instalar a aplicação com êxito, navegue até **Integrações** > **Configurações de integrações** e localize o bloco Secureworks CTP Integração de ingestão de tíquete.

3. Para configurar a aplicação, clique em **Novo**.
4. Como alternativa, se um botão **Configurar** for exibido em um bloco, clique nele para editar uma configuração existente.
5. Na caixa de diálogo exibida, preencha os campos.
6. Clique em **Enviar**.
   Depois de validada e enviada com sucesso, cada configuração é salva na página Integrações de segurança como um bloco.

Resultado

Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança. No canto superior direito da página, na lista de seleção **Mostrar configurações**, clique em **Sim**.

Criar um perfil para integração de ingestão de tíquete do Secureworks CTP

Crie um perfil em sua instância Now Platform e determine quais tíquetes precisam ser ingeridos e quais serão usados para criar incidentes de segurança. Antes que os incidentes de segurança sejam criados a partir de tíquetes ingeridos, os valores de campo dos tíquetes são exibidos em um layout de um incidente de segurança Now Platform para que você possa visualizar como o incidente de segurança real será exibido.

A integração permite ingerir tíquetes com base nos perfis configurados no ambiente Security Operations da sua instância. Todos os tíquetes são ingeridos inicialmente para um tipo de tíquete configurado em um perfil. Os tíquetes ingeridos podem ser filtrados para especificar quais tíquetes criam incidentes de segurança.

Por exemplo, você pode preferir filtros que criam incidentes de segurança somente para tíquetes identificados como de alto risco. Antes de um perfil ser ativado e criar incidentes de segurança a partir de tíquetes ingeridos, os valores de campo individuais nos tíquetes

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

são mapeados para campos correspondentes em um layout de incidente de segurança para uma visualização.

Identificar a origem do perfil

Especifique o nome e a origem do perfil.

Antes de Iniciar

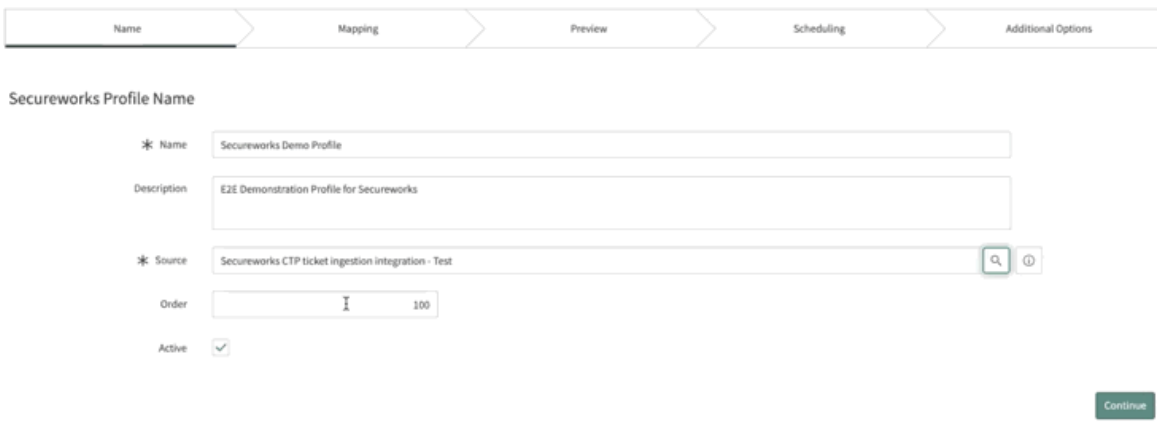
Função necessária: sn_si.admin

Procedimento

1. Para criar um perfil para um tíquete na sua instância Now Platform, navegue até **Integração de ingestão de tíquete do Secureworks** > **Perfis do Secureworks**.
2. Clique em **Nova**.
3. Preencha os campos.

   Um exemplo de formulário preenchido segue a tabela.

   A figura a seguir é um exemplo de um formulário preenchido.



O que Fazer Depois

Mapeie os campos de tíquete.

Mapeamento de campos de tíquete para a integração do SecureWorks CTP

Mapeie os campos de tíquete e evento para os campos no formulário de incidente de segurança.

Para a etapa de mapeamento, você deve primeiro ingerir tíquetes de amostra e, em seguida, garantir que todos os campos de tíquete relevantes estejam mapeados para o local apropriado no formulário Security Incident Response e, em seguida, visualizar o incidente de segurança na seção de visualização.

O mapeamento dos campos de tíquete de amostra envolve o seguinte:

- Buscando e preenchendo os dados de amostra: consulte Ingestão de tíquetes de amostra do Secureworks
- Mapeamento dos campos de tíquete para o incidente de segurança: consulte Mapeamento de campos de tíquete do Secureworks para campos de resposta a incidentes de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ingestão de tíquetes de amostra do Secureworks

Selecione os tíquetes de amostra que serão ingeridos.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Você pode extrair os cinco tíquetes de amostra mais recentes ou fornecer os IDs de tíquete exclusivos dos tíquetes específicos que deseja usar para sua experiência de mapeamento.
   Na lista de seleção **Preferência de ingestão**, selecione uma das seguintes opções:
   - Recuperar tíquetes mais recentes: os 5 tíquetes mais recentes são recuperados.
   - Selecionar tíquetes com base no ID do tíquete: especifique o ID do tíquete a ser recuperado. Você pode especificar no máximo 5 IDs de tíquete separados por vírgulas.
3. Clique em **Buscar dados de amostra** para extrair os dados de tíquete de amostra mais recentes do servidor Secureworks CTP.
   A extração de tíquetes de amostra pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela. Os tíquetes recuperados são exibidos como guias individuais. Clique em uma guia para exibir os dados do tíquete. Para cada tíquete, você pode ver os campos de tíquete e seus valores, além dos detalhes do evento de contribuição que acionou o tíquete.

Nota:
Você verá os detalhes dos eventos de contribuição somente se eles tiverem ocorrido nos últimos 7 dias. Eventos com mais de 7 dias não são exibidos.

O que Fazer Depois
Depois de buscar os dados de amostra, a próxima etapa é mapear os campos de tíquete para o incidente de segurança.

Mapeamento de campos de tíquete do Secureworks para campos de resposta a incidentes de segurança

Mapeie campos de tíquete individual ou evento para campos em um incidente de segurança Now Platform SIR.

Mapeamento de campo de tíquete

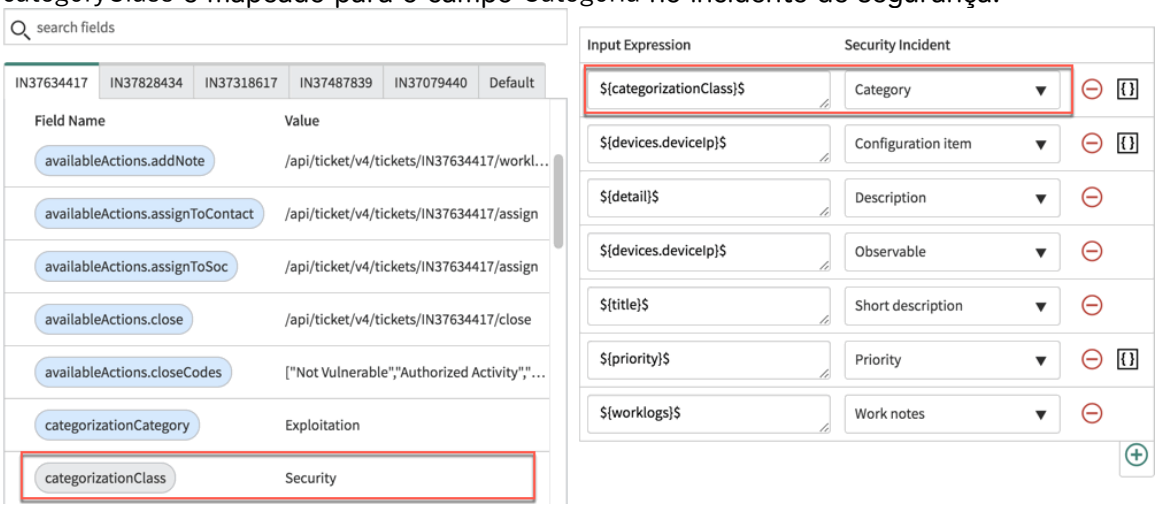
Como um usuário com a função sn_si.admin, use os campos da seção de tíquetes de exemplo à esquerda e mapeie-os para os campos de incidente de segurança na coluna **Mapeamento de campo de incidente SIR**. Edite a configuração de mapeamento arrastando os campos de tíquete ou evento do lado esquerdo e soltando-os na seção Mapeamento de campo de incidente SIR à direita. O mapeamento à direita associa o campo de tíquete de entrada a um campo de incidente de segurança de saída.

1. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e mantenha pressionado um nome de campo azul no lado esquerdo do formulário.
2. Você pode inserir manualmente o nome do campo na coluna Expressão de entrada ou arrastar e soltar o nome do campo. Por exemplo, descriçãoe solte-o em um campo na coluna **Expressão de entrada** ao lado de um nome de campo na coluna **Incidente de segurança**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, categoryClass é mapeado para o campo Categoria no incidente de segurança.



Nota:
Se você inserir o nome do campo de evento manualmente na seção **Expressão de entrada**, deverá adicionar um prefixo como *`${Event:eventfield}$`* antes do nome do campo que está sendo mapeado.

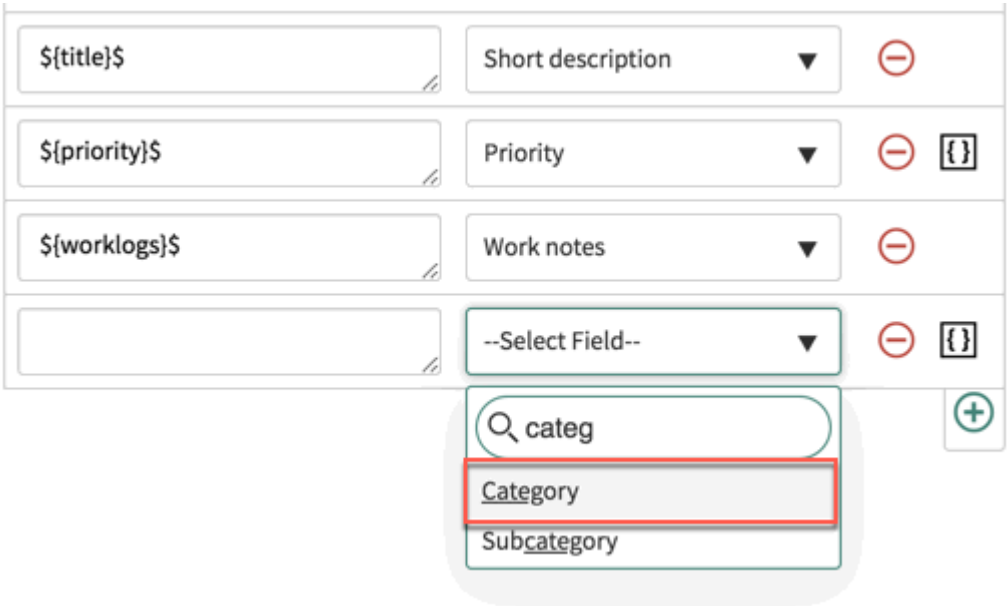
Para ajudar a garantir que nenhum campo de tíquete ou evento seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. A codificação por cores dos campos de tíquete ajuda a rastrear os valores de tíquete que você já mapeou, conforme eles se tornam esmaecidos, enquanto todos os campos não mapeados restantes aparecem em azul. Isso ajuda a visualizar melhor quais valores de campo foram adicionados ao incidente de segurança e se alguma informação importante de tíquete restante permanece não mapeada.

Os campos azul claro à esquerda indicam que um campo de tíquete ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um tíquete de entrada ou campo de evento a mais de um campo em um incidente de segurança. Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação de cores ajuda a rastrear o mapeamento.

3. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas:
   a. À direita do formulário na seção SIR Mapeamento de campo de incidente, na parte inferior da grade, clique no ícone de adição (+). Um novo campo é exibido.
   b. Na coluna Incidente de segurança, expanda a lista de seleção exibida e selecione um campo.

      Na lista de seleção expandida para o novo campo, alguns campos estão sombreados. Na figura a seguir, Categoria tem um plano de fundo cinza porque foi mapeada no incidente de segurança. Semelhante à codificação de cores dos campos de tíquete no lado esquerdo do formulário, essa codificação de cores para os campos de incidente de segurança à direita ajuda a rastrear os campos de incidente SIR já mapeados.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:
Como vários observáveis podem ser exibidos no mesmo incidente de segurança, o campo Observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho oferecem suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, será exibida uma mensagem de erro informando que não há nenhum valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista de seleção na qual você pode escolher várias opções e você tentar mapear uma opção para esse campo que não é exibido na lista de seleção, o campo não será preenchido no incidente de segurança.

c. Como alternativa, digite um valor no campo Pesquisar da nova linha.

d. No lado esquerdo do formulário, selecione o campo de tíquete e arraste e solte-o em um campo de incidente de segurança apropriado à direita.

4. Remova campos usando o ícone - ao lado do nome do campo na seção Mapeamento de campo de incidente de SIR.

5. Continue mapeando adicionando ou removendo valores de campo para o mapeamento.

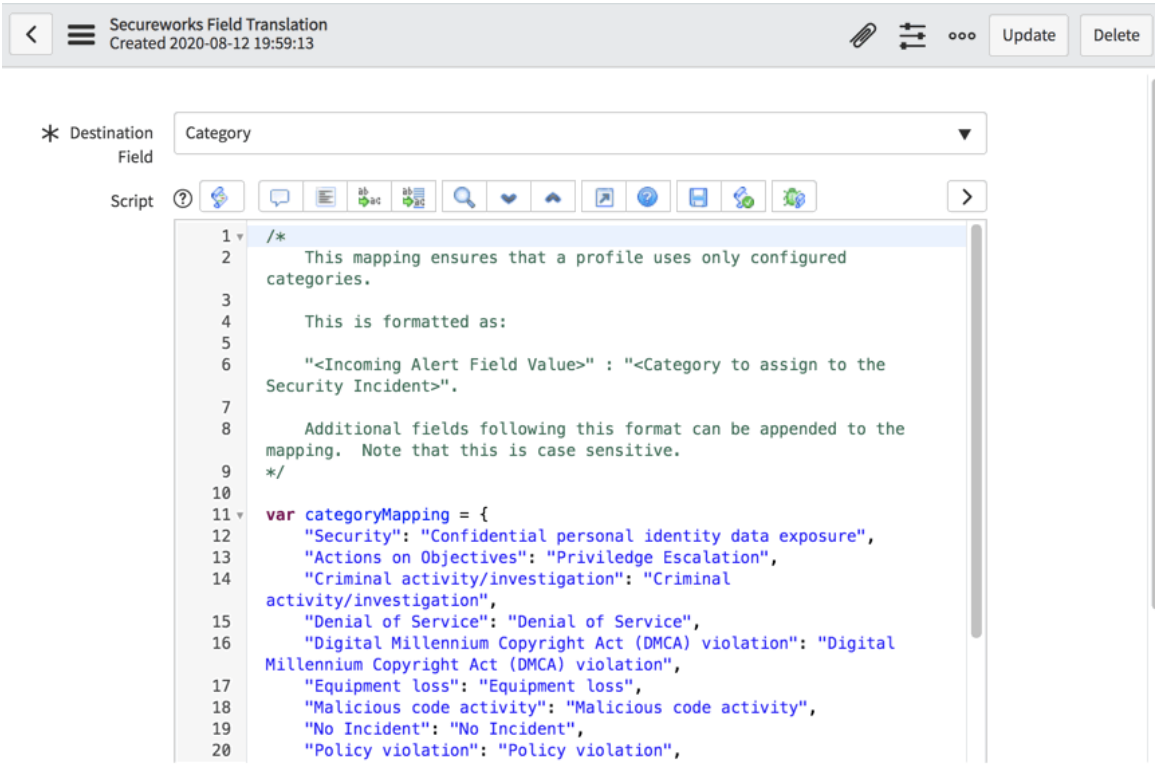
Formatar tradução de campo

Em determinados casos, os campos de tíquete podem não ser traduzidos diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de script se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de script, um valor de categoria de Alerta de malware e Infecção de vírus pode ter valores de campo diferentes para a categoria de origem, mas ambos os valores podem ser convertidos em uma Atividade de código malicioso comum no campo Categoria no incidente de segurança SIR usando o Funcionalidade de tradução de campo de formato.

Para usar o editor de script, clique no ícone {} ao lado do campo Categoria. O editor de script é exibido

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



.

Insira as mudanças no script e clique em **Atualizar** para salvar as mudanças e retornar à página Mapeamento.

Condições de geração de incidentes

Depois que a seção de mapeamento estiver concluída, você poderá definir condições de filtro para especificar quais tíquetes devem criar incidentes de segurança e quais devem ser filtrados, por exemplo, tíquetes de prioridade baixa. Você pode usar os mesmos valores de campo no construtor Condições de geração de incidentes para definir critérios adicionais que um tíquete de entrada deve satisfazer para criar um incidente de segurança. Para definir condições de geração de incidentes, siga estas etapas.

1. Role até a seção **Condições de geração de incidente** no formulário e marque a caixa de seleção **Filtrar com base nas condições** para habilitar a opção.

   O construtor de Condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

   As opções nas listas de seleção para o primeiro campo no construtor de Condições de filtro correspondem aos campos exibidos na seção **Exemplo de ingestão de tíquete** para os tíquetes ingeridos. Esses campos são dinâmicos e mudam de acordo com os tíquetes que você ingere. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas e devem corresponder exatamente aos valores do tíquete Secureworks CTP. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao console Secureworks CTP e revisar seus tíquetes para as palavras-chave.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Os campos de *logs*de trabalho , *dispositivos*, *anexos*, *observadores*, *availableactions*e tíquete *closeCodes* podem ter vários valores (já que os valores são armazenados em matrizes). Como a condição do filtro pode recuperar somente cadeias de caracteres, você deve usar a condição do filtro " *contém* " para esses campos para garantir que os dados sejam filtrados corretamente.

2. Usando as listas de seleção e os campos do construtor de condições, defina filtros para a primeira linha.
3. Para adicionar mais condições, à direita dos campos, clique em **E** ou **OU**.
   - Se **AND** for selecionado, todas as condições deverão ser correspondidas.
   - Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida.
4. (Opcional) Na segunda linha, defina uma segunda condição de filtro.

   Esse tipo de filtragem de condição de geração de incidente ajuda a restringir os tíquetes e limita o número de incidentes de segurança desnecessários que você cria sem modificar a regra ou os filtros subjacentes. Se critérios de filtragem adicionais forem definidos, somente os tíquetes que corresponderem a todos os critérios serão mapeados para incidentes de segurança.

Critérios de agregação de tíquete para lidar com tíquetes semelhantes e evitar incidentes duplicados

Defina critérios de agregação de tíquete adicionais que agregam um tíquete de entrada a um incidente de segurança SIR existente em vez de criar incidentes semelhantes, potencialmente duplicados. Usando critérios de valor de correspondência de campo para cada perfil, essa capacidade de agregação adicional pode reduzir o número de incidentes de segurança ativos e sobrepostos, colocando todos os dados de tíquete relacionados em um único incidente de segurança. Para definir os critérios, siga estas etapas abaixo:

1. Role até a seção **Critérios de agregação de tíquete** no formulário e marque a caixa de seleção **Condições de agregação** para habilitar essa opção.

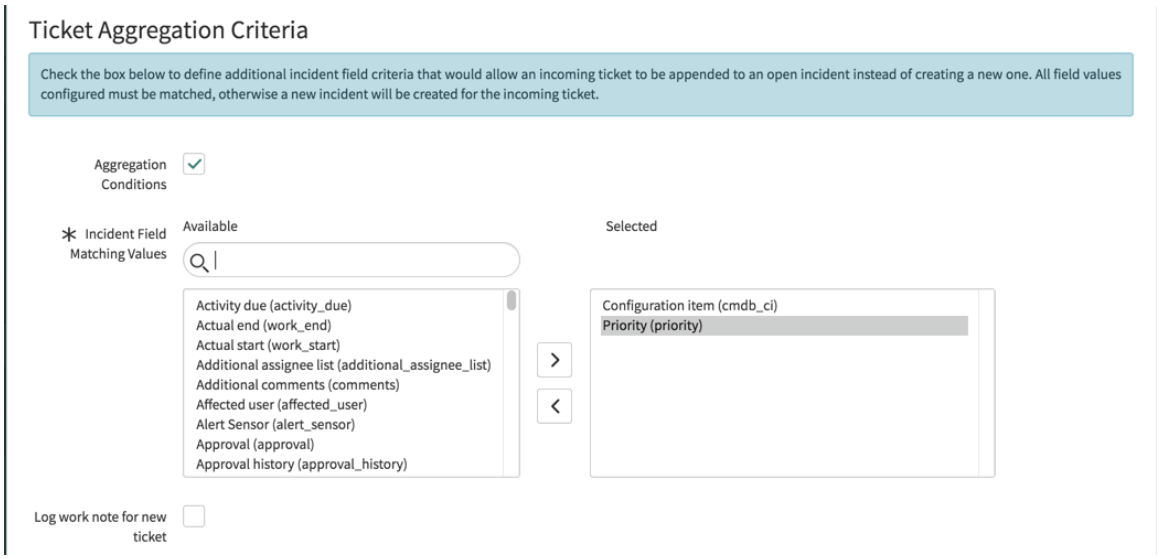
   As colunas Valores correspondentes do campo de incidente são exibidas. Esses nomes de campo são os campos no incidente de segurança que incluem todos os campos personalizados que estão configurados no incidente de segurança SIR.

2. Na lista Disponível, selecione os valores de campo que você deseja corresponder aos incidentes de segurança existentes na sua NOW Platform e mova-os para a lista Selecionado.

   Todos os valores de campo selecionados devem ser correspondidos para anexar este tíquete de entrada a um incidente de segurança existente. Isso inclui campos, como observáveis e itens de configuração, que podem ter vários valores de campo de tíquete mapeados para eles. Todos os valores devem corresponder. Se apenas um subconjunto dos valores for correspondido, as condições de agregação de tíquete não serão atendidas e um novo incidente de segurança será criado. Veja a captura de tela abaixo para mapeamento de campo de vários valores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se um novo tíquete corresponder a todos os valores selecionados nas condições de campo de agregação na etapa de mapeamento, o novo tíquete será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os tíquetes agregados adicionados em uma lista relacionada em um incidente de segurança. Esta lista detalha os carimbos de data/hora associados e os valores de campos agregados. Essas informações ajudam a entender por que esses tíquetes estão sendo agregados a incidentes de segurança existentes. Se esta guia não for exibida em um incidente de segurança, role até o lado esquerdo do registro em **Links relacionados** e clique no link **Mostrar todas as listas** relacionadas.

Nota:
A lista relacionada de tíquetes agregados do Secureworks não está disponível com o sistema de base. Você deve configurar o layout da Lista relacionada e incluí-lo explicitamente com as outras listas relacionadas.

3. (Opcional) Para registrar uma anotação de trabalho para um novo tíquete que foi adicionado recentemente ao incidente de segurança, marque a caixa de seleção para habilitar esta opção. A anotação de trabalho registra que um novo tíquete foi adicionado junto com um link para os detalhes do tíquete e quaisquer outros detalhes que possam ter sido adicionados ao campo de anotação de trabalho na seção de mapeamento.

   Você mapeou com sucesso valores de um tíquete Secureworks CTP para campos em um incidente de segurança. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem de geração de incidentes. Você também anexa tíquetes a incidentes de segurança existentes quando os valores de campos de tíquete correspondem aos critérios de agregação configurados.

4. Clique em **Continuar** para prosseguir com a configuração do perfil. A próxima etapa é visualizar os campos mapeados em um incidente de segurança SIR

Visualizar os valores mapeados no incidente de segurança

Depois de concluir a etapa de mapeamento, visualize os valores que você mapeou em um incidente de segurança SIR. Esta etapa de visualização permite que você verifique se mapeou todos os campos de tíquete que deseja exibir no incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou para preencher dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação. As visualizações de SIR incidentes de segurança não são salvas como incidentes reais no produto Security Incident Response.

Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualizar** na barra de andamento.
   Os tíquetes são exibidos como guias.
2. Clique em uma guia para visualizar o incidente de segurança.
   Esta exibição é somente leitura e um registro deste incidente de segurança não é salvo.
3. Revise o mapeamento de campo dos valores de tíquete no incidente de segurança.

A imagem anterior é um exemplo de uma visualização com um erro de mapeamento das amostras que foram ingeridas.

4. Para resolver esse erro, clique em **Mapeamento** na barra de andamento.
5. Edite o mapeamento para corrigir valores incorretos ou preencha os dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir os erros descritos nas mensagens de erro.

O que Fazer Depois
Se nenhuma mensagem de erro for exibida, e você estiver satisfeito com o mapeamento de campo no incidente de segurança. Defina a programação.

Definir programação para ingestão de tíquete de CTP do Secureworks

Verifique as configurações padrão para recuperação de tíquete ou modifique a programação conforme necessário. Esta etapa permite filtrar a recuperação do tíquete com base em um intervalo de datas e um intervalo de pesquisa.

Antes de Iniciar
Função necessária: sn_si.admin

Tradução automática

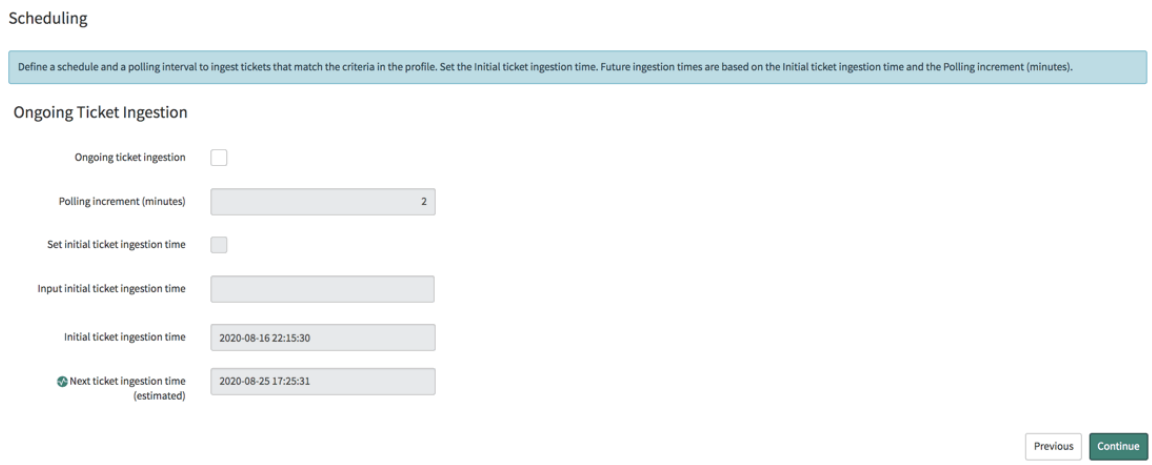
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você também escolhe com que frequência pesquisará tíquetes futuros que correspondam à configuração do perfil de tíquete. Configure esses intervalos de pesquisa por perfil. Ao programar, talvez você prefira equilibrar a carga do sistema em relação à urgência do incidente. Um valor padrão de um minuto é definido para qualquer perfil, mas você pode preferir modificar essa configuração com base na urgência do incidente e na carga antecipada em seu sistema.

Procedimento

1. Se a página Programação na barra de andamento não for exibida, selecione **Programação**.
2. Escolha um para programar como e quando os tíquetes serão obtidos do portal Secureworks CTP.



3. Clique em **Continuar** para navegar até a página Opções adicionais.

Automatizar atualizações e fechamento de tíquetes com base no status do incidente no SIR

A integração de ingestão de tíquete Secureworks CTP tem uma interface bidirecional que permite que ambos os tíquetes criem incidentes de segurança, bem como a capacidade de atualizar os tíquetes depois que o incidente de segurança é criado e/ou encerrado com detalhes relevantes do incidente, como o número do incidente de segurança , grupo de atribuição, URL do incidente de segurança e assim por diante.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais**.
2. Conclua a configuração para atualizar tíquetes quando o incidente de segurança for criado.
3. Clique em **Concluir** para concluir a configuração e mover o perfil para o estado **Aguardando**.
   Uma caixa de diálogo de confirmação é exibida. Você configurou o perfil com sucesso. Ative este perfil para extrair tíquetes do portal Secureworks CTP com base na sua programação.

Opcional: copiar um perfil CTP do Secureworks

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, convém copiar os perfis para economizar tempo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Como um usuário com a função sn_si.admin, se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado está desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

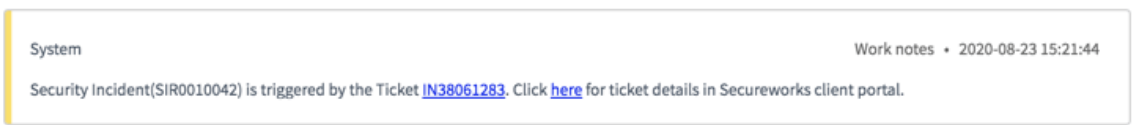
Procedimento
1. Navegar até **Todos** > **Integração de ingestão de tíquete do Secureworks** > **Perfil do Secureworks**.
2. Na lista Perfis do Secureworks exibida, selecione um perfil que você deseja copiar e, na lista de seleção **Ações nas linhas selecionadas**, clique em **Copiar**.
   O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo o mapeamento e a configuração de programação. O nome do perfil contém (cópia). Embora o perfil original esteja habilitado (verdadeiro), a cópia está desabilitada neste ponto (falso). Você pode editar os valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil, conforme necessário.

   Você copiou com sucesso as configurações de um perfil existente para um novo perfil. Observe que o status da coluna **Ativa** está definido como falso, pois o perfil precisa ser ativado.

O que Fazer Depois
Você será solicitado a ativar (habilitar) o novo perfil depois de concluir as etapas de configuração.

O formulário do Security Incident Response muda após a ingestão do tíquete
Depois que um tíquete Secureworks CTP for ingerido, um incidente de segurança será criado e as atualizações correspondentes serão feitas no registro do incidente de segurança.

Anotações de trabalho
Uma anotação de trabalho é publicada com detalhes do tíquete que acionou o incidente de segurança.



Clique no link do tíquete para navegar até o registro interno do tíquete do Secureworks para a tarefa. O hiperlink **Clique aqui** leva você para o painel Secureworks CTP, onde é possível exibir os detalhes do tíquete.

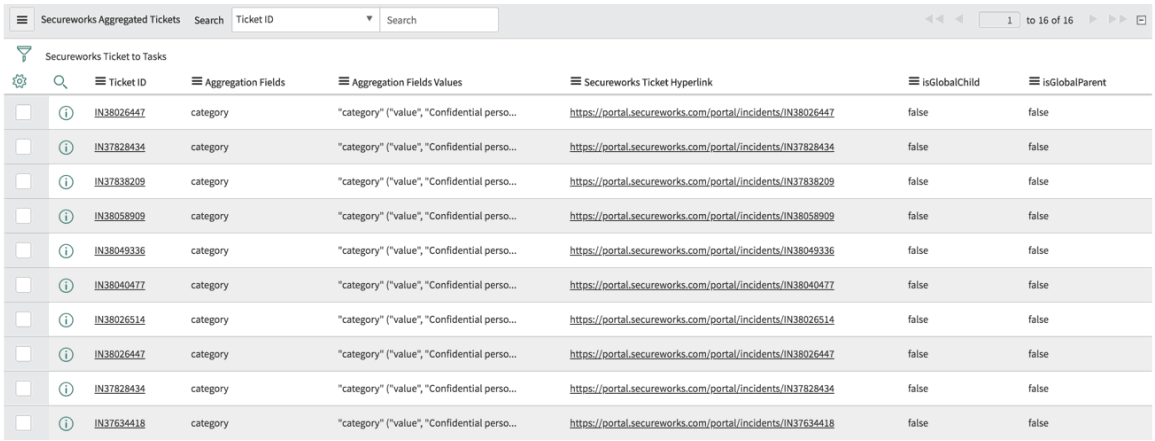
Se você tiver selecionado a opção **Registrar anotação de trabalho para novo tíquete** nos Critérios de agregação de tíquete, conforme descrito na página Criar perfil: mapeamento, uma anotação de trabalho será publicada quando o tíquete for agregado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tíquetes agregados

Clicar **Listas relacionadas** > **Tíquetes agregados do Secureworks** para exibir o tíquete agregado ao incidente de segurança. Clique no hiperlink do tíquete para exibir o tíquete no painel Secureworks CTP.

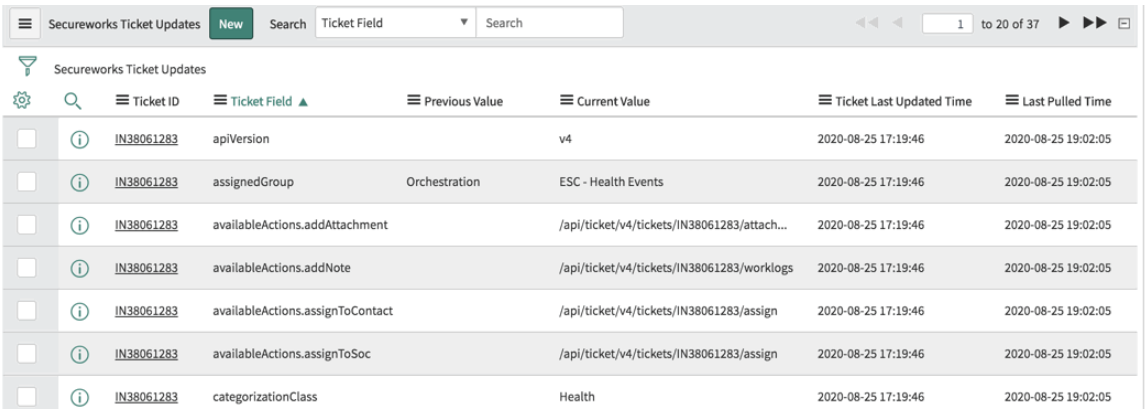


Criar incidente de segurança: selecione um tíquete na lista, clique no menu **Ações** e clique em **Criar incidente de segurança**. Esta opção cria um novo incidente de segurança para o tíquete e este tíquete é desagregado do incidente de segurança primário.

Excluir registro de tíquete: selecione um tíquete na lista, clique no menu **Ações** e clique em **Excluir**. Esta opção exclui o registro do tíquete.

Atualizações de tíquete do Secureworks

Isso mostra os campos de tíquete padrão e rastreia as mudanças nos tíquetes durante cada intervalo de pesquisa. Isso é útil, pois você pode exibir todas as atualizações de tíquete diretamente sem navegar até o painel Secureworks CTP. Todas as mudanças nos valores são exibidas nos campos Valor anterior e Valor atual.

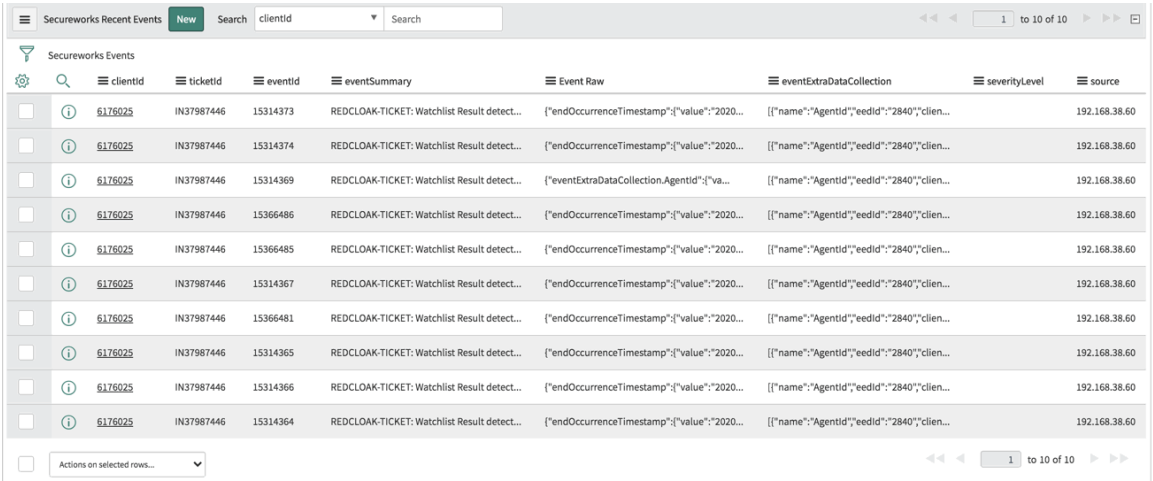


Eventos recentes do Secureworks

Clique na opção **Buscar eventos do Secureworks recentes** nos **Links relacionados** para exibir os eventos do Secureworks mais recentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Por padrão, um número máximo de 50 eventos será exibido. Você pode modificar esta configuração padrão nas Configurações de integração do Secureworks.

Exibir os tíquetes do Secureworks e os incidentes de segurança correspondentes

Os tíquetes Secureworks CTP importados são armazenados inicialmente na tabela Importação de tíquete. Exiba todos os Secureworks CTP tíquetes que foram importados antes que qualquer condição de filtro seja aplicada.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Integração de ingestão de tíquete do Secureworks** > **Importação segura de tíquete**.
2. Você pode exibir todos os Secureworks CTP tíquetes que foram importados antes de serem agregados ou de qualquer condição de filtro ser aplicada.
3. Clique em um ID de tíquete para ver os dados brutos do tíquete.
4. Navegar até **Ingestão de tíquete do Secureworks** > **Tíquetes do Secureworks para a tarefa**.
   Os Secureworks CTP tíquetes com seus incidentes de segurança correspondentes são exibidos.

Aviso de fechamento do tíquete principal do CTP do Secureworks

Antes de fechar um incidente de segurança criado por um tíquete principal Secureworks CTP, você deve verificar se todos os tíquetes secundários associados ao tíquete principal estão fechados.

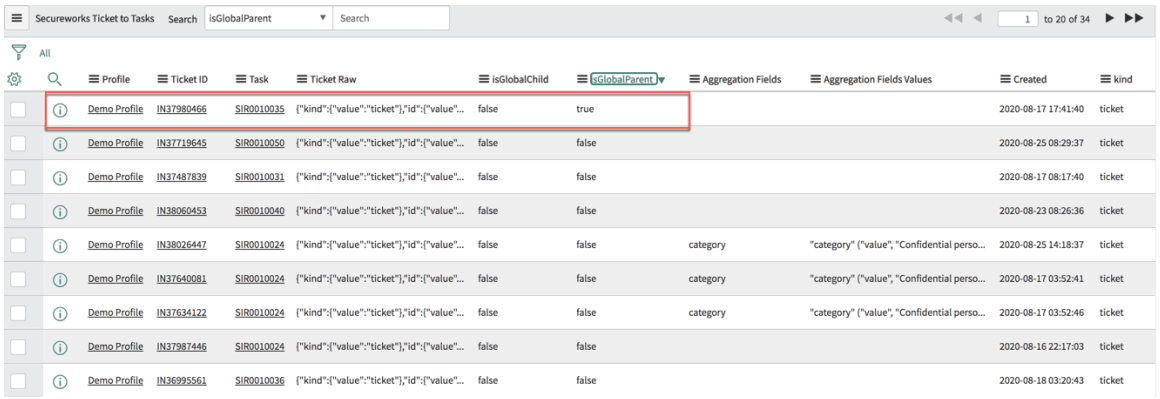
Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Ingestão de tíquete do Secureworks** > **Tíquetes do Secureworks para a tarefa**.
   Os Secureworks CTP tíquetes com seus incidentes de segurança correspondentes são exibidos.

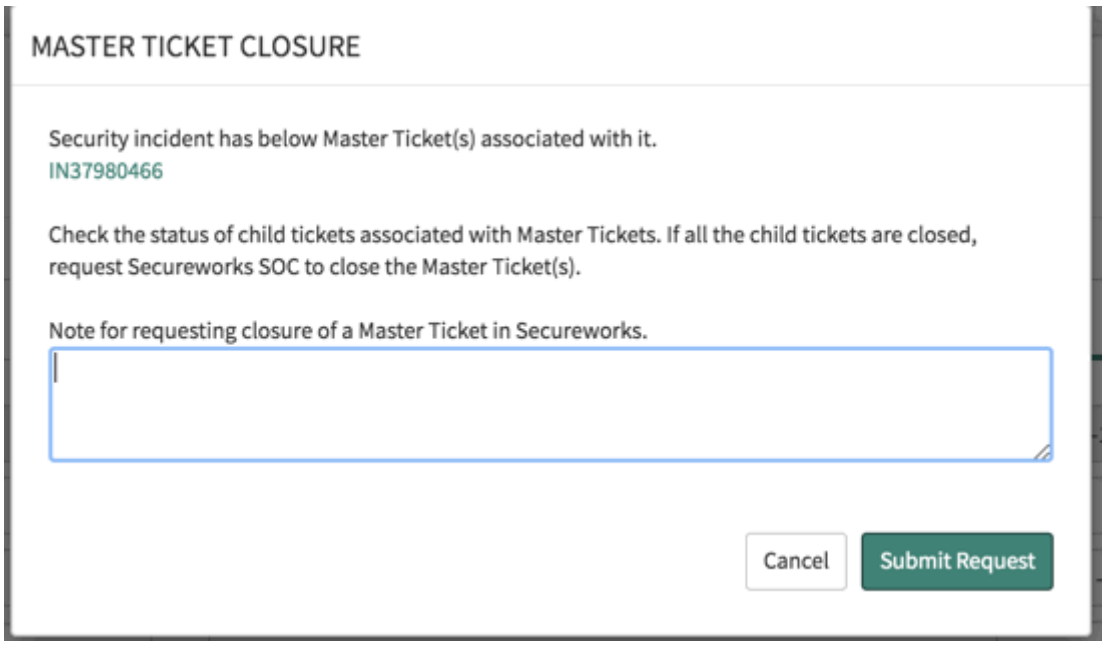
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Clique no incidente de segurança com o campo **isGlobalParent** definido como **verdadeiro.**

3. Altere o Estado do incidente de segurança para **Encerrado**, especifique os códigos de encerramento e clique em **Salvar**.
   A caixa de diálogo a seguir é exibida.



Este incidente de segurança está associado a um tíquete principal do Secureworks. Um tíquete principal pode ter um ou mais tíquetes secundários associados a ele. Antes que o tíquete mestre possa ser fechado, você deve primeiro verificar se todos os tíquetes secundários associados a este tíquete mestre foram fechados.

4. Adicione uma nota solicitando o fechamento do tíquete principal no Secureworks e clique em **Enviar solicitação**.
   O tíquete mestre agora foi reatribuído à equipe SOC do Secureworks.

5. Depois que a solicitação for enviada, você poderá fechar o incidente de segurança.

6. Navegar até **Aplicação** > **Módulo**.

Definições de configuração de integração do Secureworks CTP

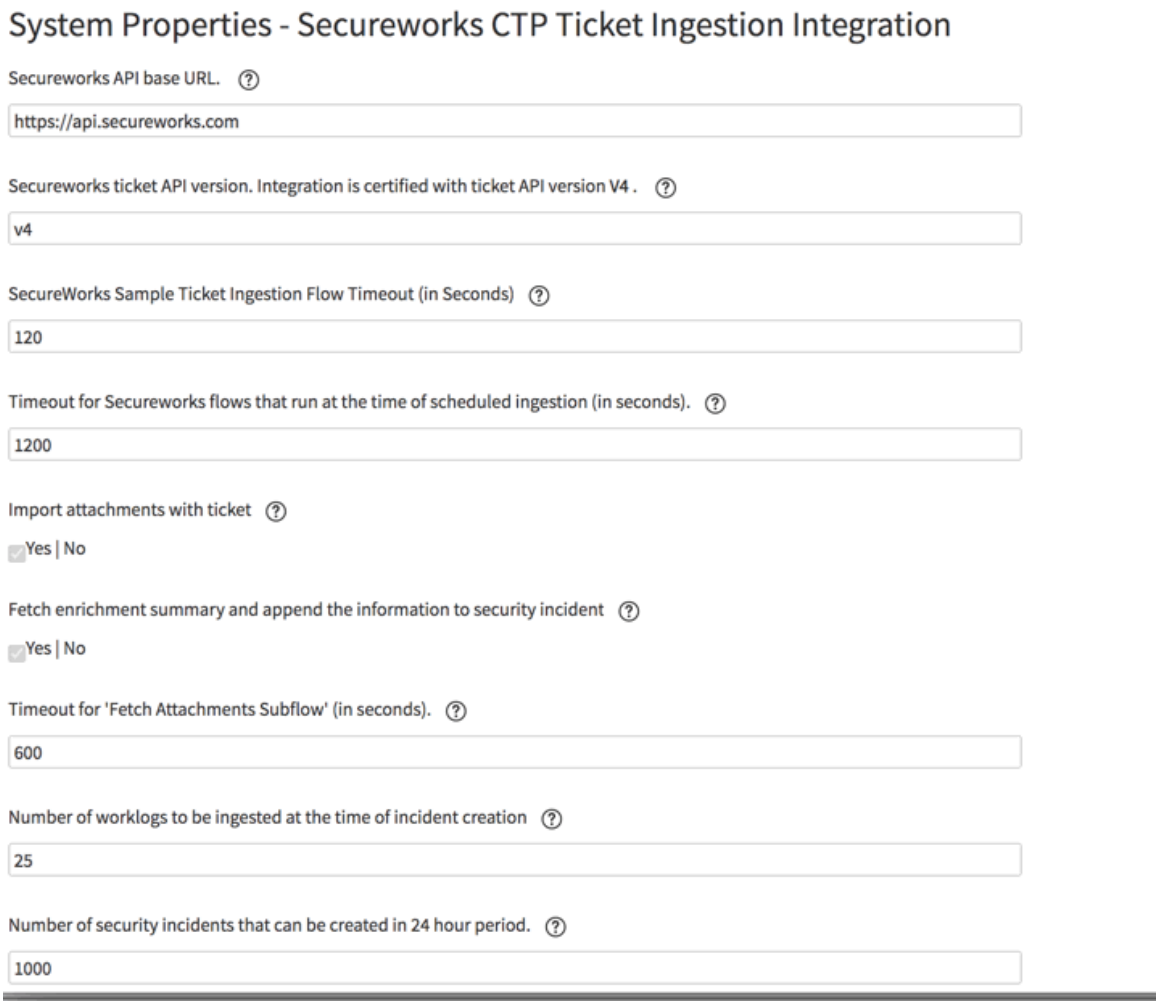
Use esta opção para modificar as propriedades do sistema padrão de integração de ingestão de tíquete Secureworks CTP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para modificar as propriedades do sistema, faça login como um usuário com a função *sn_si.admin* e navegue até **Integração de ingestão de tíquete do Secureworks** > **Configurações de integração do Secureworks**.

As definições de configuração padrão são exibidas. Você pode modificar essas configurações, se necessário.



Todas as configurações de integração modificadas serão aplicadas durante o próximo intervalo de pesquisa, conforme definido no perfil.

Integração do Security Incident Response com Zscaler

Você pode usar o produto Integração do Security Incident Response com Zscaler para conectar os logs do servidor Zscaler Internet Access (ZIA) com o Now Platform. Esta integração permite que você exiba painéis, crie alertas personalizados e ajude a investigar incidentes de segurança.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral

O Zscaler produto de gateway de internet e web é entregue a partir da nuvem. Ele fornece os principais pontos de dados e informações sobre seu ambiente de segurança empresarial.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração do Security Incident Response com Zscaler conecta o produto Zscaler Internet Access à sua instância Now Platform. Ao usar o produto Zscaler no Now Platform, você obtém mais informações sobre o uso da internet pela sua organização.

Principais recursos da integração

Esta integração inclui os seguintes recursos principais:

- Pesquisa de reputação de observáveis em relação à biblioteca de ameaças global que o produto Zscaler mantém.

  Nota:
  A biblioteca de ameaças globais Zscaler lista as ameaças por tendências, país de origem, destino, volume e várias categorias de ameaça. Esta biblioteca de ameaças global permite que você investigue seus observáveis em relação ao cenário de ameaça global.

- Manutenção de observáveis em uma lista de bloqueios ou lista de permissões no produto Zscaler.
- Capacidade de buscar e revisar relatórios de área restrita do produto Zscaler para um hash MD5. O recurso Cloud Sandbox no produto Zscaler é executado e analisa os arquivos em um ambiente virtual para detectar comportamento mal-intencionado.
- Alertas de segurança de eventos de paciente 0 que são gerados no produto Zscaler quando um usuário faz download de um arquivo mal-intencionado desconhecido.
- Várias listas de categorias de URL que atuam como listas de bloqueio ou listas de permissões, conforme definido no produto Zscaler.
- Now Platform incidentes de segurança que podem ser marcados para identificar a categoria de URL à qual os observáveis são adicionados.
- Períodos de expiração que mantêm o tamanho das entradas da lista de categorias de URL expirando ou removendo automaticamente as entradas mais antigas.
- Fluxo de trabalho de aprovação para adicionar e remover observáveis das listas de categorias de URL.
- Entradas de categoria de URL que podem ser vinculadas a registros observáveis e incidentes de segurança que incluem resultados de inteligência contra ameaças e detalhes sobre o motivo pelo qual uma entrada está bloqueada.

Conheça esta integração

Identificador de documento	Título do documento
Zscaler site da documentação do produto	Site de documentação do produto ZScaler
ServiceNow site da documentação do produto	Site de documentação do produto da ServiceNow

Comece com Integração do Security Incident Response com Zscaler

Ative e configure o produto Zscaler Internet Access para interagir com sua instância [Now Platform e produto Security Incident Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição

Atribua e verifique as funções Now Platform e Security Incident Response.	Essas funções são necessárias para configuração e verificação dos resultados esperados:
	• A função de administrador instala a integração do ServiceNow Store e atribui a função sn_si.admin.
	• A função sn_si.admin executa as seguintes tarefas:
	  ○ Configura a integração.
	  ○ Cria, ativa e remove as listas de categorias de URL.
	  ○ Atribui a função sn_si.analyst.
	• A função sn_si.analyst cria entradas e trabalha com incidentes de segurança.

Verifique se as aplicações principais ServiceNow estão instaladas e ativadas antes de configurar esta integração.	O plug-in ServiceNow IntegrationHub Enterprise Pack Installer [com.glide.hub.integrations.enterprise] é necessário. O plug-in Security Incident Response (com.snc.security_incident) é necessário. Este plug-in instala automaticamente todas as dependências do produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras aplicações Security Operations para a integração. Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se essas aplicações ainda não estiverem instaladas, instale e ative cada aplicação uma de cada vez na seguinte ordem: **1.** Security Incident Response Dependência (com.snc.si_dep) **2.** Security Integration Framework **3.** Security Support Common **4.** Orquestração de suporte de segurança **5.** Inteligência contra ameaças Suporte Comum **6.** Trusted Security Circles

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	7. Security Operations Assistente de configuração 8. Security Incident Response
Verifique as versões Zscaler.	• Esta integração é compatível com a Zscaler Internet Access versão 1.0 ou posterior. • Esta integração foi testada com as seguintes Zscaler versões: ○ Conector de cliente Zscaler para Windows - 3.0 ○ Conector de cliente Zscaler para macOS - 3.0 ○ Conector de cliente Zscaler para Linux - Beta ○ Conector de nuvem Zscaler - 6.1
Verifique se você tem as permissões Zscaler necessárias e configurou acesso ao Zscaler Internet Access APIs.	• Você deve ter as credenciais de administrador para Zscaler Internet Access. • Você deve ter uma assinatura de API de serviço em nuvem válida. Zscaler O suporte deve fornecer sua chave. • Você deve ter Zscaler Internet Access credenciais de administrador (nome de usuário e senha). A autenticação de API é baseada em uma combinação da chave de API e Zscaler Internet Access credenciais de administrador. **Nota:** Para obter mais informações sobre como gerenciar as chaves de API Zscaler Internet Access, consulte a documentação do Zscaler.

Configurar acesso a Zscaler Internet Access APIs

Configure o acesso ao servidor Zscaler Internet Access para autenticar a conexão segura entre a instância Now Platform e o servidor Zscaler.

Antes de Iniciar

Função necessária: administrador do Zscaler Internet Access

Por Que e Quando Desempenhar Esta Tarefa

Depois que Zscaler habilita sua assinatura de API para o serviço em nuvem da sua organização, ela fica disponível na página de gerenciamento de chave de API Zscaler Internet

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Access com o URL base. Sua organização só pode ter uma chave de API ou token. Exclua a chave ou o token existente antes de adicionar um novo.

O URL base da API é ${Cloud_Name}/api/v1. Verifique o nome da nuvem Zscaler que foi provisionado para sua organização e use-o para substituir {Cloud_Name} no URI base. Alguns exemplos do URL base são:

- exemplo.zscalerbeta.net
- exemplo.zscalerone.net
- exemplo.zscalertwo.net
- exemplo.zscaler.net
- exemplo.zscloud.net

Nota:
Para obter mais informações sobre o portal de administração Zscaler Internet Access, consulte a documentação de gerenciamento de chaves da API do Zscaler e a documentação do portal do Zscaler .

Procedimento

1. Faça login como administrador no portal de administração Zscaler Internet Access.
2. Navegar até **Administração** > **Gestão de chaves de API**.
3. Clique **em Adicionar chave de API**.
   Se você não vir a opção **Adicionar chave de API**, exclua a chave existente.
   A nova chave de API é válida imediatamente e é exibida na guia.

Resultado
Você recuperou o URL base e a chave de API para configurar o acesso a Zscaler da instância Now Platform.

Instalar e configurar Integração do Security Incident Response com Zscaler

Instale e configure o produto de acesso à Internet [Integração do Security Incident Response com Zscaler do ServiceNow Store para começar a usar a integração na sua instância Now Platform.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

1. Baixe o produto Integração do Security Incident Response com Zscaler do ServiceNow Store e instale-o.
2. Navegar até **Security Operations** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco Integração do Security Incident Response com Zscaler e clique em **Configurar** > **Criar nova configuração**.
4. No formulário, preencha os campos.

Zscaler Formulário de configuração

Campo	Descrição
Nome do Servidor	Zscaler nome do servidor. Por exemplo, ZSserver.
Ativo	Indicador de que o perfil está ativo.

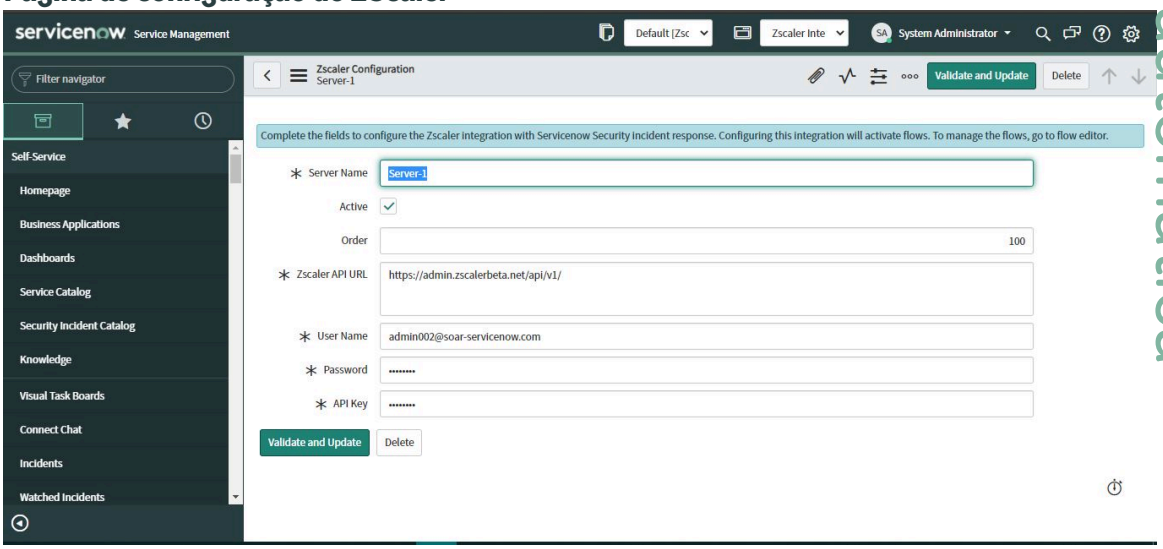
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ordem	Prioridade de fluxo. O valor deste campo indica a ordem dos fluxos de trabalho quando dois ou mais perfis compartilham condições de acionamento. O fluxo com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300, 400. O padrão é 100.
Zscaler URL da API	URL base que hospeda a API Zscaler. Por exemplo, https://example.zscalerbeta.net
Nome de usuário	Nome de usuário da conta de administrador Zscaler Internet Access.
Senha	Senha para a conta de administrador Zscaler Internet Access.
Chave de API	Chave de API que você obteve no portal de administração Zscaler Internet Access.

O exemplo a seguir mostra a página de configuração do Zscaler.

Página de configuração do ZScaler



5. Clique **em Validar e atualizar**.

Resultado
Depois de validar e salvar esta configuração, retorne à página Zscaler Configurações.

Adicionar Zscaler Internet Access listas de categorias de URL

Adicione as categorias de URL que estão disponíveis no produto de acesso à Internet ZscalerNow Platform à instância [] para especificar uma ação para cada URL para que você tenha acesso fácil para filtragem granular e criação de política.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
O Integração do Security Incident Response com Zscaler fornece uma lista de permissões padrão e listas de categoria de URL de lista de proibições para ajudar a filtrar o conteúdo.

As categorias de URL adicionadas na instância Now Platform já devem estar em seu ambiente Zscaler Internet Access. Você não pode usar Integração do Security Incident Response com Zscaler para criar categorias de URL em Zscaler.

Nota:
Para obter mais informações sobre listas de categorias de URL no produto Zscaler, consulte a documentação do Zscaler em Categorias de URL .

Procedimento
1. Navegar até **Todos** > **Integração do ZScaler** > **Listas de categorias de URL do ZScaler**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Zscaler Formulário Listas de categorias de URL

Campo	Descrição
Origem	Nome do servidor. Você pode exibir somente os servidores Zscaler Internet Access configurados anteriormente na lista de categorias de URL.
Ativo	Indicador de que a lista de categorias de URL está ativa.
Categoria de URL	Campo que é habilitado depois que você seleciona a origem. Você pode exibir a lista de categorias de URL criadas em Zscaler.
Período de Expiração (dias)	Período de expiração da lista de categorias de URL. 0 (por padrão) indica que a entrada da lista de categorias de URL nunca expira. Ao alterar este valor, qualquer observável que foi adicionado a esta categoria de URL está ativo pelo número de dias que você inserir. Você pode inserir um valor mínimo de 1. Por exemplo, se você definir o período de expiração como 30 dias, as entradas serão removidas da lista de categorias após 30 dias.
Marcador de exibição	Marcador de segurança que aparece no incidente de segurança SIR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Quando você habilita a opção **Exibir marcador**, o campo Zscaler Marcador para observáveis fica disponível no formulário.
Criar solicitação de mudança	Solicitação de mudança e tarefas de mudança em sua instância Now Platform para os registros anexados à lista de categorias de URL. Quando você habilita a opção **Criar solicitação de mudança**, o campo **Solicitação** de mudança fica disponível no formulário.
Requer Aprovação	Lista de grupos de aprovadores. Depois de enviar uma solicitação, é necessária uma aprovação do grupo para concluir a solicitação. Quando você habilita a opção **Requer aprovação**, o campo **Aprovadores** fica disponível no formulário.
Descrição	Descrição da lista de categorias de URL Zscaler. Use este campo para adicionar mais detalhes sobre o registro da categoria de URL.

4. Clique em **Enviar**.
   Um envio bem-sucedido aciona uma notificação por e-mail para o grupo de aprovação.

Enviar observáveis de um registro de incidente de segurança para uma lista de categorias de URL

Envie observáveis que estão anexados a um registro de incidente de segurança para uma lista de categoria de URL configurada usando a solicitação de permissão ou bloqueio. Adicionar observáveis à lista de permissões ou bloqueios para verificações de segurança permite que os usuários revisem o conteúdo desses URLs e obtenham acesso a conteúdo confiável.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Você envia entradas de observável usando a ação de solicitação de permissão ou bloqueio da lista relacionada Observáveis associados. Observáveis são artefatos encontrados em uma rede ou sistema operacional que provavelmente indicam uma invasão. Use a lista de Categorias de URL configuradas anteriormente para selecionar o observável que você deseja enviar. Depois de enviar a solicitação, uma solicitação de aprovação será enviada ao seu grupo de aprovação.

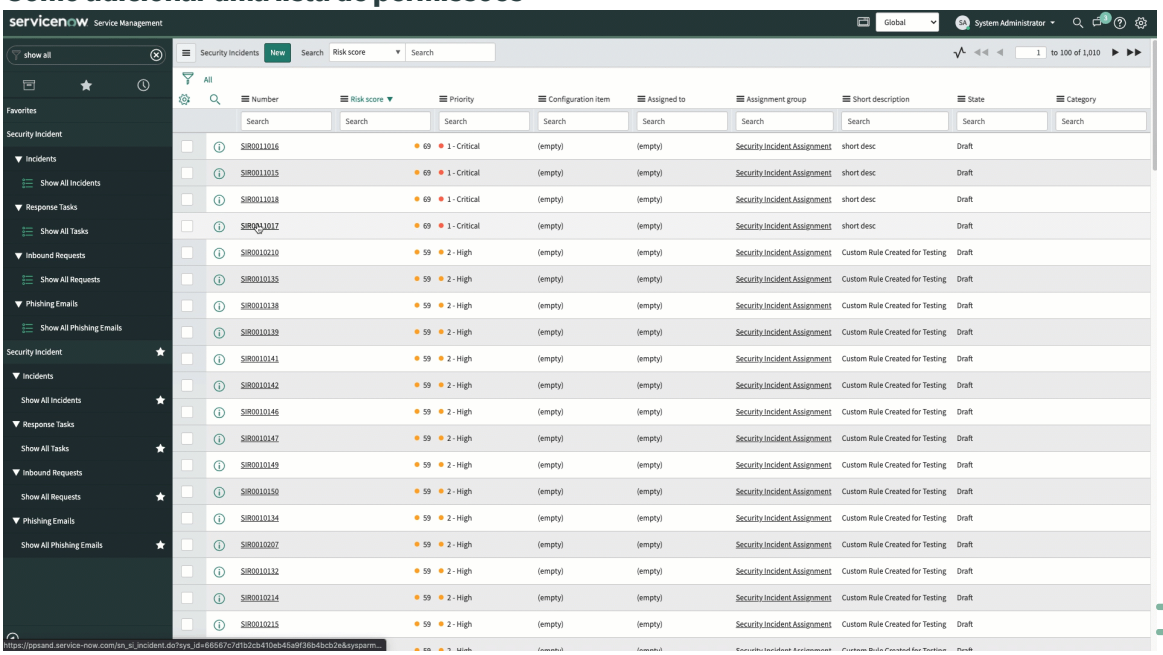
Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar Todos os Incidentes**.
   Neste exemplo, você vê como selecionar um incidente de segurança e um observável e como adicionar uma lista de permissões.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como adicionar uma lista de permissões



2. Selecione o incidente de segurança que você deseja associar à solicitação de permissão ou bloqueio Zscaler.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Observáveis associados**.
   Se você não encontrar nenhum observável, clique em **Novo**.
4. Selecione um observável e, no menu de ações, clique em **Permitir/bloquear solicitação**.
5. Na caixa de diálogo Solicitação de permissão/bloqueio, selecione se deseja executar a solicitação de permissão ou bloqueio no observável.
6. Clique em **Enviar**.
7. Exiba as anotações de trabalho para ver o status do seu envio e os marcadores de segurança.
   Clique nos links das Anotações de trabalho para obter mais informações sobre o status ou para analisar os detalhes no Flow Designer. Os marcadores de segurança são metadados no registro de resposta e definem quem deve ter acesso a tipos específicos de conteúdo de segurança.
8. Para exibir o status do observável que você selecionou, navegue até **Integração do Zscaler** > **Entradas da Lista de Categorias de URL do Zscaler**.
9. Na página Entradas da lista de categorias de URL do Zscaler, clique no observável para exibir o registro.

Aprovar observáveis para listas de categorias de URL

Aprove observáveis que são adicionados a uma lista de categorias de URL para que as entradas de observáveis estejam nas listas de permissões ou proibições apropriadas.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Integração do Zscaler** > **Aprovações do Zscaler**.
2. Selecione o registro a ser aprovado.
3. Clique em **Aprovar**.
   O grupo de aprovadores recebe uma notificação por e-mail da solicitação de aprovação. Depois que os aprovadores clicam no link **Aprovar/Rejeitar** no e-mail, o status muda para aprovado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Enviar o incidente de segurança para a Zscaler lista de categorias de URL

Envie entradas diretamente para observáveis que não estão associados a um registro de incidente de segurança Now Platform específico para que as entradas do observável estejam nas listas de permissões ou proibições apropriadas.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Você também pode adicionar observáveis à lista de categorias de URL diretamente do registro do observável.

Procedimento

1. Navegar até **Todos** > **Integração do Zscaler** > **Entradas da Lista de Categorias de URL do Zscaler**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Zscaler Formulário de Entradas de listas de categorias de URL

Campo	Descrição
Valor de Entrada	Nome do observável. Se um observável correspondente for encontrado, o restante do formulário será preenchido automaticamente. Se nenhum observável correspondente for encontrado, você deverá preencher o restante das informações manualmente.
Observável	Valor (por exemplo, endereço IP ou hash) que está associado ao observável.
Tipo de Observável	Classificação de observável, como um endereço IP ou hash de arquivo.
Lista de categorias de URL	Categoria de URL. Por exemplo, se uma organização usa example.com para serviços do Office 365, Zscaler categoriza example.com como Serviços profissionais e Office 365.
Origem	Nome do servidor. Você pode exibir somente os servidores Zscaler configurados anteriormente na lista de categorias de URL.
Contagem de incidentes	Número de incidentes em que este observável aparece. Este valor é atualizado automaticamente quando o observável é adicionado a outro incidente manualmente ou por meio de um fluxo de trabalho.
Ativo	Indicador de que a lista de categorias de URL está ativa.
Status	Status se o observável for aprovado ou rejeitado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Período de Expiração (dias)	Período de expiração da lista de categorias de URL. 0 (por padrão) indica que a entrada da lista de categorias de URL nunca expira. Ao alterar este valor, qualquer observável adicionado a esta categoria de URL ficará ativo pelo número de dias inserido. Você pode inserir um valor mínimo de 1. Por exemplo, se você definir o período de expiração como 30 dias, as entradas serão removidas da lista de categorias após 30 dias. **Nota:** Se você alterar o período de expiração padrão da entrada da lista de categorias de URL, verá um aviso de que o período é diferente do período configurado na lista de categorias de URL selecionada.
Informação adicional	Campo em que você pode adicionar mais detalhes sobre o observável.

4. Clique em **Enviar**.

Executar uma pesquisa de ameaças usando a biblioteca de ameaças global Zscaler

Execute uma pesquisa de ameaça em um observável usando a biblioteca de ameaças global do produto Zscaler Internet Access. Zscaler oferece suporte a pesquisas em IPs, URLs e domínios de tipo de observável.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode executar pesquisas de inteligência contra ameaças em um ou mais observáveis para determinar se eles estão associados a ameaças de segurança conhecidas. Quando um observável é associado a um incidente de segurança pela primeira vez, todas as implementações de pesquisa de ameaças ativas no Now Platform executam uma pesquisa de ameaça automática. Você pode exibir os resultados na lista relacionada Resultados de pesquisa de ameaças.

Por padrão, a configuração com a menor ordem é selecionada para executar a pesquisa de ameaças na Zscaler Internet Access biblioteca global de ameaças do produto. Você também pode executar a pesquisa de ameaças manualmente.

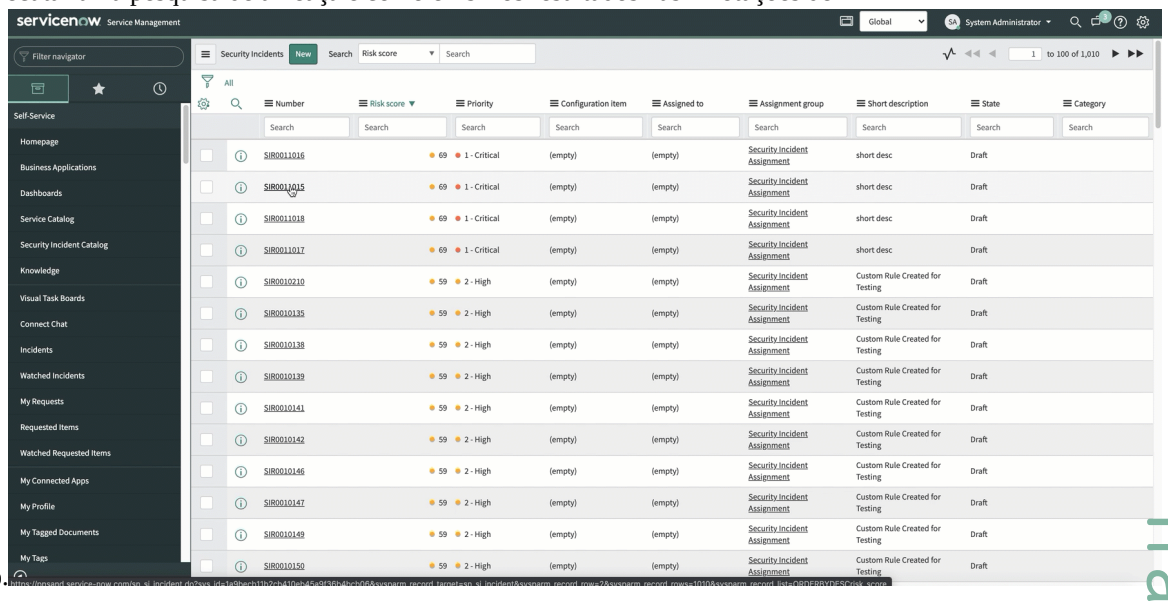
Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança no qual você deseja executar a pesquisa de ameaças.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Observáveis associados**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione o observável e, no menu Ações, clique em **Executar pesquisa de ameaças**.
   Neste exemplo, você vê como selecionar um incidente de segurança e um observável, como executar uma pesquisa de ameaça e como exibir os resultados nas Anotações de trabalho.



Resultado

Depois de iniciar a pesquisa de ameaças, você pode exibir as Anotações de trabalho para ver o status do envio.

Enviar para Zscaler análise da área restrita

Use o serviço de área restrita de produtos Zscaler Internet Access para analisar arquivos em um ambiente virtual para detectar comportamento mal-intencionado.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Quando você cria uma configuração Zscaler, um envio de área restrita Zscaler é criado por padrão no módulo Configuração de área restrita do Zscaler.

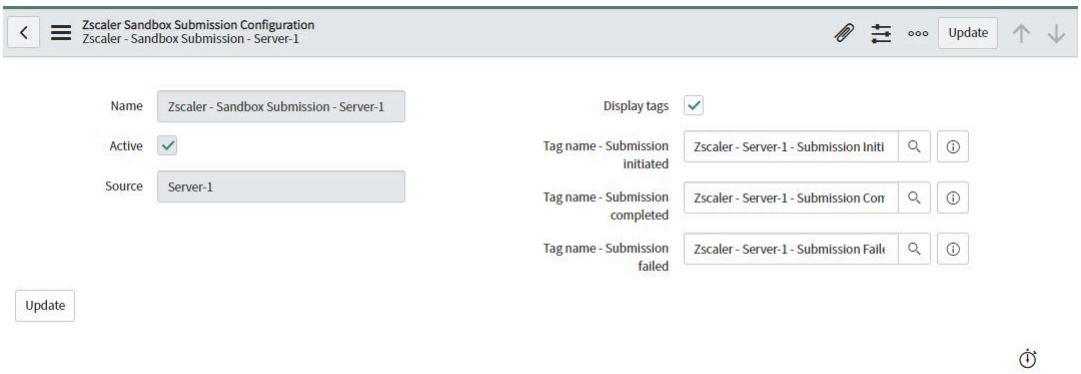
Os campos de nome e origem são preenchidos automaticamente e a configuração é habilitada por padrão. Você pode editar somente o marcador de exibição e as opções ativas. O produto Zscaler Internet Access permite que você busque somente o relatório da área restrita para os observáveis do tipo de hash MD5.

A análise do arquivo associado ao hash MD5 deve ser concluída e o relatório correspondente deve estar na área restrita Zscaler. Se o hash MD5 enviado não tiver um relatório em Zscaler, você receberá uma mensagem de erro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Envio da área restrita do Zscaler



Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança no qual você deseja executar a análise da área restrita.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Observáveis associados**.
4. Selecione um observável de tipo de hash MD5 e, no menu Ações, selecione **Enviar para área restrita**.
   Crie um observável de tipo de hash MD5 se você não encontrar um observável de tipo de hash MD5 existente.
5. Na caixa de diálogo Envio de arquivo, selecione a opção **Zscaler - Envio da área restrita - Servidor** na configuração de envio e clique em **Enviar para área restrita**.
   Depois de iniciar o envio da área restrita, você pode exibir as Anotações de trabalho para ver o status do envio. Um marcador também é anexado ao incidente de segurança.
6. Nas Anotações de trabalho, clique no link da publicação Resultado de envio da área restrita.

Resultado

Você também pode exibir os resultados na guia Mostrar todas as listas relacionadas e resultados de envio da área restrita.

Configurar alertas de e-mail para eventos do paciente 0

Configure o produto Zscaler Internet Access para identificar e verificar arquivos desconhecidos e potencialmente maliciosos, como eventos do paciente 0 para que você possa proteger sua rede contra arquivos maliciosos.

Antes de Iniciar

Função necessária: sn_si.admin, Zscaler Internet Access admin

Por Que e Quando Desempenhar Esta Tarefa

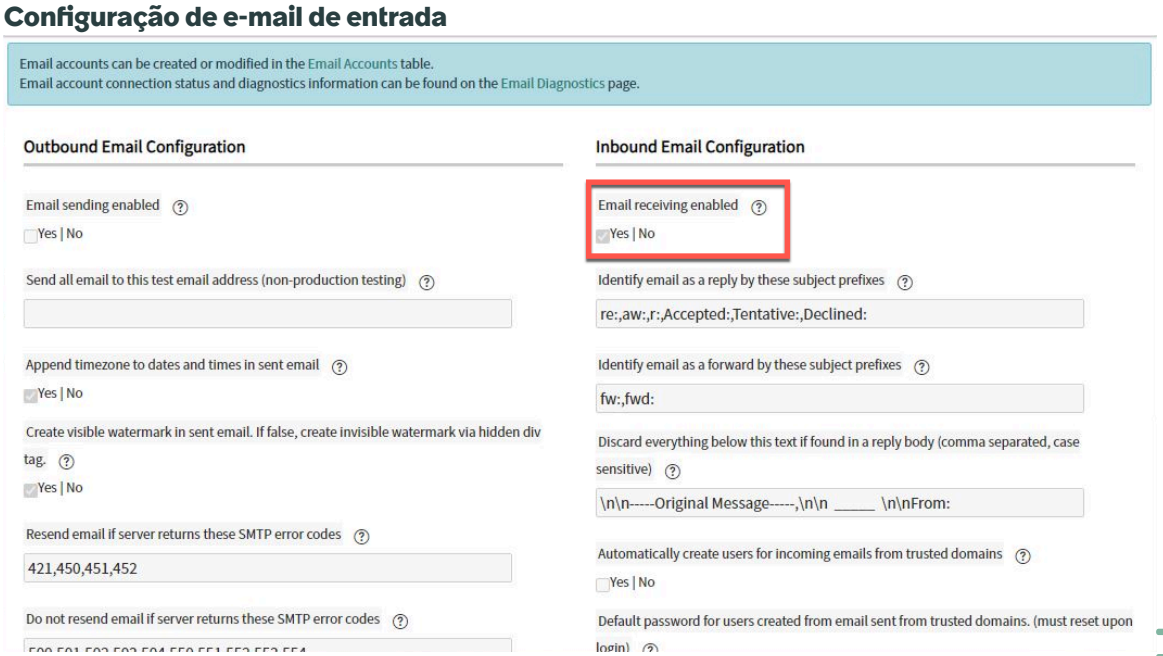
O paciente O é uma classe de alerta que inclui um arquivo desconhecido que foi autorizado a baixar, mas é considerado mal-intencionado. O evento do paciente 0 é classificado como crítico. Você pode configurar o Now Platform para receber alertas de e-mail em intervalos regulares para eventos do paciente 0.

Procedimento

1. Navegar até **Todos** > **Caixas de Correio do Sistema** > **Administração** > **Propriedades do E-mail**.
2. Na seção Configuração de e-mail de entrada, selecione a opção Recebimento de e- **mail habilitado**.

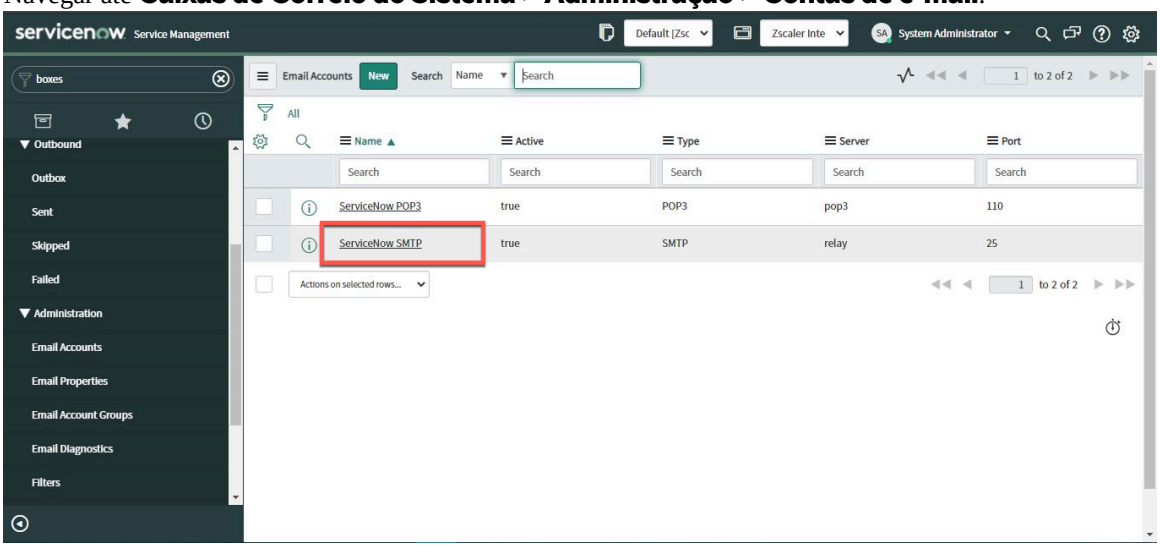
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em **Salvar**.

4. Navegar até **Caixas de Correio do Sistema** > **Administração** > **Contas de e-mail**.

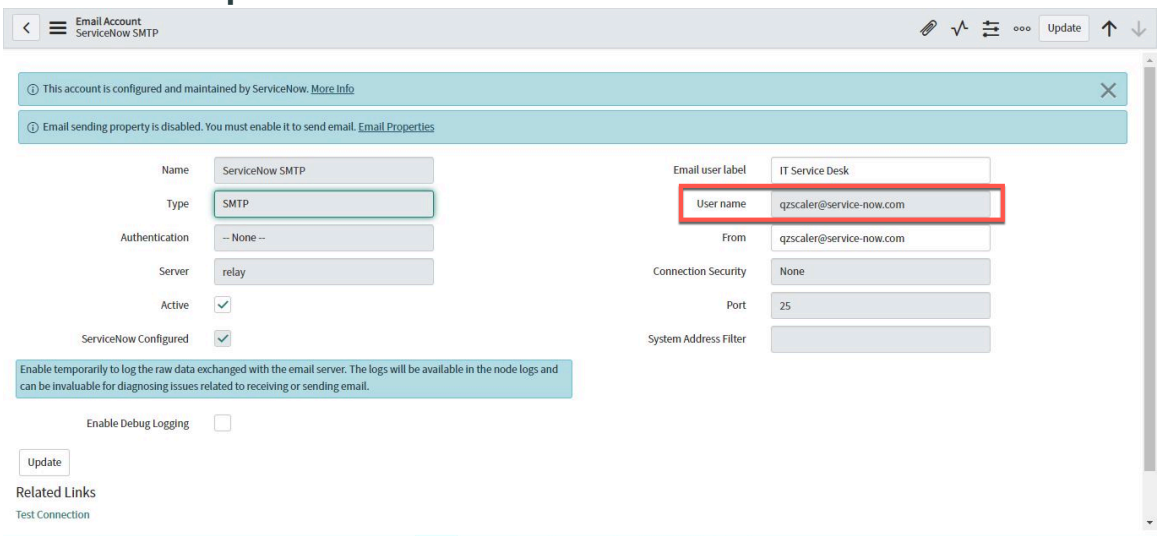


5. Selecione a conta de e-mail **SMTP da ServiceNow**.
   Anote o nome de usuário. O nome de usuário identificado aqui é o endereço de e-mail Now Platform que você usa para configurar em Zscaler para alertas do paciente 0.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome de usuário para a conta SMTP da Now Platform



6. Faça login no portal de administração Zscaler Internet Access.

> **Nota:**
> Para obter mais informações sobre o portal de administração Zscaler Internet Access, consulte a documentação do Zscaler .

7. Navegar até **Administração** > **Alertas** > **Publicar alertas**.
8. Clique **em Adicionar assinatura de alerta**.
9. No formulário, preencha os campos.

Formulário Adicionar assinatura de alerta

Campo	Descrição
E-mail	Now Platform Endereço de e-mail da conta SMTP.
Descrição	Campo para adicionar mais detalhes sobre os alertas do paciente 0.

10. Clique em **Salvar**.

ServiceNow Security Operations Visão geral do complemento para Splunk

O complemento ServiceNow Security Operations para Splunk permite que um administrador de software Splunk colete dados e crie incidentes e eventos no Now Platform.

O complemento é instalado do Splunkbase.

> **Importante:**
> Splunk também é compatível com o ambiente de provedor de serviço gerenciado (MSP).

Configuração da integração do Splunk

Os procedimentos de configuração do complemento ServiceNow Security Operations para Splunk incluem o download do arquivo do complemento no Splunk, a instalação do complemento e a configuração da instância ServiceNow em que os incidentes e eventos de segurança são criados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária

Antes de executar os procedimentos de configuração de integração do Splunk, certifique-se de definir um usuário de integração com as funções sn_si.integration_user e sn_si.analyst em sua instância da ServiceNow. Além disso, para executar importações, você precisa da função import_transformer para obter permissão de leitura e gravação nas tabelas de segurança. A função sn_si.integration_user deve ser definida com a parte import_transformer da função.

Baixe a aplicação Security Operations da ServiceNow

A primeira etapa na configuração da integração ServiceNow-to-Splunk é baixar a aplicação ServiceNow Security Operations do Splunkbase.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Abra o Splunkbase.
2. Pesquise por ServiceNow Security Operations Integration .
3. Baixe a aplicação.

Instalar o complemento ServiceNow Security Operations para Splunk

Instale o **complemento ServiceNow Security Operations para Splunk** para vincular o Splunk ao ServiceNow.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Abra o Splunk.
2. Clique no ícone de engrenagem de **aplicativos** ou no item de menu de atalho **Gerenciar aplicativos**.
3. Clique **em Instalar app do arquivo**.
4. Clique em **Escolher arquivo**, selecione sn_sec_ops.spl e clique em **Carregar**.
5. Se solicitado, reinicie Splunk.
   O complemento ServiceNow Security Operations para Splunk está instalado e pronto para ser configurado.

Configurar ou mudar a instância em que os incidentes ou eventos são criados

Para configurar ou mudar a instância ServiceNow em que novos incidentes e eventos de segurança são criados, use a ação Configurar na lista de aplicações.

Antes de Iniciar
Função necessária: sn_si.admin

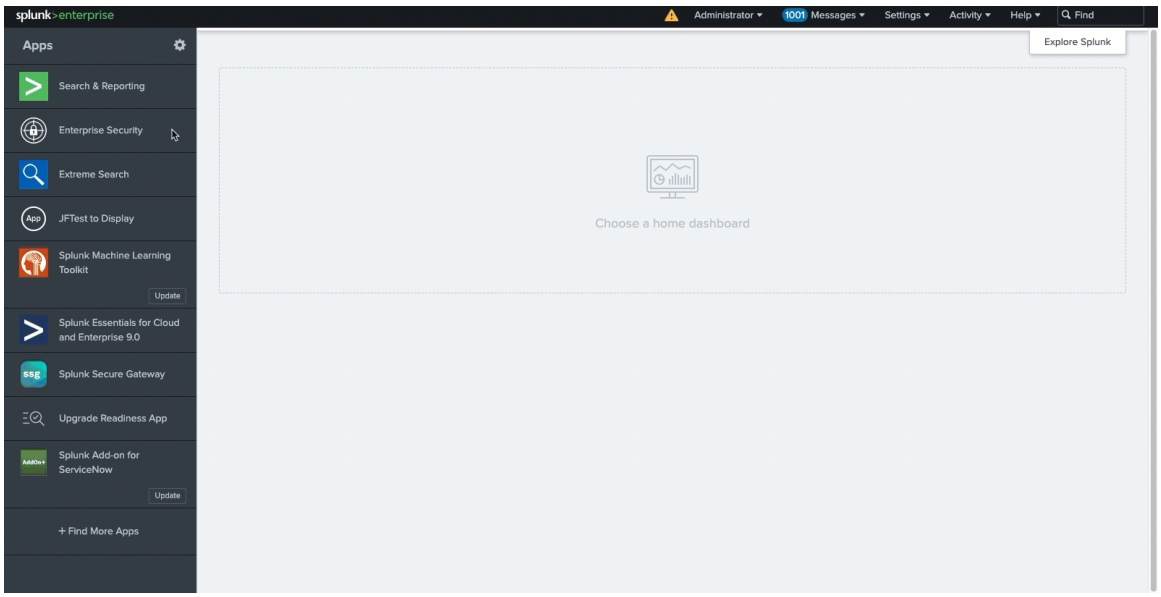
Procedimento

1. Abra o **Splunk**.
2. Clique no ícone de engrenagem de **aplicativos** ou no item de menu de atalho **Gerenciar aplicativos**.
3. Na lista de aplicações, pesquise por aplicações da **ServiceNow** usando o filtro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Procure a **Integração do Security Operations da ServiceNow**e clique na ação **Configurar** correspondente.
5. No formulário, preencha os campos.



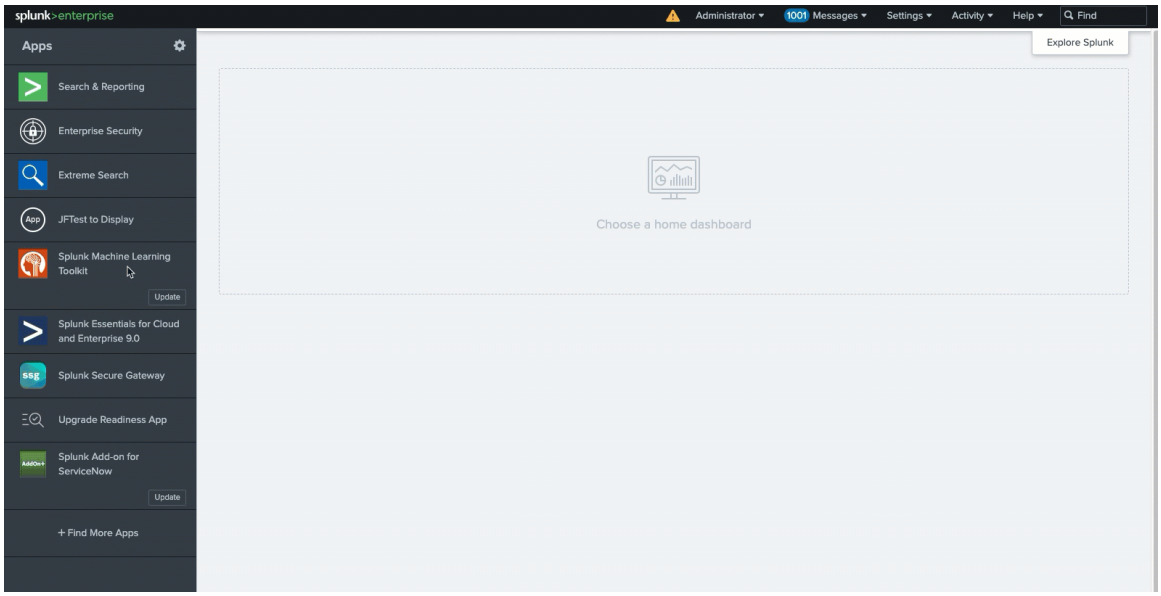
6. Clique em **Salvar**.
7. Como alternativa, procure a **Integração de ingestão de eventos da ServiceNow**e clique na ação **Configurar** correspondente.

   A Integração de ingestão de eventos da ServiceNow é configurada em três guias diferentes.

   - **Splunk primário**: a configuração padrão ou primária do Splunk.
   - **Splunk secundário**: (opcional) o backup ou a segunda configuração do Splunk.
   - **Nível de registro**em log : o nível de logs de relatórios gerados pela integração, ou seja, o nome do tipo de informação.
8. Selecione a guia **Splunk primário**.
9. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



10. **Opcional:** Selecione a guia **Splunk secundário**.
11. **Opcional:** No formulário, preencha os campos.
12. Selecione a guia **Nível de registro em log**.
13. No formulário, preencha os campos.
14. Clique em **Salvar**.
    Depois que a validação for concluída com sucesso, a página Integrações de segurança será exibida com cada uma das suas configurações. Em cada bloco de configuração válido, os botões **Atualizar** e **Excluir** são exibidos, conforme mostrado na figura a seguir.

    Nota:
    Você precisa usar somente a Autenticação básica ou a Autenticação OAuth 2.0. Habilite uma das autenticações e insira os detalhes de autenticação correspondentes. Habilitar ambos exibirá um erro.

    Depois de validada e enviada com sucesso, cada configuração de servidor de ingestão de eventos Splunk é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista Mostrar configurações, clique em **Sim**.

Configurar o registro da aplicação na instância da ServiceNow

Registre a aplicação com a instância para usar a autorização do OAuth.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **OAuth de Sistema** > **Registro de aplicações**.
2. Clique em **Nova**.
3. Clique em **Criar um endpoint da API do OAuth para clientes externos**.
4. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**.
6. Clique em **Enviar**.

Comandos de pesquisa manual

Os comandos de pesquisa manual são inseridos em qualquer janela de pesquisa. Você pode criar um incidente ou evento de segurança. Após o comando, há pares de nomes de campo e valores usados para criar o registro desejado.

Evento de segurança

O comando de evento de segurança, **snsevent**, cria um evento em ServiceNow com a classificação de Segurança.

Esses eventos podem ser revisados por conta própria, ou as regras de alerta em ServiceNow ou as ações manuais podem transformar um evento ou uma coleção de eventos em um incidente de segurança.

Se o evento se tornar um incidente de segurança e cada parâmetro for enviado para o evento, esses dados serão usados para preencher o incidente de segurança da seguinte forma:

Evento de segurança

Nome do parâmetro	Necessários	Usar	Uso no incidente de segurança
node	Sim	O nó representa o servidor ou o item de configuração do evento. O ideal é que este nó seja mapeado para um IC existente em ServiceNow.	Uso no incidente de segurança
tipo	Sim	A categoria do evento.	Descrição resumida
recurso	Sim	O item de configuração.	Descrição resumida

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Evento de segurança

Nome do parâmetro	Necessários	Usar	Uso no incidente de segurança
fonte	Não	A origem desses dados. Por padrão, o servidor Splunk gera os dados.	Log de atividades
external_url	Não	O URL de detalhamento a ser usado em ServiceNow para retornar aos dados do Splunk em relação a este evento. Por padrão, este URL contém o link do resultado de qualquer alerta ou um link para a página de pesquisa padrão do Splunk.	URL externo acessado por meio do botão **Detalhamento** no formulário de Incidente de segurança
time_of_event	Não	A hora em que o evento foi registrado no Splunk.	N/D
Todos os outros valores (categoria, subcategoria no exemplo)	Não	Qualquer campo que não faça parte do campo de informações no evento. Se um incidente de segurança for criado, ele será usado.	Se o campo existir e não estiver preenchido, o incidente de segurança usará esse valor. Por exemplo, a categoria passada pelo Evento se torna a categoria do novo incidente de segurança. Se um campo com este nome não existir, o valor será colocado no log de atividades.

Incidente de segurança

O comando Incidente de segurança, **snsecincident**, cria um incidente de segurança na sua instância ServiceNow.

Incidente de segurança

Parâmetro	Necessários	Usar
short_description	Sim	Uma descrição resumida de uma linha do incidente.
categoria	Não	A categoria do incidente de segurança. Se esta categoria não existir, ela será criada.
subcategoria	Não	A subcategoria. Se esta subcategoria não existir, ela será criada.
cmdb_ci	Não	O item de configuração do incidente de segurança. O ideal é

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incidente de segurança

Parâmetro	Necessários	Usar
		que este item seja mapeado para um IC existente em ServiceNow.
descrição	Não	A descrição mais longa e detalhada do incidente.

Há muitas colunas úteis possíveis - qualquer coisa no mapa de transformação de Incidente de segurança pode ser usada. Se novas colunas forem adicionadas ao incidente de segurança, elas também serão usadas, desde que estejam no mapa de transformação. Algumas colunas úteis: location, prioridade, assign_group, assigned_to, afetado_usuário, ataque_vetor e watch_list.

Ações de evento do Splunk

Ao revisar os logs do Splunk, você pode criar rapidamente eventos e incidentes de segurança a partir de qualquer item no log usando as Ações de evento.

Clicar em uma dessas ações cria um comando de pesquisa manual preenchido com os dados na entrada de log e o executa para gerar o novo registro.

Essas ações são facilmente configuradas para adicionar campos aos dados normalizados. No Splunk, usando **Configurações** > **Campos** > **Ações de Fluxo de Trabalho**, você pode selecionar e editar qualquer uma dessas ações usando os campos de pesquisa manual.

Você pode escolher onde a ação é mostrada, para quais campos e modificar a cadeia de caracteres de pesquisa que contém um comando de pesquisa para criar seu registro.

Alertas do Splunk de registro único

Em qualquer alerta, você pode especificar eventos de segurança ou incidentes de segurança a serem criados quando o alerta for acionado.

Abra ou crie seu alerta e, ao editar ações, selecione o tipo de registro desejado e preencha a caixa de diálogo de alerta.

Alertas do Splunk de campo personalizado com vários registros

Os alertas de vários registros (definidos usando as ações do gatilho **Criar vários incidentes de segurança da ServiceNow** e **Criar vários eventos de segurança da ServiceNow**) podem criar automaticamente registros com qualquer conjunto de campos compatíveis.

Eles agem de forma diferente das outras ações de alerta em que os valores padrão são fornecidos. No entanto, a maioria dos dados vem do resultado da pesquisa desse alerta.

Nota:
Em versões anteriores do complemento e nesta documentação, os alertas com script eram compatíveis. Esse recurso foi descontinuado e substituído por estas instruções.

Criar um alerta do Splunk de vários registros e de campo personalizado

Para criar um alerta do Splunk de vários registros com campos personalizados, você deve criar uma pesquisa projetada para corresponder às colunas da ServiceNow que deseja preencher.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até **Pesquisar**.
2. Na caixa **Pesquisar**, crie uma pesquisa que gere seus dados de registro.
   Consulte os exemplos para obter os critérios de pesquisa recomendados.
3. Clique **em Salvar como** e selecione **Alerta**.
4. Defina o nome, as permissões e a programação, conforme necessário.
5. Clique **em Adicionar ações**.
6. Faça uma das seguintes seleções.
   - Para criar um evento por resultado da pesquisa, selecione **Criar vários eventos de segurança da ServiceNow**.
   - Para criar um incidente por resultado de sua pesquisa, selecione **Criar vários incidentes de segurança da ServiceNow**.
7. Defina padrões, conforme necessário.
   Se o campo no resultado da pesquisa estiver em branco ou ausente, os padrões serão usados. Se houver um valor no resultado, os padrões serão substituídos.

Exemplos de alerta do Splunk de vários registros e de campo personalizado

Ao criar vários alertas do Splunk de registro com campos personalizados, você precisa definir os critérios de pesquisa para gerar dados de alerta. São mostrados exemplos de critérios de pesquisa para incidentes e eventos de segurança.

Pesquisa de incidente de segurança

Para um incidente de segurança, este critério cria uma pesquisa para preencher as colunas na tabela de incidentes de segurança.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval contact_type="Monitoring" |
eval cmdb_ci=host |
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Pesquisa de evento de segurança

Para um evento de segurança, esta é a mesma pesquisa, mas preenche os campos de Evento. Se este evento for transformado em um incidente de segurança e todos os campos que não existem no evento forem preenchidos, eles serão transferidos para o incidente de segurança. Caso contrário, eles permanecerão no campo de informações adicionais do evento e do alerta.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval type="Monitoring" |
eval node=host |
eval source=source
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Os critérios de pesquisa usados adicionarão todos os registros encontrados na pesquisa. Pode adicionar 5 ou 10.000.000.000 de registros. Portanto, este NÃO é um método recomendado para a transferência de dados em massa. A intenção deste método é adicionar um registro por chamada REST à instância da ServiceNow.

Relatório de erros do Splunk

Sempre que ocorre um problema de conectividade com sua instância da ServiceNow, um erro é registrado no Splunk com informações que descrevem o problema.

As mensagens de erro são armazenadas em um novo índice chamado **servicenow** com sourcetype **servicenow**.

Para pesquisar logs de erro, certifique-se de especificar o índice da **ServiceNow** em sua pesquisa. Como alternativa, consulte a documentação atual do Splunk sobre como adicionar o novo índice da **ServiceNow** aos índices de pesquisa padrão.

Splunk Enterprise Event Ingestion integração para Security Operations por ServiceNow

O evento Splunk Enterprise e a integração de dados de alerta com o produto Security Incident Response (SIR) permitem que os analistas de incidentes de segurança coletem e processem logs de segurança e dados de eventos relacionados.

Visão geral

Os dados são coletados em tempo real e usados por analistas para identificar e relatar possíveis ameaças cibernéticas. Os eventos de segurança coletados podem ser processados em alertas acionados que são ingeridos automaticamente com esta integração. Além disso, eventos de segurança individuais podem ser encaminhados manualmente sob demanda da interface de pesquisa e relatório Security Incident Response [] para o produto Splunk Enterprise do Now Platform para criar incidentes de segurança. Você pode recuperar eventos notáveis da pesquisa Splunk Enterprise com a configuração de cluster principal de pesquisa. Você pode fazer isso usando o URL e a porta de API de qualquer cabeçalho de pesquisa que faça parte do cluster.

Esta integração fornece a um analista do centro de operações de segurança (SOC) visibilidade de eventos e dados de alerta relacionados. Esses dados podem ser integrados em Now Platform Security Incident Response (SIR) incidentes de segurança para investigação e correção adicionais. Perfis para Splunk alertas ingeridos em andamento e eventos encaminhados são criados na sua instância Now Platform. Esses perfis personalizam como diferentes Splunk campos de alerta e evento são exibidos em SIR incidentes de segurança. É fornecido um mapeamento padrão de campos de alerta que pode ser editado e aumentado para atender às necessidades específicas do cliente.

Principais recursos

Esta integração inclui os seguintes recursos principais:

- Crie vários perfis de ingestão de alertas para criar incidentes de segurança SIR para tipos específicos de ameaças, como phishing e malware.
- Crie vários perfis de evento para encaminhamento de eventos sob demanda do console Splunk para criar incidentes de segurança SIR.
- Mapeamento de arrastar e soltar de Splunk valores de campo de alerta e evento para campos de incidente de segurança SIR associados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Uma visualização do layout do incidente de segurança SIR com base em alertas ou eventos de amostra para validar a configuração do perfil.
- Inclua alertas históricos, bem como alertas futuros em andamento em intervalos configuráveis.
- Agregue eventos ou alertas a incidentes de segurança SIR existentes com base em valores de campo correspondentes para evitar incidentes de segurança duplicados.

Now Platform Versões compatíveis

O plug-in com.snc.si_dep é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Security Operations aplicações.

As aplicações Security Operations a seguir devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative um aplicativo de cada vez na ordem listada abaixo para garantir uma instalação sem problemas:

1. Security Integration Framework
2. Security Support Common
3. Orquestração de suporte de segurança
4. Security Incident Response

Para obter mais informações sobre como instalar as aplicações principais Security Operations, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

ServiceNow Complementos

O ServiceNow Complemento de ingestão de eventos do Security Operations para Splunk Enterprise será necessário somente se você preferir encaminhar eventos manualmente do console [Splunk Enterprise para a instância Now Platform. Este ServiceNow addon está disponível em splunkbase .

Este ServiceNow Complemento de ingestão de eventos do Security Operations para a aplicação Splunk Enterprise no splunkbase não é necessário para a ingestão de alertas automatizada compatível com a integração.

Versões compatíveis do Splunk

Esta integração é compatível com a versão 6.0 ou posterior do Splunk Enterprise. A integração também oferece suporte ao serviço Splunk Enterprise Cloud.

MID Server

Esta integração requer um MID Server instalado e configurado em sua instância Now Platform® para se conectar ao serviço Splunk se o servidor Splunk for implantado em sua rede corporativa. Se você estiver usando o serviço Splunk Cloud, um MID Server não será necessário. Para obter mais informações sobre MID Servers, consulte MID Server .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Arquitetura de integração e conexão de sistemas

Para obter mais informações sobre a arquitetura da integração, incluindo termos-chave e detalhes de conexão de sistemas externos, consulte Arquitetura de integração e conexão de sistemas externos para a integração Splunk Enterprise Event Ingestion.

Check-list

Para obter uma check-list imprimível desses tópicos, consulte Check-list para a integração de ingestão de eventos notáveis Splunk Enterprise Security. Você pode usar essa lista para monitorar seu andamento enquanto trabalha nas tarefas da integração.

As imagens usadas nos tópicos a seguir foram geradas para a versão Kingston do Now Platform. Para obter informações sobre a interface do usuário San Diego, consulte Gerenciar ameaças à segurança usando o Security Analyst Workspace.

Os tópicos a seguir são numerados. Siga os tópicos listados abaixo na ordem em que são apresentados para uma instalação e configuração simples da aplicação.

Configure sua instância Now Platform® para a integração Splunk Enterprise Event Ingestion

A seção a seguir lista as tarefas de configuração que você deve concluir em sua instância Now Platform® antes de instalar a aplicação do ServiceNow Store.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração sem problemas.

Procedimento

1. Verifique se você atribuiu as funções Now Platform® e Security Incident Response (SIR) necessárias.

As funções a seguir são necessárias para a instalação, configuração e uso da integração na sua instância Now Platform®.

- Um usuário com a função de administrador Now Platform® (admin) instala a aplicação a partir do ServiceNow Store e atribui a função de administrador de incidente de segurança (sn_si.admin).
- Se você quiser encaminhar eventos manualmente de Splunk Enterprise para esta integração, um usuário com a função de administrador Now Platform® atribuirá um usuário com a função (sn_sec_splunk_v2.api_account_access) no Now Platform®. Esta função permite que um usuário com a função de administrador Splunk Enterprise acesse a API no Now Platform® que é necessário para o encaminhamento manual de eventos para esta integração.

  A função (sn_sec_splunk_v2.api_account_access) não será necessária para a integração se você estiver ingerindo alertas automaticamente de Splunk Enterprise para sua instância Now Platform®.

- Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no Now Platform®:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Nomeia, cria e edita perfis de alerta e evento.
- Seleciona e mapeia valores de alertas e eventos para Now Platform® incidentes de segurança.
- Visualiza os detalhes do incidente de segurança para precisão antes de finalizar a configuração.
- Programa a ingestão de alertas em andamento.
- Atribui a função de analista de incidente de segurança (sn_si.analyst).
- Usuários com o sn_si.analyst trabalham com incidentes de segurança.

Para obter mais informações sobre funções e atribuição de funções a usuários, consulte Managing roles .

2. Verifique se você está usando a versão 6.0 ou posterior da API Splunk.

   Se você tiver acesso ao console Splunk Enterprise, terá acesso à API necessária para esta integração. Não há nenhuma outra configuração especial necessária para a API.

3. Verifique se você instalou e configurou um MID Server.

   Um MID Server em sua instância Now Platform® é necessário para se conectar ao serviço Splunk se o servidor Splunk for implantado em sua rede corporativa. Para obter mais informações sobre MID Servers, consulte MID Server .

   Se você estiver usando o serviço Splunk Cloud, um MID Server não será necessário.

4. Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas.

   O plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras aplicações Security Operations necessárias para a integração.

   Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas.

   a. Security Incident Response
   b. Security Integration Framework
   c. Security Support Common
   d. Orquestração de suporte de segurança

   Para obter mais informações sobre como instalar as aplicações principais Security Operations, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

O que Fazer Depois

Você configurou com sucesso sua instância Now Platform® para a integração. A próxima etapa é instalar a aplicação [Splunk Enterprise Event Ingestion de ServiceNow Store para a integração. Para obter mais informações, consulte Instalar e configurar a aplicação ServiceNow para a integração Splunk Enterprise Event Ingestion.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você não salvou pesquisas no console Splunk Enterprise para ingestão ou se estiver executando a configuração inicial desta integração no console Splunk Enterprise e no produto Security Operations da sua instância Now Platform® simultaneamente, consulte Salvar pesquisas no console Splunk Enterprise para a integração Splunk Enterprise Event Ingestion para obter mais informações.

Se você quiser exportar eventos manualmente e sob demanda do console Splunk Enterprise para a integração, consulte Configure seu ambiente Splunk para ingestão manual de eventos para a integração de ingestão de eventos Splunk Enterprise para obter mais informações.

Instalar e configurar a aplicação ServiceNow para a integração Splunk Enterprise Event Ingestion

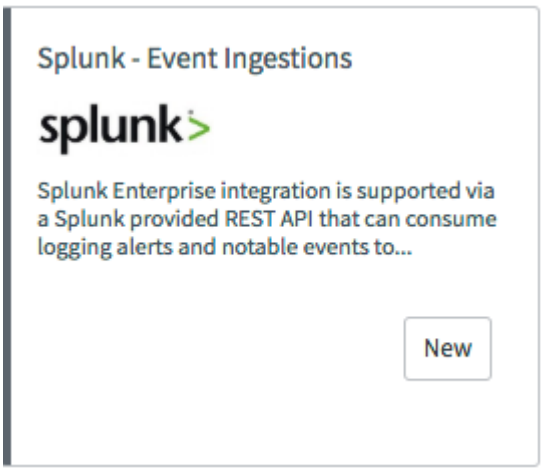
Antes de executar a integração na sua instância Now Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente aos produtos Security Incident Response e Security Operations na sua instância Now Platform®.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Se você não instalou a aplicação [Splunk Enterprise Event Ingestion de ServiceNow Store para a integração, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.
2. Depois de instalar a aplicação com êxito, navegue até **Integrações** > **Configurações de integrações** e localize o bloco Splunk Ingestões de evento.
3. Para configurar a aplicação, clique em **Novo**.

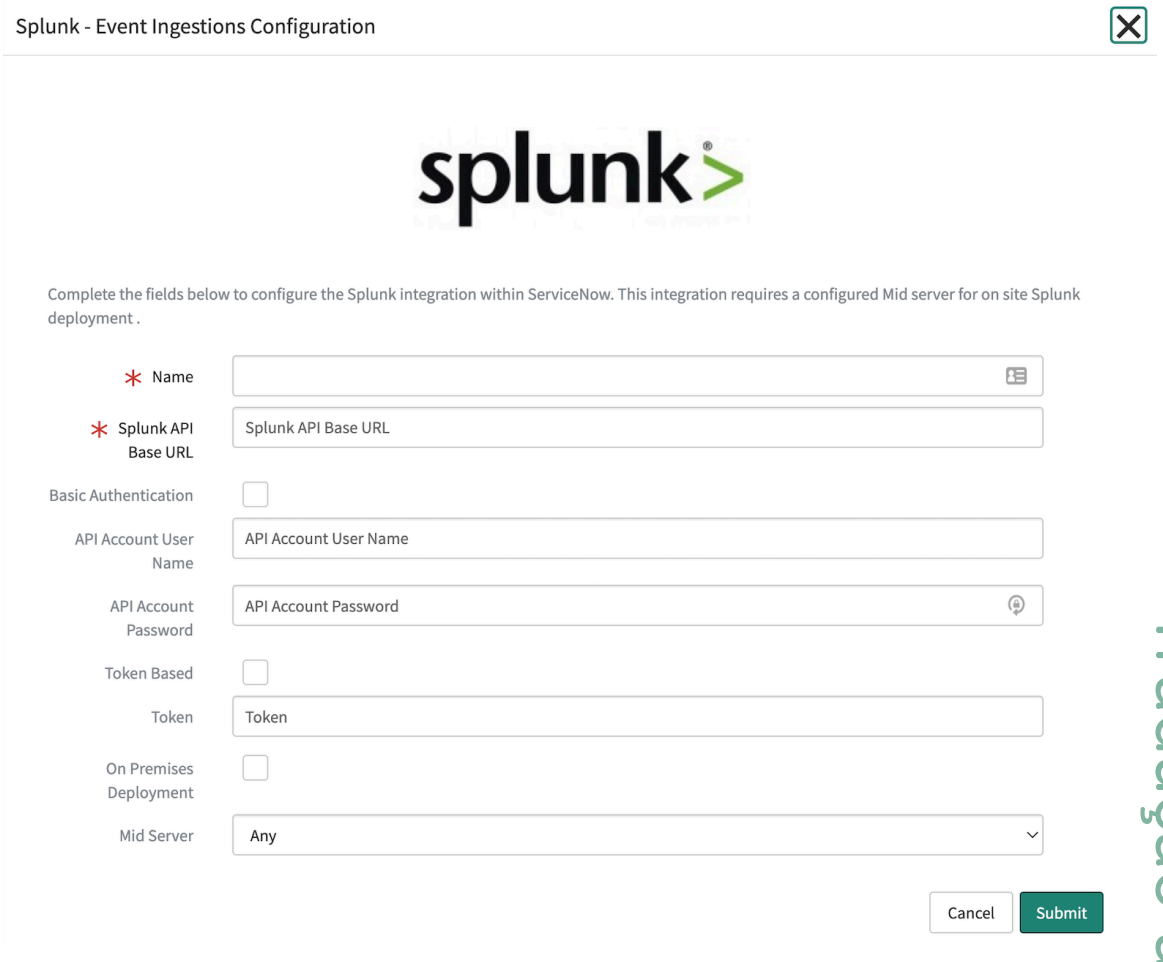


4. Como alternativa, se um botão **Configurar** for exibido em um bloco, clique nele para editar uma configuração existente.
5. Na caixa de diálogo Configuração de ingestão de eventos exibida, preencha os campos.

   A figura a seguir é um exemplo de um formulário preenchido para uma configuração de uma versão local do Splunk Enterprise com um MID Server.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Cada alerta Splunk Enterprise que você ingere do console Splunk Enterprise requer um perfil de evento exclusivo em sua instância Now Platform®. No entanto, a origem que você configura no formulário Configuração de ingestão de eventos pode ser reutilizada para vários perfis Now Platform®, desde que cada perfil inclua alertas acionados Splunk exclusivos.

6. Clique em **Enviar**.
   Depois que a validação for concluída com sucesso, a página Integrações de segurança será exibida com cada uma das suas configurações. Em cada bloco de configuração válido, os botões **Configurar** e **Excluir** são exibidos, conforme mostrado na figura a seguir.

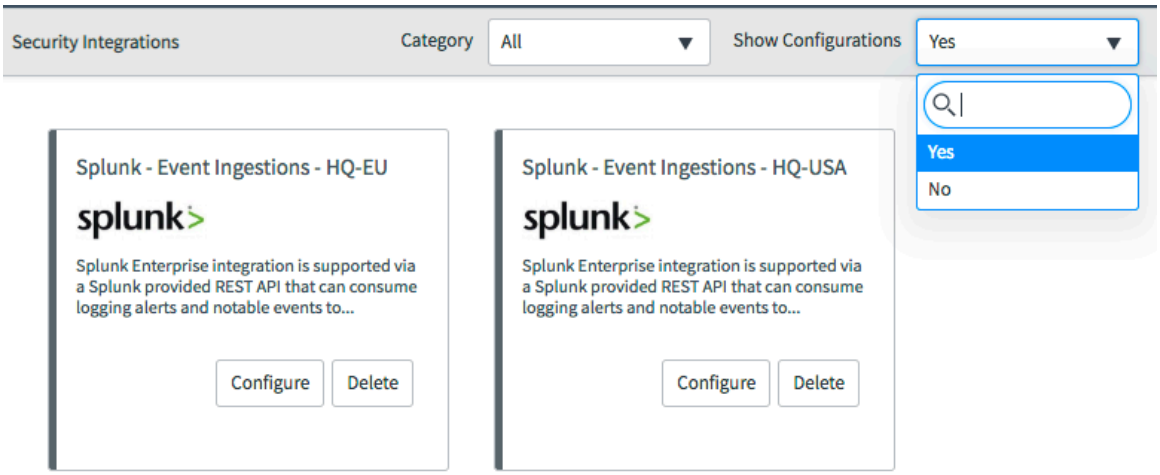
Nota:
Você precisa usar somente a Autenticação básica ou a Autenticação baseada em token. Habilite uma das autenticações e insira os detalhes de autenticação correspondentes. Habilitar ambos exibirá um erro.

Depois de validada e enviada com sucesso, cada configuração de servidor de ingestão de eventos Splunk é salva na página Integrações de segurança como um bloco. Se os blocos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista de seleção Mostrar configurações, clique em **Sim**.



Trouble?

Se uma mensagem de erro for exibida depois de clicar em **Enviar**, insira suas informações novamente e clique em **Enviar**.

O que Fazer Depois

Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar um perfil de evento.

Definir configurações de ingestão de eventos do Splunk Enterprise

Use as configurações de ingestão de eventos do Splunk Enterprise para modificar as configurações predefinidas e seus valores de acordo com seus requisitos.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Splunk Integration** > **Configurações de integração do Splunk**.
2. No formulário, preencha os campos.

Configurações de integração do Splunk

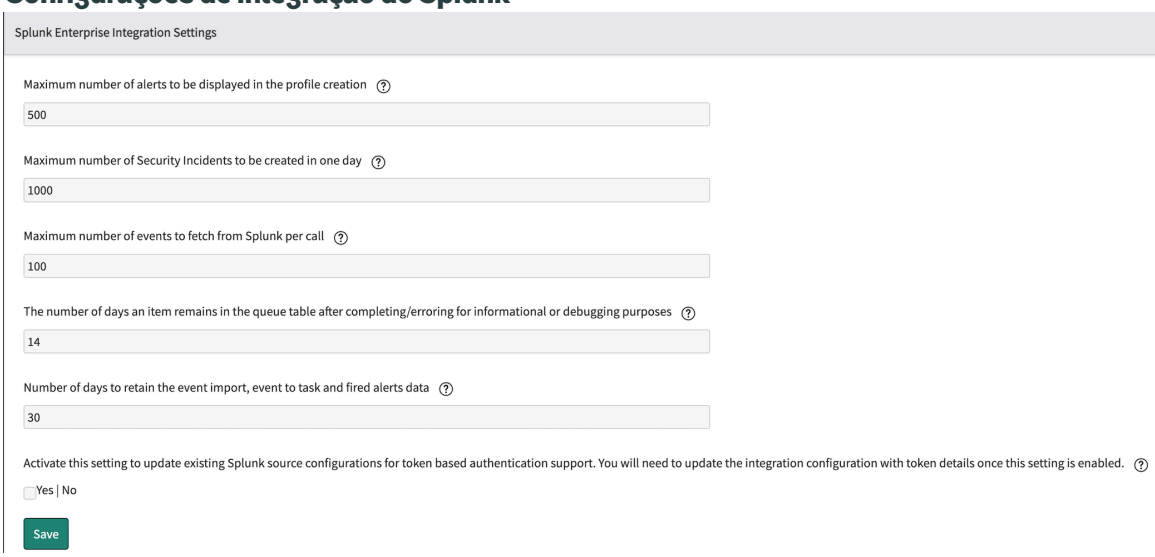
Campo	Descrição
Número máximo de alertas a serem exibidos na criação do perfil	Opção para definir o número máximo de alertas que você deseja exibir ao criar um perfil de evento. Por padrão, o valor é definido como 500.
Número máximo de incidentes de segurança a serem criados em um dia	Opção para definir o número máximo de incidentes de segurança que podem ser criados em um dia. Por padrão, o valor é definido como 1000.
Número máximo de eventos a serem obtidos do Splunk por chamada	Opção para definir o número máximo de eventos a serem recuperados do Splunk para cada chamada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Por padrão, o valor é definido como 100.
O número de dias que um item permanece na tabela da fila após a conclusão/erro para fins de informação ou depuração	Opção para definir o número de dias para um item permanecer na tabela de fila após a conclusão ou a ocorrência de erro devido a informações ou fins de depuração. Por padrão, o valor é definido como 14.
Número de dias para reter a importação de evento, evento para tarefa e dados de alertas disparados	Opção para determinar o número de dias que você deseja reter a importação de evento, o evento para tarefa e os dados de alertas disparados. Por padrão, o valor é definido como 30.
Ative esta configuração para atualizar as configurações de origem do Splunk existentes para suporte à autenticação baseada em token. Você precisará atualizar a configuração de integração com detalhes do token quando essa configuração estiver habilitada.	Opção para atualizar a configuração de origem do Splunk existente para suporte à autenticação baseada em token de uma versão existente. **Nota:** Depois de atualizar para a nova versão, o campo de token ficará indisponível. Você precisa habilitar esta configuração para obter a autenticação baseada em token, após o qual você precisa atualizar a configuração de integração com detalhes de token. Por padrão, o valor é definido como Não.

Configurações de integração do Splunk



3. Clique em **Salvar**.

Criar e nomear um perfil de evento para a integração Splunk Enterprise Event Ingestion

Crie um perfil de evento em sua instância Now Platform e determine quais alertas Splunk criam incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Antes que os incidentes de segurança Now Platform Security Incident Response (SIR) sejam criados a partir de alertas ingeridos, os valores de campo dos alertas são exibidos em um layout de um incidente de segurança Now Platform para que você possa visualizar como o incidente de segurança real será exibido.

De uma perspectiva de integração usando APIs disponíveis, os eventos Splunk são encaminhados individual e manualmente como eventos discretos ou são combinados em alertas acionados que são ingeridos automaticamente no ambiente Security Operations da sua instância Now Platform. Os fluxos de trabalho de integração ingerem diferentes tipos de alertas, como tentativas de acesso não autorizado e malware, por exemplo.

Esses alertas são ingeridos com base nos perfis que você configura no ambiente Security Operations da sua instância. Todos os alertas são ingeridos inicialmente para um tipo de alerta configurado em um perfil. Os alertas ingeridos podem ser filtrados para especificar quais alertas criam incidentes de segurança. Por exemplo, você pode preferir filtros que criem incidentes de segurança somente para alertas identificados como de alto risco. Antes de um perfil ser ativado e criar incidentes de segurança a partir de alertas ingeridos, os valores de campo individuais nos alertas filtrados são mapeados para campos correspondentes em um layout de incidente de segurança para uma visualização.

Os nomes de alerta para perfis de evento na sua instância Now Platform devem ser exclusivos e só podem ser mapeados para um perfil de evento ativo de cada vez. Estes são os nomes de alertas acionados que você configurou no serviço Splunk como parte da configuração da integração. Para obter mais informações sobre como configurar alertas em seu ambiente Splunk Enterprise, consulte Salvar pesquisas no console Splunk Enterprise para a integração Splunk Enterprise Event Ingestion.

O Now Platform ingere alertas específicos usando os fluxos de trabalho da integração. Todos os alertas que atendem aos critérios de seleção no console corporativo Splunk são ingeridos inicialmente na instância Now Platform.

Um perfil no seu Now Platform é um encapsulamento de um alerta [Splunk no console empresarial Splunk. Há um relacionamento um para um entre alertas que são ingeridos com um perfil e conexões com o console empresarial Splunk : um alerta para uma conexão. Há uma única conexão https para um cabeçalho de pesquisa no console Splunk Enterprise. Vários alertas podem vir de um único cabeçalho de pesquisa. Se você se conectar a vários cabeçalhos de pesquisa no console Splunk Enterprise, deverá criar vários perfis na instância Now Platform para ingerir esses alertas.

Etapas para criar perfis para ingestão de alerta programada

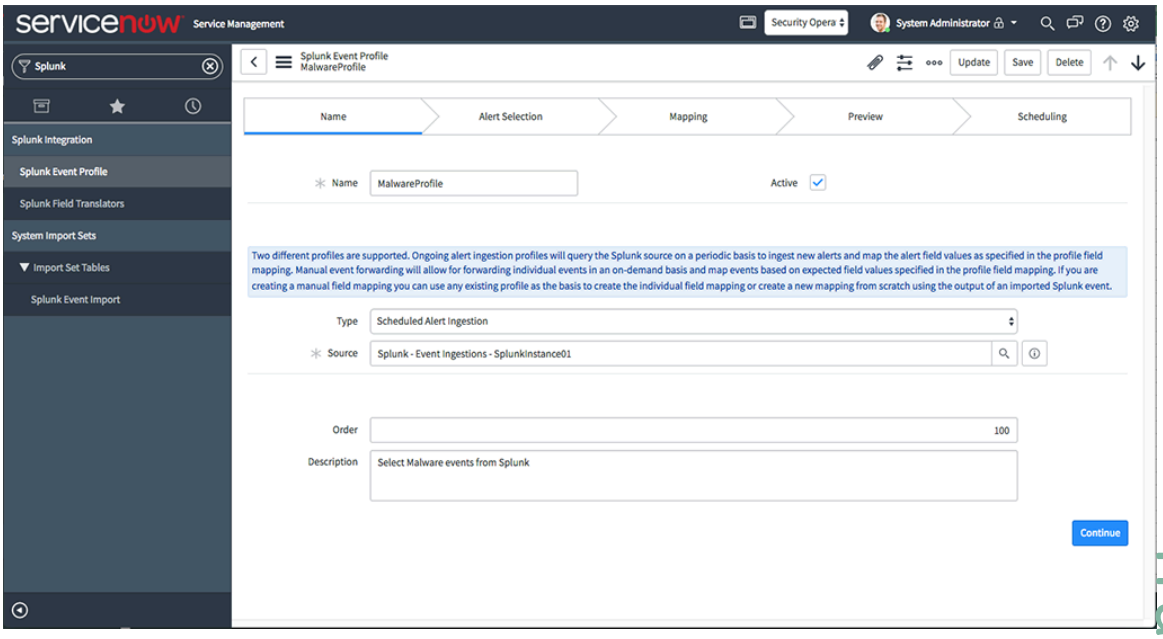
Procedimento
1. Para criar um perfil de evento para um alerta, na sua instância Now Platform, navegue até **Splunk Integration** > **Perfil de evento do Splunk**.
2. Se o formulário de Perfil de evento Splunk não for exibido, clique em **Nome** na barra de andamento.
3. Clique em **Nova**.
4. Preencha os campos.

   Um exemplo de formulário preenchido segue a tabela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A figura a seguir é um exemplo de um formulário preenchido para um alerta programado.



5. Para um perfil com um alerta programado, escolha uma opção para continuar com a configuração do perfil. Etapas para criar perfis para encaminhamento de evento manual
6. Para criar um perfil que ofereça suporte ao encaminhamento manual de eventos, siga estas etapas.

   Para eventos que você encaminha sob demanda do console empresarial Splunk, é possível basear o mapeamento de campo individual em qualquer perfil existente. Como alternativa, você pode criar uma nova grade de mapeamento para dados de anexo exportados. Os eventos encaminhados manualmente não são programados no perfil de evento.

   a. Se ainda não estiver selecionado, na lista de seleção do campo Tipo, selecione **Encaminhamento manual de eventos**.

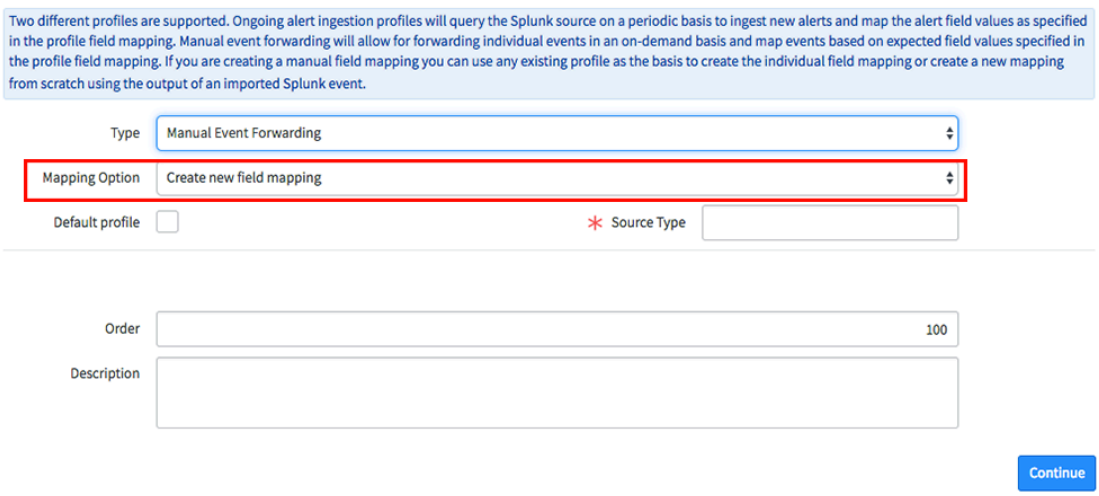
   b. No campo Opção de mapeamento exibido, na lista de seleção, escolha uma opção de mapeamento para continuar.

      Consulte as imagens e tabelas a seguir para obter mais informações sobre as opções de mapeamento disponíveis na lista de seleção Opções de mapeamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar nova opção de mapeamento de campo



Criar nova opção de mapeamento de campo

Opção ou campo	Descrição
Criar nova opção de mapeamento de campo	Novo mapeamento de campo para o seu evento. Se você não tiver um mapeamento de campo semelhante ao perfil que está criando, selecione esta opção para criar um novo mapa.
Perfil padrão	Perfil de encaminhamento de evento padrão para todos os eventos Splunk. O padrão é desabilitado. Quando esta opção está habilitada, este perfil se torna o perfil padrão para encaminhamento de evento manual. Este perfil é o único perfil que está ativo e usado para cada mapeamento de campo de evento Splunk para um incidente de segurança SIR. Um perfil se adapta a todos os eventos encaminhados. O campo Origem não estará disponível se a opção de perfil padrão estiver habilitada.
Tipo de origem	Splunk servidor. Este campo não estará disponível se a opção de perfil padrão estiver habilitada. Se disponível, a opção Tipo de origem permite o mapeamento de campo de evento exclusivo para campos de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou campo	Descrição
	incidente de segurança com base no tipo de origem Splunk. Se você quiser gerenciar eventos de log de firewall de forma diferente dos eventos de detecção de endpoint e eles tiverem diferentes tipos de origem Splunk, você poderá criar diferentes perfis de evento com base nos tipos de origem para atender a esse requisito.
Ordem	O padrão é 100. Deixe esta configuração como padrão. Se você tiver criado um grande número de perfis, este valor fornecerá uma prioridade de execução em tempo de execução quando dois ou mais perfis compartilharem condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este perfil de outros perfis.

Para um perfil com um novo mapeamento de campo, verifique se você inseriu um valor no campo Tipo de origem e clique em **Continuar** para prosseguir para a etapa de mapeamento da configuração.

Para obter um perfil com um mapeamento de campo existente, consulte a figura e a tabela a seguir para obter mais informações.

Selecione o perfil existente para a opção de mapeamento de campo

Selecione o perfil existente para a opção de mapeamento de campo

Opção ou campo	Descrição
Selecionar perfil existente para mapeamento de campo	Um mapeamento de campo existente para o seu evento. O campo Copiar do perfil é exibido. Siga estas etapas para copiar um mapeamento de campo existente para este perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou campo	Descrição
	i. À esquerda do campo Copiar do perfil exibido, clique no ícone de pesquisa. ii. Na lista Perfis de evento Splunk exibida, clique no nome do perfil que tem o mapa que você deseja copiar. O nome do perfil é exibido no campo Copiar do perfil.
Perfil padrão	Perfil de encaminhamento de evento padrão para todos os eventos Splunk. O padrão é desabilitado. Quando esta opção está habilitada, este perfil se torna o perfil padrão para encaminhamento de evento manual. Este perfil é o único perfil que está ativo. Ele é usado para cada mapeamento de campo de evento Splunk para um incidente de segurança SIR. Um perfil se adapta a todos os eventos encaminhados. O campo Origem não estará disponível se a opção de perfil padrão estiver habilitada.
Tipo de origem	Splunk servidor. Este campo não estará disponível se a opção de perfil padrão estiver selecionada. Se disponível, a opção Tipo de origem permite o mapeamento de campo de evento exclusivo para campos de incidente de segurança com base no tipo de origem Splunk. Se você quiser gerenciar eventos de log de firewall de forma diferente dos eventos de detecção de endpoint e eles tiverem diferentes tipos de origem Splunk, você poderá criar diferentes perfis de evento com base nos tipos de origem para atender a esse requisito.
Ordem	O padrão é 100. Deixe esta configuração como padrão. Se você tiver criado vários perfis, este valor fornecerá uma prioridade de execução em tempo de execução quando dois ou mais perfis compartilharem condições de acionamento. O fluxo de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou campo	Descrição
	trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este perfil de outros perfis.

Na parte inferior do formulário para selecionar um mapeamento existente para o seu perfil, clique em **Concluir** para concluir a configuração do perfil.

O que Fazer Depois

Você concluiu com sucesso as etapas para criar perfis para alertas programados e encaminhamento de evento manual. Para perfis de encaminhamento manual de eventos, você concluiu a configuração do perfil. A próxima etapa é carregar os dados do anexo na etapa de mapeamento.

Para perfis de alertas programados, a próxima etapa é selecionar alertas para ingestão automática.

Selecione alertas programados para a integração Splunk Enterprise Event Ingestion

Depois de criar um perfil para um alerta programado, selecione um alerta Splunk para este perfil que você deseja mapear para um incidente de segurança Now Platform Security Incident Response.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Exiba os alertas disponíveis na sua instância Now Platform para saber quais valores de campo estão disponíveis para mapeamento. Selecione um alerta para verificar se você recebe os resultados esperados no layout de formulário básico antes de mapear os valores para campos em SIR incidentes de segurança. Você só pode selecionar um alerta na lista deste formulário.

Procedimento

1. Se a página Seleção de alerta não for exibida, selecione-a na barra de andamento para exibi-la. Por padrão, o app principal de pesquisa e relatório é selecionado.
2. Se o alerta a ser ingerido fizer parte de um app Splunk diferente, selecione **Seleção de app Splunk** e escolha seu app Splunk na lista de **Apps selecionados**.
3. Na **Lista de alertas**, escolha um alerta e mova-o da coluna **Disponível** para a coluna **Selecionado**. Você também pode escolher vários alertas. Se os alertas forem selecionados como parte de um único perfil, os alertas terão mapeamentos de campo e configurações de perfil comuns.

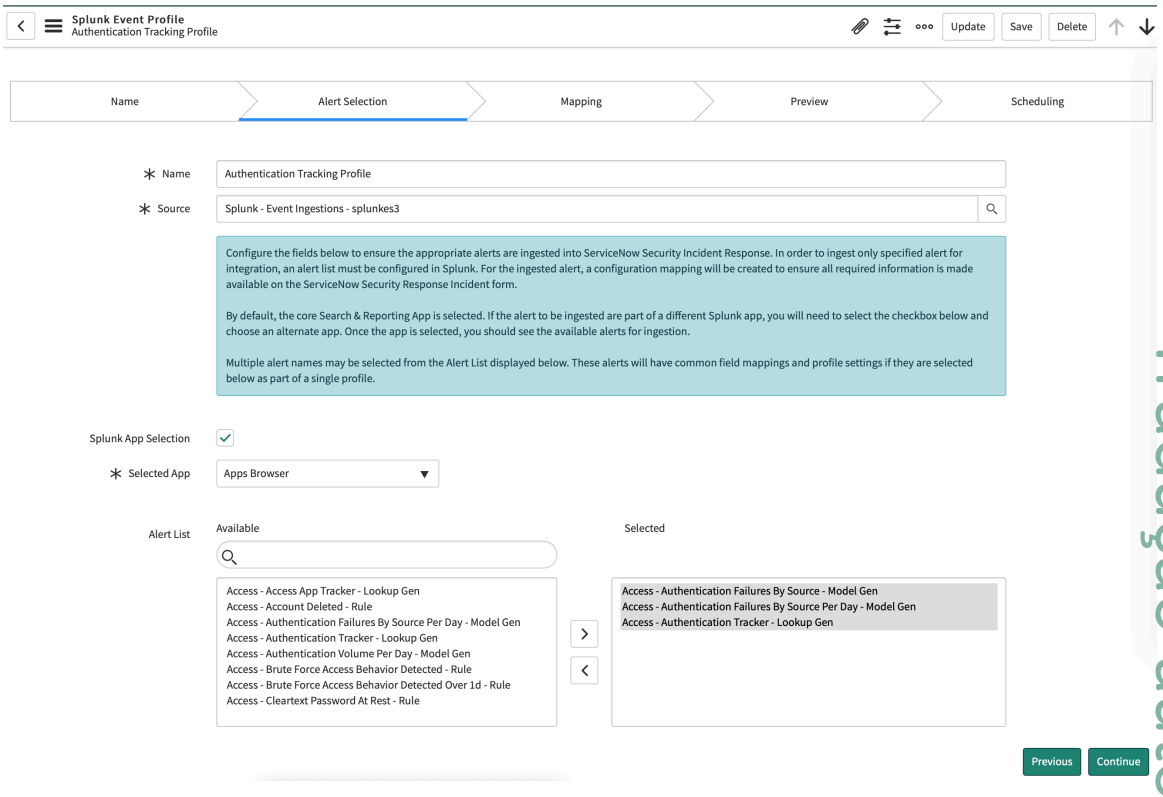
   A lista de alertas neste formulário corresponde à lista de alertas no seu console Splunk. Até 500 alertas são exibidos neste formulário. Se houver mais de 500 alertas listados no console do Splunk na página Alertas, somente os primeiros 500 alertas serão exibidos neste formulário na sua instância Now Platform.

Opção	Descrição
No campo de pesquisa Lista de alertas, insira o texto.	A coluna abaixo do campo de pesquisa é filtrada com as opções disponíveis com base no texto inserido. Selecione um alerta e, com as teclas de seta, mova o alarme selecionado de **Disponível** para **Selecionado**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Na Lista de alertas, clique duas vezes em um Alerta.	A coluna **Selecionado** é preenchida com sua seleção.
Na Lista de alertas, clique uma vez em uma regra de alarme.	O alarme está selecionado. Com as teclas de seta, mova o alerta selecionado de **Disponível** para **Selecionado**.



4. Escolha uma opção para continuar.

O que Fazer Depois

Você selecionou com sucesso um alerta para um perfil de alerta programado. A próxima etapa é mapear valores de alerta para campos em um incidente de segurança.

Mapeamento de alertas e eventos para a integração Splunk Enterprise Event Ingestion

Depois de identificar as origens para ingestão de alerta programada ou encaminhamento de evento manual, a próxima etapa é mapear campos de evento individuais para os campos em um incidente de segurança Now Platform Security Incident Response (SIR).

Visão geral

Para a etapa de mapeamento, como um usuário com a função sn_si.admin, você ingere alertas de amostra do console Splunk Enterprise ou exporta dados de evento para um evento Splunk Enterprise.

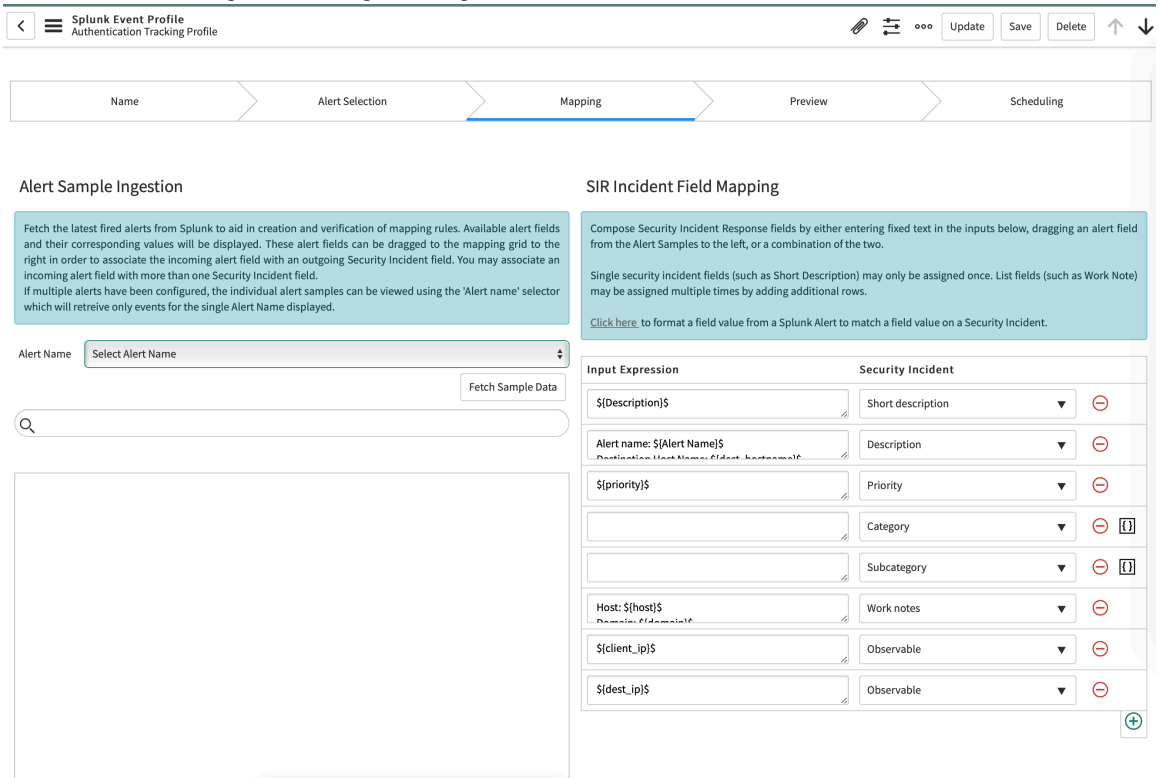
As imagens a seguir são exemplos das grades de mapeamento padrão fornecidas para cada tipo de perfil de evento. Este mapeamento padrão pode ser editado. Esta modificação permite que você personalize os campos que preenchem o incidente de segurança. Com a etapa de mapeamento, você pode visualizar como a adição ou a remoção de campos de evento afeta os valores do campo de incidente de segurança SIR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Selecione o **Nome do alerta**e, depois de clicar para **Buscar dados de amostra**, os valores do campo de alerta Splunk serão preenchidos no lado esquerdo do formulário quando os alertas de amostra forem ingeridos pelo perfil. Estes são os campos de alerta Splunk que você mapeia para os campos de incidente de segurança SIR.

Formulário de mapeamento padrão para alertas

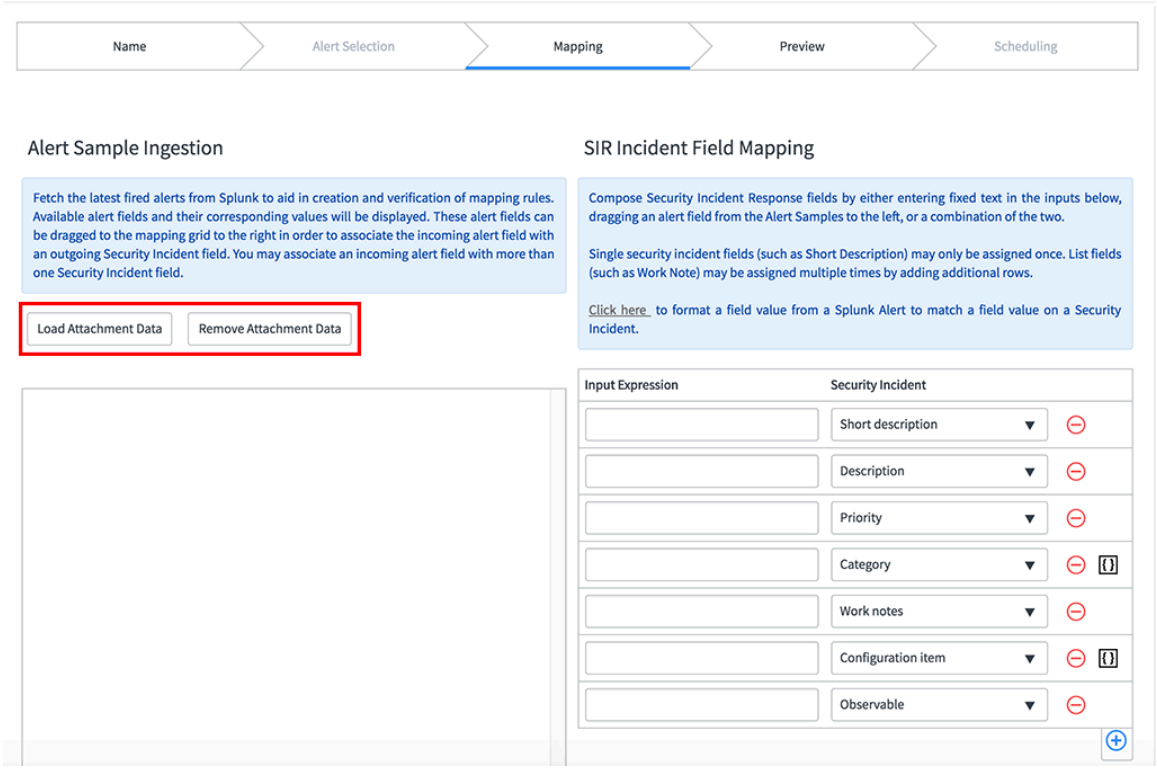


Depois de clicar para carregar dados de anexo para eventos encaminhados, os campos de evento Splunk são preenchidos no lado esquerdo do formulário. Estes são os campos de dados Splunk que são mapeados para os campos de incidente de segurança SIR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de mapeamento padrão para eventos encaminhados



Você pode preferir revisar alguns alertas de amostra no console Splunk para incluir na etapa de configuração de mapeamento de campo. Esta etapa é rotulada como **Mapeamento** na barra de andamento. Se esta página não for exibida, clique em **Mapeamento** na barra de andamento.

O mapeamento de alertas e a exportação de eventos sob demanda do console empresarial Splunk incluem os seguintes conceitos e tarefas:

- Busca dados de amostra para perfis de alerta ingeridos automaticamente. Depois que os dados são obtidos (extraídos) de um alerta acionado no console Splunk Enterprise, os campos de alerta disponíveis e seus valores correspondentes são exibidos em um layout de mapeamento padrão no lado esquerdo do formulário de mapeamento. As guias são exibidas para você exibir os valores de um ID de alerta que você extraiu. Verifique se todos os campos críticos da seção Ingestão de amostra de alerta à esquerda do formulário estão mapeados para a grade à direita do formulário.
- Se necessário, carregue dados de amostra de evento para todos os perfis de evento encaminhados manualmente. Dados de amostra para esses eventos são exportados em um arquivo .xml do console Splunk Enterprise e carregados em sua instância Now Platform®. Os dados importados são exibidos na seção Ingestão de amostra de alerta à esquerda do formulário.
- Edite a configuração de mapeamento arrastando alertas do lado esquerdo e soltando-os na grade de mapeamento à direita. A grade de mapeamento à direita associa o campo de alerta de entrada a um campo de incidente de segurança de saída.
- Personalize a grade de mapeamento adicionando ou removendo campos. Rastreie campos ignorados ou duplicados com a codificação de cores fornecida.
- Defina condições de filtro para que você possa especificar quais alertas são ingeridos na aplicação SIR e quais alertas são filtrados.
- Defina critérios de campo de incidente adicionais que agregam um alerta de entrada a um incidente de segurança SIR existente para evitar incidentes duplicados. Essa filtragem

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

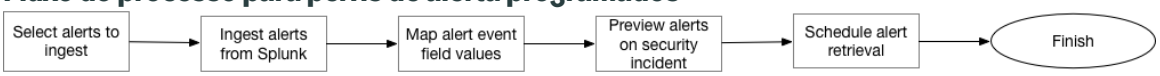
adicional pode reduzir o número de incidentes de segurança ativos e sobrepostos, colocando todos os dados de evento de segurança relacionados em um único incidente de segurança.

- Em determinados casos, os valores do campo de evento no console empresarial Splunk podem não ser traduzidos diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de script se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de script, os valores do campo Alerta de malware e Infecção por vírus no console Splunk são convertidos em Atividade de código malicioso no campo Categoria no incidente de segurança SIR.

Perfis de alerta programado

Depois de criar um perfil de alerta programado, o fluxo do processo para a configuração é mostrado na figura a seguir.

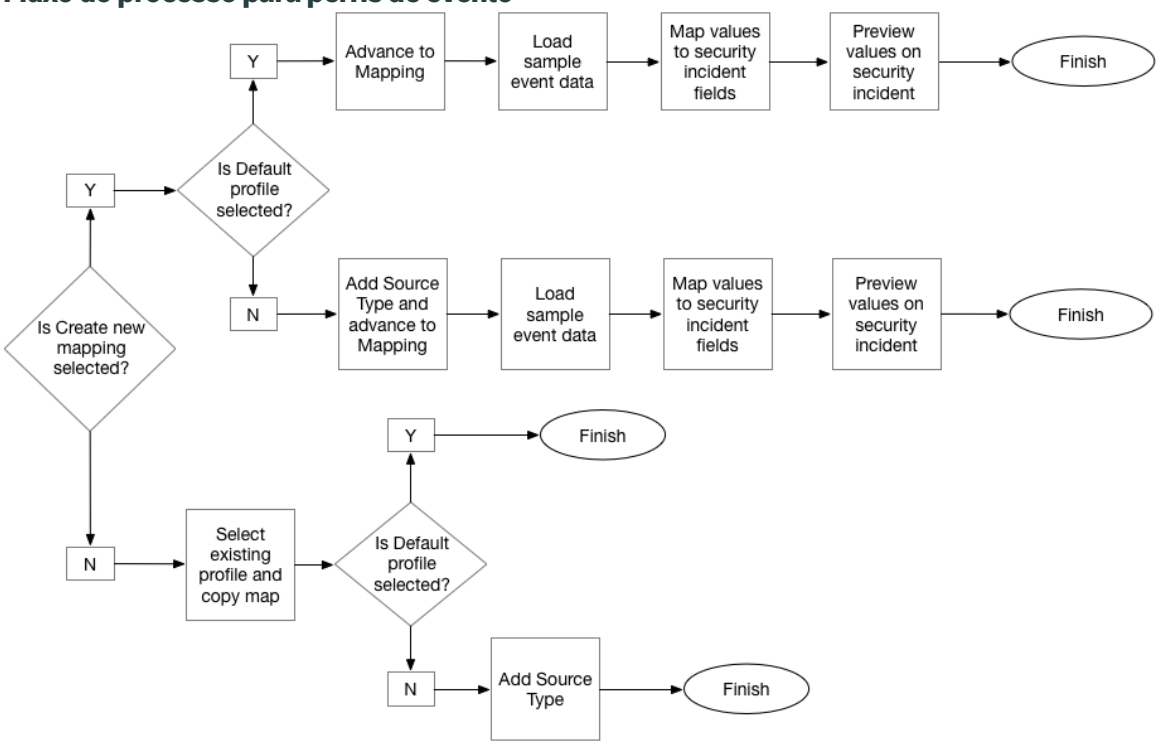
Fluxo do processo para perfis de alerta programados



Perfis de encaminhamento de evento manual

Depois de criar um perfil para um evento, o fluxo do processo para a configuração é mostrado na figura a seguir.

Fluxo do processo para perfis de evento



A próxima etapa é ingerir alertas acionados ou exportar dados e mapear valores para os campos de incidente de segurança SIR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapear alertas para a integração Splunk Enterprise Event Ingestion

Durante a etapa de mapeamento de campo de evento, você mapeia campos de evento individuais de alertas acionados ou dados de evento importados para campos em um incidente de segurança Now Platform Security Incident Response (SIR).

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

A grade de mapeamento pré-configurada dos campos de incidente de segurança padrão pode ser editada. A codificação de cores dos campos de evento ajuda a monitorar os valores de campo que você já mapeou. Esta etapa ajuda a visualizar como suas edições afetam os campos no incidente de segurança.

Mapeie até cinco alertas da coluna Ingestão de amostra de alerta à esquerda do formulário para os campos de incidente de segurança na coluna Mapeamento de campo de incidente SIR à direita.

Crie mapas personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Personalizar os campos permite mapear Splunk campos que não são exibidos na grade de mapeamento padrão no incidente de segurança SIR.

Procedimento

1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Para um perfil com um alerta programado, abaixo de Ingestão de amostra do alarme, selecione o alerta no **Nome** do alerta e clique em **Buscar dados de amostra** para extrair a instância mais recente de um alerta acionado no console Splunk Enterprise.

   Os alertas são exibidos como guias. Você pode ingerir até cinco dos alertas mais recentes.

   A extração de eventos de amostra pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela.

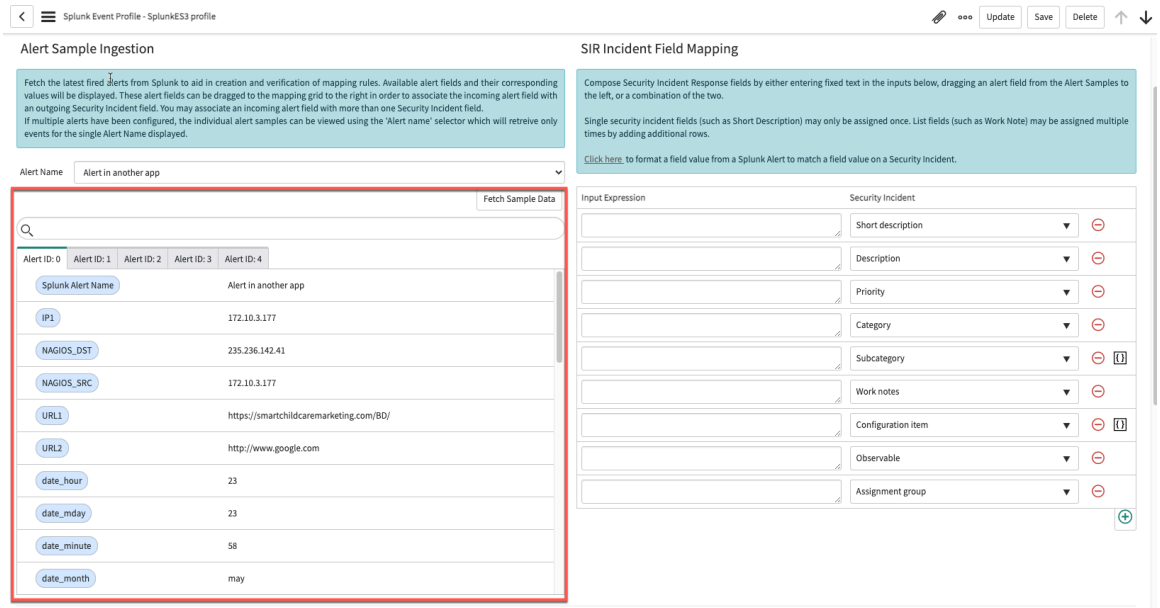
   Nota:
   Um campo de mapeamento adicional, **Splunk Alert Name**, é adicionado pela integração para permitir o rastreamento de um evento para a regra de alerta de origem em Splunk. Isso pode ser útil em cenários em que vários alertas Splunk são combinados em um único perfil.

   Quando um único campo contém vários valores, esses valores são analisados e mapeados para entradas de campo individuais na seção de mapeamento de campo de incidente SIR. Por exemplo, os endereços IP de origem, os nomes de ativos ou os URLs podem ter várias entradas de campo observáveis ou vários ICs, que são analisados e mapeados para entradas de campo individuais na seção de mapeamento de campo de incidente SIR.

   Na figura a seguir, os pares de valor de nome de campo para o alerta ingerido ou o evento de amostra importado são exibidos no lado esquerdo deste formulário após a conclusão da extração. Esses valores são os valores que você mapeia para os campos de incidente de segurança no lado do mapeamento de campo de incidente de SIR do formulário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para perfis de alerta programados, prossiga para a etapa cinco para mapear os valores.
4. Como alternativa, para um perfil de um tipo de evento que você deseja exportar do console Splunk Enterprise, siga estas etapas para carregar dados de anexo na instância Now Platform®.
   a. Se ainda não estiver conectado, faça login no console Splunk Enterprise.
   b. Navegue até a guia Pesquisar e insira um nome para uma pesquisa que tenha os dados do evento que você deseja exportar.

      Por exemplo, malware é um termo de pesquisa usado para todos os eventos de malware que você pode encaminhar com o fluxo de trabalho desta integração.

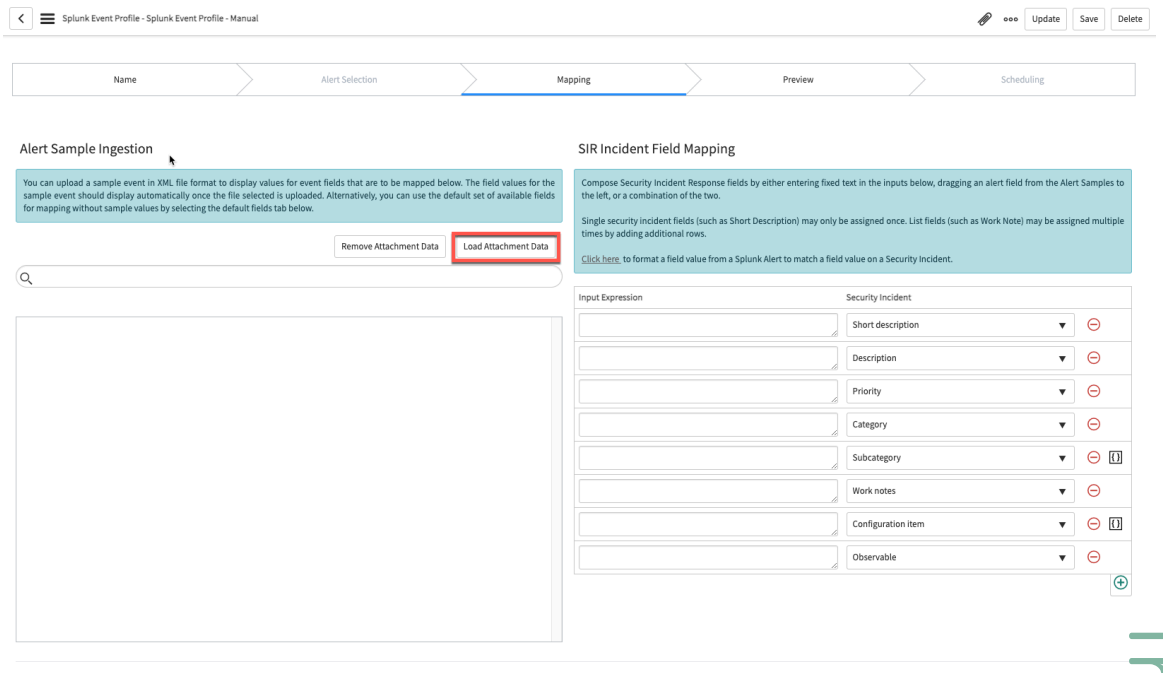
   c. Expanda o evento e, na coluna Campo, selecione os campos que deseja importar.

      Esses campos são os pares de campo-valor que são exportados e exibidos na página Mapeamento na sua instância Now Platform®.

   d. No console Splunk Enterprise, no canto superior direito da página de pesquisa, clique no ícone **Exportar**.
   e. Na lista do campo Formato na caixa de diálogo exibida, clique em **Formato XML**.
   f. **Opcional:** Insira um novo nome de arquivo.
   g. Clique em **Exportar**.
      O arquivo é baixado para sua instância Now Platform®.
   h. Se a página Mapeamento ainda não estiver exibida na sua instância Now Platform®, clique em **Mapeamento** na barra de andamento.
   i. Na coluna Ingestão de amostra de alerta, clique em **Carregar dados de anexo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



j. Na caixa de diálogo exibida, clique em **Escolher arquivos**, navegue até o arquivo .xml que você exportou e clique em **Abrir**.
Os pares de valores dos campos que você exportou para o evento são exibidos no lado esquerdo do formulário de mapeamento.

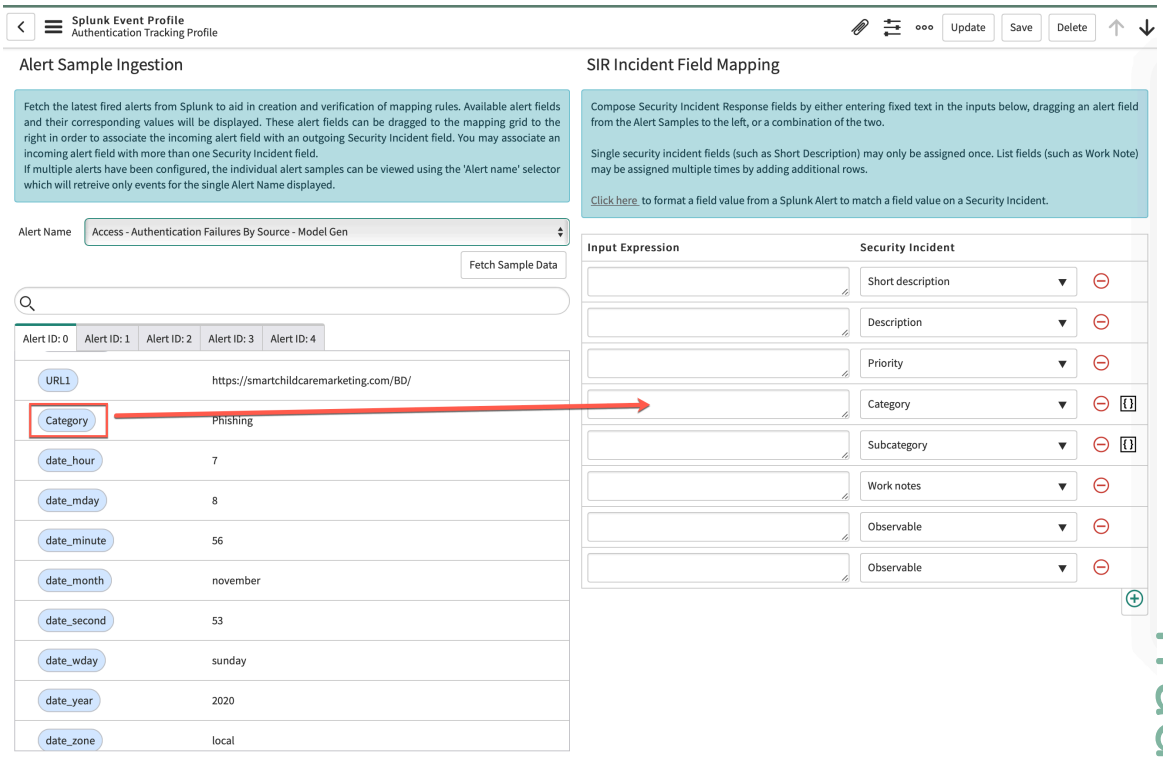
Na figura a seguir, os pares de dados para um alerta programado ingerido são exibidos no lado esquerdo deste formulário. Pares de valores para eventos importados também são exibidos neste lado do formulário. Esses valores são os valores de campo que você mapeia para os campos de incidente de segurança no lado Mapeamento de campo de incidente de Sir do formulário.

5. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e mantenha pressionado um nome de campo azul no lado esquerdo do formulário.

6. Arraste o nome do campo, por exemplo, `category`e solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.

Tradução automática

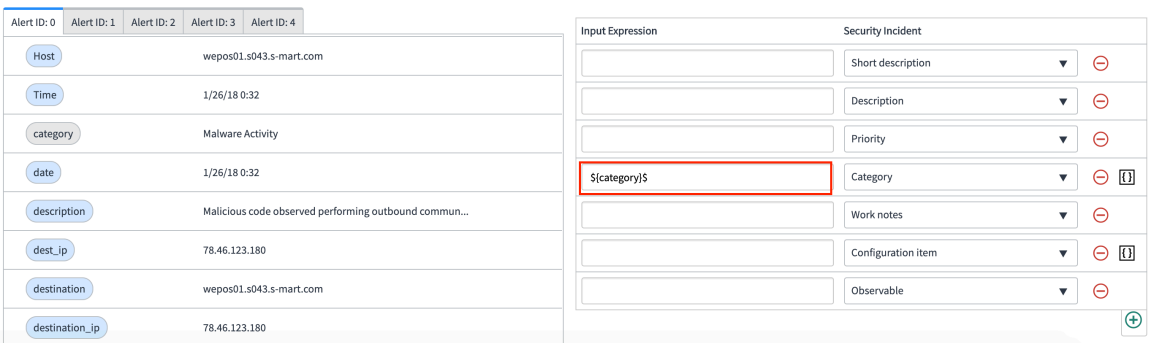
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, a categoria é mapeada para o campo de categoria no incidente de segurança. No entanto, você pode corresponder qualquer valor do lado esquerdo a um campo do lado direito. Verifique se o valor está mapeado corretamente no incidente de segurança durante a etapa de visualização.

Para ajudar a garantir que nenhum evento seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. Os campos azul claro à esquerda indicam que um campo ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de alerta de entrada a mais de um campo em um incidente de segurança.

Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação de cores ajuda a rastrear o mapeamento porque, em determinados casos, os campos de evento de alerta podem ser atribuídos apenas uma vez. Por exemplo, você só pode atribuir valores a campos como Descrição resumida uma vez. No entanto, você pode atribuir campos de lista, como Anotação de trabalho, várias vezes adicionando linhas adicionais à grade de mapeamento.

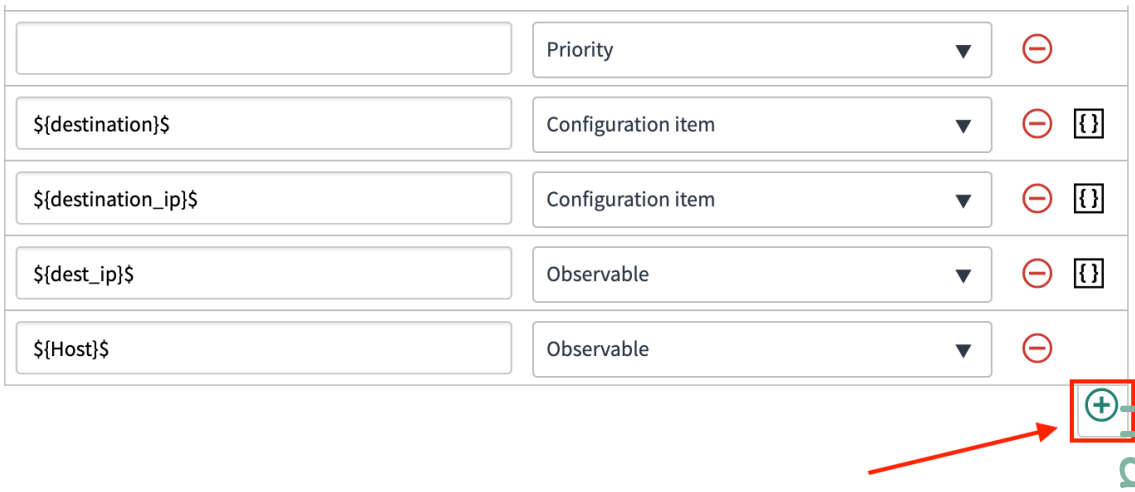


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Para adicionar campos ao mapeamento padrão do incidente de segurança no lado direito do formulário, siga estas etapas.

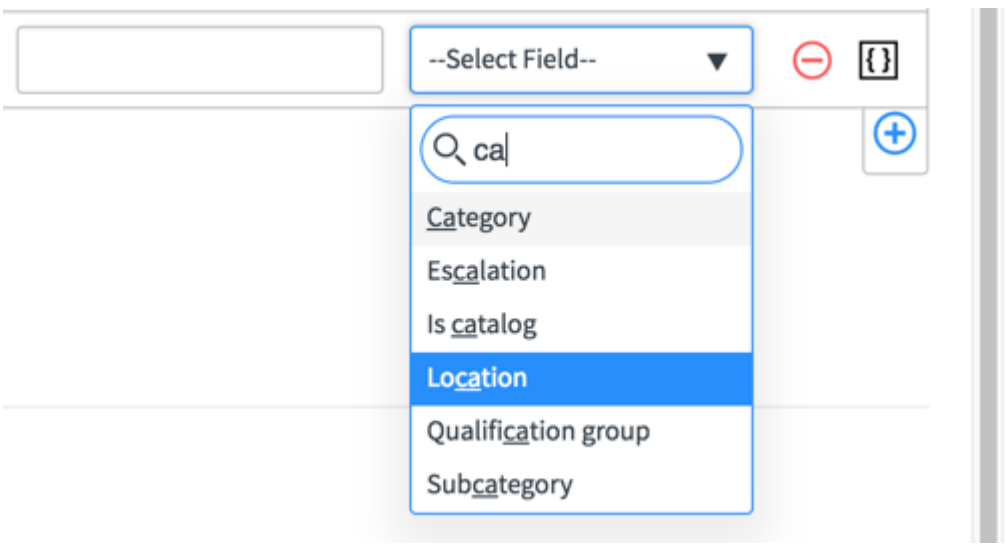
   a. À direita do formulário na seção Mapeamento de campo de incidente de SIR, na parte inferior da grade, clique no ícone de adição.



   Um novo campo é exibido.

   b. Na coluna Incidente de segurança, expanda a lista exibida e selecione um campo.

   Na lista expandida do novo campo, alguns campos estão sombreados. Na figura a seguir, Categoria tem um plano de fundo cinza porque foi mapeada no incidente de segurança. Semelhante à codificação de cores dos campos de alerta no lado esquerdo do formulário, essa codificação de cores para os campos de incidente de segurança à direita ajuda a rastrear o mapeamento.



Tradução automática

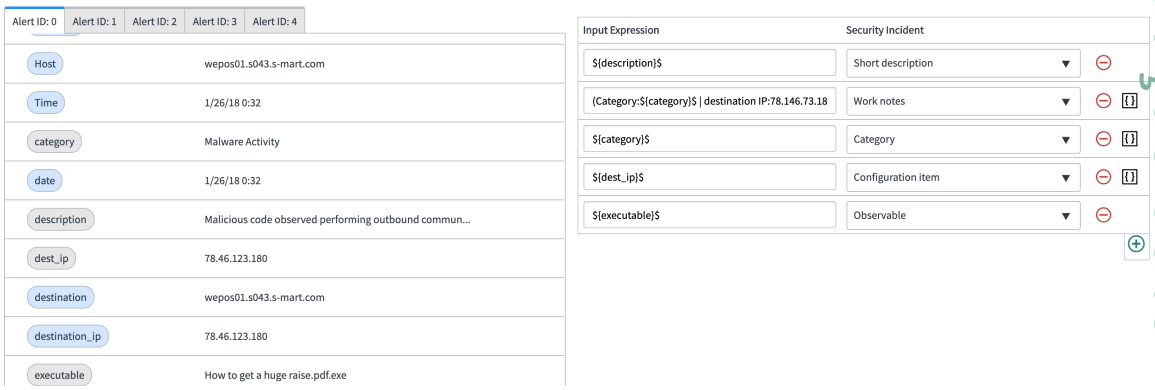
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Para que vários observáveis possam ser exibidos no mesmo incidente de segurança, o campo Observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho oferecem suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, será exibida uma mensagem de erro informando que não há nenhum valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista na qual você pode escolher várias opções e você tentar mapear uma opção para esse campo que não é exibido na lista, o campo não será preenchido no incidente de segurança.

c. Como alternativa, digite um valor no campo Pesquisar da nova linha.

d. No lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar o **ID de alerta** desejado no campo Expressão de entrada.
Com o recurso de arrastar, mapeie-o ao lado do novo campo.

8. Continue mapeando adicionando ou removendo campos e adicionando valores ao mapa.
A figura a seguir é um exemplo de uma grade de mapeamento editada. No campo inferior à direita, o campo Anotações de trabalho é adicionado e tem mais de um valor. Os valores são separados por espaços e sinais de pontuação (Category:${category} | IP de destino:78.146.73.180).



Na visualização, esses valores são exibidos nas Anotações de trabalho no incidente de segurança. Como o valor é para um campo que você adicionou à grade e há vários valores mapeados para o campo Anotações de trabalho, os valores são exibidos conforme inseridos. Neste exemplo, os espaços e os sinais de pontuação que você inseriu no campo são exibidos na seção Itens relacionados como uma anotação de trabalho na visualização do incidente de segurança.

A imagem a seguir é um exemplo de como os valores da imagem anterior são exibidos no incidente de segurança.

Condições de filtragem de geração de incidentes

9. Opcional: Depois de concluir as etapas de mapeamento no nível de campo anteriores, você pode usar os mesmos valores de campo no construtor de Condições de filtro para definir critérios adicionais que um alerta de entrada deve satisfazer para criar um incidente de segurança SIR.
Para definir condições de filtragem, siga estas etapas.

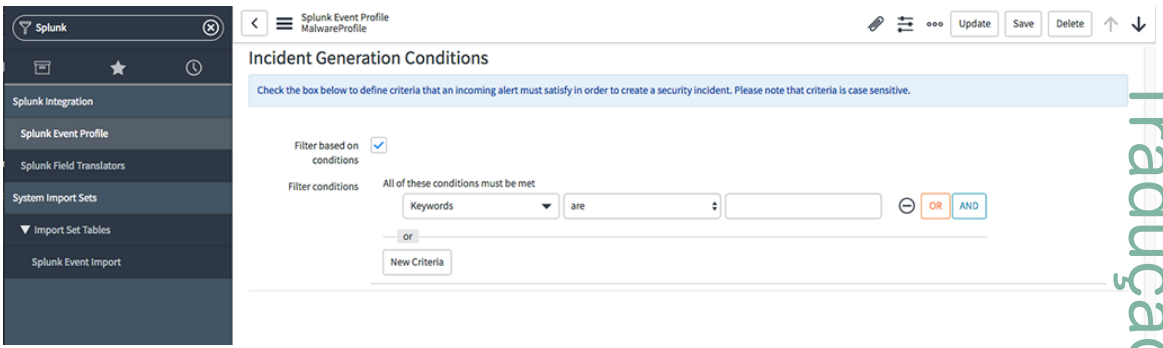
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Role até a seção Condições de geração de incidente no formulário e marque a caixa de seleção **Filtrar com base nas condições** para habilitar a opção.

(Optional) O construtor de Condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

As opções nas listas para o primeiro campo no construtor de Condições de filtro correspondem aos campos exibidos na seção Ingestão de amostra de alerta para o alerta que você ingeriu. Esses campos são dinâmicos e mudam dependendo do alerta Splunk que você ingere ou do evento que você encaminha manualmente. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas e devem corresponder exatamente aos valores do alerta ou evento Splunk Enterprise. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao console Splunk Enterprise e revisar seus alertas e eventos para as palavras-chave.

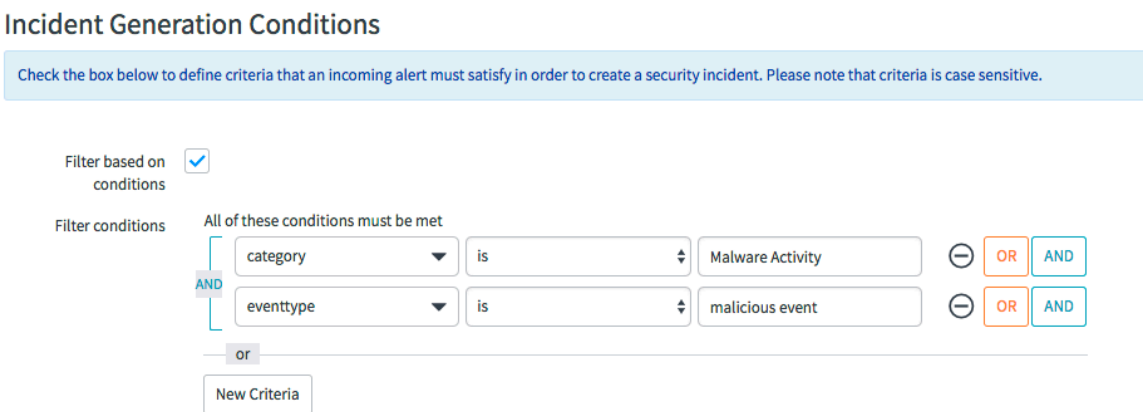


b. Usando as listas e os campos do construtor de condições, defina filtros para a primeira linha.

c. Para adicionar mais condições, à direita dos campos, clique em **E** ou **OU**.
Se **AND** for selecionado, todas as condições deverão ser correspondidas. Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida.

d. Opcional: Na segunda linha, defina uma segunda condição de filtro.

(Optional) A imagem a seguir é um exemplo com duas condições que devem ser correspondidas antes que os incidentes de segurança sejam criados.



(Optional) Você definiu as condições de gatilho para que os incidentes de segurança sejam criados somente quando ambas as condições de filtragem inseridas forem correspondidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

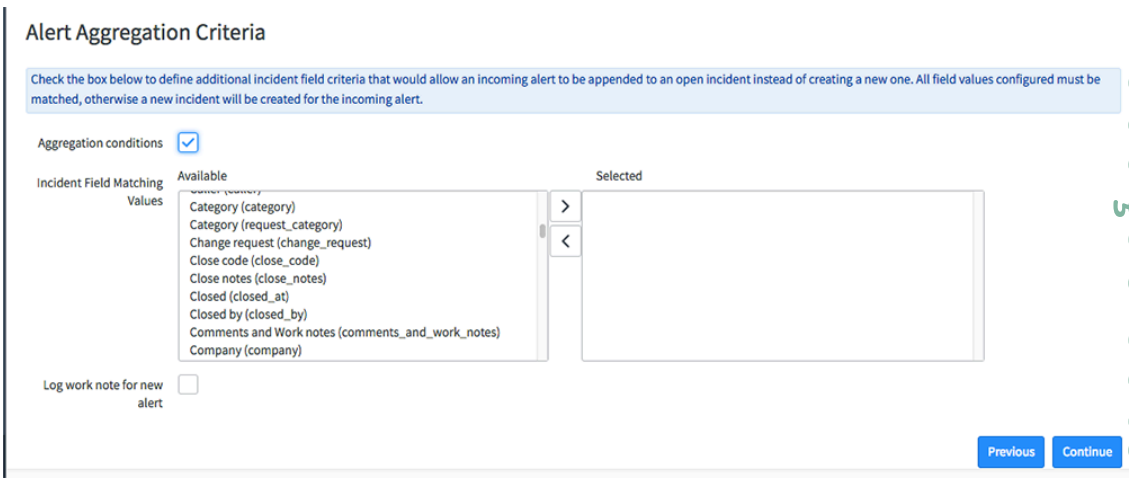
Esse tipo de filtragem ajuda a isolar eventos de segurança e limita o número de incidentes de segurança que você cria. Se critérios de filtragem adicionais forem definidos, somente os alertas necessários serão ingeridos sem precisar mudar a consulta Splunk ou a configuração do alerta acionado.

Alertas de agregação para evitar incidentes duplicados

10. **Opcional:** Para evitar a criação de incidentes de segurança duplicados, defina critérios de campo de incidente adicionais para que os alertas recebidos sejam agregados a um incidente de segurança em aberto. Para definir esses critérios, siga estas etapas.

    a. Role até a seção Critérios de agregação de alertas no formulário e marque a caixa de seleção Condições agregadas para habilitar essa opção.

    (Optional) As colunas Valores correspondentes do campo de incidente são exibidas. Esses nomes de campo são os campos no incidente de segurança que incluem todos os campos personalizados que estão configurados no incidente de segurança SIR.



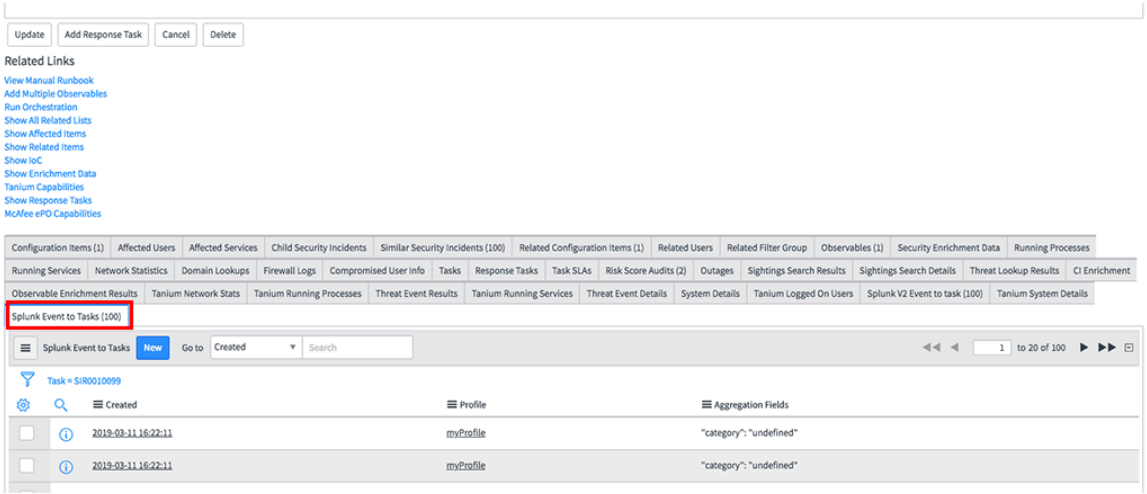
    b. Na lista Disponível, selecione os valores de campo que você deseja corresponder aos incidentes de segurança existentes no seu Now Platform e mova-os para a lista Selecionado.

    (Optional) Todos os valores de campo selecionados devem ser correspondidos para anexar este alerta de entrada a um incidente de segurança existente. Se você preferir revisar os valores de campo em incidentes de segurança a serem usados para esses critérios, navegue até **Incidentes** > **Mostrar todos os incidentes**.

    Se um novo alerta corresponder a todos os valores selecionados nas condições de campo de agregação na etapa de mapeamento, o alerta será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os alertas agregados adicionados em uma lista relacionada em um incidente de segurança. Todos os alertas agregados em um incidente de segurança são exibidos na lista relacionada Splunk de Evento para Tarefas. Esta lista detalha os carimbos de data/hora associados e os valores de campos agregados. Essas informações ajudam a entender por que os alertas são adicionados a incidentes de segurança existentes. Se esta guia não for exibida, role até o lado esquerdo do registro em Links relacionados e clique no link **Mostrar todas as listas** relacionadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Opcional: Para registrar uma anotação de trabalho para um novo alerta que foi adicionado recentemente ao incidente de segurança, marque a caixa de seleção para habilitar esta opção.
A anotação de trabalho registra que um novo alerta foi adicionado junto com um link para os detalhes do alerta.

Você mapeou com sucesso valores de um alerta ou evento Splunk para campos em um incidente de segurança SIR. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem. Você também anexou alertas ou eventos a incidentes de segurança SIR existentes.

11. Opcional: Abra o editor de script e continue editando.

(Optional) Para obter mais informações sobre o editor de script, consulte Use o editor de script para formatar valores de alerta para a integração Splunk Enterprise Event Ingestion.

12. Escolha um para continuar com a configuração do perfil.

O que Fazer Depois

A próxima etapa é visualizar os valores mapeados no incidente de segurança.

Visualizar o incidente de segurança para a integração Splunk Enterprise Event Ingestion

Depois de concluir a etapa de mapeamento, visualize os valores mapeados em um incidente de segurança Now Platform® Security Incident Response (SIR). Esta etapa de visualização permite que você verifique se mapeou todos os campos de alerta que deseja exibir no incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou para preencher dados ausentes. Se a visualização não for concluída com sucesso, você não poderá prosseguir para a etapa de programação.
As visualizações de SIR incidentes de segurança não são salvas como incidentes reais no produto SIR.

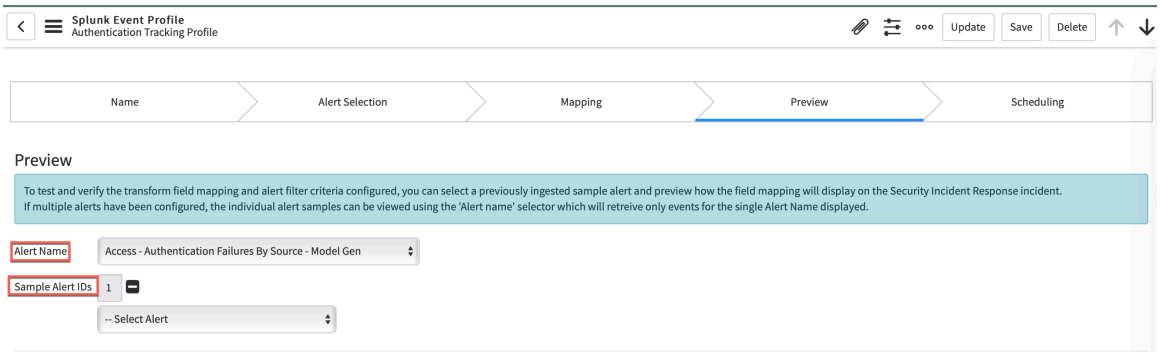
Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualizar** na barra de andamento.

2. Selecione o **Nome do alerta** e selecione um item na lista de **IDs de alerta de amostra**.

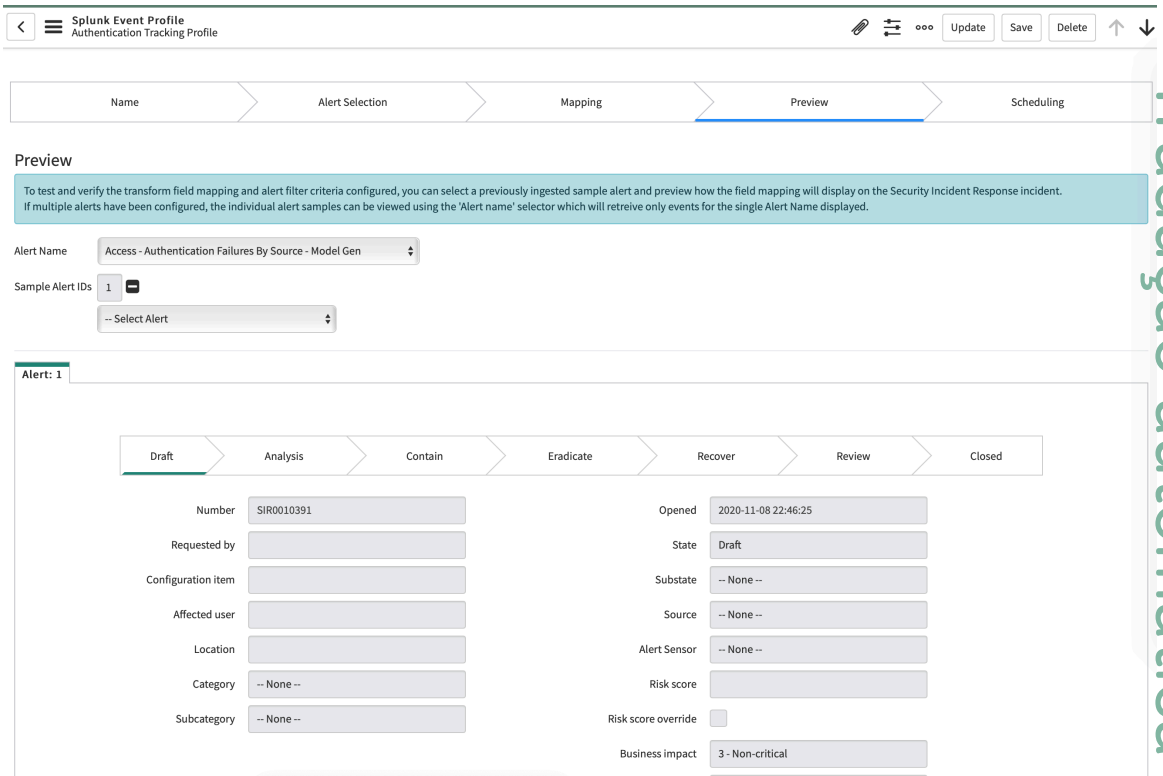
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O incidente de segurança é exibido. Não altere nenhuma informação nos campos. Esta exibição é somente leitura e um registro deste incidente de segurança não é salvo.

3. Revise o mapeamento de campo dos valores de alerta no incidente de segurança.



A imagem anterior é um exemplo de uma visualização com um erro de mapeamento. Neste exemplo, um campo no incidente de segurança não existe para um valor ou o campo não oferece suporte ao valor que você mapeou. Uma mensagem de erro é exibida indicando que um valor de entrada não foi encontrado para o campo Item de configuração.

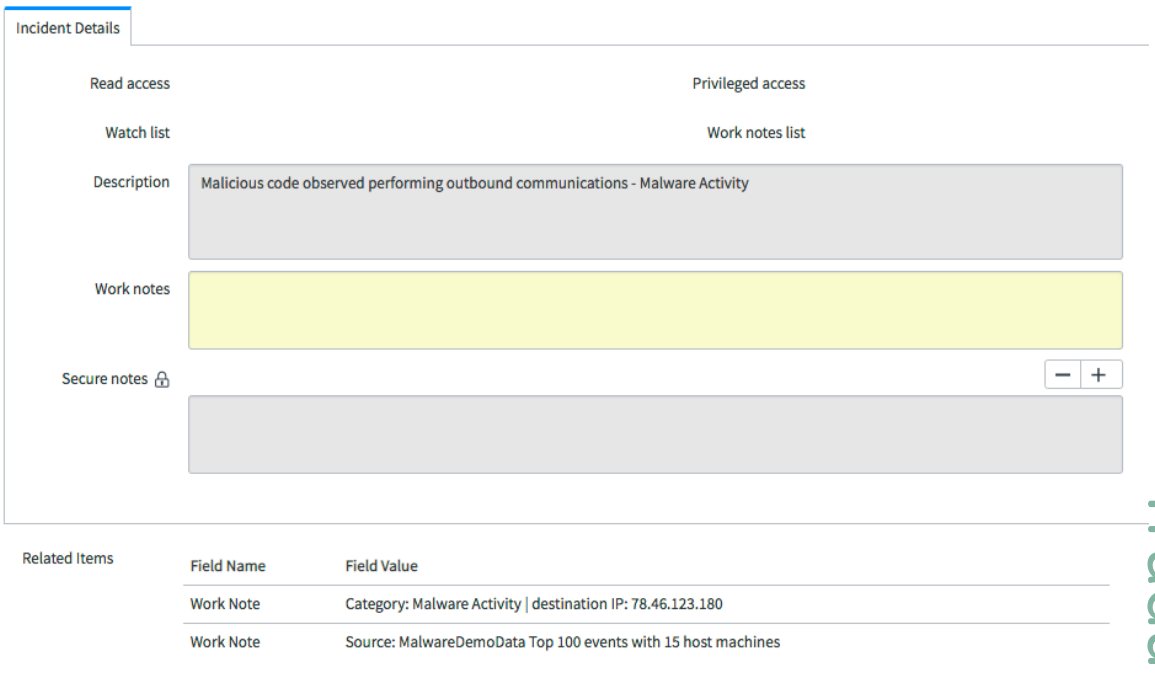
4. Para resolver esse erro, clique em **Mapeamento** na barra de andamento.
5. Edite o mapeamento para corrigir valores incorretos ou preencha os dados ausentes.
6. Visualize o mapeamento novamente e continue a corrigir os erros descritos nas mensagens de erro.

A figura a seguir é um exemplo da guia Detalhes do incidente na metade inferior de um incidente de segurança SIR depois que todas as mensagens de erro são resolvidas. Para este exemplo, os campos Descrição e Anotações de trabalho foram mapeados e esses campos são preenchidos com os valores dos pares de valores extraídos do console Splunk Enterprise. O primeiro campo Anotações de trabalho não tem valor. Este campo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

foi deixado em branco na grade de mapeamento durante a etapa de mapeamento. Os campos de anotações de trabalho adicionais que têm valores foram adicionados à grade de mapeamento durante a etapa de mapeamento.



7. Depois de corrigir todos os erros e verificar se os campos estão como você deseja, escolha uma opção para continuar.

O que Fazer Depois

Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campo no incidente de segurança, a próxima etapa será Programar e recuperar alertas para a integração Splunk Enterprise Event Ingestion.

Programar e recuperar alertas para a integração Splunk Enterprise Event Ingestion

Para perfis de ingestão de alertas automatizados, esta etapa é a etapa final da configuração do perfil de evento. Durante esta etapa, você pode verificar as configurações padrão para recuperação de alerta ou modificar a programação conforme necessário. Esta etapa permite filtrar a recuperação do alerta com base em um intervalo de datas.

Antes de Iniciar

Função necessária: função sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Depois de concluir todas as etapas na barra de andamento da configuração do perfil, conforme mostrado na figura a seguir, você concluiu a configuração dos perfis para encaminhamento manual de eventos. Não há programação disponível para eventos encaminhados manualmente do console Splunk Enterprise. Para perfis de ingestão de alertas automatizados, você escolhe se deseja incluir alertas históricos durante a etapa de Programação. Você também escolhe com que frequência pesquisará alertas futuros que correspondam à configuração do perfil de alerta.

Barra de andamento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

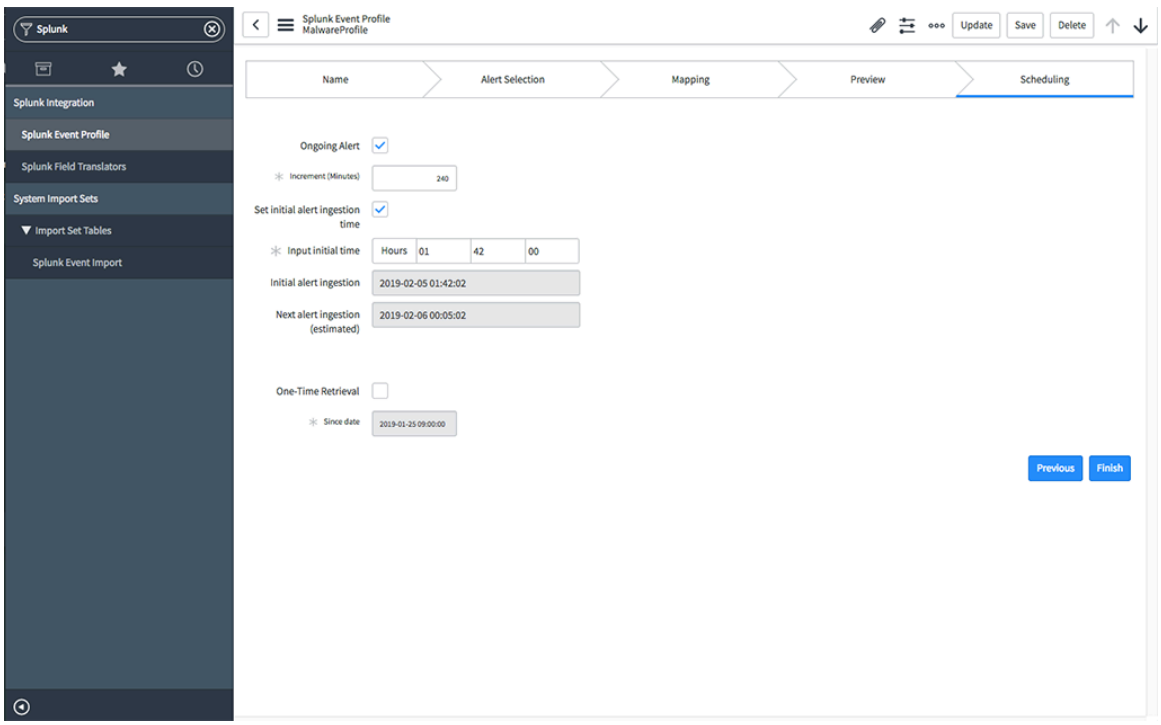
Para perfis de ingestão de alertas automatizados, antes de o perfil ser ativado, você verifica e modifica a programação e a recuperação do alerta. Esta etapa é a etapa final do processo de configuração do perfil de evento para perfis de alerta programado.

Configure esses intervalos de pesquisa por perfil. O desempenho da integração de ingestão de eventos Splunk é afetado pelos diferentes intervalos de pesquisa. Ao programar, talvez você prefira equilibrar a carga do sistema em relação à urgência do incidente. Um valor padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração com base na urgência do incidente e na carga antecipada em seu sistema.

No console Splunk Enterprise, você define um alerta a ser acionado com base em incrementos ou em um horário específico. Use esta configuração para ajudá-lo a configurar a programação na instância Now Platform para que os incrementos de tempo no console Splunk Enterprise sejam sincronizados com a programação configurada na instância Now Platform.

Procedimento

1. Se a página Programação na barra de andamento não for exibida, selecione **Programação**.
2. Escolha um para programar como e quando os alertas são extraídos do console Splunk Enterprise.



Como exemplo de programação, se você tiver um alerta diário Splunk que é executado uma vez por dia às 4h no horário local, é possível configurar o perfil de alerta correspondente em sua instância Now Platform para ser executado às 4h05 no horário local para capturar o alerta imediatamente e cria um incidente de segurança. Insira `04 05 00` no campo **Ingestão de alerta inicial**. No campo **Incrementar (minutos)**, insira `1440` (24 horas) para programar a próxima ingestão de alerta por 24 horas a partir da ingestão de alerta inicial. O tempo de ingestão do alerta inicial e o próximo tempo de ingestão do alerta são exibidos nos campos.

3. Para definir as configurações deste exemplo, siga estas etapas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Com a página Programação exibida, marque a caixa de seleção **Alerta contínuo** para habilitar esta opção.

b. No campo **Incrementar (minutos)**, insira `1440` (24 horas).

c. Clique na caixa de seleção **Selecionar ingestão de alerta inicial** para habilitar a edição dos campos Ingestão de alerta inicial e Próxima ingestão de alerta.

d. No campo Ingestão de alerta inicial, insira `04 05 00`.
No campo **Próxima ingestão de alerta (estimada)**, a hora da próxima ingestão de alerta é exibida.

4. Clique em **Concluir** para concluir a configuração.
Uma caixa de diálogo de confirmação é exibida. Você concluiu com êxito a instalação e a configuração da integração. Este perfil está ativado e extrai alertas do console Splunk Enterprise com base na sua programação. Há um limite de 1.000 incidentes de segurança que podem ser criados em um período de 24 horas. Até 100 eventos são por alerta acionado. Os eventos subsequentes serão ignorados depois que os limites forem atingidos.

Arquitetura de integração e conexão de sistemas externos para a integração Splunk Enterprise Event Ingestion

O tópico a seguir descreve a arquitetura de integração desenvolvida para oferecer suporte à ingestão de alertas acionados do console Splunk Enterprise. Essas informações esclarecem, em alto nível, a operação conceitual da integração. Ele também explica por que há etapas de configuração necessárias antes de instalar a aplicação do ServiceNow Store.

Termos-chave usados para esta integração

Os termos-chave a seguir são usados durante a instalação e a configuração. Para obter mais informações sobre esses termos, consulte o site de Documentação do produto da ServiceNow e o site e recursos do Splunk na página Recursos do Splunk.

Now Platform

Um produto empresarial ServiceNow. O Now Platform é a base sobre a qual componentes individuais, como Security Incident Response (SIR), IT Service Management (ITSM) e outros produtos são criados.

ServiceNow Complemento Splunkbase

Uma aplicação ServiceNow que é instalada no console Splunk Enterprise que oferece suporte à opção de encaminhamento de evento manual da integração. O encaminhamento manual de eventos é um recurso opcional da integração. Este ServiceNow addon Splunkbase não é necessário para a ingestão de alerta automatizada fornecida pela integração.

Security Incident Response (SIR)

Uma aplicação Now Platform que rastreia o andamento dos incidentes de segurança desde a descoberta e a análise inicial, passando pela contenção, erradicação e recuperação, até a revisão e fechamento pós-incidente finais.

Splunk Enterprise

Um produto de gestão de eventos de incidentes de segurança (SIEM) ou serviço em nuvem que coleta dados usados para análise e gestão de incidentes. Este serviço está em um host que às vezes também é conhecido como console Splunk neste guia.

Splunk alerta

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma pesquisa que você configura e salva em Splunk para verificar dados específicos com base nos parâmetros configurados no serviço Splunk Enterprise. Ao extrair alertas de Splunk, você também extrai todos os eventos associados a esse alerta.

Splunk alerta acionado

Uma pesquisa configurada no console Splunk Enterprise que retorna resultados e sinaliza esses resultados como alertas acionados. Os alertas acionados são ingeridos do console Splunk para sua instância Now Platform para esta integração. Os alertas acionados têm um ou mais eventos Splunk.

Splunk evento

Um ou mais elementos de dados que resultam nos alertas acionados do serviço Splunk. Na sua instância Now Platform, você pode pesquisar quais eventos [Splunk acionaram Now Platform incidentes de segurança.

MID Server

Esta aplicação facilita a comunicação e a movimentação de dados entre Now Platform e aplicações externas, fontes de dados e serviços. Esta aplicação é normalmente necessária para integração com tecnologias no local e, para esta integração Splunk Enterprise Event Ingestion, o MID Server facilita a comunicação entre o Now Platform e a instância local de Splunk Enterprise. Um MID Server não é necessário se você estiver integrando sua instância Now Platform com uma instância Splunk Cloud.

Administrador de incidentes de segurança (sn_si.admin)

O usuário com esta função supervisiona a configuração da integração com o produto SIR em sua instância Now Platform.

Analista de incidentes de segurança (sn_si.analyst)

O usuário com esta função interage com e analisa incidentes de segurança no produto ServiceNow Security Incident Response.

Conexão de sistemas externos

Um perfil de evento é um contêiner que você cria, nomeia e configura para uma conexão única e chama o serviço Splunk para extrair os alertas acionados mais atuais que correspondem a critérios específicos. Depois que os alertas acionados que correspondem ao seu perfil forem extraídos de Splunk, selecione qual desses alertas deseja exibir como um incidente de segurança Now Platform Security Incident Response SIR. Uma exibição padrão dos campos de alerta Splunk Enterprise está disponível e você edita este mapeamento de campos de alerta para os campos em um incidente de segurança SIR para atender às suas necessidades. Você visualiza seu mapeamento para verificar se todos os valores de campo de alerta necessários estão preenchidos no incidente de segurança SIR. Para concluir a configuração do perfil de alerta, programe a recuperação de alertas e ative o perfil. Depois de ativar o perfil no Now Platform, você está pronto para incluir alertas históricos e em andamento Splunk automaticamente.

Como um usuário com a função sn_si.admin, se você determinar que um novo alerta acionado é semelhante aos alertas ingeridos anteriormente, poderá agregar novos alertas acionados a incidentes de segurança SIR existentes. Você define critérios para especificar valores de campo de destino correspondentes no perfil de alerta Splunk Enterprise que definem quando um incidente de segurança existente é atualizado e quando um novo incidente de segurança é criado. Se o recurso de agregação estiver habilitado no seu perfil de evento, quando o conjunto de importação for transformado, sua instância Now Platform verificará se há um registro existente na tabela de destino que tenha o mesmo valor nos campos de destino e de origem. Se um registro existente com um valor correspondente na tabela de destino for encontrado, esse registro será atualizado. Se nenhum registro correspondente for encontrado, um novo registro será criado na tabela de destino. Se

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

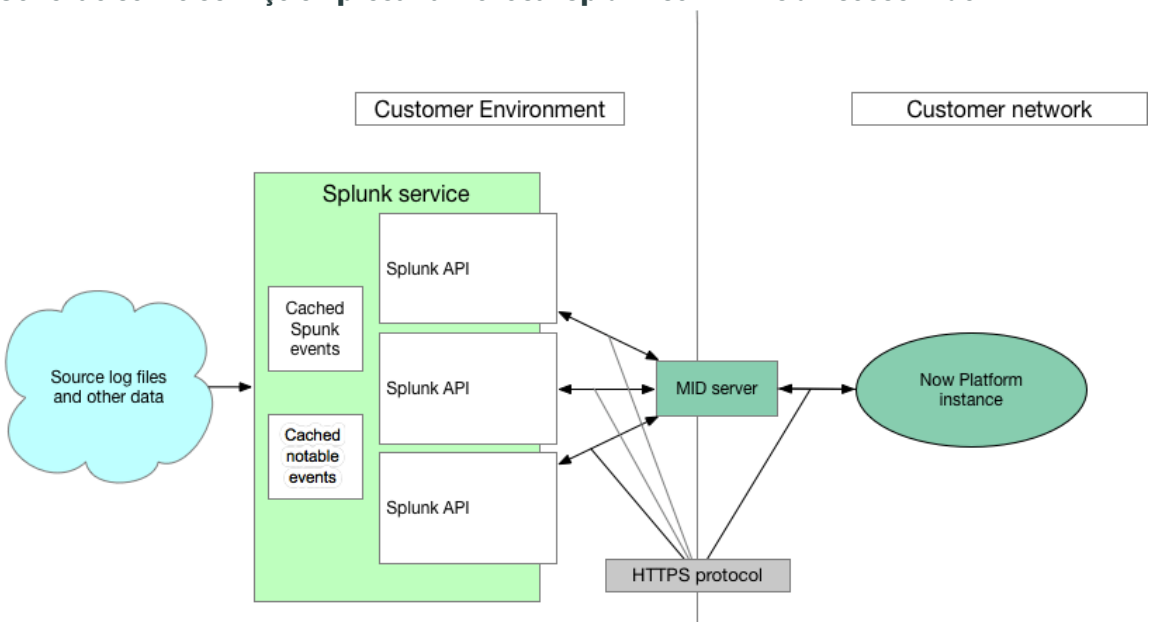
habilitada, a opção de agregação atualiza os incidentes de segurança existentes com novos alertas acionados e você evita a criação de vários incidentes de segurança. Para obter mais informações sobre como atualizar registros usando opções de agregação, consulte Atualização de registros usando aglutinação .

Esta aplicação usa o serviço de API Splunk para recuperar informações do serviço Splunk. Uma conexão HTTPS de saída do MID Server para este ambiente é necessária para que a integração funcione corretamente.

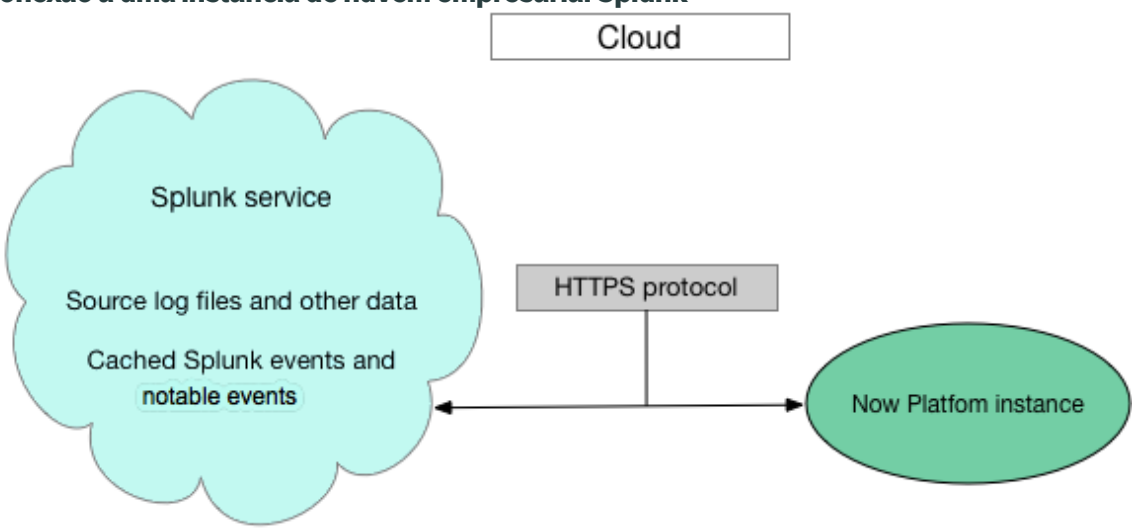
Depois de conectada ao serviço Splunk, a integração oferece suporte à extração e ingestão de alertas e eventos acionados que acionam incidentes de segurança.

O fluxo de dados básico é ilustrado nas imagens a seguir. Em cada figura, seu Now Platform está extraindo (ingerindo) dados. Splunk não está inserindo dados para alertas programados.

Conexão com o serviço empresarial no local Splunk com MIDs únicosservidor



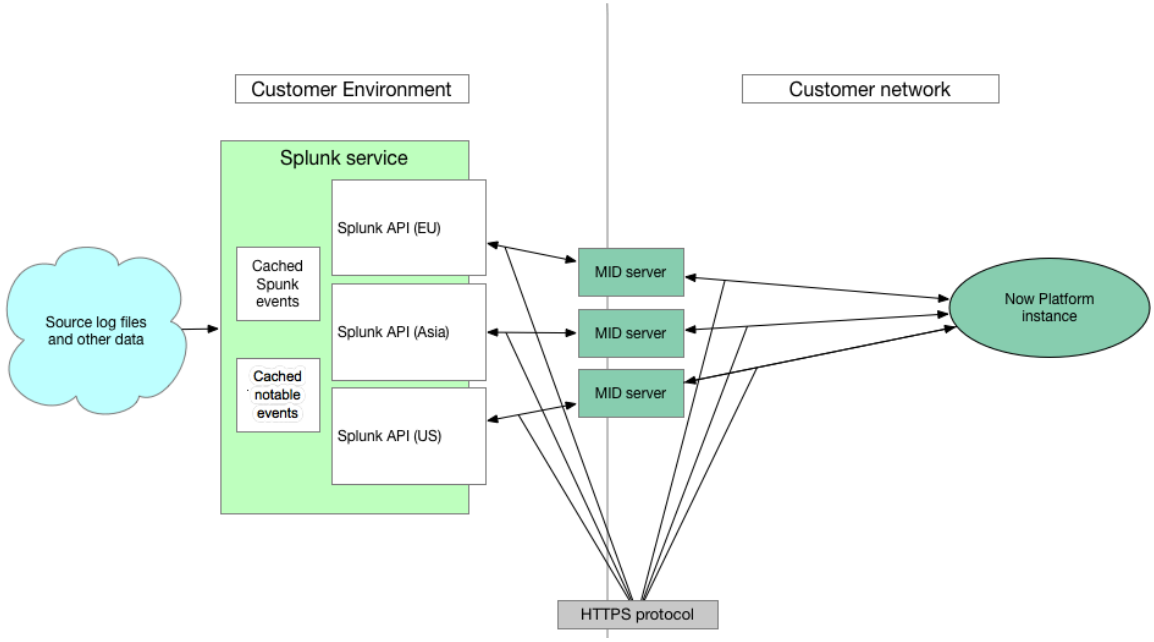
Conexão a uma instância de nuvem empresarial Splunk



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Várias conexões com o serviço corporativo Splunk usando vários MID Servers



Copiar Splunk Enterprise Event Ingestion perfis de uma instância para outra usando a funcionalidade de exportação/importação

Você pode exportar e importar configurações de perfis [Splunk Enterprise Event Ingestion de uma instância Now Platform para uma instância Now Platform diferente.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Esta funcionalidade permite que o administrador de segurança copie perfis que foram testados e verificados em uma instância Now Platform, por exemplo, em não produção, para outra instância Now Platform, por exemplo, produção, sem a necessidade de refazer todas as definições de configuração. As configurações exportadas e importadas incluem nome do perfil, regras de correlação, mapeamentos, filtros, critérios de agregação, traduções de campos, dados de amostra obtidos, programação e informações de origem do bloco de configuração.

Nota:
Quando você exporta um tipo de perfil de encaminhamento de evento manual, os dados de anexo usados para o mapeamento de campo de amostra são copiados, no entanto, o arquivo de anexo em si não é exportado.

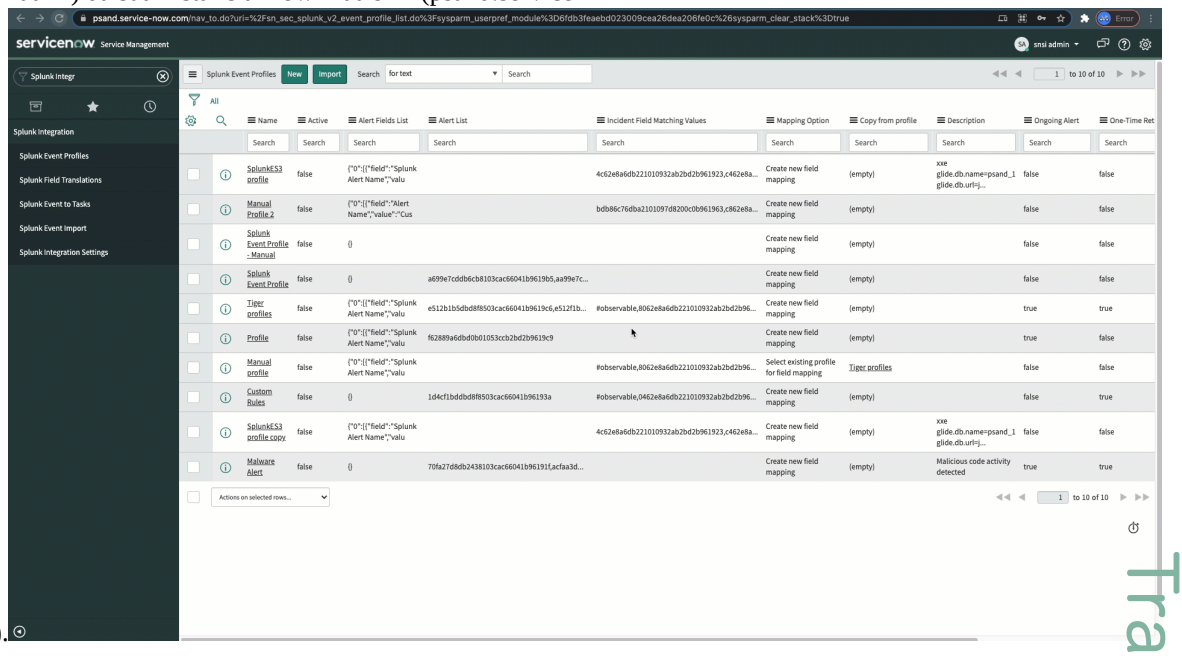
Procedimento

1. Navegar até **Todos** > **Splunk Integration** > **Perfis de evento do Splunk**.
2. Selecione um perfil que você deseja exportar para outra instância Now Platform.
   Você pode selecionar vários perfis para exportação.
3. No menu Ações, clique em **Exportar**.
4. Quando a mensagem de conclusão da exportação for exibida, clique em **Download**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ilustração a seguir mostra a exportação de um perfil Splunk (Perfil Manual 2) da sua instância Now Platform (psand.service-now.com).



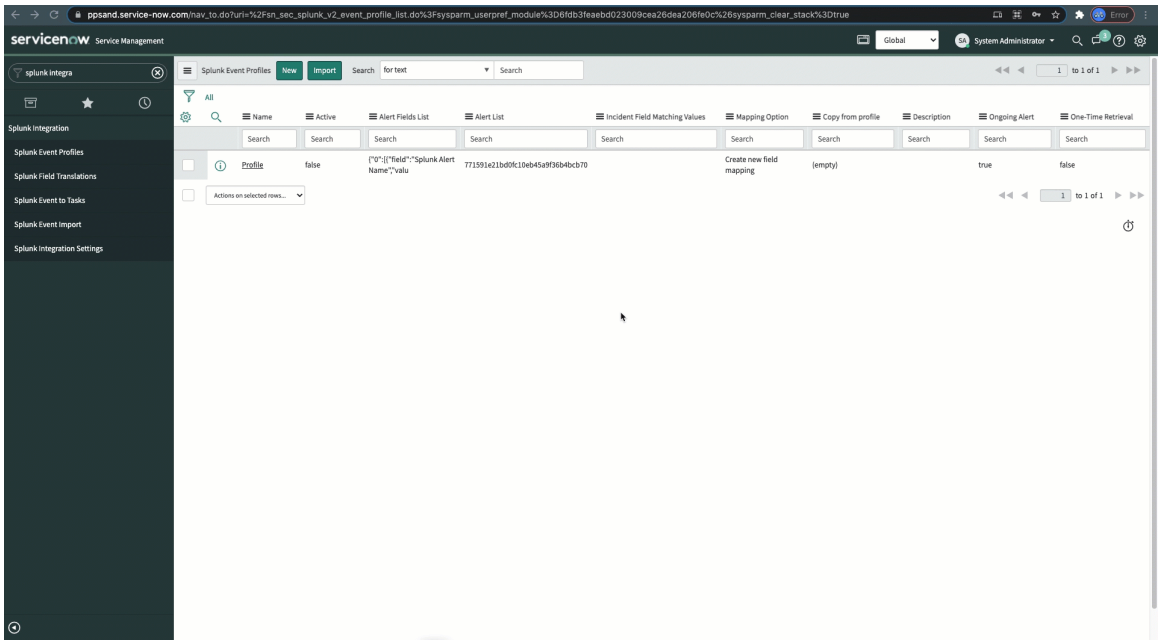
O arquivo payload.xml exportado é baixado no seu computador. O arquivo contém o nome do perfil, regras de correlação, mapeamentos, filtros, critérios de agregação, traduções de campos, dados de amostra obtidos, programação e informações de origem do bloco de configuração. Quando você seleciona e baixa vários perfis, eles aparecem no mesmo arquivo payload.xml.

Agora você pode prosseguir para importar o perfil em outra instância Now Platform.

5. Navegar até **Splunk Integration** > **Perfis de evento do Splunk**.
6. Clique em **Importar**.
7. Clique **em Escolher arquivo** e selecione o arquivo xml no seu computador.
8. Clique em **Carregar**.
9. Clique **em Fechar e Recarregar Perfis**.
   A ilustração a seguir mostra a importação de um perfil Splunk (Manual Profile 2) da instância Now Platform (psand.service-now.com) para outra instância Now Platform (ppsand.service-now.com).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você importou com sucesso o perfil de outra instância Now Platform.

Verifique se a origem exportada (Splunk conta da API e Splunk URL do servidor) e as configurações do MID Server são válidas e estão disponíveis na instância Now Platform importada. Atualize sua configuração Splunk Enterprise Event Ingestion, se necessário.

10. **Opcional:** Verifique as configurações do MID Server após importar um perfil.
11. **Opcional:** Navegar até **Security Operations** > **Configurações de Integração**.
12. **Opcional:** Selecione o bloco de configuração Splunk Enterprise Event Ingestion e clique em **Atualizar**.
13. **Opcional:** Revise e atualize a origem e os detalhes do MID Server conforme necessário.

Copiar um perfil de evento para a integração Splunk Enterprise Event Ingestion

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, convém copiar os perfis de alarme para economizar tempo.

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Copiar um perfil existente e suas configurações associadas é opcional.

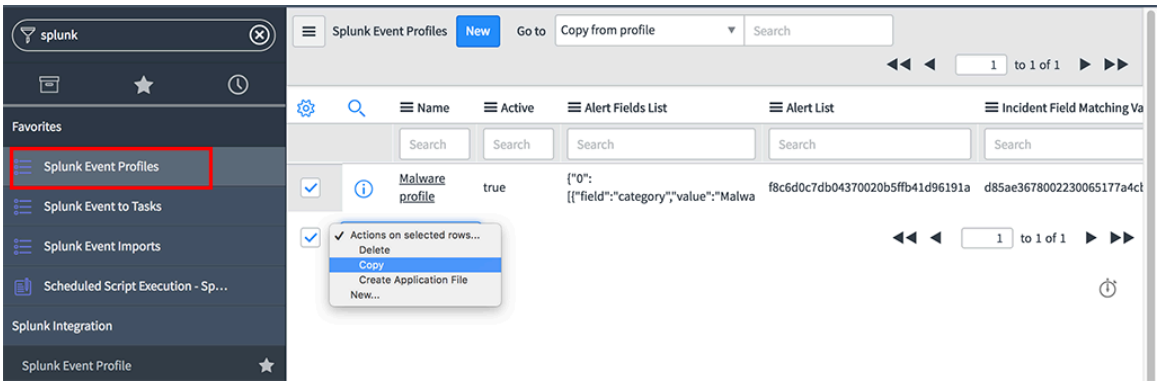
Se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado está desabilitado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Procedimento

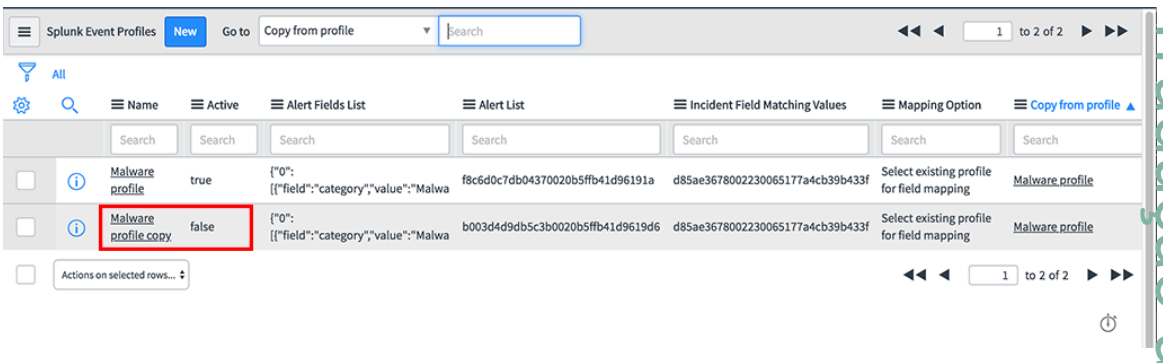
1. Navegar até **Todos** > **Splunk Integration** > **Perfil de evento do Splunk**.
2. Na lista Splunk Perfis de evento exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Copiar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo o mapeamento e a configuração de programação. O nome do perfil contém cópia. Embora o perfil original esteja habilitado (verdadeiro), a cópia está desabilitada neste ponto (falso). Você pode editar os valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil, conforme necessário.



Você copiou com sucesso as configurações de um perfil existente para um novo perfil.

O que Fazer Depois

Você será solicitado a ativar (habilitar) o novo perfil depois de concluir as etapas de configuração.

Configure seu ambiente Splunk para ingestão manual de eventos para a integração de ingestão de eventos Splunk Enterprise

Se você quiser exportar eventos manualmente e sob demanda do console Splunk Enterprise para esta integração, instale e configure o aplicativo ServiceNow Security Operations Event Ingestion Addon para Splunk Enterprise no console corporativo Splunk ou na instância do Splunk Cloud.

Antes de Iniciar

Verifique se você instalou a aplicação para esta integração do ServiceNow Store antes de instalar o plug-in do complemento do splunkbase que é necessário para a ingestão manual de eventos. Se você não instalou o aplicativo para a integração do ServiceNow Store, consulte Instalar e configurar a aplicação ServiceNow para a integração Splunk Enterprise Event Ingestion e siga as instruções para instalá-lo.

Função necessária: Now Platform administrador (admin)

Por Que e Quando Desempenhar Esta Tarefa

A instalação e configuração do Complemento de ingestão de eventos do Security Operations ServiceNow é opcional.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você quiser exportar eventos manualmente e sob demanda do console Splunk Enterprise para a integração, baixe, instale e configure o ServiceNow Complemento de ingestão de eventos do Security Operations para Splunk Enterprise do splunkbase no console Splunk Enterprise.

Este complemento de extensão ServiceNow é necessário para que os incidentes de segurança possam ser criados a partir de eventos exportados manualmente em sua instância Now Platform. Esta aplicação ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise está disponível em splunkbase .

Para o encaminhamento manual de eventos, você pode identificar até dois Now Platform endpoints (instâncias) diferentes no console Splunk Enterprise. Você encaminha os eventos para o endpoint ou endpoints manualmente para criar incidentes de segurança. Por exemplo, você pode especificar uma instância de preparação (desenvolvimento) e uma instância de produção. Ao especificar instâncias separadas e nomear fluxos de trabalho primários e secundários para cada instância, você pode escolher para onde deseja encaminhar eventos diferentes.

Procedimento

1. Se você ainda não instalou o ServiceNow Complemento de ingestão de eventos do Security Operations para Splunk Enterprise, siga estas etapas para instalá-lo e configurá-lo.

   a. Navegue até splunkbase .

   b. Pesquise o ServiceNow Security Operations Complemento de ingestão de eventos do Security Operations para Splunk Enterprise.

   Nota:
   Verifique se você selecionou ServiceNow Security Operations Complemento de ingestão de eventos para Splunk Enterprise. Há complementos ServiceNow adicionais que são exibidos nesta lista. Esses complementos são para diferentes integrações ServiceNow Splunk e não são necessários para esta integração.

   c. Baixe a aplicação.

   d. Abra sua conta Splunk Enterprise.

   e. Na página Aplicativos, clique no ícone de engrenagem ou no atalho **Gerenciar aplicativos** na lista suspensa do menu.

   f. No canto superior esquerdo da página Aplicativos exibida, clique em **Instalar aplicativo do arquivo**.

   g. Clique em **Escolher arquivo**, selecione ServiceNow Complemento de ingestão de eventos do Security Operations para Splunk Enterprisee clique em **Carregar**.

   h. Se solicitado, reinicie Splunk Enterprise.
   O ServiceNow Complemento de ingestão de eventos do Security Operations para Splunk Enterprise está instalado no console empresarial Splunk Enterprise. A próxima etapa é configurar o complemento.

2. Para configurar o complemento, siga estas etapas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Em Splunk Enterprise, clique no ícone de engrenagem de **aplicativos** ou em **Gerenciar aplicativos** na lista suspensa do menu.

b. Na lista de aplicações exibida, na coluna **Ações**, clique em **Configurar** para ServiceNow Security Operations Complemento de ingestão de eventos para Splunk Enterprise.

c. Preencha o formulário.

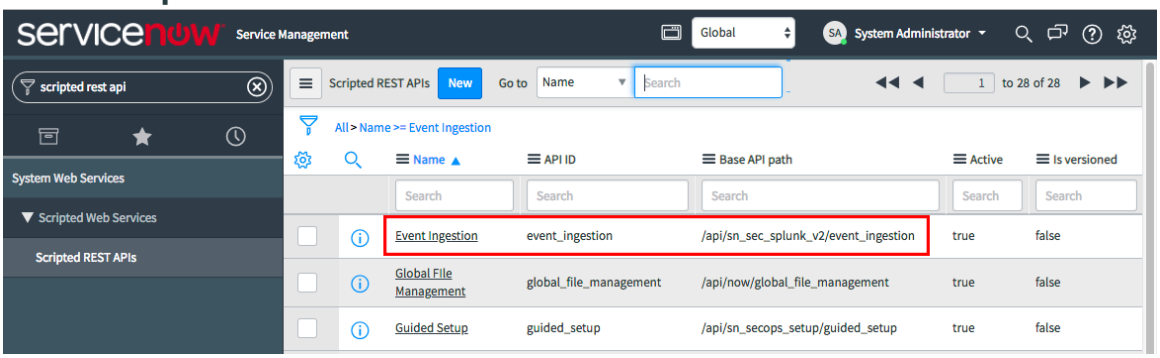
A figura a seguir é um exemplo de um formulário preenchido no console Splunk Enterprise.

A figura a seguir é um exemplo da lista de Scripted REST APIs em seu Now Platform. A lista exibe o local do valor do endpoint de uma instância Now Platform que você insere no formulário como parte da configuração da extensão ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise no console Splunk Enterprise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista de Scripted REST APIs na Now Platform



3. No formulário de configuração do console Splunk Enterprise, clique em **Salvar** para salvar suas edições.

   Após alguns momentos, na parte superior esquerda do formulário no console Splunk Enterprise, será exibida uma mensagem informando que o registro foi atualizado com sucesso.

   Depois de salvar o formulário, os nomes (rótulos de ação de fluxo de trabalho) das instâncias Now Platform que você criou no formulário estão disponíveis na lista de seleção Ações de evento em um evento selecionado de uma pesquisa no console Splunk Enterprise.

O que Fazer Depois

Se você ainda não salvou pesquisas no console Splunk Enterprise, a próxima etapa é salvar pesquisas como alertas no console Splunk Enterprise.

Salvar pesquisas no console Splunk Enterprise para a integração Splunk Enterprise Event Ingestion

As etapas a seguir para salvar pesquisas no console Splunk Enterprise são fornecidas para um usuário com a função de administrador Splunk Enterprise.

Antes de Iniciar

Se você já tiver pesquisas salvas e alertas acionados no console Splunk Enterprise, não será necessário modificar essas pesquisas para esta integração.

A integração do produto Now Platform® Security Operations com o serviço de notificação de evento Splunk extrai informações de evento e alerta de Splunk.

Antes de ingerir alertas em seu ambiente Security Operations, configure as pesquisas no console Splunk Enterprise para que você extraia automaticamente os eventos de segurança relevantes em Splunk Enterprise que deseja salvar como alertas.

Se você não tiver pesquisas salvas e alertas acionados estabelecidos para notificação quando ocorrerem eventos de segurança importantes no console Splunk Enterprise, siga estas etapas para salvar pesquisas.

Função necessária: Splunk Enterprise administrador

Procedimento

1. Faça login na sua conta Splunk Enterprise.
2. Clique na guia **Pesquisar**.
3. No campo Nova pesquisa exibido, insira um valor para o alerta, por exemplo, Malware.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Para exibir os eventos relacionados à sua pesquisa, à direita do campo Nova pesquisa, clique no ícone de pesquisa ou pressione Enter.
   Os resultados da pesquisa com eventos são exibidos.
5. Para salvar a pesquisa como um alerta, no canto superior direito da página, expanda a lista de seleção Salvar como e selecione **Alerta**.
6. No formulário exibido, preencha os campos.
7. Clique em **Salvar**.
   Seu alerta é salvo e exibido na guia Alertas na página Pesquisar.
   O serviço Splunk extrai os eventos correspondendo aos critérios que você configurou no alerta. Ele armazena em cache os eventos e você solicita esses eventos dos perfis configurados na sua instância Now Platform. Como a extração de ingestão de eventos ocorre de um cache no serviço Splunk, essa ingestão de Now Platform não afeta o desempenho na plataforma Splunk.

O que Fazer Depois

Você concluiu com sucesso a configuração necessária para a integração no console do Splunk Enterprise. Se você ainda não instalou a aplicação para a integração de ServiceNow Store, a próxima etapa é instalar a aplicação para a integração e configurá-la.

Use o editor de script para formatar valores de alerta para a integração Splunk Enterprise Event Ingestion

Use o editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento.

Antes de Iniciar

Além dos campos mapeados diretamente dos valores de alerta extraídos e dos valores de alerta inseridos manualmente, você pode opcionalmente usar o editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. O editor de script muda os valores de um alerta Splunk para que os valores compatíveis com o incidente de segurança Now Platform® Security Incident Response sejam mapeados para os campos Categoria, Item de configuração (IC) e Observável.

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

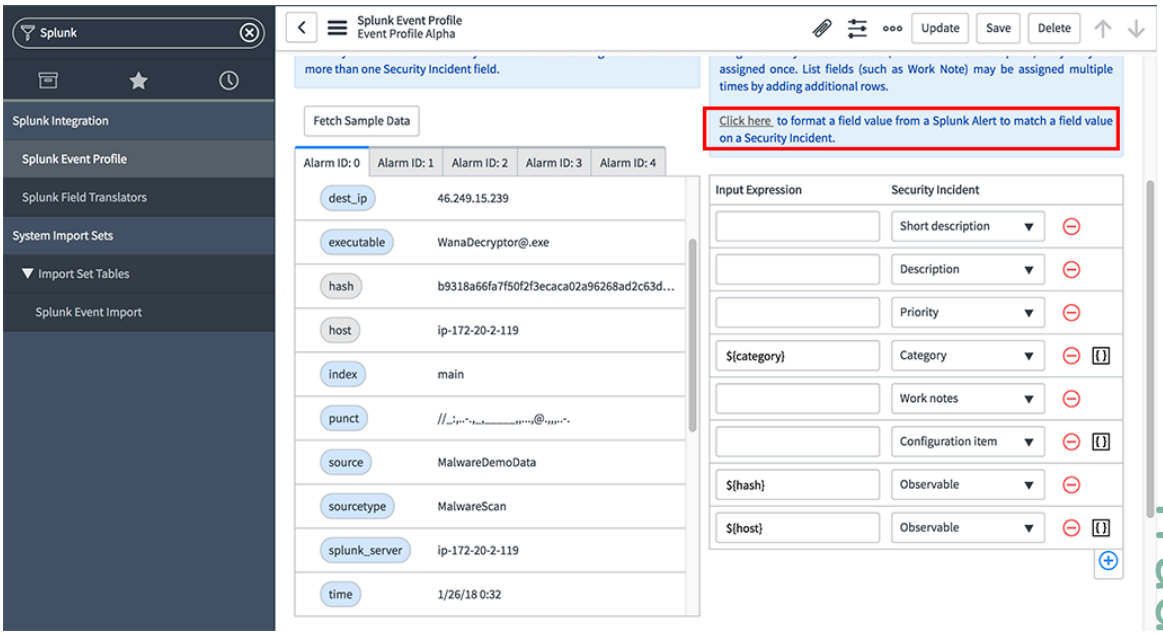
Em determinados casos, os valores de alerta Splunk Enterprise são mapeados para os campos Categoria, Item de configuração (IC) e Observável no incidente SIR e não são compatíveis. Você pode preferir editar os valores mapeados. Se você quiser traduzir o valor de um alerta Splunk Enterprise para um valor que seja compatível com esses campos no incidente de segurança SIR, use o editor de script.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Com o formulário de mapeamento exibido, clique no link para abrir o editor de script.

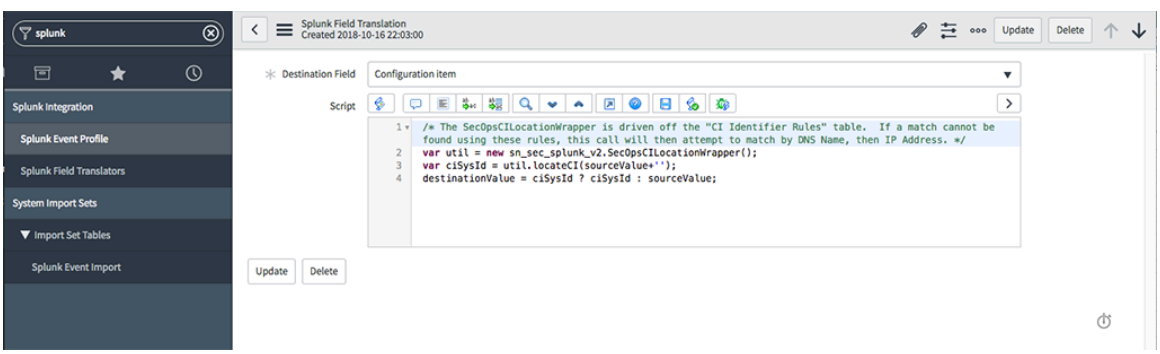


2. Na lista de seleção, selecione um campo de destino para o valor que você deseja editar.
3. Como alternativa, na seção Mapeamento de campo de incidente de SIR, clique no ícone de colchete [{}] ao lado de um campo para abrir o editor de script desse campo.

   Em determinadas instâncias, uma inclusão de script pode ser apropriada para o campo Item de configuração. Para um alerta, por exemplo, um valor para o Item de configuração pode não ser correspondido.

   Conforme mostrado na figura a seguir, se uma correspondência para um nome de host não puder ser encontrada no Now Platform® CMBD para o campo Item de configuração, você poderá editar a regra para que, se um endereço IP for encontrado, ele preencha o campo Item de configuração. Se não houver valor para o alarme, o campo no incidente de segurança será definido como nulo.

   O editor é aberto com o campo exibido no Campo de destino. A imagem a seguir mostra o editor com o campo Item de configuração como o Campo de destino.



4. Insira as mudanças no script e clique em **Atualizar** para salvar as mudanças.
   A tabela Splunk Traduções de campo é exibida.
5. Feche a tabela para retornar ao formulário de mapeamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list para a integração Splunk Enterprise Event Ingestion

Use esta check-list para orientar você em todas as tarefas da integração. A check-list a seguir inclui tarefas de configuração e instalação e exemplos de casos de uso que incluem os resultados esperados para a integração.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Acompanhe seu progresso com a instalação e configuração da integração com a tabela a seguir. Conclua todas as tarefas de uma etapa antes de passar para a próxima. Cada linha da tabela lista as tarefas e identifica as funções necessárias para executar as tarefas. Tópicos numerados do guia de instalação e configuração também são referenciados.

Funções necessárias: as funções são listadas para cada etapa abaixo.

Procedimento

1. Como um usuário com a função de administrador Now Platform, configure sua instância Now Platform.
   - Atribua usuários com as funções sn_si.admin e sn_si.analyst conforme necessário.
   - Instale e configure um MID Server se o servidor Splunk for implantado em sua rede corporativa.
   - Verifique se os plug-ins ServiceNow Security Incident Response estão ativados para sua versão do Now Platform.
   - Se você quiser encaminhar eventos manualmente do console [Splunk Enterprise para a instância Now Platform, verifique se você atribuiu a função (sn_sec_splunk_v2.api_account_access) a um usuário com a permissão de administrador da empresa Splunk Enterprise.

   Para obter mais informações, consulte Configure sua instância Now Platform para a integração Splunk Enterprise Event Ingestion.

   Você concluiu com sucesso as etapas de configuração e verificou os resultados esperados para a integração.
2. Como um usuário com a função de administrador Now Platform, instale e configure a aplicação Splunk Enterprise Event Ingestion do ServiceNow Store.
   a. Baixe e instale a aplicação na sua instância Now Platform.
   b. Configure a aplicação e conecte ao seu console Splunk Enterprise.

   Para obter mais informações, consulte Instalar e configurar a aplicação ServiceNow para a integração Splunk Enterprise Event Ingestion.
3. **Opcional:** Se você pretende exportar eventos manualmente do console [Splunk Enterprise para a instância Now Platform, execute as seguintes tarefas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Como administrador Splunk Enterprise, instale, configure e habilite o ServiceNow Complemento de ingestão de eventos do Security Operations para Splunk Enterprise do splunkbase no console do Splunk Enterprise.

b. Como administrador Splunk Enterprise, se ainda não estiver configurado, salve pesquisas como alertas no console Splunk Enterprise.

(Optional) Para obter mais informações, consulte Configure seu ambiente Splunk para ingestão manual de eventos para a integração de ingestão de eventos Splunk Enterprise e Salvar pesquisas no console Splunk Enterprise para a integração Splunk Enterprise Event Ingestion.

4. Como um usuário com a função Now Platform sn_si.admin, crie e nomeie um perfil de evento.

Selecione o tipo de perfil na lista de seleção. As opções são um perfil de alerta programado que você usa para ingerir dados de amostra ou um perfil de evento que você usa para exportar dados de anexo manualmente do seu console Splunk Enterprise.

- Para um alerta programado, selecione um alerta disponível.
- Para o perfil de dados exportados manualmente, crie um novo mapa ou copie um mapa existente.

Para obter mais informações, consulte Criar e nomear um perfil de evento para a integração Splunk Enterprise Event Ingestion.

5. Como um usuário com a função Now Platform sn_si.admin, mapeie valores ingeridos ou dados de anexo que são exportados de Splunk Enterprise para Now Platform incidentes de segurança.

a. Buscar dados de amostra para um alerta programado.

b. Exporte dados de anexo manualmente de Splunk Enterprise para um evento.

c. Edite a configuração de mapeamento padrão.

d. Opcionalmente, adicione critérios de filtragem, anexe um alerta a um incidente de segurança existente e use o editor de script.

Para obter mais informações, consulteMapeamento de alertas e eventos para a integração Splunk Enterprise Event Ingestion e Mapear alertas para a integração Splunk Enterprise Event Ingestion.

6. Como um usuário com a função Now Platform sn_si.admin, visualize os dados de Splunk Enterprise que são exibidos em um incidente de segurança Now Platform.

Corrija erros ou adicione dados ausentes para que nenhuma mensagem de erro seja exibida.

Para obter mais informações, consulte Visualizar o incidente de segurança para a integração Splunk Enterprise Event Ingestion.

7. Como um usuário com a função Now Platform sn_si.admin, programe a recuperação de alerta para um perfil com um alerta programado.

Para obter mais informações, consulte Programar e recuperar alertas para a integração Splunk Enterprise Event Ingestion.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Splunk Enterprise Security integração de ingestão de eventos para Security Operations por ServiceNow

A integração de ingestão de eventos notáveis Splunk Enterprise Security com o produto Security Incident Response (SIR) permite que os analistas de incidentes de segurança coletem e processem dados de eventos notáveis (conhecidos como notáveis).

Visão geral

Os dados são ingeridos continuamente com base em uma programação de pesquisa configurada e são usados pelos analistas para identificar e responder a possíveis ameaças cibernéticas. Os eventos de segurança coletados podem ser correlacionados em eventos notáveis em Splunk Enterprise Security e ingeridos automaticamente com esta integração. Além disso, eventos notáveis individuais podem ser encaminhados manualmente sob demanda do console de análise de incidentes Splunk Enterprise Security e da interface de relatório para o produto Security Incident Response do Now Platform para criar incidentes de segurança.

Esta integração fornece a um analista do centro de operações de segurança (SOC) visibilidade de eventos notáveis e dados de evento de contribuição relacionados. Esses dados podem ser integrados em Now Platform Security Incident Response (SIR) incidentes de segurança para investigação e correção adicionais. Os perfis são criados na sua instância Now Platform para lidar com diferentes tipos de evento notáveis que são criados por meio de pesquisas de correlação em Splunk Enterprise Security. Esses perfis personalizam como diferentes Splunk campos de evento são exibidos em SIR incidentes de segurança.

Principais recursos

Esta integração inclui os seguintes recursos principais:

- Crie vários perfis de ingestão de eventos notáveis para criar incidentes de segurança SIR para tipos específicos de ameaças, como phishing e malware e tentativas de acesso não autorizado.
- Crie vários perfis de evento para encaminhamento de eventos sob demanda do console de revisão de incidentes Splunk ES para criar incidentes de segurança SIR.
- Mapeamento de arrastar e soltar de Splunk valores de campo de evento notáveis para campos de incidente de segurança SIR associados.
- Uma visualização do layout do incidente de segurança SIR com base em eventos notáveis de amostra para validar os detalhes do mapeamento de eventos.
- Inclua eventos notáveis históricos, bem como eventos notáveis em andamento, novos e atualizados em intervalos configuráveis.
- Filtrar eventos notáveis que não atendem aos critérios de geração de incidentes do SIR, por exemplo, eventos de baixa prioridade, eventos que ainda não atingiram um status específico e assim por diante.
- Agregue eventos ou alertas a incidentes de segurança SIR existentes com base em valores de campo correspondentes para evitar incidentes de segurança duplicados.
- Atualize eventos notáveis com base na criação de incidentes SIR e/ou condicionais de fechamento por meio de uma interface bidirecional para manter Splunk ES atualizações de eventos notáveis em sincronia com o ServiceNow status do incidente SIR.

Now Platform Versões compatíveis

O plug-in com.snc.si_dep é necessário para esta integração. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras Security Operations aplicações.

As aplicações Security Operations a seguir devem ser instaladas e ativadas a partir do ServiceNow Store. Instale e ative um aplicativo de cada vez na ordem listada abaixo para garantir uma instalação sem problemas:

1. Security Integration Framework
2. Security Support Common
3. Security Incident Response

Para obter mais informações sobre como instalar as aplicações principais Security Operations, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

ServiceNow Complementos

O ServiceNow Complemento de ingestão de eventos do Security Operations para Splunk ES será necessário somente se você preferir encaminhar eventos manualmente do console de revisão de incidentes Splunk Enterprise Security] para a instância Now Platform. Este ServiceNow addon está disponível em splunkbase .

Este ServiceNow Complemento de ingestão de eventos do Security Operations para a aplicação Splunk Enterprise no splunkbase não é necessário para a ingestão de alertas automatizada compatível com a integração.

Versões compatíveis do Splunk

Esta integração foi testada com a Splunk Enterprise versão 8.0.1 e com a aplicação Splunk Enterprise Security versão 6.2.1.

MID Server

Esta integração requer um MID Server instalado e configurado em sua instância Now Platform® para se conectar ao serviço Splunk quando o servidor Splunk é implantado em sua rede corporativa. Se você estiver usando o serviço Splunk Cloud, um MID Server não será necessário. Consulte MID Server para obter mais informações sobre MID Servers.

Referências

Referência	Identificador de documento	Título do Documento
1	Splunk site do produto	Site do produto Splunk Enterprise Security .

Check-list

Para obter uma check-list imprimível desses tópicos, consulte Check-list para a integração de ingestão de eventos notáveis Splunk Enterprise Security. Você pode usar essa lista para monitorar seu andamento enquanto trabalha nas tarefas da integração.

Termos-chave usados nesta integração

Esta seção descreve alguns dos principais termos usados nesta integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os termos-chave a seguir são usados durante a instalação e a configuração. Para obter mais informações sobre esses termos, consulte o site de Documentação do produto da ServiceNow e o site e recursos do Splunk na página Recursos do Splunk.

Now Platform

Um produto empresarial ServiceNow. O Now Platform é a base sobre a qual componentes individuais, como Security Incident Response (SIR), IT Service Management (ITSM) e outros produtos são criados.

ServiceNow Complemento Splunkbase

Uma aplicação ServiceNow que é instalada no console Splunk Enterprise Security que oferece suporte à opção de encaminhamento de evento manual da integração. O encaminhamento manual de eventos é um recurso opcional da integração. Este ServiceNow complemento Splunkbase não é necessário para a ingestão automatizada de eventos notáveis que é fornecida pela integração que extrai eventos de Splunk.

Security Incident Response (SIR)

Uma aplicação Now Platform que rastreia o andamento dos incidentes de segurança desde a descoberta e a análise inicial, passando pela contenção, erradicação e recuperação, até a revisão e fechamento pós-incidente finais.

Splunk Enterprise Security

Splunk Enterprise Security ajuda as equipes a obter visibilidade e inteligência de segurança em toda a organização para monitoramento contínuo, resposta a incidentes, operações SOC e fornecendo aos executivos uma janela para o risco dos negócios. Splunk Enterprise Security é uma solução de segurança premium que requer uma licença paga. Este serviço está em um host ou em uma oferta de nuvem Splunk que é chamada de console Splunk neste guia.

Splunk Enterprise Security evento relevante

Quando uma pesquisa de correlação identifica um evento ou um padrão de eventos, ela cria um evento relevante. As pesquisas de correlação filtram os dados de segurança e correlacionam eventos para identificar um tipo específico de incidente (ou padrão de eventos) e, em seguida, criar eventos notáveis.

Splunk evento

Um ou mais elementos de dados que resultam nos eventos notáveis do serviço Splunk. Na sua instância Now Platform, você pode pesquisar quais eventos [Splunk acionaram Now Platform incidentes de segurança.

MID Server

Esta aplicação facilita a comunicação e a movimentação de dados entre Now Platform e aplicações externas, fontes de dados e serviços. Esta aplicação é normalmente necessária para integração com tecnologias no local e, para esta integração de ingestão de eventos Splunk Enterprise Security, o MID Server facilita a comunicação entre o Now Platform e a instância local de Splunk Enterprise Security. Um MID Server não é necessário se você estiver integrando sua instância Now Platform com uma instância Splunk Cloud.

Administrador de incidentes de segurança (sn_si.admin)

O usuário com esta função supervisiona a configuração da integração com o produto SIR em sua instância Now Platform.

Analista de incidentes de segurança (sn_si.analyst)

O usuário com esta função interage com e analisa incidentes de segurança no produto ServiceNow Security Incident Response.

Configure sua instância Now Platform® para a integração Splunk Enterprise Security

A seção a seguir lista as tarefas de configuração que você deve concluir em sua instância Now Platform® antes de instalar a aplicação do ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: administrador

Consulte a tabela a seguir e verifique se você concluiu todas as tarefas listadas antes de baixar e instalar a aplicação para garantir uma instalação e configuração sem problemas.

1. Verifique se você atribuiu as funções Now Platform® e Security Incident Response (SIR) necessárias.

   As funções a seguir são necessárias para a instalação, configuração e uso da integração na sua instância Now Platform®.

   - Um usuário com a função de administrador Now Platform® (admin) instala a aplicação a partir do ServiceNow Store e atribui a função de administrador de incidente de segurança (sn_si.admin).
   - Se você quiser encaminhar eventos notáveis manualmente de Splunk Enterprise Security para esta integração, um usuário com a função de administrador Now Platform® atribuirá um usuário com a função (sn_sec_splunkes.api_account_access) no Now Platform®. Esta função permite que um usuário com a função de administrador Splunk Enterprise Security acesse a API no Now Platform® que é necessário para o encaminhamento manual de eventos para esta integração.

     A função (sn_sec_splunkes.api_account_access) não será necessária para a integração se você estiver ingerindo eventos notáveis automaticamente de Splunk Enterprise Security para sua instância Now Platform®.

   - Um usuário com a função sn_si.admin supervisiona as seguintes tarefas no Now Platform®:
     - Nomeia, cria e edita perfis de evento.
     - Seleciona e mapeia valores de Splunk Enterprise Security a Now Platform® incidentes de segurança.
     - Visualiza os detalhes do incidente de segurança para precisão antes de finalizar a configuração.
     - Programa a ingestão de eventos notáveis em andamento.
     - Habilita atualizações de eventos notáveis quando um incidente de SIR é criado e encerrado.
     - Atribui a função de analista de incidente de segurança (sn_si.analyst).
     - Usuários com o sn_si.analyst trabalham com incidentes de segurança.

   Para obter mais informações, consulte Managing roles .

2. Atribua a função de usuário Splunk.

   Atribua uma função de usuário de Analista de segurança (ess_analyst) no Splunk ES para executar todas as atividades relacionadas à integração no servidor Splunk.

3. Verifique se você está usando a versão 7.2.6 ou posterior da API Splunk. Versões anteriores não são compatíveis.

   Se você tiver acesso ao console Splunk Enterprise Security, terá acesso à API necessária para esta integração. Não há nenhuma outra configuração especial necessária para a API.

4. Verifique se você instalou e configurou um MID Server.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um MID Server em sua instância Now Platform® é necessário para se conectar ao serviço Splunk se o servidor Splunk for implantado em sua rede corporativa. Para obter informações, consulte MID Server .

Se você estiver usando o serviço em nuvem Splunk Enterprise Security, um MID Server não será necessário.

5. Verifique se as ServiceNow aplicações principais necessárias para oferecer suporte à integração estão instaladas e ativadas.

   O plug-in Security Incident Response Dependency (com.snc.si_dep) é necessário. Este plug-in instala automaticamente todas as dependências necessárias para oferecer suporte ao produto Security Incident Response. Instale e ative este plug-in antes de instalar e ativar as outras aplicações Security Operations necessárias para a integração.

   Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas.

   a. Security Incident Response
   b. Security Integration Framework
   c. Security Support Common

   Para obter mais informações sobre como instalar as aplicações principais Security Operations, consulte Obter direito para um produto ou aplicação Security Operations e Ativar uma aplicação ServiceNow Store.

Você configurou com sucesso sua instância Now Platform® para a integração. A próxima etapa é instalar a aplicação Notable Event Ingestion [Splunk Enterprise Security do ServiceNow Store para a integração. Para obter mais informações, consulte Instalar e configurar a aplicação ServiceNow para a integração de ingestão de eventos notáveis Splunk Enterprise Security.

Se você quiser exportar eventos notáveis manualmente e sob demanda do console Splunk Enterprise Security para a integração, consulte Configure seu ambiente Splunk para ingestão manual de eventos para a integração de ingestão de eventos notáveis Splunk Enterprise Security para obter mais informações.

Instalar e configurar a aplicação ServiceNow para a integração de ingestão de eventos notáveis Splunk Enterprise Security

Antes de executar a integração na sua instância Now Platform®, conclua estas etapas de instalação e configuração para que a aplicação se integre corretamente aos produtos Security Incident Response e Security Operations na sua instância Now Platform®.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Se você não instalou a aplicação de ingestão de eventos [Splunk Enterprise Security do ServiceNow Store para a integração, consulte Instalar uma integração Security Operations e siga as etapas para instalá-lo.
2. Depois de instalar a aplicação com êxito, navegue até **Integrações** > **Configurações de integrações** e localize o bloco Splunk Ingestões de evento.
3. Para configurar a aplicação, clique em **Novo**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

4. Como alternativa, se um botão **Configurar** for exibido em um bloco, clique nele para editar uma configuração existente.
5. Na caixa de diálogo Configuração de ingestão de eventos exibida, preencha os campos.

   A figura a seguir é um exemplo de um formulário preenchido para uma configuração de uma versão local do Splunk Enterprise Security com um MID Server.

   Cada tipo de evento notável Splunk Enterprise Security que você ingere do console de revisão de incidente Splunk Enterprise Security requer um perfil de evento exclusivo em sua instância Now Platform®. No entanto, a origem que você configura no formulário Configuração de ingestão de eventos pode ser reutilizada para vários perfis Now Platform®, desde que cada perfil inclua tipos de evento notáveis exclusivos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Enviar**.
   Depois que a validação for concluída com sucesso, a página Integrações de segurança será exibida com cada uma das suas configurações. Em cada bloco de configuração válido, os botões **Atualizar** e **Excluir** são exibidos, conforme mostrado na figura a seguir.

Nota:
Os usuários precisam usar a Autenticação básica ou a Autenticação baseada em token. Habilitar ambos resultará no seguinte erro.

Nota:
Se os usuários preferirem atualizar os blocos de configuração existentes para baseados em token, eles precisarão habilitar a configuração Ativar esta configuração para atualizar as configurações de origem Splunk existentes para o suporte à autenticação baseada em token no módulo Splunk Configurações do Enterprise.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de validada e enviada com sucesso, cada configuração de servidor de ingestão de eventos Splunk é salva na página Integrações de segurança como um bloco. Se os blocos de configuração salvos não forem exibidos na página Integrações de segurança, no canto superior direito da página, na lista Mostrar configurações, selecione **Sim**.

O que Fazer Depois

Você instalou e configurou a aplicação com sucesso. A próxima etapa é criar um perfil de evento.

Definir Splunk configurações de segurança empresarial

Use as configurações de Splunk Enterprise Security (ES) para modificar as configurações predefinidas e seus valores de acordo com seus requisitos.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Splunk ES Integration** > **Configurações do Splunk ES**.
2. No formulário, preencha os campos.

Configurações do Splunk ES

Campo	Descrição
Imponha um limite no número de eventos notáveis que podem ser agregados a um único incidente.	Opção para impor um limite ao número de eventos notáveis que você deseja agregar a um único incidente. Por padrão, o valor é definido como 100.
Imponha um limite para o número de incidentes de segurança que podem ser criados em um período de 24 horas.	Opção para impor um limite ao número de incidentes de segurança que podem ser criados em um período de 24 horas. Por padrão, o valor é definido como 1000.
Imponha um limite no número de valores a serem analisados em cada campo recebido de Splunk.	Opção para impor um limite no número de valores que você deseja analisar para cada campo recebido de Splunk. Por padrão, o valor é definido como 1000.
Número de regras de correlação para extrair de Splunk.	Opção para definir o número de regras de correlação a serem recuperadas de Splunk. Por padrão, o valor é definido como 500.
O parâmetro de tempo de vida útil do trabalho de pesquisa Splunk em segundos.	Opção para definir o parâmetro Tempo de vida útil da pesquisa Splunk na forma de segundos. Por padrão, o valor é definido como 600.
Número de tipos notáveis para lote em uma pesquisa.	Opção para definir o número total de tipos notáveis que você deseja agrupar em uma única pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Por padrão, o valor é definido como 20.
Número de dias para reter os metadados do trabalho de pesquisa [Splunk em ServiceNow	Opção para definir o número de dias que você deseja reter os metadados do trabalho de pesquisa do Splunk em ServiceNow. Por padrão, o valor é definido como 30.
O caractere delimitador para dividir os valores em mapeamentos de campo.	Opção para definir o caractere delimitador para dividir os valores em mapeamentos de campo. Por padrão, o valor é definido como (,).
Número de minutos de sobreposição a serem adicionados ao buscar os eventos de Splunk (para superar o atraso de indexação do Splunk)	Opção para definir o número de minutos de sobreposição a serem adicionados ao recuperar os eventos de Splunk para superar o atraso de indexação de Splunk. Por padrão, o valor é definido como 30.
Extrair eventos notáveis atualizados	Opção para recuperar eventos notáveis atualizados. Por padrão, o valor é definido como Não.
Ative esta configuração para atualizar as configurações de origem Splunk existentes para suporte à autenticação baseada em token. Você deve atualizar a configuração de integração com detalhes de token depois que esta configuração for habilitada.	Opção para atualizar a configuração de origem Splunk existente para suporte à autenticação baseada em token de uma versão existente. **Nota:** Depois de atualizar para a nova versão, o campo de token ficará indisponível. Você deve habilitar esta configuração para obter a autenticação baseada em token e, em seguida, atualizar a configuração de integração com detalhes do token. Por padrão, o valor é definido como Não.

3. Clique em **Salvar**.

Erros de autenticação

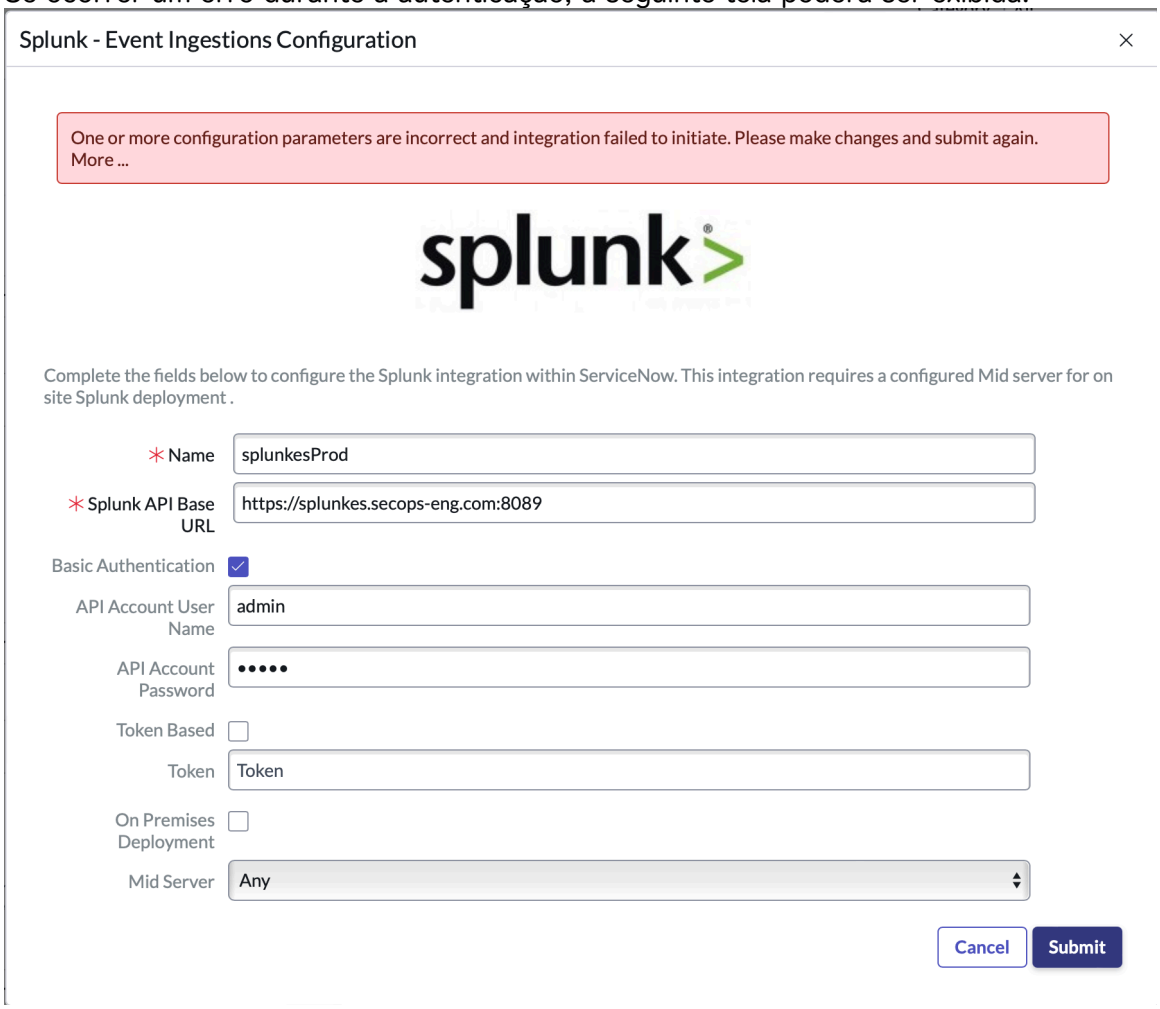
Esta seção descreve alguns erros comuns de autenticação e como eles podem ser resolvidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Problema de validação de certificado

Se ocorrer um erro durante a autenticação, a seguinte tela poderá ser exibida:



Se você verificou que as credenciais da conta da API e as informações do URL base do Splunk estão corretas, esse erro pode ser devido a um problema com o certificado do Splunk para a comunicação da porta 8089. A instância ServiceNow® requer um certificado válido com um nome comum que corresponda ao nome do host do servidor para estabelecer conexões seguras. Para obter mais informações, consulte Certificados . Se você vir este erro, poderá verificar se o problema se deve a um problema de certificado exibindo os logs do sistema.

Uma condição de erro semelhante à seguinte provavelmente aparecerá:

Para prosseguir com a autenticação, você deve substituir o certificado padrão do Splunk fornecido para acesso à API na porta 8089. Para obter instruções detalhadas sobre como substituir o certificado SSL, consulte KB0778285 .

Criar e nomear um perfil de evento para a integração de ingestão de eventos Splunk Enterprise Security

Você cria um perfil de evento em sua instância Now Platform e determina quais eventos notáveis Splunk criam incidentes de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Antes que os incidentes de segurança Now Platform Security Incident Response (SIR) sejam criados a partir de eventos notáveis ingeridos, os valores de campo dos alertas são exibidos em um layout de um incidente de segurança Now Platform para que você possa visualizar como o incidente de segurança real será criado.

De uma perspectiva de integração usando as APIs disponíveis, Splunk ES eventos notáveis são encaminhados individual e manualmente como eventos notáveis discretos ou são ingeridos automaticamente no ambiente Security Operations da sua instância Now Platform, dependendo do tipo de perfil definido.

Os fluxos de trabalho de integração ingerem diferentes tipos de eventos notáveis, como tentativas de acesso não autorizado e malware, por exemplo. Esses eventos notáveis são ingeridos com base nos perfis que você configura no ambiente Security Operations da sua instância.

Todos os notáveis são ingeridos inicialmente para um tipo de pesquisa de correlação configurado em um perfil. Os notáveis ingeridos podem ser filtrados para especificar quais notáveis criam incidentes de segurança. Por exemplo, você pode preferir filtros que criam incidentes de segurança somente para eventos notáveis que são identificados como de alto risco. Antes de um perfil ser ativado e criar incidentes de segurança a partir de eventos notáveis ingeridos, os valores de campo individuais nos eventos notáveis são mapeados para campos correspondentes em um layout do incidente de segurança para uma visualização.

Procedimento

1. Os nomes dos perfis de evento na sua instância Now Platform devem ser exclusivos e só podem ser mapeados para um perfil de evento ativo por vez.
2. O Now Platform ingere notáveis específicos usando os fluxos de trabalho da integração.
   Todos os eventos notáveis que atendem aos critérios de seleção no console Splunk ES são ingeridos inicialmente na instância Now Platform.
3. Um perfil no seu Now Platform é um encapsulamento de um evento notável no seu console Splunk ES.
   Há um relacionamento um para um entre eventos notáveis que são ingeridos com um perfil e conexões com o console Splunk ES : um tipo de evento notável para uma conexão.
4. Para criar perfis para eventos notáveis programados, consulte Configurar um perfil para ingestão de eventos notáveis programados.
5. Para criar perfis para encaminhamento de evento manual, consulte Configurar um perfil para encaminhamento manual de eventos.

Configurar um perfil para ingestão de eventos notáveis programados

Dependendo do perfil definido, Splunk ES eventos notáveis são ingeridos automaticamente no ambiente Security Operations da sua instância Now Platform.

A tabela a seguir mostra a lista de tarefas que você precisa seguir para configurar um perfil para ingestão programada de eventos notáveis:

Etapas para configurar um perfil para ingestão de eventos notáveis programados

Tarefa	Seção
Criar um perfil de evento	Veja Criar perfis para ingestão de eventos notáveis programados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Etapas para configurar um perfil para ingestão de eventos notáveis programados

Tarefa	Seção
Selecione eventos notáveis com base no nome da pesquisa de correlação	Veja Selecione eventos notáveis com base no nome da regra de correlação para o perfil da integração de ingestão de eventos Splunk ES
Mapear campos de evento notáveis	Veja Mapeamento de campos de evento notáveis para a integração Splunk Enterprise Security
Criar mapeamentos personalizados	Veja Criar mapeamentos para Splunk ES revisão de incidente de evento notável e detalhes do evento de contribuição (ingestão programada)
Visualizar o incidente de segurança	Veja Visualizar o incidente de segurança para a integração de ingestão de eventos Splunk Enterprise Security
Programar e recuperar eventos notáveis novos e atualizados	Veja Programe e recupere eventos notáveis novos e atualizados para a integração de ingestão de eventos Splunk Enterprise Security
Automatizar atualizações de eventos notáveis e fechamento com base no status do incidente SIR	Veja Automatizar atualizações de eventos notáveis e fechamento com base no status do incidente SIR

Criar perfis para ingestão de eventos notáveis programados

Você pode configurar um perfil para que eventos notáveis sejam ingeridos automaticamente.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

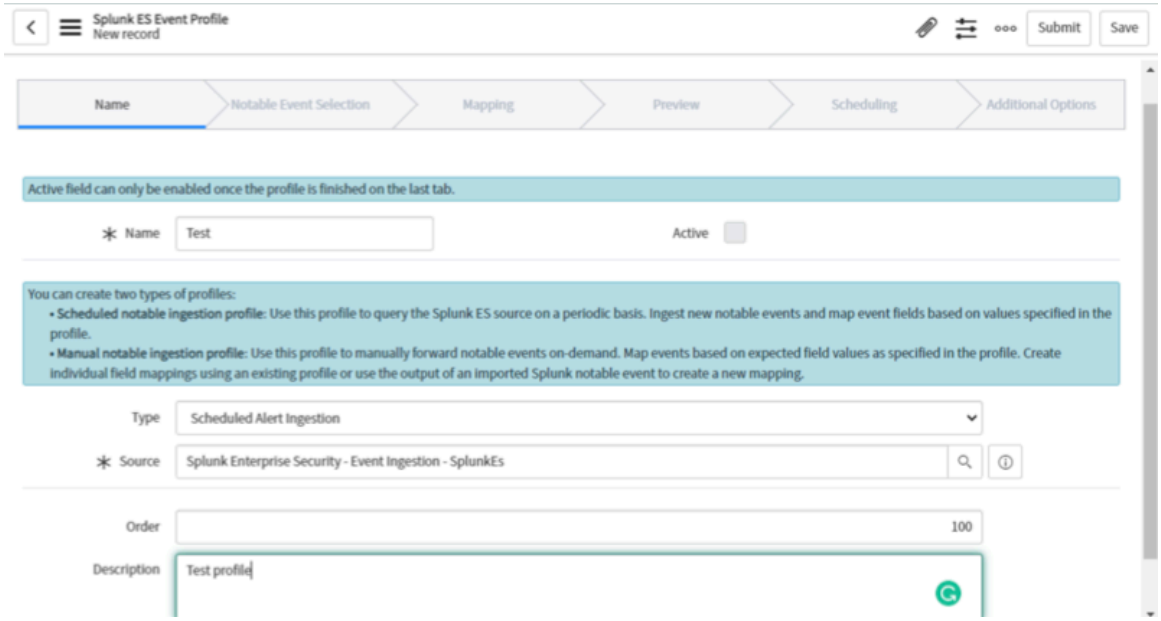
1. Para criar um perfil de evento para um evento notável ou tipo de regra de correlação na sua instância Now Platform, navegue até **Splunk Integration** > **Perfil de evento do Splunk**.
2. Se o formulário de Perfil de evento Splunk não for exibido, clique em **Nome** na barra de andamento.
3. Clique em **Nova**.
4. Preencha os campos.

   Um exemplo de formulário preenchido segue a tabela.

   A figura a seguir é um exemplo de um formulário preenchido para um tipo de evento notável programado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Para um perfil com um evento memorável programado, escolha uma opção para continuar com a configuração do perfil.

O que Fazer Depois

A próxima etapa é selecionar eventos notáveis para ingestão automática.

Selecione eventos notáveis com base no nome da regra de correlação para o perfil da integração de ingestão de eventos Splunk ES

Depois de criar um perfil para uma ingestão de tipo de evento notável programado, selecione um nome de regra de correlação Splunk Enterprise Security para este perfil para o qual você deseja mapear eventos notáveis correspondentes a um incidente de segurança Now Platform Security Incident Response.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Exiba as regras de correlação disponíveis em sua instância Now Platform para conhecer os tipos de evento notáveis para os quais você deseja ingerir e criar incidentes de segurança. Selecione uma regra de correlação. Você pode selecionar um ou mais eventos notáveis na lista deste formulário.

Procedimento

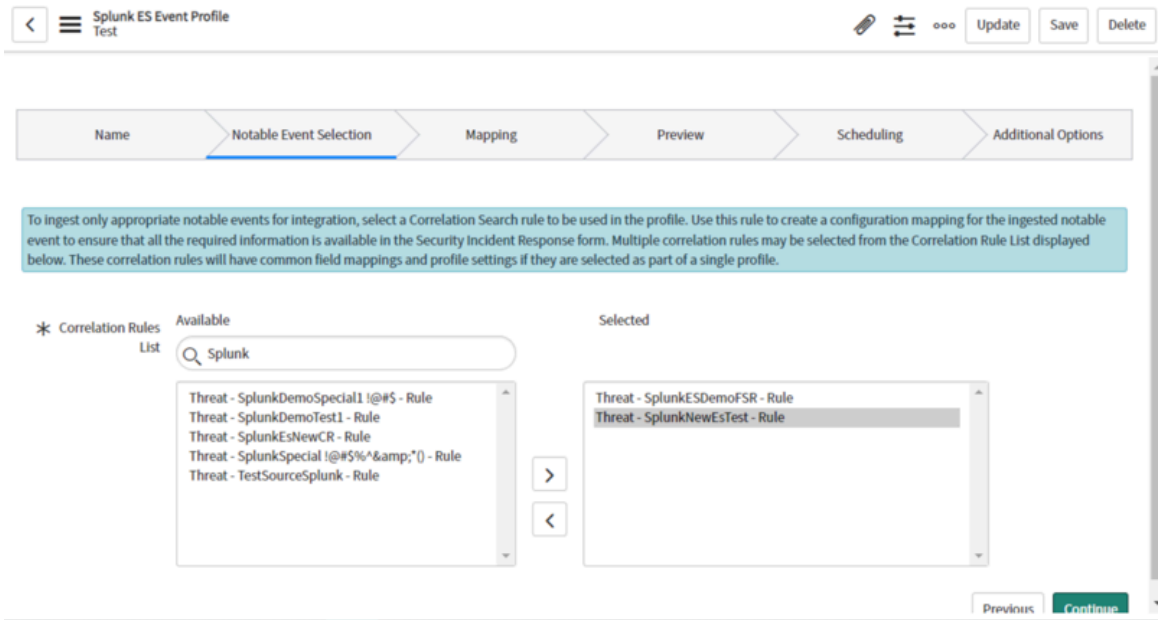
1. Se a página Seleção de evento notável não for exibida, selecione-a na barra de andamento para exibi-la.
2. Na Lista de regras de correlação, escolha uma das opções a seguir para selecionar uma única regra de correlação ou várias regras de correlação e movê-las e movê-las da coluna Disponível para a coluna Selecionada.

   A lista de regras de correlação neste formulário corresponde à lista de regras de correlação no seu console de revisão de incidentes Splunk ES. Até 500 regras de correlação são exibidas neste formulário. Se houver mais de 500 regras de correlação listadas em sua Splunk ES, somente os primeiros 500 eventos notáveis serão exibidos neste formulário em sua instância Now Platform.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
No campo de pesquisa Lista de regras de correlação, insira o texto.	A coluna abaixo do campo de pesquisa é filtrada com as opções disponíveis com base no texto inserido. Selecione uma regra de correlação e, com as teclas de seta, mova o alarme selecionado de **Disponível** para **Selecionado**.
Na Lista de Regras de Correlação, clique duas vezes em uma Regra de Correlação.	A coluna **Selecionado** é preenchida com sua seleção.
Na Lista de Regras de Correlação, clique uma vez em uma Regra de Correlação.	A regra de correlação é selecionada. Com as teclas de seta, mova a regra de correlação selecionada de **Disponível** para **Selecionada**.



3. Escolha uma opção para continuar.

O que Fazer Depois

Você selecionou com sucesso uma regra de correlação para um perfil programado Splunk Enterprise Security. A próxima etapa é mapear valores de evento notáveis para campos em um incidente de segurança.

Mapeamento de campos de evento notáveis para a integração Splunk Enterprise Security

Depois de identificar a regra de correlação específica e o tipo de evento notável para o perfil, a próxima etapa é mapear campos de evento notáveis individuais para os campos em um incidente de segurança Now Platform Security Incident Response (SIR).

Visão geral

Para a etapa de mapeamento, você pode ingerir eventos notáveis de amostra para a regra de correlação selecionada ou exportar dados de evento notáveis para eventos notáveis encaminhados manualmente. O processo de mapeamento de evento é idêntico, independentemente do tipo de perfil que você está criando.

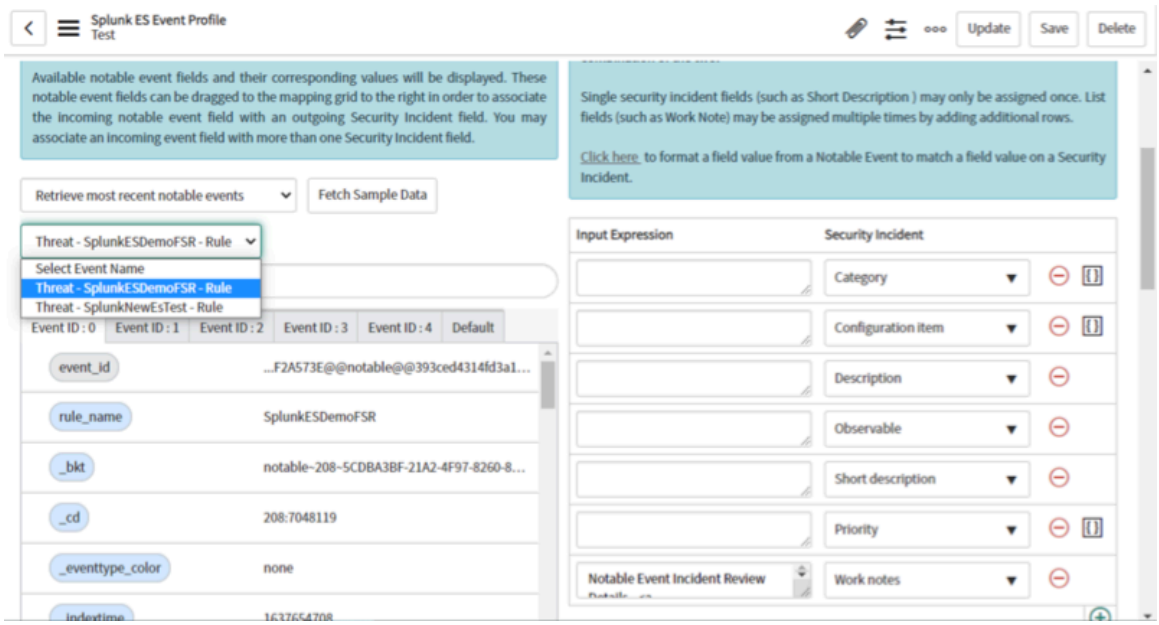
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As imagens a seguir são exemplos das configurações de mapeamento padrão fornecidas para cada tipo de perfil de evento. Você pode personalizar os campos que preenchem o incidente de segurança. Durante esta fase de mapeamento, você pode garantir que todos os dados relevantes do campo de evento notáveis sejam mapeados para o local apropriado no formulário de incidente SIR e, em seguida, visualizar o incidente SIR na seção de visualização.

Se Várias correlações forem usadas, os eventos notáveis poderão ser obtidos selecionando o Evento necessário. Use o **Nome do alerta** para escolher seu alerta se você tiver configurado vários alertas para ingestão.

Depois de clicar para buscar dados, os nomes de campo de evento notáveis Splunk e os valores correspondentes são preenchidos no lado esquerdo do formulário. Estes são os Splunk campos de evento notáveis que estão disponíveis para mapear para os campos de incidente de segurança SIR. Alguns campos podem ser mapeados várias vezes para os campos de incidente de segurança SIR.



Você pode preferir revisar alguns eventos notáveis de amostra no console Splunk para incluir na etapa de configuração de mapeamento de campo. Esta etapa é rotulada como Mapeamento na barra de andamento. Se esta página não for exibida, clique em **Mapeamento** na barra de andamento. Você pode ingerir até cinco eventos notáveis de amostra de Splunk Enterprise Security para ajudar no processo de mapeamento de campo de evento notável. Há opções para ingerir os cinco eventos notáveis mais recentes para a regra de correlação selecionada ou ingerir até cinco eventos notáveis específicos com base nos IDs de evento notáveis.

Abaixo está um resumo das etapas necessárias para mapear eventos notáveis:

- Ingestão de dados de amostra de evento notável programado: para dados de amostra que são usados para perfis de evento notáveis ingeridos automaticamente, os campos de evento notáveis disponíveis e seus valores correspondentes são exibidos em um layout de mapeamento padrão no lado esquerdo do formulário de mapeamento depois que os dados de amostra são recuperados. As guias são exibidas para você exibir os valores de um ID de evento específico específico que você extraiu. Verifique se todos os campos críticos da seção de ingestão de amostra de evento à esquerda do formulário estão mapeados para ServiceNow campos de incidente de segurança à direita do formulário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Mapeamento de campo: edite a configuração de mapeamento arrastando os campos de evento notáveis do lado esquerdo e soltando-os na seção de mapeamento de incidente SIR ServiceNow à direita. O mapeamento à direita associa o campo de evento notável de entrada a um campo de incidente de segurança de saída.
- Experiência de mapeamento: personalize a grade de mapeamento adicionando ou removendo campos usando o ícone + na parte inferior da seção de mapeamento de campo de incidente SIR. Rastreie campos ignorados ou duplicados com a codificação de cores fornecida (os campos mapeados ficam esmaecidos, os campos azuis não estão mapeados).
- Condições de geração de incidentes: depois que a seção de mapeamento estiver concluída, você poderá definir condições de filtro para especificar quais eventos notáveis devem criar incidentes de segurança e quais eventos notáveis devem ser filtrados, por exemplo, eventos notáveis de baixa prioridade. Isso é feito na seção Condições de geração de incidentes localizada abaixo da seção Mapeamento de eventos notáveis.
- Critérios de agregação de eventos: definem critérios adicionais de agregação de eventos que agregam um evento notável de entrada a um incidente de segurança SIR existente, em vez de criar incidentes semelhantes, potencialmente duplicados. Usando critérios de valor de correspondência de campo para cada perfil, essa capacidade de agregação adicional pode reduzir o número de incidentes de segurança ativos e sobrepostos, colocando todos os dados de evento notáveis de segurança relacionados em um único incidente de segurança.
- Tradução de campo de formato: em determinados casos, os valores de campo de evento nos eventos notáveis do Splunk Enterprise podem não ser traduzidos diretamente para os campos no incidente de segurança SIR. Para esses valores, você pode usar um editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento. Use o editor de script se quiser formatar valores semelhantes, mas não idênticos. Por exemplo, com o editor de script, um valor de categoria de Alerta de malware e Infecção de vírus pode ter valores de campo diferentes para a categoria de origem, mas ambos os valores podem ser convertidos em uma Atividade de código malicioso comum no campo Categoria no incidente de segurança SIR usando o Funcionalidade de tradução de campo de formato.

A próxima etapa é ingerir eventos notáveis e mapear valores para os campos de incidente de segurança SIR.

Criar mapeamentos para Splunk ES revisão de incidente de evento notável e detalhes do evento de contribuição (ingestão programada)

Durante a etapa de mapeamento de campo de evento notável, você mapeia campos de evento individuais de eventos notáveis para campos em um incidente de segurança Now Platform Security Incident Response (SIR).

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
A grade de mapeamento pode ser personalizada para o tipo de evento relevante selecionado na seleção da regra de correlação. A codificação por cores dos campos de evento ajuda a rastrear os valores de evento que você já mapeou conforme eles se tornam esmaecidos, enquanto todos os campos não mapeados restantes aparecem em azul. Isso ajuda a visualizar melhor quais valores de campo foram adicionados ao incidente de segurança e se alguma informação de evento importante restante permanece não mapeada.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeie até cinco eventos notáveis da coluna Ingestão de amostra de evento notável à esquerda do formulário para os campos de incidente de segurança na coluna Mapeamento de campo de incidente SIR à direita.

Crie mapeamentos personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Os campos padrão que são normalmente campos importantes a serem preenchidos no formulário de resposta a incidentes de segurança são exibidos. No entanto, esses campos podem ser removidos e quaisquer campos adicionais podem ser exibidos usando os botões + e -. Crie mapas personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Personalizar os campos permite mapear Splunk campos que não são exibidos na grade de mapeamento padrão no incidente de segurança SIR.

Procedimento

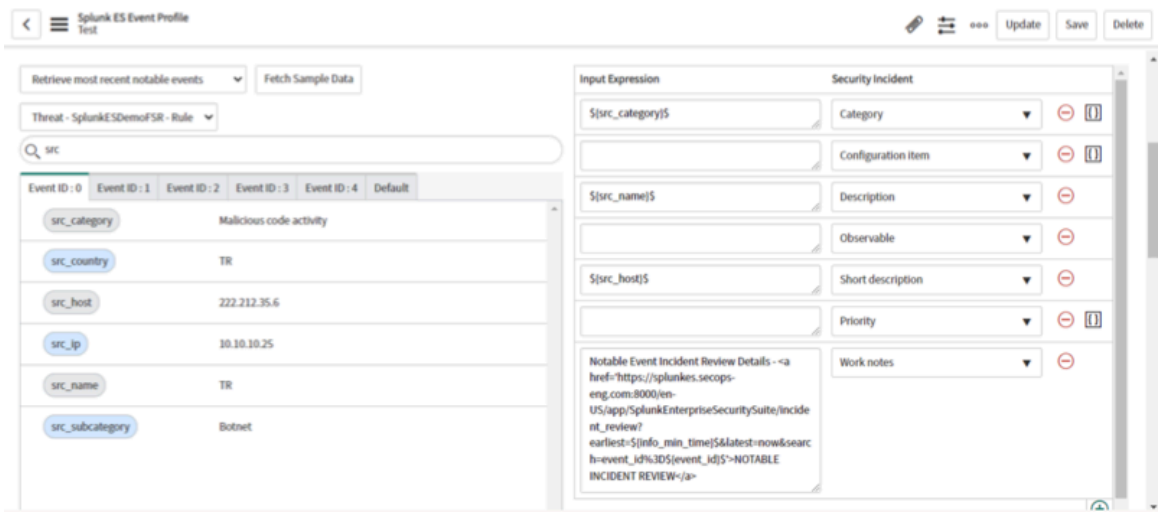
1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Para um perfil com uma ingestão programada, abaixo de Ingestão de amostra de evento notável, clique em **Buscar dados de amostra** para extrair os eventos notáveis de amostra mais recentes do console Splunk Enterprise para a regra de correlação selecionada.

   Nota:
   Você pode extrair os eventos notáveis de amostra mais recentes ou fornecer os IDs de evento notáveis exclusivos para os eventos notáveis específicos que você deseja usar para sua experiência de mapeamento de eventos notáveis.

   Os campos de evento notáveis e os resultados dos valores são exibidos como guias individuais. Você pode ingerir até cinco eventos notáveis.

   A extração de eventos notáveis de amostra pode levar alguns minutos. Uma mensagem indicando que a transação está funcionando é exibida na parte superior da tela.

   Na figura a seguir, os pares de valor de nome de campo para o evento notável ingerido ou os eventos de amostra importados são exibidos no lado esquerdo deste formulário após a conclusão da extração de ingestão. Esses valores são os valores que você mapeia para os campos de incidente de segurança no lado do mapeamento de campo de incidente de SIR do formulário.

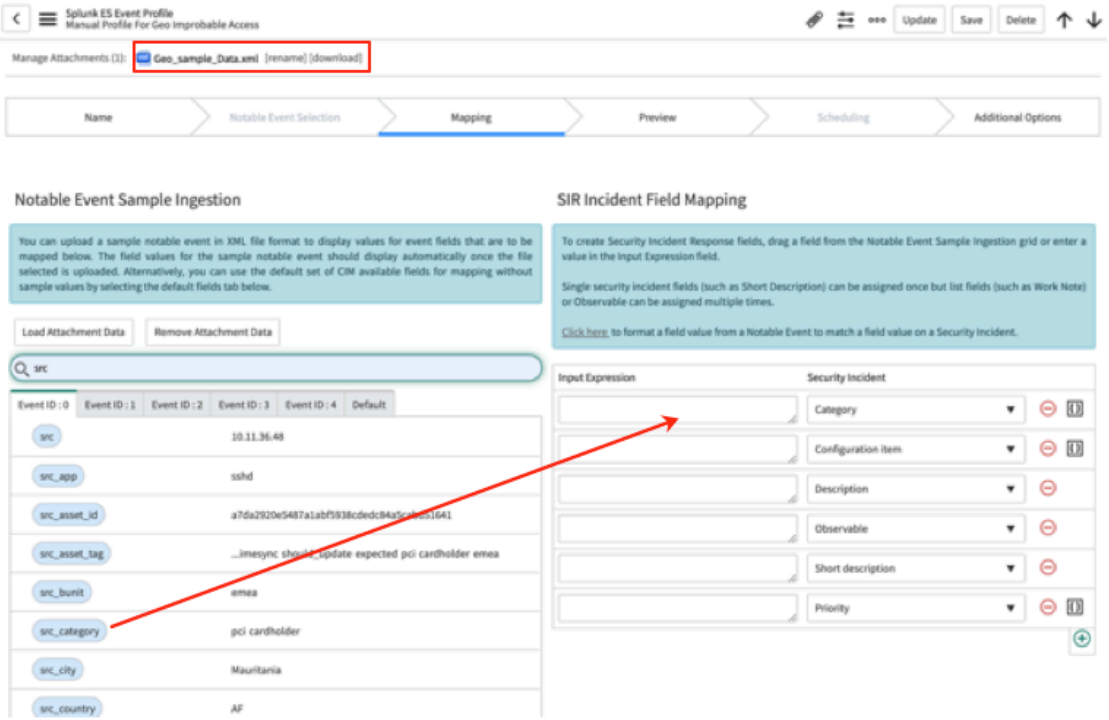


3. Para mapear um valor de campo do lado esquerdo do formulário para um campo no incidente de segurança no lado direito do formulário, clique e mantenha pressionado um nome de campo azul no lado esquerdo do formulário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Arraste o nome do campo, por exemplo, src_categorye solte-o em um campo na coluna Expressão de entrada ao lado de um nome de campo na coluna Incidente de segurança.



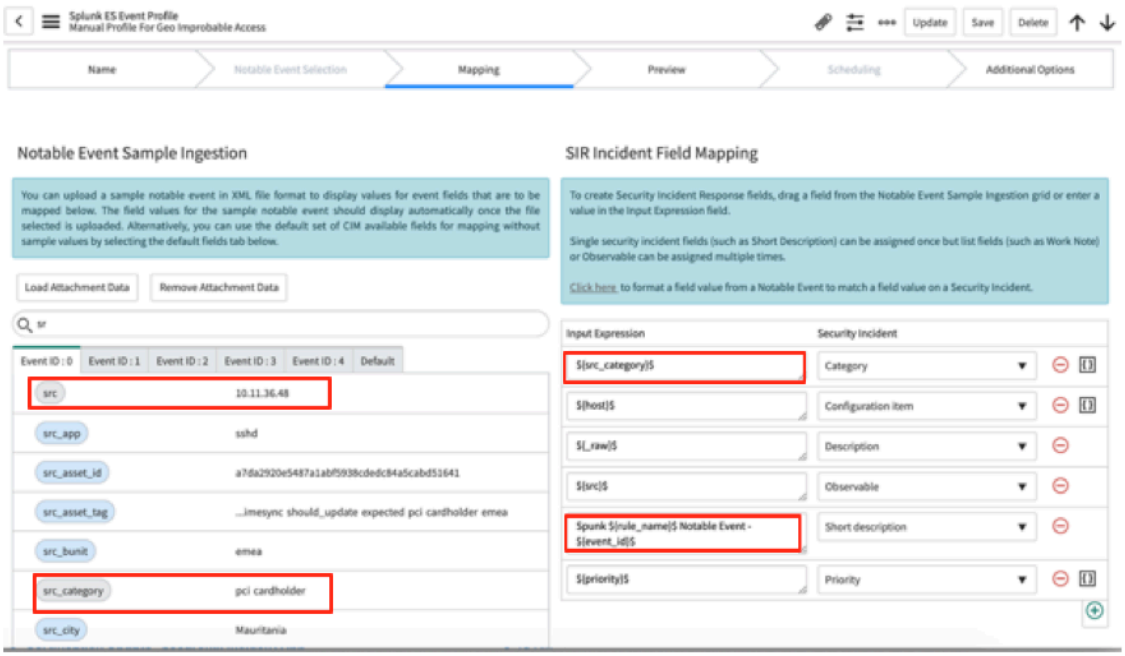
O valor do campo é exibido na coluna Expressão de entrada. Na imagem a seguir, src_category é mapeado para o campo de categoria no incidente de segurança. No entanto, você pode corresponder qualquer valor do lado esquerdo a um campo do lado direito. Verifique se o valor está mapeado corretamente no incidente de segurança durante a etapa de visualização.

Para ajudar a garantir que nenhum campo de evento seja ignorado ou duplicado no processo de mapeamento, os campos são codificados por cores. Os campos azul claro à esquerda indicam que um campo de evento relevante ainda não foi selecionado e mapeado no incidente de segurança. Você pode preferir associar um campo de entrada notável a mais de um campo em um incidente de segurança.

Um campo cinza indica que um campo foi selecionado e mapeado para um campo no incidente de segurança. Essa codificação de cores ajuda a rastrear o mapeamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Para adicionar campos aos campos padrão exibidos no incidente de segurança no lado direito do formulário, siga estas etapas.

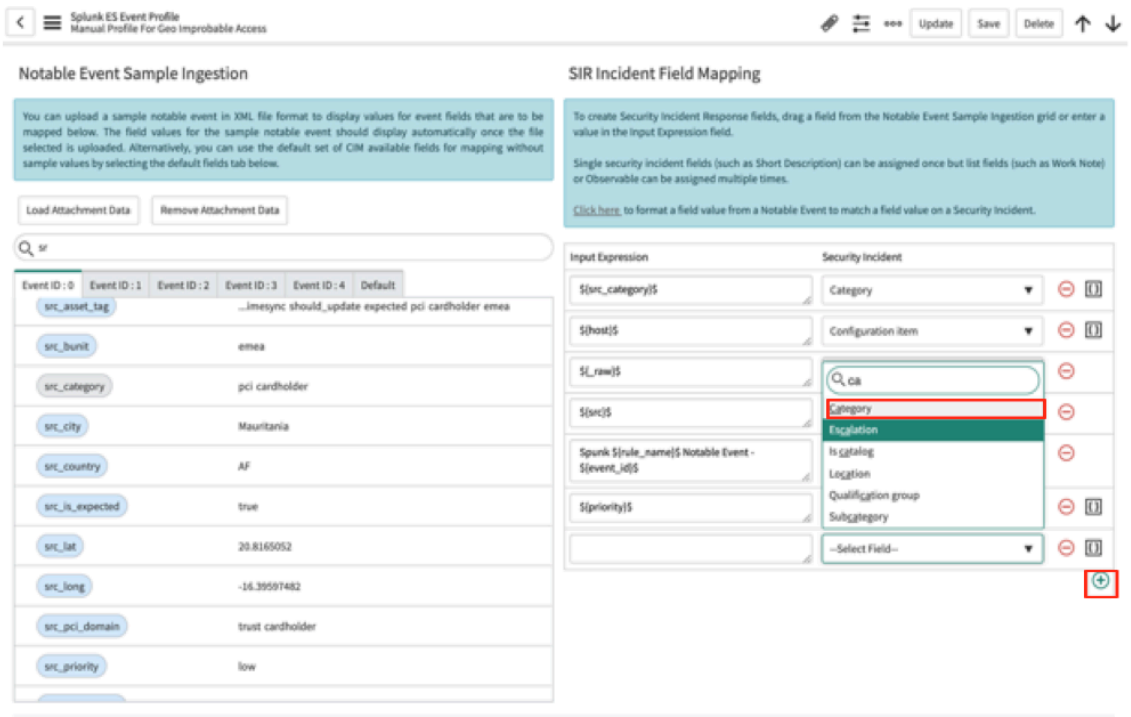
a. À direita do formulário na seção Mapeamento de campo de incidente de SIR, na parte inferior da grade, clique no ícone de adição.
Um novo campo é exibido.

b. Na coluna Incidente de segurança, expanda a lista exibida e selecione um campo.

Na lista expandida do novo campo, alguns campos estão sombreados. Na figura a seguir, Categoria tem um plano de fundo cinza porque foi mapeada no incidente de segurança. Semelhante à codificação de cores dos campos de eventos notáveis no lado esquerdo do formulário, essa codificação de cores para os campos de incidente de segurança à direita ajuda a rastrear os campos de incidente SIR já mapeados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:
Para que vários observáveis possam ser exibidos no mesmo incidente de segurança, o campo Observável pode ser mapeado várias vezes com valores diferentes. Da mesma forma, os campos Item de configuração e Anotações de trabalho oferecem suporte a vários valores. Se você tentar mapear dois valores para um campo que não pode oferecer suporte a vários valores, ao visualizar o incidente, será exibida uma mensagem de erro informando que não há nenhum valor para o campo. Da mesma forma, se um campo em um incidente de segurança tiver uma lista na qual você pode escolher várias opções e você tentar mapear uma opção para esse campo que não é exibido na lista, o campo não será preenchido no incidente de segurança.

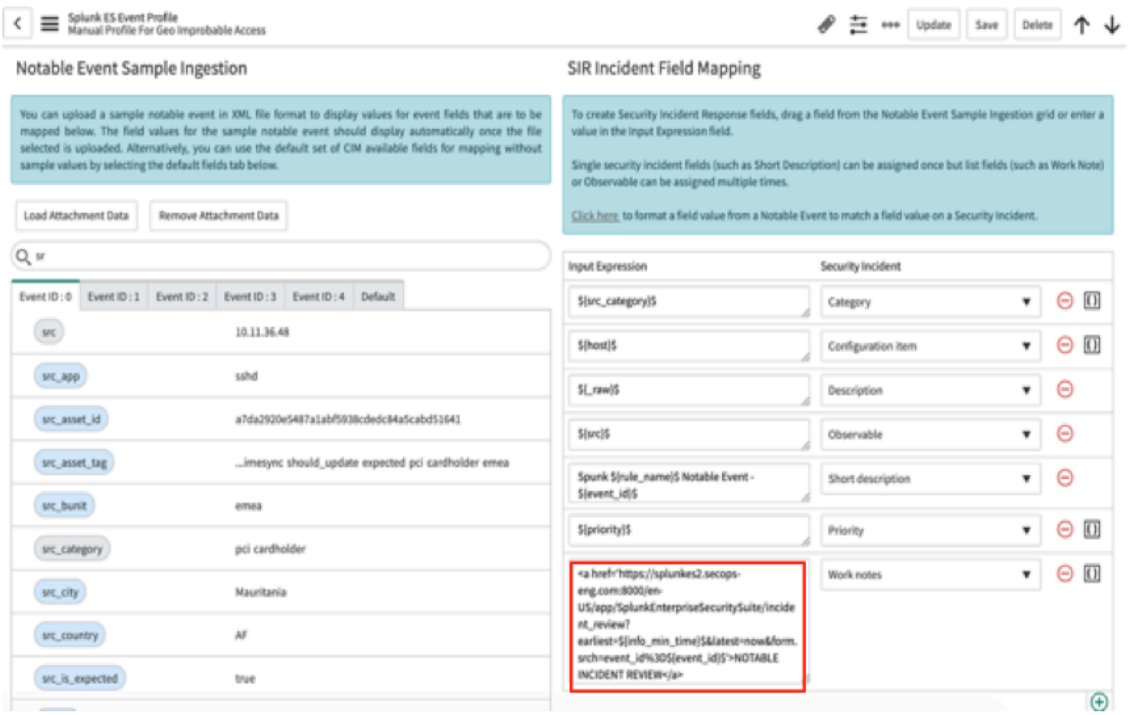
c. Como alternativa, digite um valor no campo Pesquisar da nova linha.

d. No lado esquerdo do formulário, clique com o botão esquerdo do mouse para selecionar o **ID do evento** desejado no campo Expressão de entrada.

6. Continue mapeando adicionando ou removendo valores de campo para o mapeamento.
A figura a seguir é um exemplo de um mapeamento editado. No campo inferior à direita, o campo Anotações de trabalho é adicionado e tem mais de um valor. Observe que, para o campo de cadeia de caracteres de texto longo, você pode expandir o campo de mapeamento para ver a cadeia de caracteres completa e redimensionar conforme necessário, puxando o canto inferior direito do campo conforme indicado na captura de tela abaixo com o campo de Anotações de trabalho adicionado:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



⚠ Aviso:
Observe que na seção **Mapeamento de campo de incidente SIR**, o URL e o número da porta mencionados no campo **Expressão de entrada** são apenas um exemplo e não o URL ou o número da porta fornecidos prontos para uso.

Na visualização, esses valores são exibidos nas Anotações de trabalho no incidente de segurança. Como o valor é para um campo que você adicionou à seção de mapeamento e há vários valores mapeados para o campo Anotações de trabalho, os valores são exibidos conforme inseridos. Neste exemplo, os espaços e os sinais de pontuação que você inseriu no campo são exibidos na seção Itens relacionados como uma anotação de trabalho na visualização do incidente de segurança.

A imagem a seguir é um exemplo de como os valores da imagem anterior são exibidos no incidente de segurança.

7. **Opcional:** Abra o editor de script e continue editando.

(Optional) Para obter mais informações sobre o editor de script, consulte Use o editor de script para formatar valores de alerta para a integração Splunk Enterprise Event Ingestion.

Incluindo hiperlinks para revisão de incidentes de eventos notáveis e eventos de contribuição

Além de mapear campos, o `sn_si.admin` pode mapear um valor de cadeia de caracteres que permite ao analista de segurança que está trabalhando em um incidente fazer um link de volta para a revisão de incidente de evento relevante no console Splunk Enterprise

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Security, bem como para os eventos de contribuição subjacentes que fazem parte da pesquisa de detalhamento.

Os valores de cadeia de caracteres a seguir contêm o nome do servidor Splunk Enterprise Security e as variáveis apropriadas que podem ser usadas para vincular esses detalhes:

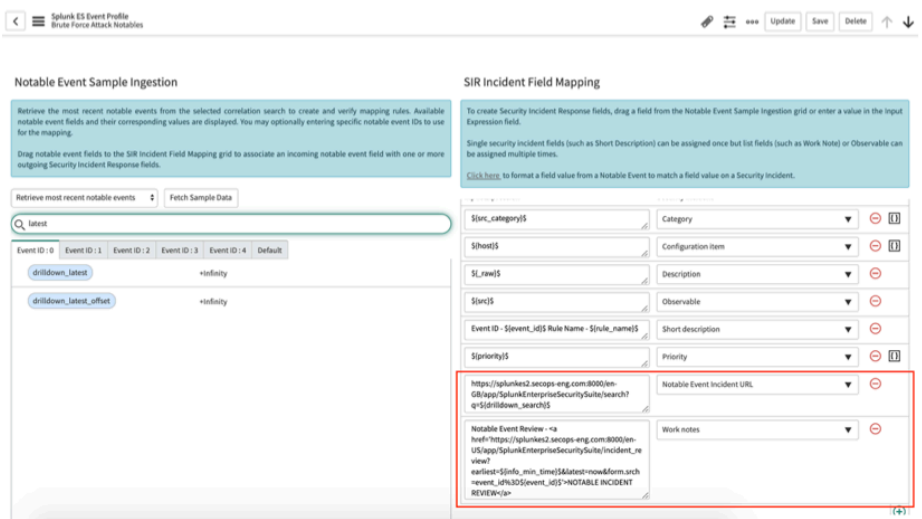
- **Hiperlink de análise de incidentes de eventos notáveis**: https://splunkes2.secops-eng.com:8000/en-US/app/SplunkEnterpriseSecuritySuite/incident_review?earlist=${info_min_time}$&latest=now&form.srch=event_id%3D${event_id} $

  em que splunkes2.secops-eng.com:8000 é a origem do servidor Splunk e info_min_time e event_id são valores de campo de evento extraídos dos eventos notáveis.

- **Eventos de contribuição de evento notáveis (pesquisa de detalhamento) Hiperlink**: https://splunkes2.secops-eng.com:8000/en-GB/app/SplunkEnterpriseSecuritySuite/search?q=${drilldown_search}$

  em que splunkes2.secops-eng.com:8000 é a origem do servidor Splunk e Drilldown_search é um valor de campo de evento extraído dos eventos notáveis.

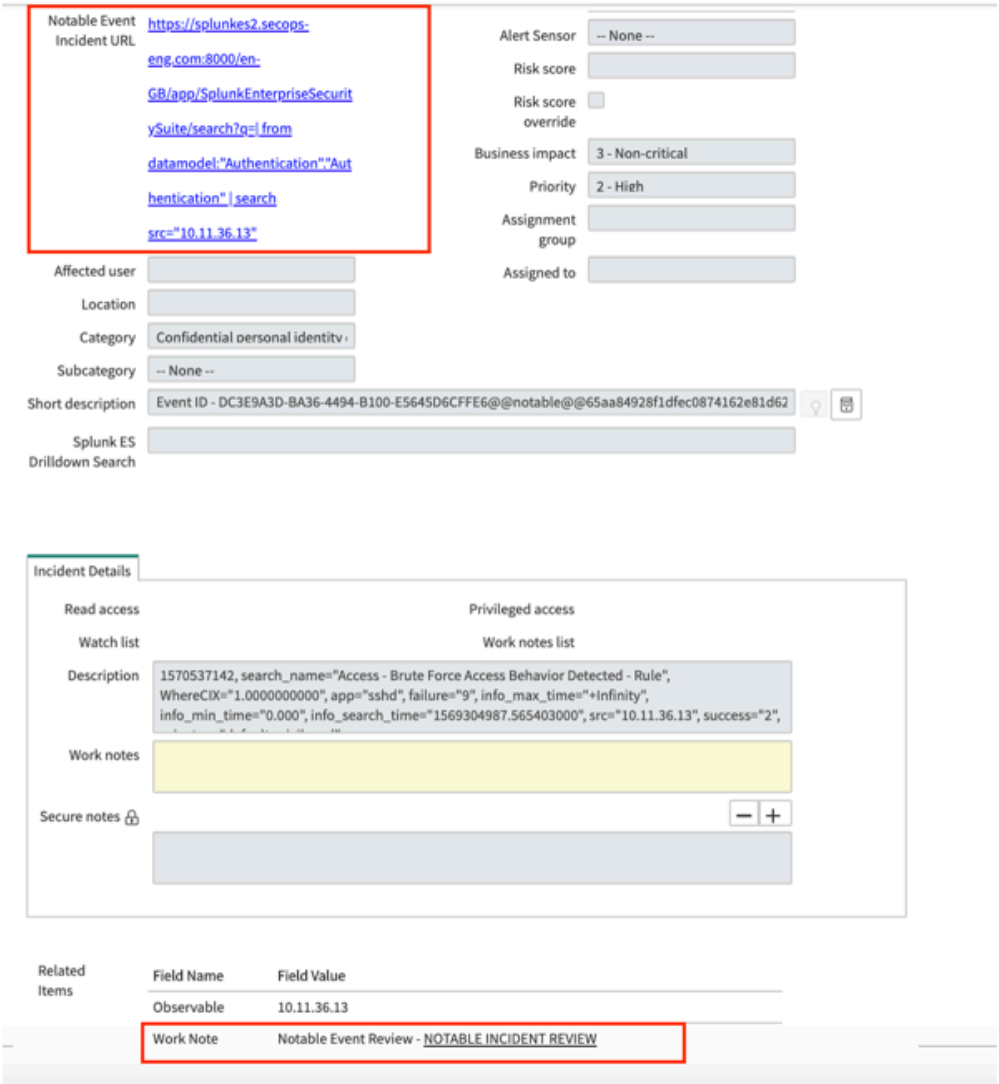
A imagem a seguir mostra o URL de revisão de incidente de evento notável mapeado para o campo de anotação de trabalho e o hiperlink de eventos de contribuição de evento notável (pesquisa de detalhamento) mapeado para um campo personalizado chamado URL de incidente de evento notável:



A imagem a seguir é a visualização do incidente de SIR com o hiperlink de revisão de incidentes de eventos notáveis e a URL

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Condições de filtragem de geração de incidentes

8. **Opcional:** Depois de concluir as etapas de mapeamento de campo anteriores, você pode usar os mesmos valores de campo no construtor de Condições de geração de incidentes para definir critérios adicionais que um evento notável de entrada deve satisfazer para criar um incidente de segurança SIR.
Para definir condições de geração de incidentes, siga estas etapas.

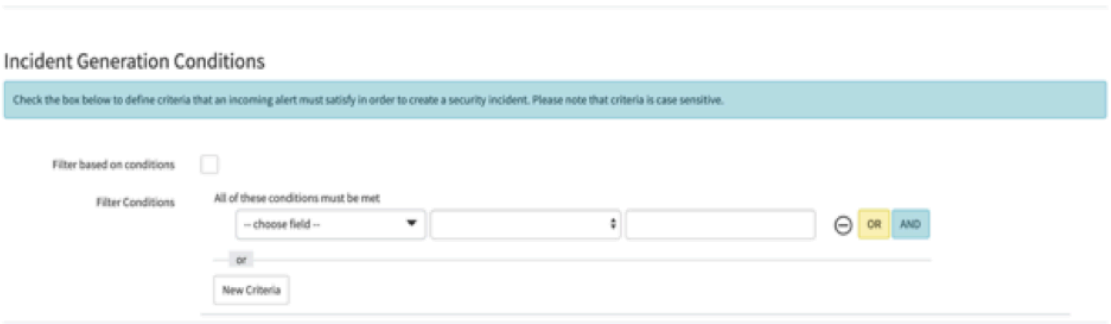
   a. Role até a seção Condições de geração de incidente no formulário e marque a caixa de seleção **Filtrar com base nas condições** para habilitar a opção.

      (Optional) O construtor de Condições de filtro é exibido. Use esses filtros para criar incidentes de segurança que correspondam às condições específicas descritas pelos campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As opções nas listas para o primeiro campo no construtor de condições do filtro correspondem aos campos exibidos na seção Ingestão de amostra de evento notável para os eventos que você ingeriu. Esses campos são dinâmicos e mudam dependendo dos Splunk eventos notáveis que você ingere ou do evento que você seleciona para as amostras de evento notáveis encaminhadas manualmente. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas e devem corresponder exatamente aos valores do evento relevante Splunk Enterprise Security. Se você não tiver certeza sobre os valores a serem inseridos nos campos de filtro, talvez prefira retornar ao console Splunk Enterprise Security e revisar os eventos notáveis para as palavras-chave.

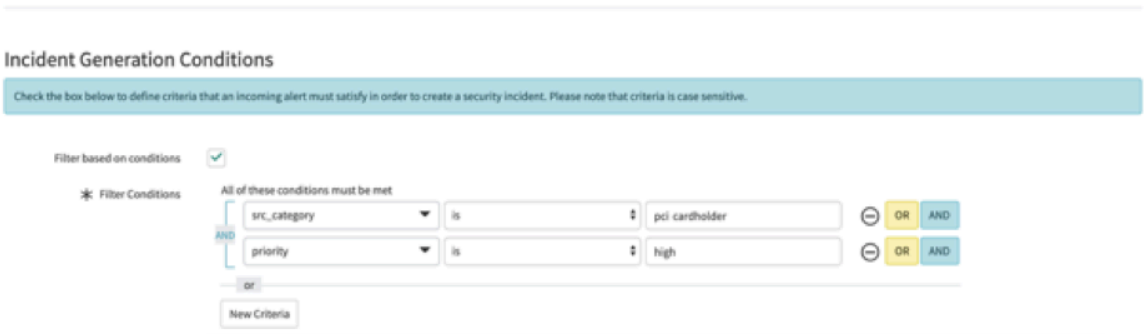


b. Usando as listas e os campos do construtor de condições, defina filtros para a primeira linha.

c. Para adicionar mais condições, à direita dos campos, clique em **E** ou **OU**.
Se **AND** for selecionado, todas as condições deverão ser correspondidas. Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida.

d. Opcional: Na segunda linha, defina uma segunda condição de filtro.

(Optional) A imagem a seguir é um exemplo com duas condições que devem ser correspondidas antes que os incidentes de segurança sejam criados.



(Optional) Você definiu as condições de geração de incidentes para que os incidentes de segurança sejam criados somente quando ambas as condições de filtragem inseridas forem correspondidas.

Esse tipo de filtragem de condição de geração de incidente ajuda a restringir os eventos de segurança e limita o número de incidentes de segurança desnecessários que você cria sem modificar a pesquisa de correlação subjacente ou os filtros em

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Splunk. Se critérios de filtragem adicionais forem definidos, somente eventos notáveis que correspondam a todos os critérios serão mapeados para incidentes.

Nota:
Se algum dos nomes de campo de evento tiver caracteres especiais, como aspas (“), hifens ('), sublinhados (-), arroba (@) ou e comercial (&), esses caracteres poderão precisar ser substituídos para fins de tradução de mapeamento e, possivelmente, crie um nome de evento duplicado. O mapeamento pode ser feito de forma apropriada, mas um sufixo numérico é anexado para diferenciar campos com nomes de evento duplicados. Por exemplo, se o primeiro campo de evento for `alerts.alert` e o segundo campo de evento for `alerts@alerts`, esses campos não poderão ser identificados exclusivamente, pois os caracteres de texto padrão restantes são os mesmos. Nesse caso, um sufixo é adicionado ao segundo campo de evento e o campo é renomeado para `alerts@alert(1)`.

(Optional) Critérios de agregação de eventos para lidar com notáveis semelhantes e evitar incidentes duplicados

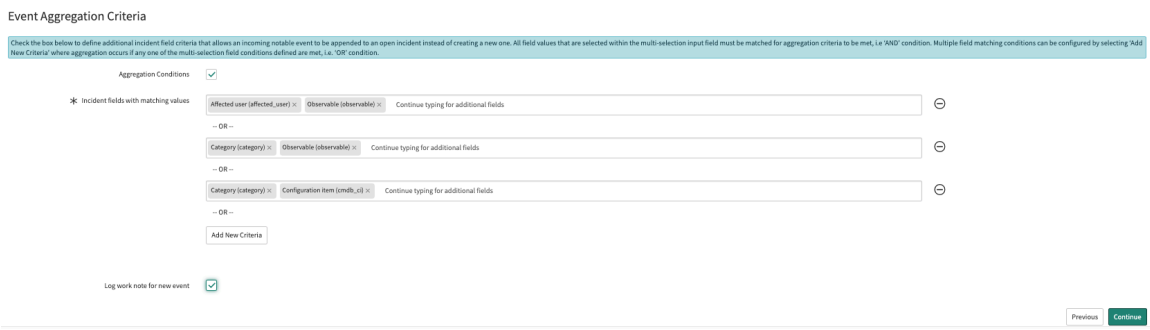
9. **Opcional:** Para evitar a criação de incidentes de segurança duplicados, defina critérios de agregação de eventos adicionais para que os eventos notáveis de entrada sejam agregados a um incidente de segurança em aberto.
Para definir os critérios, siga estas etapas abaixo.

   a. Role até a seção Critérios de agregação de evento no formulário e marque a caixa de seleção **Condições agregadas** para habilitar essa opção.

      (Optional) Os campos de incidente com valores correspondentes são exibidos. Esses nomes de campo são os campos no incidente de segurança que incluem todos os campos personalizados que estão configurados no incidente de segurança SIR.

   b. No campo de entrada de seleção múltipla, selecione os valores de campo que você deseja corresponder aos incidentes de segurança existentes em seu Now Platform.

   c. Use **Adicionar Novos Critérios** para selecionar várias condições de correspondência de campo. Todos os valores de campo selecionados no campo de entrada de seleção múltipla são correspondidos para critérios de agregação usando a condição E. Clique em **Adicionar novos critérios** para selecionar várias condições de correspondência de campo em que a agregação ocorre se qualquer uma das condições de campo de seleção múltipla definidas for atendida usando a condição OU.

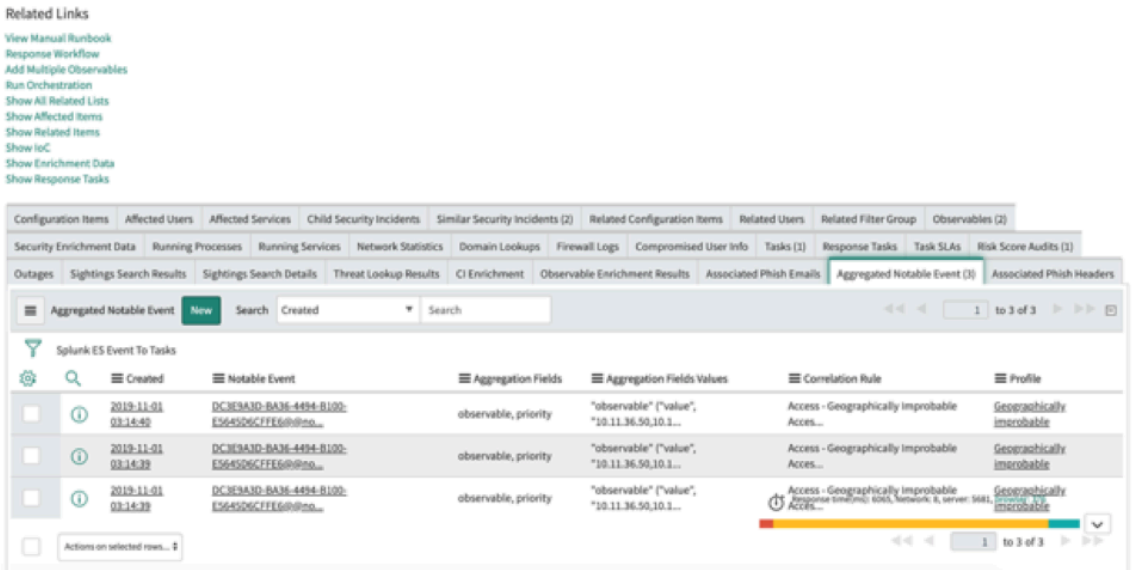


Se um novo evento relevante corresponder a todos os valores selecionados nas condições de campo de agregação na etapa de mapeamento, o novo evento relevante será adicionado automaticamente ao incidente de segurança aberto mais recentemente com os mesmos valores de campo. Como um usuário com a função sn_si.analyst trabalhando com incidentes de segurança, você pode exibir todos os eventos notáveis agregados adicionados em uma lista relacionada em um incidente de segurança. Todos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

os eventos notáveis agregados em um incidente de segurança são exibidos na lista relacionada Splunk de eventos para tarefas. Esta lista detalha os carimbos de data/hora associados e os valores de campos agregados. Essas informações ajudam a entender por que esses eventos notáveis estão sendo agregados a incidentes de segurança existentes. Se esta guia não for exibida, role até o lado esquerdo do registro em Links relacionados e clique no link **Mostrar todas as listas** relacionadas.



d. Opcional: Para registrar uma anotação de trabalho para um novo evento importante que foi adicionado recentemente ao incidente de segurança, marque a caixa de seleção para habilitar esta opção.
A anotação de trabalho registra que um novo notável foi adicionado junto com um link para os detalhes do alerta e quaisquer outros detalhes que possam ter sido adicionados ao campo de anotação de trabalho na seção de mapeamento.

Você mapeou com sucesso valores de um evento notável Splunk para campos em um incidente de segurança SIR. Além disso, você configurou condições adicionais para limitar a criação de incidentes de segurança com critérios de filtragem de geração de incidentes. Você também anexou eventos notáveis a incidentes de segurança SIR existentes quando os valores do campo de evento correspondem aos critérios de agregação configurados.

10. Escolha um para continuar com a configuração do perfil.

O que Fazer Depois

A próxima etapa é visualizar os valores mapeados no incidente de segurança.

Visualizar o incidente de segurança para a integração de ingestão de eventos Splunk Enterprise Security

Depois de concluir a etapa de mapeamento, visualize os valores mapeados em um incidente de segurança Now Platform® Security Incident Response (SIR). Esta etapa de visualização permite que você verifique se mapeou todos os campos notáveis que deseja exibir no incidente de segurança.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Visualize um incidente de segurança e edite o mapeamento novamente conforme necessário para corrigir campos com erros ou para preencher dados ausentes. Se a visualização não

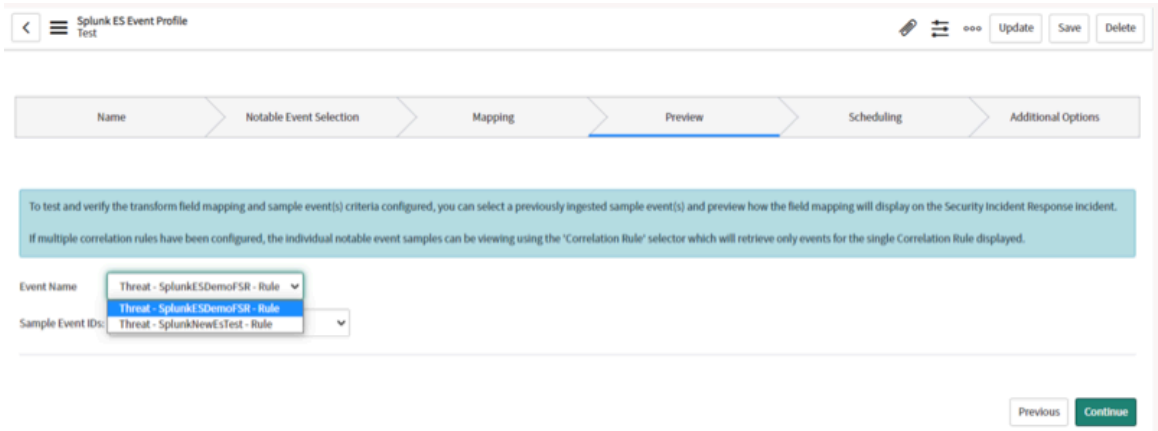
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

for concluída com sucesso, você não poderá prosseguir para a etapa de programação. As visualizações de SIR incidentes de segurança não são salvas como incidentes reais no produto SIR.

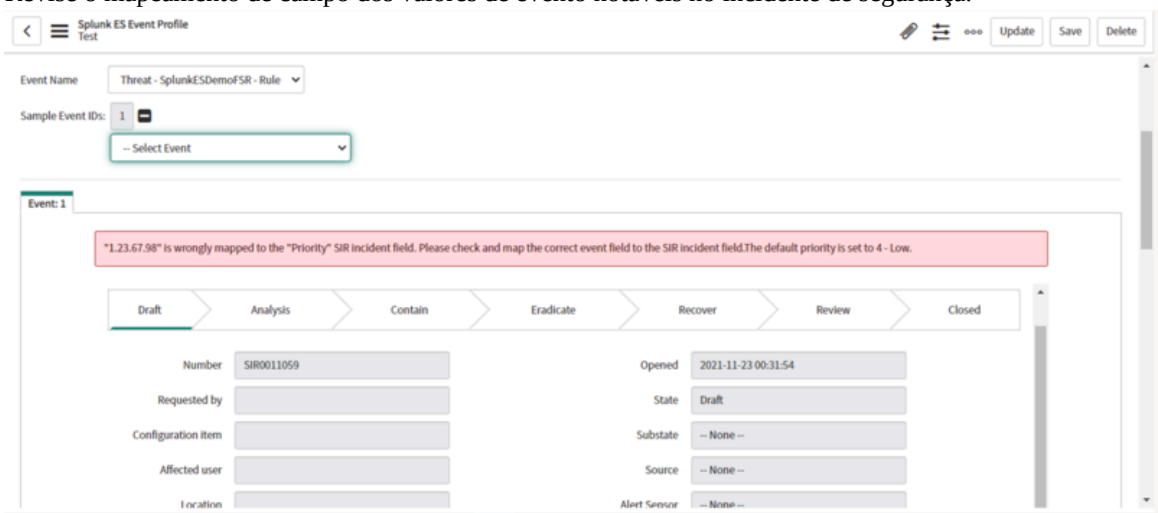
Procedimento

1. Se a visualização do incidente de segurança não for exibida, clique em **Visualizar** na barra de andamento.
2. Na lista de seleção Nome do evento, selecione um item se vários eventos forem usados.
3. Selecione IDs de evento na lista de seleção Amostra de IDs de evento notáveis.
4. Na lista de seleção Amostra de IDs de evento notáveis, selecione um item.



O incidente de segurança é exibido. Não altere nenhuma informação nos campos. Esta exibição é somente leitura e um registro deste incidente de segurança não é salvo.

5. Revise o mapeamento de campo dos valores de evento notáveis no incidente de segurança.



A imagem anterior é um exemplo de uma visualização com um erro de mapeamento. Neste exemplo, um valor de campo do evento notável não tem um valor aceitável para o campo de referência no formulário de incidente SIR. Uma mensagem de erro é exibida indicando que um valor de entrada não foi encontrado para o campo Item de configuração no ServiceNow® banco de dados de gestão de clientes (CMDB). Como resultado, este valor de campo mapeado não aparecerá no formulário de incidente de segurança SIR sem modificação adicional.

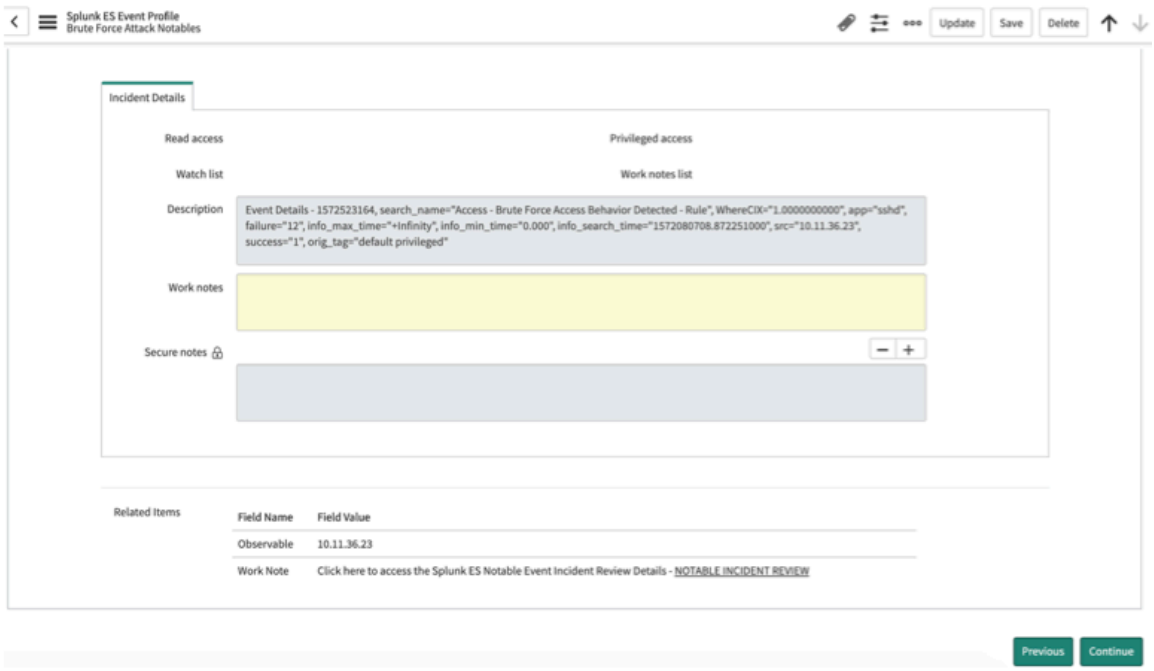
6. Para resolver esse erro, clique em **Mapeamento** na barra de andamento.
7. Edite o mapeamento para corrigir valores incorretos ou preencha os dados ausentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Visualize o mapeamento novamente e continue a corrigir os erros descritos nas mensagens de erro.

   A figura a seguir é um exemplo da guia Detalhes do incidente na metade inferior de um incidente de segurança SIR depois que todas as mensagens de erro são resolvidas. Para este exemplo, os campos Descrição e Anotações de trabalho foram mapeados e esses campos são preenchidos com os valores dos pares de valores extraídos das Splunk Enterprise Security amostras de evento notáveis. O primeiro campo Anotações de trabalho não tem valor. Este campo foi deixado em branco na grade de mapeamento durante a etapa de mapeamento. Os campos de anotações de trabalho adicionais que têm valores foram adicionados à seção de mapeamento.



9. Depois de corrigir todos os erros e verificar se os campos estão como você deseja, escolha uma opção para continuar.

O que Fazer Depois

Se nenhuma mensagem de erro for exibida e você estiver satisfeito com o mapeamento de campo no incidente de segurança, a próxima etapa será Programar e recuperar alertas para a integração Splunk Enterprise Event Ingestion.

Programe e recupere eventos notáveis novos e atualizados para a integração de ingestão de eventos Splunk Enterprise Security

Para perfis de ingestão de eventos notáveis automatizados, esta etapa é necessária na configuração do perfil de evento. Durante esta etapa, você pode verificar as configurações padrão para recuperação de evento notável ou modificar a programação conforme necessário. Esta etapa também permite recuperar eventos notáveis históricos usando um intervalo de datas.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Para perfis de ingestão de eventos notáveis automatizados, você escolhe se deseja ingerir eventos notáveis históricos durante a etapa de Programação. Você também escolhe com

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

que frequência pesquisará novos eventos notáveis futuros e eventos notáveis atualizados que correspondam à configuração do perfil de alerta.

Para perfis de ingestão de eventos notáveis automatizados, antes que o perfil seja ativado, você verifica e modifica a programação e a recuperação do alerta. Esta é uma etapa necessária para todos os processos de configuração de perfil de evento para perfis de alertas programados.

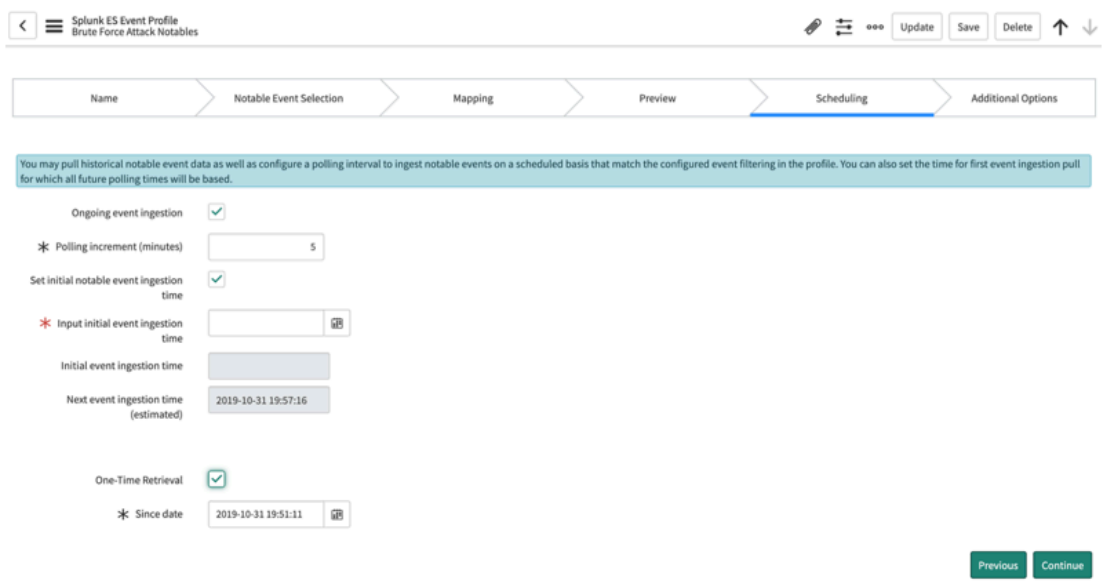
Você configura esses intervalos de pesquisa por perfil. O desempenho da integração de ingestão de eventos Splunk pode ser afetado pelos diferentes intervalos de pesquisa. Ao programar, talvez você prefira equilibrar a redução da sobrecarga de pesquisa no servidor Splunk Enterprise Security com o desejo de ser notificado o mais rápido possível quando um evento importante for criado ou atualizado. Um valor padrão de cinco minutos é definido para qualquer perfil, mas você pode preferir modificar essa configuração para um minuto, se necessário.

Extraindo eventos notáveis novos e atualizados

Quando a programação de pesquisa é definida, o trabalho programado extrai eventos notáveis novos e atualizados que foram extraídos anteriormente, mas não atenderam aos critérios de filtragem de incidentes. Isso fornece a flexibilidade para criar incidentes com base em critérios que podem não estar presentes quando um evento relevante é criado pela primeira vez, mas se torna disponível após uma atualização, por exemplo, durante a fase de investigação. Depois que um incidente é criado para um evento de registro específico, suas atualizações subsequentes são ignoradas, já que é esperado que o evento de registro agora seja tratado como um incidente de segurança ServiceNow® ativo. No entanto, todos os outros notáveis que foram ingeridos anteriormente, mas não atenderam aos critérios de geração de incidentes, continuarão a ser extraídos e verificados em relação aos critérios de geração de incidentes até que se tornem parte de um incidente ativo.

Procedimento

1. Se a página Programação na barra de andamento não for exibida, selecione **Programação**.
2. Escolha um para programar como e quando eventos notáveis são extraídos do console Splunk Enterprise Security.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como exemplo para programar um horário de ingestão de evento notável inicial, se você tiver uma verificação de segurança diária Splunk que é executada uma vez por dia às 4h no horário local, é possível configurar o perfil de evento notável correspondente na sua instância Now Platform para ser executado às 4 :05 hora local para capturar o evento de falha de segurança imediatamente e criar um incidente de segurança. Insira `04 05 00` no campo Ingestão de evento inicial. No campo Incrementar (minutos), insira `1440` (24 horas) para programar a próxima ingestão de evento por 24 horas a partir da ingestão de evento inicial. O tempo de ingestão do evento inicial e o tempo de ingestão do próximo evento são exibidos nos campos.

3. Para definir as configurações deste exemplo, siga estas etapas.

   a. Com a página Programação exibida, marque a caixa de seleção **Ingestão de evento em andamento** para habilitar esta opção.

   b. No campo Incrementar (minutos), insira `1440` (24 horas).

   c. Clique na caixa de seleção **Selecionar ingestão de evento inicial** para habilitar a edição dos campos Ingestão de evento inicial e Próxima ingestão de evento.

   d. No campo Ingestão de evento inicial, insira `04 05 00`.
   No campo Próxima ingestão de evento (estimada), a hora da próxima ingestão de evento é exibida.

4. Clique em uma das opções a seguir para continuar com a configuração do perfil.

Automatizar atualizações de eventos notáveis e fechamento com base no status do incidente SIR

Os incidentes de segurança podem ser criados e atualizados depois de criados com uma interface bidirecional com a integração Splunk Enterprise Security.

Antes de Iniciar

A integração Splunk Enterprise Security tem uma interface bidirecional que permite que eventos notáveis criem incidentes de segurança, bem como atualizem os eventos notáveis depois que o incidente de segurança for criado e/ou encerrado.

Os detalhes relevantes do incidente incluem SIR número do incidente, grupo de atribuição, SIR URL do incidente. Esta seção é a parte final da configuração do perfil que fornece recursos opcionais para atualizar os Splunk Enterprise Security eventos notáveis.

Função necessária: sn_si.admin

Procedimento

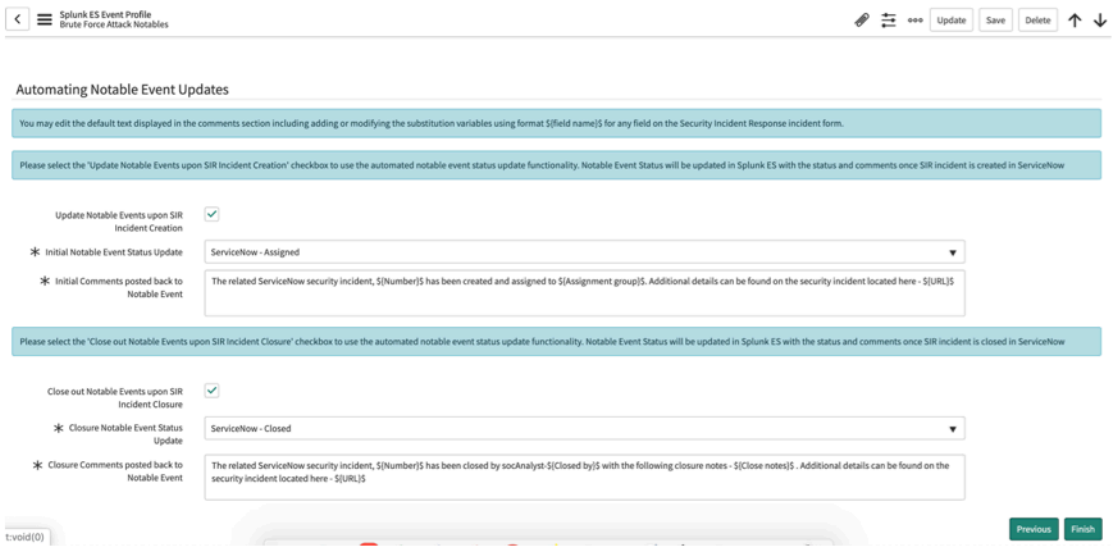
1. Se a página Opções adicionais na barra de andamento não for exibida, selecione **Opções adicionais**.
2. Siga as instruções abaixo para concluir a configuração para atualizar eventos notáveis com base em atualizações de incidentes de segurança.

3. Clique em **Concluir** para concluir a configuração.
   Uma caixa de diálogo de confirmação é exibida. Você concluiu com êxito a instalação e a configuração da integração. Ative este perfil para extrair eventos notáveis do console Splunk Enterprise Security com base em sua programação. Há um limite de 1.000 incidentes de segurança que podem ser criados em um período de 24

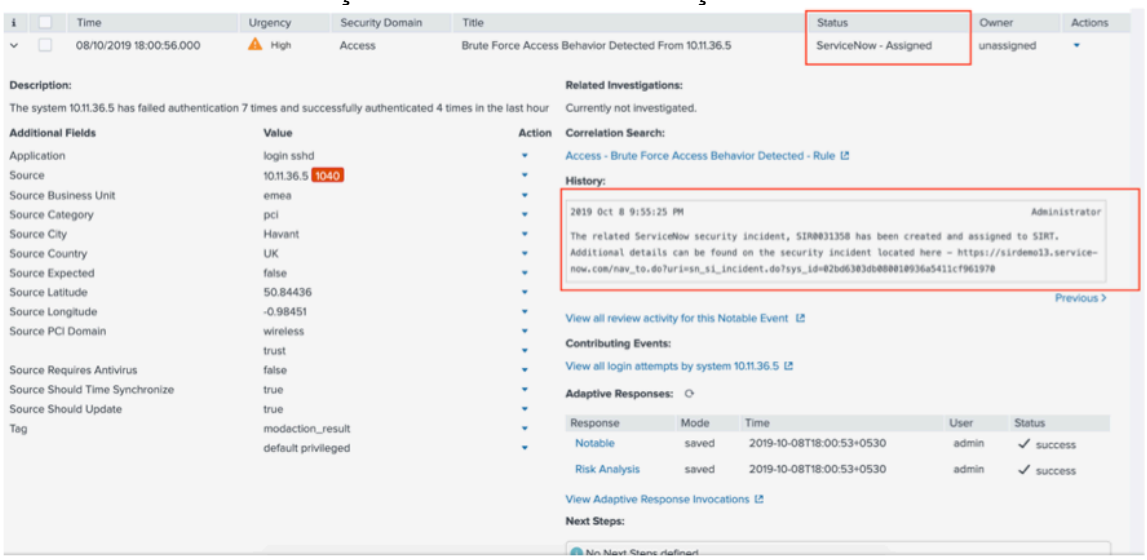
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

horas. Até 100 eventos notáveis são por alerta acionado. Os eventos notáveis subsequentes serão ignorados depois que os limites forem atingidos.

A imagem a seguir mostra a guia Opções adicionais com os valores padrão preenchidos:



Com a configuração de Opções adicionais habilitada, a revisão de incidente de evento relevante mostra a mudança de status e uma atualização dos comentários do histórico:



Configurar um perfil para encaminhamento manual de eventos

Dependendo do perfil definido, Splunk ES eventos notáveis são encaminhados manualmente como eventos notáveis discretos para o ambiente Security Operations da sua instância Now Platform.

Para configurar um perfil para encaminhamento manual de eventos notáveis:

Tarefa	Seção
Criar um perfil de evento	Veja Criar perfis para eventos encaminhados manualmente

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Seção
Mapear campos de evento notáveis	Veja Mapeamento de campos de evento notáveis para a integração Splunk Enterprise Security
Criar mapeamentos personalizados	Veja Criar mapeamentos para Splunk ES revisão de incidente de evento relevante e detalhes do evento de contribuição (encaminhamento manual)
Visualizar o incidente de segurança	Veja Visualizar o incidente de segurança para a integração de ingestão de eventos Splunk Enterprise Security
Configure seu ambiente Splunk para ingestão manual	Veja Configure seu ambiente Splunk para ingestão manual de eventos para a integração de ingestão de eventos notáveis Splunk Enterprise Security
Automatizar atualizações de eventos notáveis e fechamento com base no status do incidente SIR	Veja Automatizar atualizações de eventos notáveis e fechamento com base no status do incidente SIR

Criar perfis para eventos encaminhados manualmente

Você pode configurar um perfil para eventos encaminhados manualmente.

Antes de Iniciar
Função necessária: sn_si.admin

Procedimento

Para criar um perfil que ofereça suporte ao encaminhamento manual de eventos, siga estas etapas.

Para eventos que você encaminha sob demanda do console Splunk Enterprise Security, é possível basear o mapeamento de campo individual em qualquer perfil existente. Como alternativa, você pode criar uma nova grade de mapeamento para dados de anexo exportados. Os eventos encaminhados manualmente não são programados no perfil de evento.

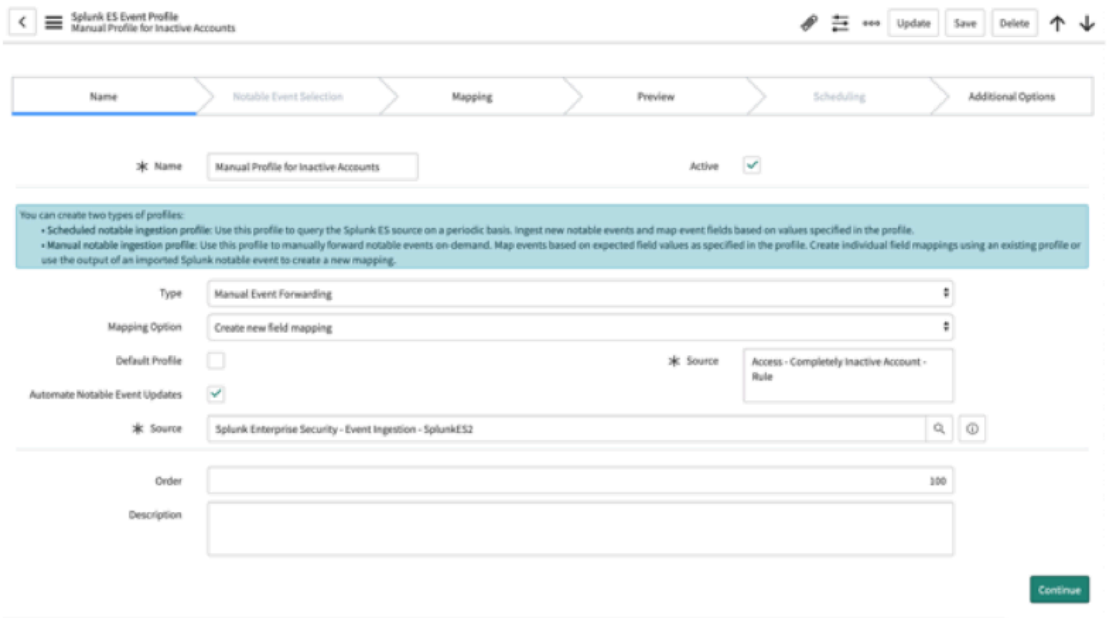
a. Se ainda não estiver selecionado, na lista de seleção do campo Tipo, selecione **Encaminhamento manual de eventos**.

b. No campo Opção de mapeamento exibido, na lista de seleção, escolha uma opção de mapeamento para continuar.

Consulte as imagens e tabelas a seguir para obter mais informações sobre as opções de mapeamento disponíveis na lista de seleção Opções de mapeamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Criar nova opção de mapeamento de campo

Opção ou campo	Descrição
Criar nova opção de mapeamento de campo	Novo mapeamento de campo para o seu evento. Se você não tiver um mapeamento de campo semelhante ao perfil que está criando, selecione esta opção para criar um novo mapa.
Perfil padrão	Perfil de encaminhamento de evento padrão para todos os eventos Splunk. O padrão é limpo (desativado). Quando esta opção está habilitada, este perfil se torna o perfil padrão para encaminhamento de evento manual. Este perfil é usado quando não há correspondência na origem do evento encaminhado manualmente. Ele se torna o perfil padrão para todos os eventos com origens desconhecidas. O campo Origem não estará disponível se a opção de perfil padrão estiver habilitada.
Origem (campo Evento Notável)	Este é um campo que normalmente define a regra de correlação que acionou o notável, por exemplo, ataques de força bruta. Este campo não estará disponível se a opção de perfil padrão estiver habilitada. Se disponível, este campo permite o mapeamento de campo de evento exclusivo para campos de incidente de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

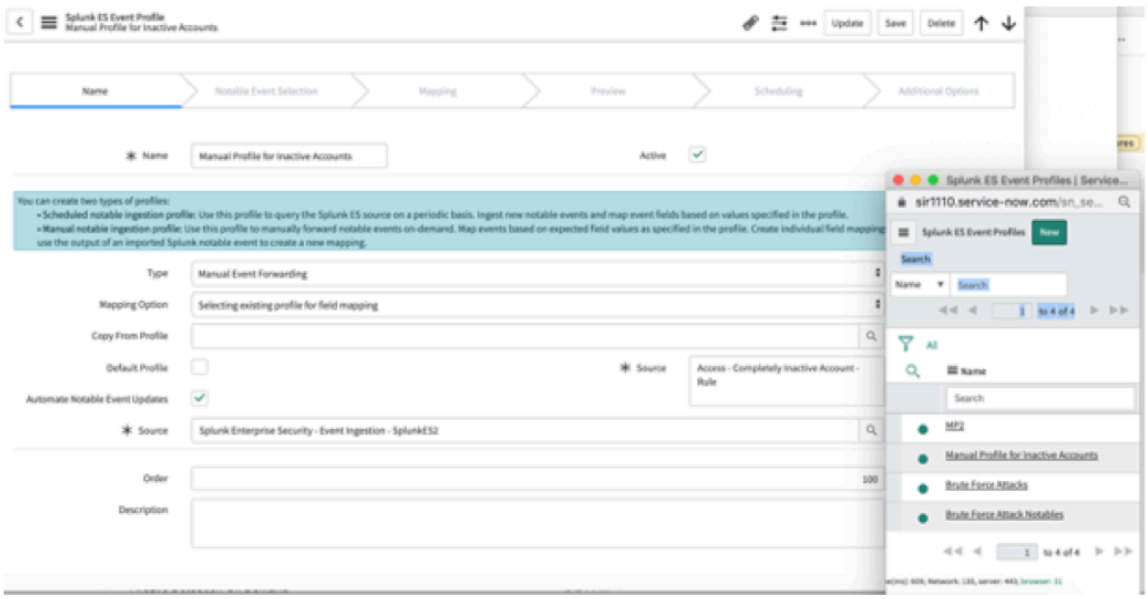
Opção ou campo	Descrição
	com base na regra de correlação de splunk que normalmente é diferente para diferentes tipos de evento. Se você quiser gerenciar diferentes regras de correlação separadamente, poderá criar diferentes perfis de evento com base na regra de correlação para atender a esse requisito.
Automatizar atualizações de eventos notáveis	Marque esta caixa de seleção se quiser atualizar o status do evento de notificação e adicionar comentários adicionais quando um incidente de SIR for criado a partir do evento de notificação e/ou quando o incidente de SIR for encerrado. Isso ocorrerá para os eventos notáveis de acionamento inicial que criam o incidente de SIR, bem como para os eventos agregados.
Origem (Splunk Servidor)	O servidor Splunk que você configurou como a origem dos eventos notáveis. Se você tiver vários servidores Splunk configurados, selecione o servidor apropriado para os tipos de evento notáveis que serão atualizados para o perfil. É necessário inserir um valor.
Ordem	O padrão é 100. Deixe esta configuração como padrão. Se você tiver criado um grande número de perfis, este valor fornecerá uma prioridade de execução em tempo de execução quando dois ou mais perfis compartilharem condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este perfil de outros perfis.

Para um perfil com um novo mapeamento de campo, verifique se você inseriu um valor no campo Tipo de origem e clique em **Continuar** para prosseguir para a etapa de mapeamento da configuração.

Para obter um perfil com um mapeamento de campo existente, consulte a figura e a tabela a seguir para obter mais informações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Selecione o perfil existente para a opção de mapeamento de campo

Opção ou campo	Descrição
Selecionar perfil existente para mapeamento de campo	Reutilize um mapeamento de campo existente para o novo perfil de evento do Notable. O campo Copiar do perfil é exibido. Siga estas etapas para copiar um mapeamento de campo existente para este perfil. **i.** À esquerda do campo Copiar do perfil exibido, clique no ícone de pesquisa. **ii.** Na lista Splunk Perfis de evento ES exibida, clique no nome do perfil que tem o mapa que você deseja copiar. O nome do perfil é exibido no campo Copiar do perfil.
Perfil padrão	Perfil de encaminhamento de evento padrão para todos os eventos notáveis Splunk com origem incompatível. O padrão é desabilitado. Quando esta opção está habilitada, este perfil se torna o perfil padrão para encaminhamento de evento manual. O campo Origem não estará disponível se a opção de perfil padrão estiver habilitada.
Origem (campo Evento Notável)	Este é um campo que normalmente define a regra de correlação que acionou o notável, por exemplo, ataques de força bruta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção ou campo	Descrição
	Este campo não estará disponível se a opção de perfil padrão estiver habilitada. Se disponível, este campo permite o mapeamento de campo de evento exclusivo para campos de incidente de segurança com base na regra de correlação de splunk que normalmente é diferente para diferentes tipos de evento. Se você quiser gerenciar diferentes regras de correlação separadamente, poderá criar diferentes perfis de evento com base na regra de correlação para atender a esse requisito.
Automatizar eventos notáveis	Marque esta caixa de seleção se quiser atualizar o status do evento de notificação e adicionar comentários adicionais quando um incidente de segurança for criado a partir do evento de notificação ou quando o incidente de segurança for encerrado. Isso ocorre para os eventos notáveis de acionamento inicial que criam o incidente de segurança, bem como para os eventos agregados.
Origem (Splunk Servidor)	Splunk servidor ou final de pesquisa que você configurou como a origem dos eventos notáveis. Se você tiver vários servidores Splunk configurados, selecione o servidor apropriado para os tipos de evento notáveis que serão atualizados para o perfil. É necessário inserir um valor.
Ordem	O padrão é 100. Deixe esta configuração como padrão. Se você tiver criado vários perfis, este valor fornecerá uma prioridade de execução em tempo de execução quando dois ou mais perfis compartilharem condições de acionamento. O fluxo de trabalho no perfil com o número mais baixo tem a prioridade mais alta.
(Opcional) Descrição	Texto para ajudá-lo a distinguir este perfil de outros perfis.

Na parte inferior do formulário para selecionar um mapeamento existente para o seu perfil, clique em **Concluir** para concluir a configuração do perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar mapeamentos para Splunk ES revisão de incidente de evento relevante e detalhes do evento de contribuição (encaminhamento manual)

Durante a etapa de mapeamento de campo de evento notável, você mapeia campos de evento individuais de eventos notáveis para campos em um incidente de segurança Now Platform Security Incident Response (SIR).

Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Mapeie até cinco eventos notáveis da coluna Ingestão de amostra de evento notável à esquerda do formulário para os campos de incidente de segurança na coluna Mapeamento de campo de incidente SIR à direita.

Crie mapeamentos personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Os campos padrão que são normalmente campos importantes a serem preenchidos no formulário de incidente SIR são exibidos. No entanto, esses campos podem ser removidos e quaisquer campos adicionais podem ser exibidos usando os botões + e -. Crie mapas personalizados adicionando ou removendo os campos na grade de mapeamento no lado direito do formulário. Personalizar os campos permite mapear Splunk campos que não são exibidos na grade de mapeamento padrão no incidente de segurança SIR.

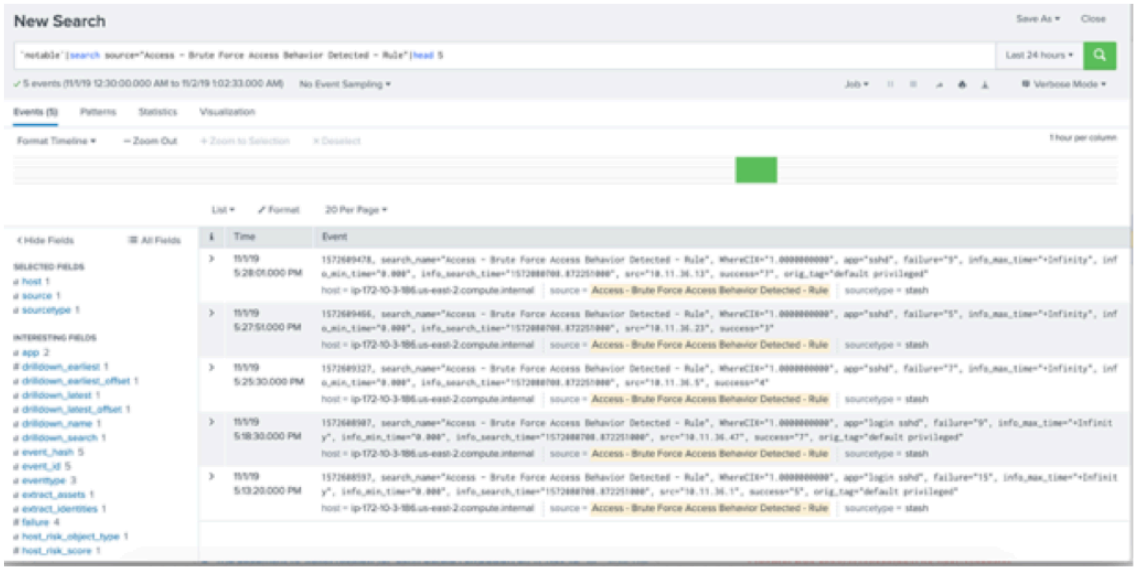
Procedimento

1. Se o formulário de mapeamento não for exibido, clique em **Mapeamento** na barra de andamento.
2. Siga estas etapas para carregar dados de anexo em sua instância Now Platform®.
   a. Se ainda não estiver conectado, faça login no console Splunk Enterprise.
   b. Navegue até a guia Pesquisar e insira um nome para uma pesquisa que tenha os dados de evento notáveis que você deseja exportar.
   Um exemplo de formato de pesquisa para recuperar eventos notáveis para a regra de correlação de comportamento de acesso de força bruta seria o seguinte: `notable`|search source="Access - Brute Force Access Behaviour Detected - Rule".
   c. Expanda o evento relevante e, na coluna Campo, selecione os campos que deseja importar.

   Esses campos são os pares de campo-valor que são exportados e exibidos na página Mapeamento na sua instância Now Platform®.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

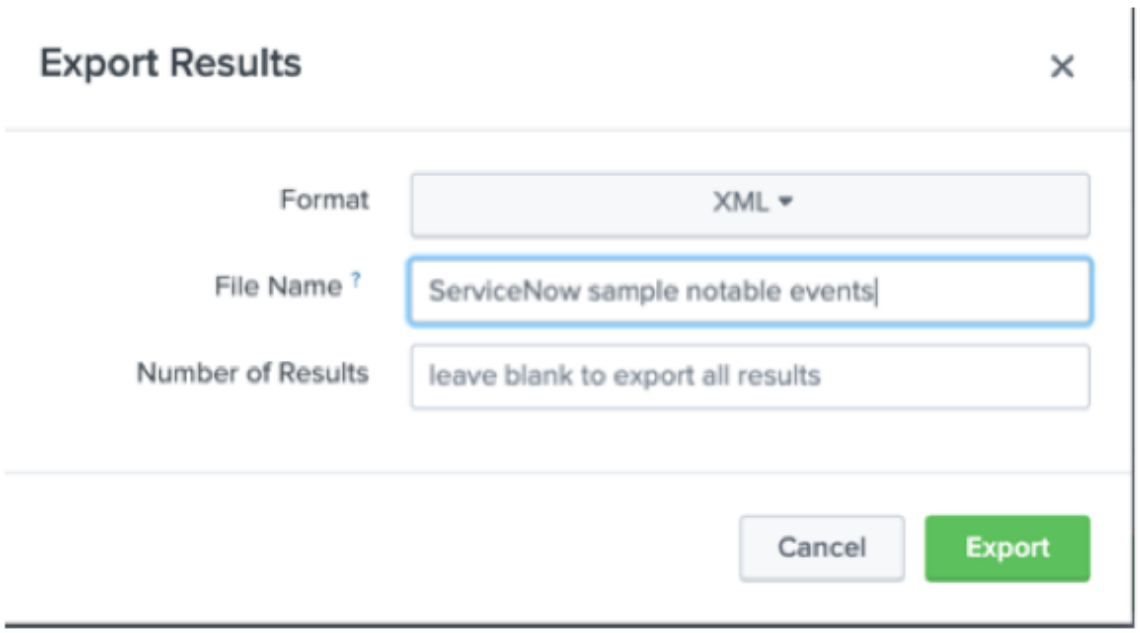


d. No console Splunk Enterprise, no canto superior direito da página de pesquisa, clique no ícone **Exportar**.

e. Na lista de seleção do campo Formato na caixa de diálogo exibida, clique em **Formato XML**.

f. Opcional: Insira um novo nome de arquivo.

g. Clique em **Exportar**.



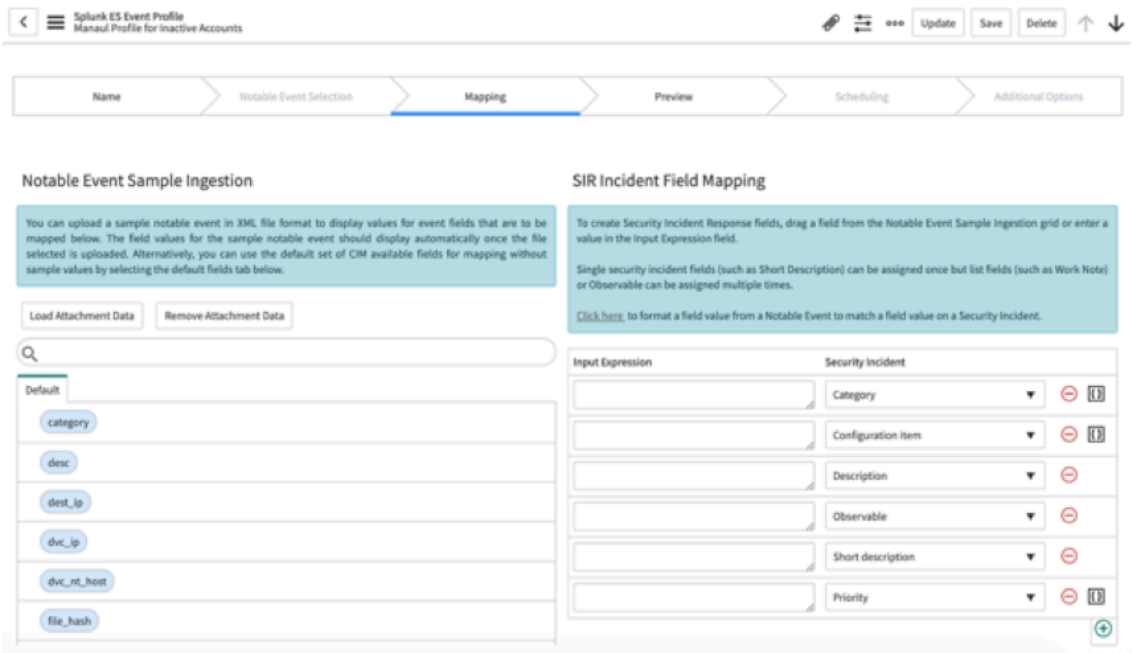
O arquivo XML de evento relevante Splunk exportado agora deve ser carregado para sua instância Now Platform®.

h. Se a página Mapeamento ainda não estiver exibida na sua instância Now Platform®, clique em **Mapeamento** na barra de andamento.

i. Na coluna Ingestão de amostra de evento notável, clique em **Carregar dados de anexo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



j. Na caixa de diálogo exibida, clique em **Escolher arquivos**, navegue até o arquivo .xml que você exportou e clique em **Abrir**.
Depois de clicar para carregar dados de anexo para eventos encaminhados manualmente, os campos de evento notáveis Splunk ES são preenchidos no lado esquerdo do formulário. Esses valores são os valores de campo que você mapeia para os campos de incidente de segurança no lado Mapeamento de campo de incidente de Sir do formulário.
Os pares de valores dos campos que você exportou para o evento são exibidos no lado esquerdo do formulário de mapeamento.

3. Siga as etapas 5 a 10 na seção Criar mapeamentos para Splunk ES revisão de incidente de evento notável e detalhes do evento de contribuição (ingestão programada).

Configure seu ambiente Splunk para ingestão manual de eventos para a integração de ingestão de eventos notáveis Splunk Enterprise Security

Instale e configure o aplicativo ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security no console empresarial Splunk ou na instância do Splunk Cloud se quiser exportar eventos manualmente e sob demanda do console Splunk Enterprise Security para esta integração.

Antes de Iniciar

Instalar e configurar a aplicação ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security no console empresarial Splunk ou na instância do Splunk Cloud é opcional.

Verifique se você instalou a aplicação para esta integração do ServiceNow Store antes de instalar o plug-in do complemento do splunkbase que é necessário para a ingestão manual de eventos. Se você não instalou o aplicativo para a integração do ServiceNow Store, consulte Instalar e configurar a aplicação ServiceNow para a integração de ingestão de eventos notáveis Splunk Enterprise Security e siga as instruções para instalá-lo.

Função necessária: Splunk Enterprise Security administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Se você quiser exportar eventos manualmente e sob demanda do console Splunk Enterprise para a integração, baixe, instale e configure o ServiceNow Complemento de ingestão de eventos do Security Operations para Splunk Enterprise Security do splunkbase no console Splunk Enterprise Security. Este complemento de extensão ServiceNow é necessário para que os incidentes de segurança possam ser criados a partir de eventos exportados manualmente em sua instância Now Platform. Esta aplicação ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security está disponível em splunkbase .

Para o encaminhamento manual de eventos, você pode identificar até dois Now Platform endpoints (instâncias) diferentes no console Splunk Enterprise Security. Você encaminha os eventos para o endpoint ou endpoints manualmente para criar incidentes de segurança. Por exemplo, você pode especificar uma instância de preparação (desenvolvimento) e uma instância de produção. Ao especificar instâncias separadas e nomear fluxos de trabalho primários e secundários para cada instância, você pode escolher para onde deseja encaminhar eventos diferentes.

Procedimento

1. Se você ainda não instalou o ServiceNow Complemento de ingestão de eventos do Security Operations para Splunk Enterprise Security, siga estas etapas para instalá-lo e configurá-lo.

   a. Navegue até splunkbase .

   b. Pesquise o ServiceNow Security Operations Complemento de ingestão de eventos do Security Operations para Splunk Enterprise Security.

   Nota:
   Verifique se você selecionou ServiceNow Security Operations Complemento de ingestão de eventos para Splunk Enterprise Security. Há complementos ServiceNow adicionais que são exibidos nesta lista. Esses complementos são para diferentes integrações ServiceNow Splunk e não são necessários para esta integração.

   c. Baixe a aplicação.

   d. Abra sua conta Splunk Enterprise Security.

   e. Na página Aplicativos, clique no ícone de engrenagem ou no atalho **Gerenciar aplicativos** na lista suspensa do menu.

   f. No canto superior esquerdo da página Aplicativos exibida, clique em **Instalar aplicativo do arquivo**.

   g. Clique em **Escolher arquivo**, selecione ServiceNow Complemento de ingestão de eventos do Security Operations para Splunk Enterprise Securitye clique em **Carregar**.

   h. Se solicitado, reinicie Splunk Enterprise.
   O ServiceNow Complemento de ingestão de eventos do Security Operations para Splunk Enterprise Security está instalado no console Splunk Enterprise Security. A próxima etapa é configurar o complemento.

2. Para configurar o complemento, siga estas etapas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Em Splunk Enterprise Security, clique no ícone de engrenagem de **aplicativos** ou em **Gerenciar aplicativos** na lista suspensa do menu.

b. Na lista de aplicações exibida, na coluna **Ações**, clique em **Configurar** para ServiceNow Security Operations Complemento de ingestão de eventos para Splunk Enterprise Security.

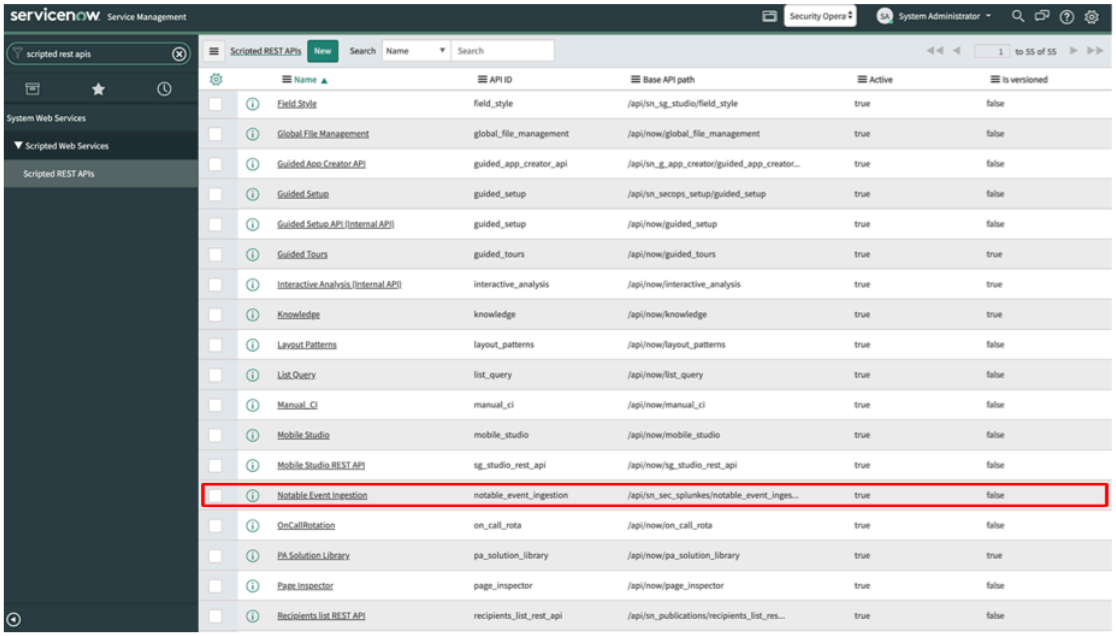
c. Preencha o formulário.

A figura a seguir é um exemplo de um formulário preenchido no console Splunk Enterprise Security.

A figura a seguir é um exemplo da lista de Scripted REST APIs em seu Now Platform. A lista exibe o local do valor do endpoint de uma instância Now Platform que você insere no formulário como parte da configuração da extensão ServiceNow Security Operations Event Ingestion Addon for Splunk Enterprise Security no console Splunk Enterprise Security.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. No formulário de configuração do console Splunk Enterprise Security, clique em **Salvar** para salvar suas edições.

   Após alguns momentos, na parte superior esquerda do formulário no console Splunk Enterprise Security, será exibida uma mensagem informando que o registro foi atualizado com sucesso.

   Depois de salvar o formulário, os nomes (rótulos de ação de fluxo de trabalho) das instâncias Now Platform que você criou no formulário estão disponíveis na lista de seleção Ações de evento em um evento selecionado de uma pesquisa no console Splunk Enterprise Security.

O que Fazer Depois

Se você ainda não salvou pesquisas no console Splunk Enterprise Security, a próxima etapa é salvar pesquisas como alertas no console Splunk Enterprise Security.

Copie um perfil de evento para a integração de ingestão de eventos Splunk Enterprise Security

Copie um perfil existente e suas configurações associadas em vez de criar novos perfis. Se você estiver criando vários perfis e quiser reutilizar as configurações de um perfil existente, convém copiar os perfis de alarme para economizar tempo.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

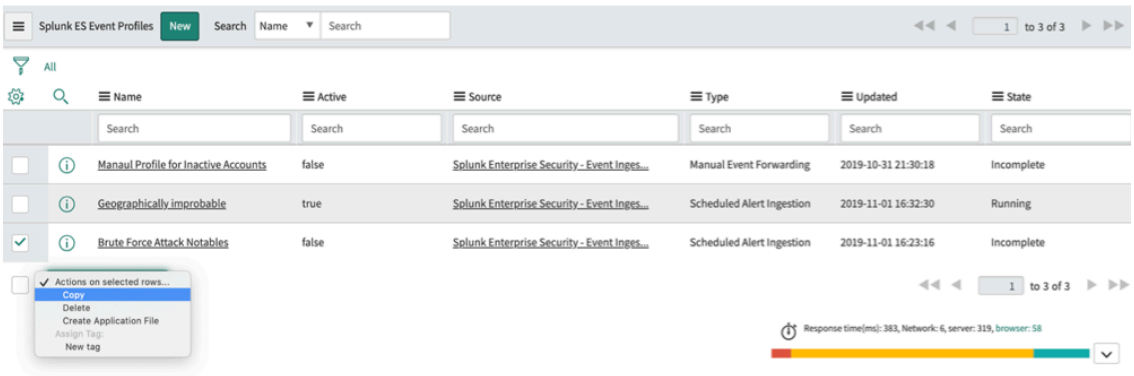
Se você copiar um perfil, o nome do perfil será modificado inicialmente para evitar perfis duplicados. Além disso, o perfil copiado é desativado (falso) para que não seja ativado acidentalmente antes de concluir a configuração. Copie perfis e use mapas existentes para incidentes de segurança que você já visualizou e verificou.

Tradução automática

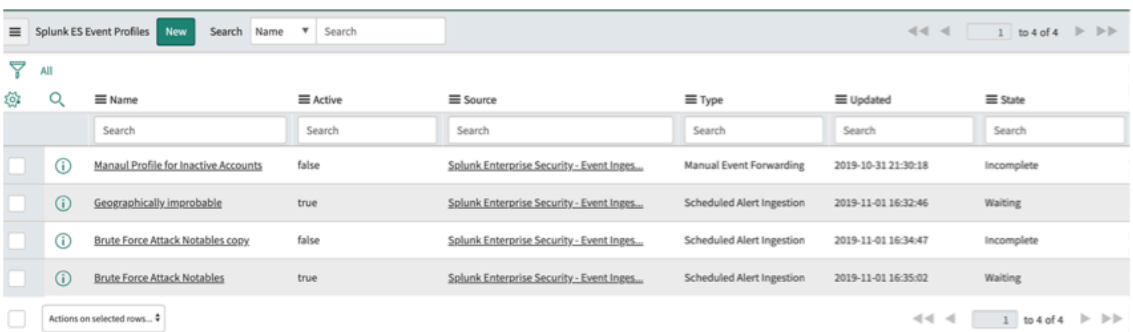
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Splunk Integration** > **Perfil de evento do Splunk**.
2. Na lista Splunk Perfis de evento exibida, selecione um perfil que você deseja copiar e, na lista de seleção Ações nas linhas selecionadas, clique em **Copiar**.



O perfil é copiado e exibido na lista. A cópia tem todas as configurações do perfil original, incluindo o mapeamento e a configuração de programação. O nome do perfil contém cópia. Embora o perfil original esteja ativado (verdadeiro), a cópia está desabilitada neste ponto (falso). Você pode editar os valores do perfil copiado e renomeá-lo para que as definições de configuração se apliquem ao novo perfil, conforme necessário.



Você copiou com sucesso as configurações de um perfil existente para um novo perfil.

O que Fazer Depois

Você será solicitado a ativar (habilitar) o novo perfil depois de concluir a etapa de configuração.

Use o editor de script para formatar valores de alerta para a integração de ingestão de eventos Splunk Enterprise Security

Além dos campos mapeados diretamente dos valores de evento notáveis ingeridos e dos valores inseridos manualmente, use o editor de script para formatar valores de campo no incidente de segurança durante a etapa de mapeamento.

Antes de Iniciar

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

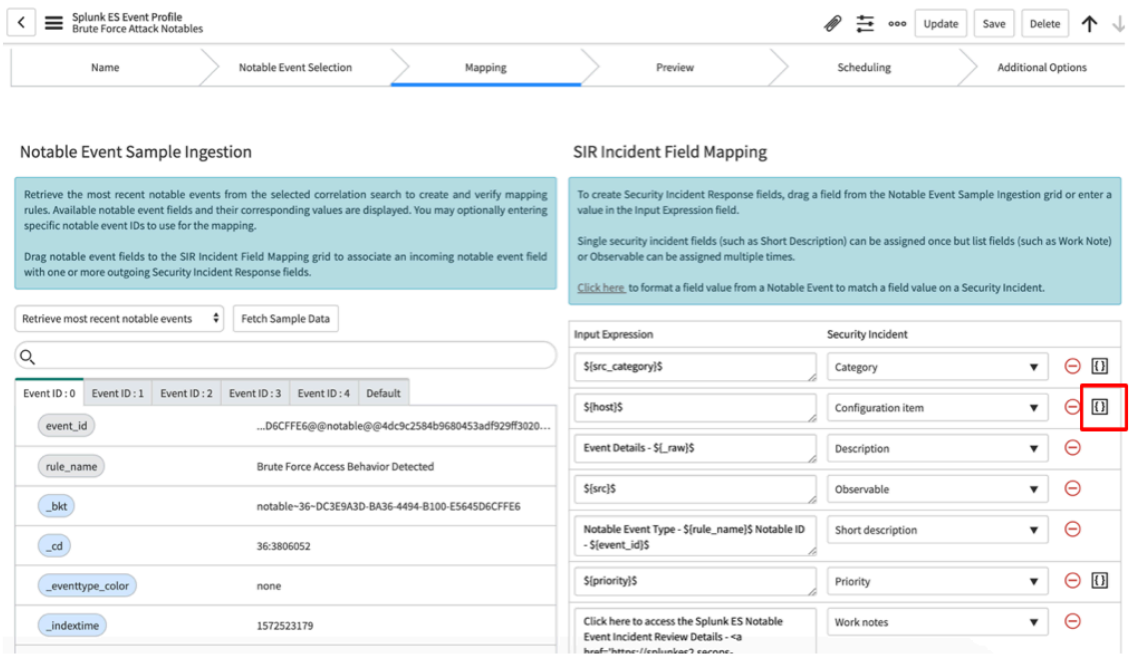
Em determinados casos, os valores de evento notáveis Splunk Enterprise Security são mapeados para a Categoria, Item de configuração (IC) e os campos Observável no incidente SIR não são compatíveis. Você pode preferir editar os valores mapeados. Se você quiser traduzir o valor de um evento notável Splunk Enterprise Security para um valor que seja compatível com esses campos no incidente de segurança SIR, use o editor de script.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Com o formulário de mapeamento exibido, clique no link para abrir o editor de script.



2. Na lista de seleção, selecione um campo de destino para o valor que você deseja editar.
3. Como alternativa, na seção Mapeamento de campo de incidente de SIR, clique no ícone de colchete [{}] ao lado de um campo para abrir o editor de script desse campo.

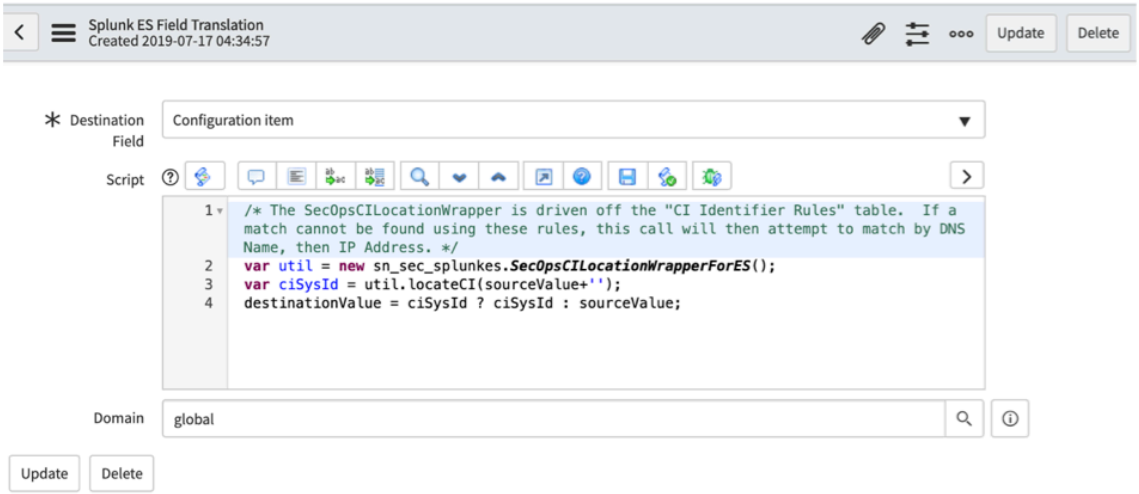
   Em determinadas instâncias, uma inclusão de script pode ser apropriada para o campo Item de configuração. Para um evento notável, por exemplo, um valor para o Item de configuração pode não ser correspondido.

   Conforme mostrado na figura a seguir, se uma correspondência para um nome de host não puder ser encontrada no Now Platform® CMDB para o campo Item de configuração, você poderá editar a regra para que, se um endereço IP for encontrado, ele preencha o campo Item de configuração. Se não houver valor para o alarme, o campo no incidente de segurança será definido como nulo.

   O editor é aberto com o campo exibido no Campo de destino. A imagem a seguir mostra o editor com o campo Item de configuração como o Campo de destino.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Insira as mudanças no script e clique em **Atualizar** para salvar as mudanças.
   A tabela Splunk Traduções de campo é exibida.
5. Feche a tabela para retornar ao formulário de mapeamento.

Copiar Splunk Enterprise Security perfis de uma instância para outra usando a funcionalidade de exportação/importação

Você pode exportar e importar configurações de perfis [Splunk Enterprise Security de uma instância Now Platform para uma instância Now Platform diferente.

Antes de Iniciar

As configurações que você pode exportar e importar incluem nome do perfil, regras de correlação, mapeamentos, filtros, critérios de agregação, traduções de campos, dados de amostra obtidos, programação e informações de origem do bloco de configuração.

Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa

Esta funcionalidade permite que o administrador de segurança copie perfis que foram testados e verificados em uma instância Now Platform, por exemplo, em não produção, para outra instância Now Platform, por exemplo, produção, sem a necessidade de refazer todas as definições de configuração. As configurações exportadas e importadas incluem nome do perfil, regras de correlação, mapeamentos, filtros, critérios de agregação, traduções de campos, dados de amostra obtidos, programação e informações de origem do bloco de configuração.

Nota:
Quando você exporta um tipo de perfil de encaminhamento de evento manual, os dados de anexo usados para o mapeamento de campo de amostra são copiados, no entanto, o arquivo de anexo em si não é exportado.

Procedimento

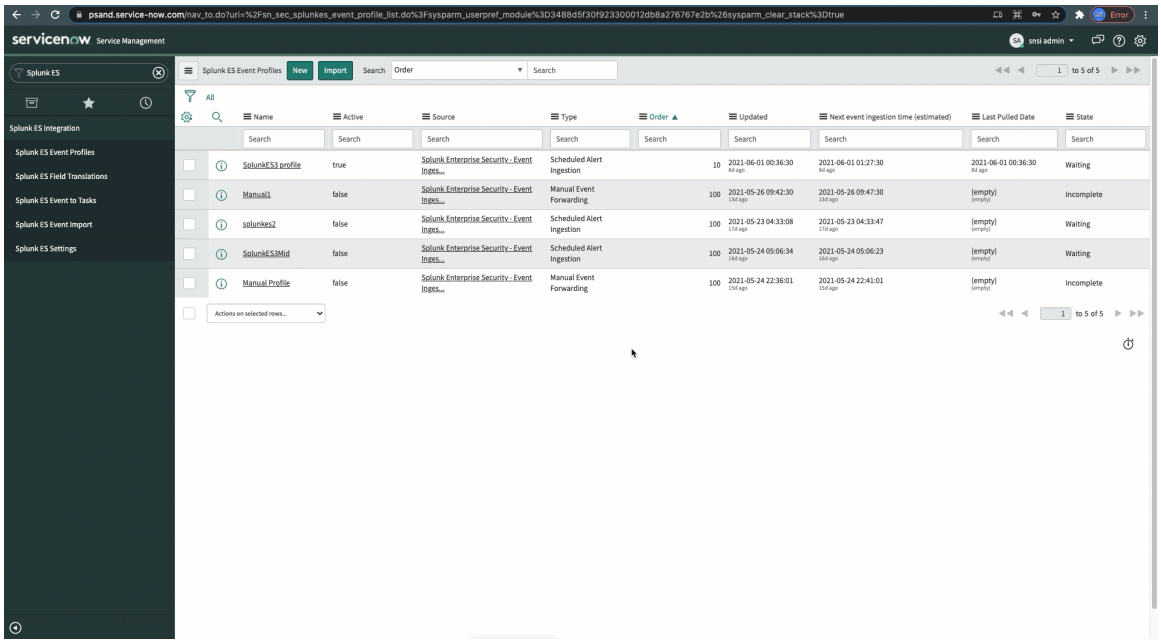
1. Navegar até **Todos** > **Splunk ES Integration** > **Splunk ES Event Profiles**.
2. Selecione um perfil que você deseja exportar para outra instância Now Platform.
   Você pode selecionar vários perfis para exportação.
3. No menu Ações, clique em **Exportar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Quando a mensagem de conclusão da exportação for exibida, clique em **Download**.

   A ilustração a seguir mostra a exportação de um perfil (SplunkES3profile) da instância Now Platform (psand.service-now.com).



   O arquivo payload.xml exportado é baixado no seu computador. O arquivo contém o nome do perfil, regras de correlação, mapeamentos, filtros, critérios de agregação, traduções de campos, dados de amostra obtidos, programação e informações de origem do bloco de configuração. Quando você seleciona e baixa vários perfis, eles aparecem no mesmo arquivo payload.xml.

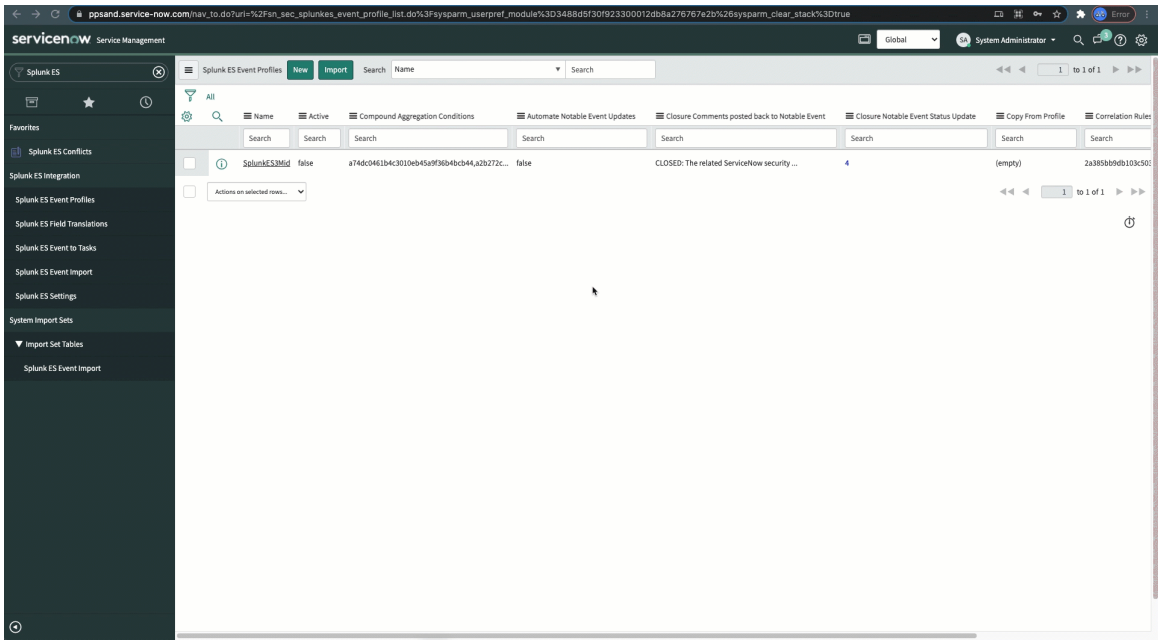
   Agora você pode prosseguir para importar o perfil em outra instância Now Platform.

5. Navegar até **Splunk ES Integration** > **Splunk ES Event Profiles**.
6. Clique em **Importar**.
7. Clique **em Escolher arquivo** e selecione o arquivo xml no seu computador.
8. Clique em **Carregar**.
9. Clique **em Fechar e Recarregar Perfis**.

   A ilustração a seguir mostra a importação de um perfil (SplunkES3profile) da instância Now Platform (psand.service-now.com) para a instância Now Platform (ppsand.service-now.com).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você importou com sucesso o perfil de outra instância Now Platform.

Verifique se a origem exportada (Splunk conta da API e Splunk URL do servidor) e as configurações do MID Server são válidas e estão disponíveis na instância Now Platform importada. Atualize sua configuração Splunk Enterprise Security, se necessário.

10. **Opcional:** Verifique as configurações do MID Server após importar um perfil.
11. **Opcional:** Navegar até **Security Operations** > **Configurações de Integração**.
12. **Opcional:** Selecione o bloco de configuração Splunk Enterprise Security e clique em **Atualizar**.
13. **Opcional:** Revise e atualize a origem e os detalhes do MID Server conforme necessário.

Check-list para a integração de ingestão de eventos notáveis Splunk Enterprise Security

Use esta check-list para orientar você em todas as tarefas da integração. A check-list a seguir inclui tarefas de configuração e instalação e exemplos de casos de uso que incluem os resultados esperados para a integração.

Antes de Iniciar

Funções necessárias: admin, sn_si.admin, sn_si.analyst, Splunk Enterprise Security administrador

Por Que e Quando Desempenhar Esta Tarefa

Acompanhe seu progresso com a instalação e configuração da integração com a tabela a seguir. Conclua todas as tarefas de uma etapa antes de passar para a próxima. Cada linha da tabela lista as tarefas e identifica as funções necessárias para executar as tarefas. Tópicos numerados do guia de instalação e configuração também são referenciados.

As funções necessárias para cada tarefa são listadas com cada etapa na tabela a seguir.

Procedimento

1. Acompanhe seu progresso com a instalação e configuração da integração.
   Conclua todas as tarefas de uma etapa antes de passar para a próxima.
2. Siga as etapas na tabela na ordem em que são apresentadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

☐	Como um usuário com a função de administrador Now Platform, configure sua instância Now Platform. ○ Atribua usuários com as funções sn_si.admin e sn_si.analyst conforme necessário. ○ Instale e configure um MID Server se o servidor Splunk for implantado em sua rede corporativa. ○ Verifique se os plug-ins ServiceNow Security Incident Response estão ativados para sua versão do Now Platform. ○ (Opcional) Se você quiser encaminhar eventos manualmente do console [Splunk Enterprise Security para a instância Now Platform, verifique se você atribuiu a função (sn_sec_splunkes.api_account_access) a um usuário com a permissão de administrador Splunk Enterprise Security. Para obter mais informações, consulte Configure sua instância Now Platform para a integração Splunk Enterprise Security.
☐	Como um usuário com a função de administrador Now Platform, instale e configure a aplicação Splunk Enterprise Security do ServiceNow Store. **a.** Baixe e instale a aplicação na sua instância Now Platform. **b.** Configure a aplicação e conecte ao seu console Splunk Enterprise Security. Para obter mais informações, consulte Instalar e configurar a aplicação ServiceNow para a integração de ingestão de eventos notáveis Splunk Enterprise Security.
☐	(Opcional) Se você pretende exportar eventos manualmente do console [Splunk Enterprise Security para a instância Now Platform, execute as seguintes tarefas: ○ Como administrador Splunk Enterprise Security, instale, configure e habilite o ServiceNow Complemento de ingestão de eventos do Security Operations para Splunk Enterprise Security do splunkbase no console do Splunk Enterprise Security. ○ Como administrador Splunk Enterprise Security, se ainda não estiver configurado, salve pesquisas como eventos notáveis no console Splunk Enterprise Security. Para obter mais informações, consulte Configure seu ambiente Splunk para ingestão manual de eventos para a integração de ingestão de eventos notáveis Splunk Enterprise Security.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

☐	Como um usuário com a função Now Platform sn_si.admin, crie e nomeie um perfil de evento. Selecione o tipo de perfil na lista de seleção. As opções são um perfil de alerta programado que você usa para ingerir dados de amostra ou um perfil de evento que você usa para exportar dados de anexo manualmente do seu console Splunk Enterprise Security. ○ Para um alerta programado, selecione um alerta disponível. ○ Para o perfil de dados exportados manualmente, crie um novo mapa ou copie um mapa existente. Para obter mais informações, consulte Criar e nomear um perfil de evento para a integração de ingestão de eventos Splunk Enterprise Security.
☐	Como um usuário com a função Now Platform sn_si.admin, mapeie valores ingeridos ou dados de anexo que são exportados de Splunk Enterprise Security para Now Platform incidentes de segurança. **a.** Buscar dados de amostra para um alerta programado. **b.** (Opcional) Exporte os dados do anexo manualmente de Splunk Enterprise Security para um evento. **c.** Edite a configuração de mapeamento padrão. **d.** Opcionalmente, adicione critérios de filtragem, anexe um alerta a um incidente de segurança existente e use o editor de script. Para obter mais informações, consulte Mapeamento de campos de evento notáveis para a integração Splunk Enterprise Security e Criar mapeamentos para Splunk ES revisão de incidente de evento notável e detalhes do evento de contribuição (ingestão programada).
☐	○ Como um usuário com a função Now Platform sn_si.admin, visualize os dados de Splunk Enterprise que são exibidos em um incidente de segurança Now Platform. ○ Corrija erros ou adicione dados ausentes para que nenhuma mensagem de erro seja exibida. Para obter mais informações, consulte Visualizar o incidente de segurança para a integração de ingestão de eventos Splunk Enterprise Security.
☐	Como um usuário com a função Now Platform sn_si.admin, programe a recuperação de alerta para um perfil com um alerta programado. Para obter mais informações, consulte Programe e recupere eventos notáveis novos e atualizados para a integração de ingestão de eventos Splunk Enterprise Security.

Você concluiu com sucesso as etapas de configuração e verificou os resultados esperados para a integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Splunk - Integração de aprimoramento de incidentes

A integração Splunk - Incident Enrichment pesquisa seus logs e adiciona informações de vista relevantes aos seus incidentes de segurança.

Explorar Integrações do Security Incident Response	Configuração Introdução ao Splunk Search integration for Security Operations
Usar • Executar uma pesquisa de vistas • Integração do Security Operations - Fluxo de trabalho de pesquisa de detecções • Fluxo de trabalho do Security Operations Integration - Splunk Sightings Search • Exibir detalhes da pesquisa de detecções • Exibir Resultados da Pesquisa de Vistas	Desenvolver • ServiceNow Security Operations diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solução de problemas e informações adicionais • Solução de problemas de integração • Faça ou responda perguntas na comunidade do Security Operations • Pesquise artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Introdução ao Splunk Search integration for Security Operations

O softwareSplunk pesquisa, monitora e analisa big data gerado por máquina e se integra facilmente com Security Operations. Antes de usar a integração Splunk - Incident Enrichment, você deve baixá-la do ServiceNow Store e adicionar a URL base da API e as credenciais de login apropriadas.

Antes de Iniciar

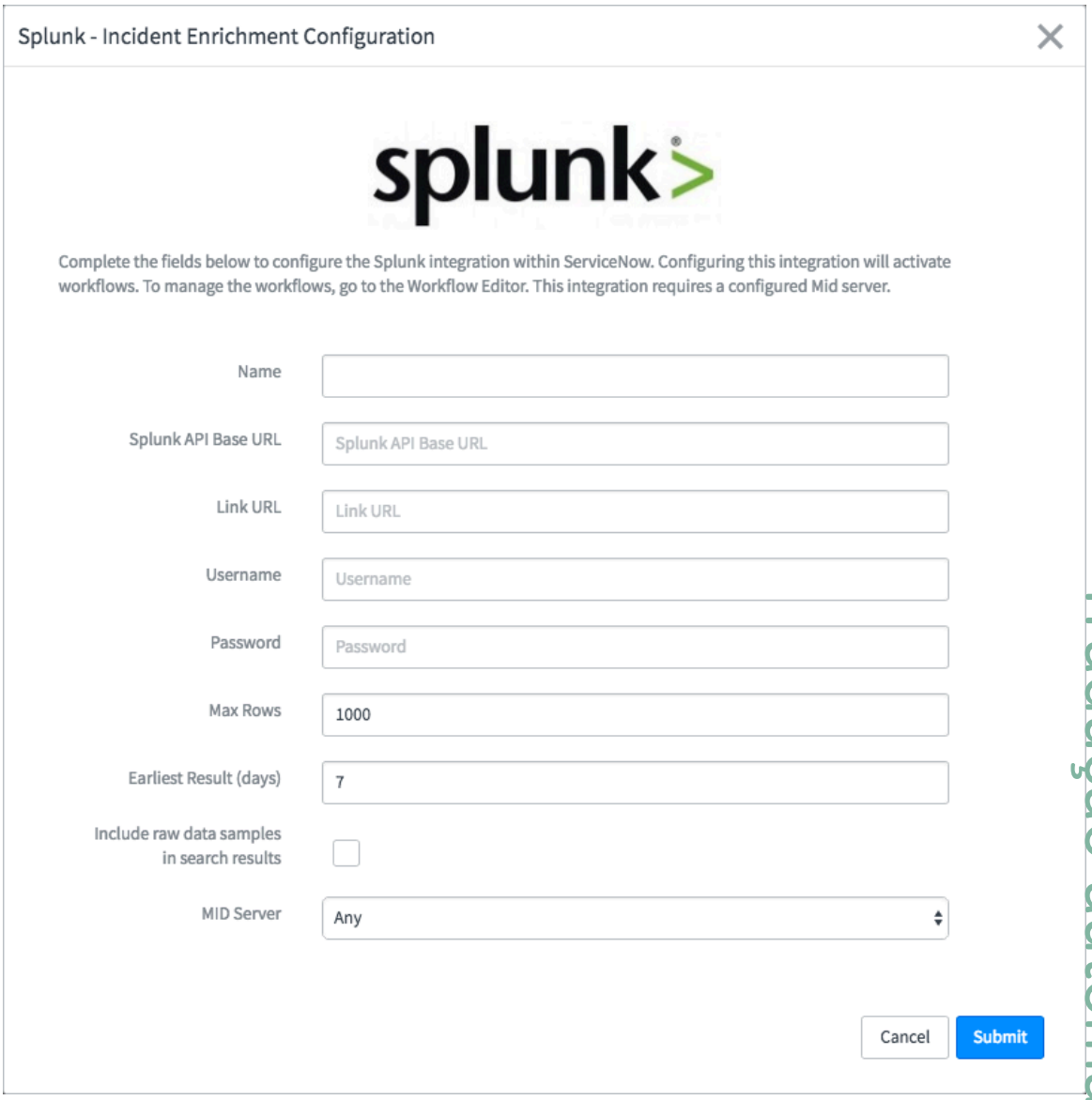
Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse Splunk e obtenha a Chave de API e o ID de API no seu perfil.
3. Em sua instância, navegue até **Security Operations** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão Splunk - Incident Enrichment, clique em **Novo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome desta configuração.
URL base da API Splunk	O URL base que você adquiriu no site Splunk.
URL do Link	[Opcional] A URL do link que vincula à interface da Web Splunk, quando disponível.
Nome do usuário	Seu nome de usuário do Splunk.
Senha	Sua senha do Splunk.
Máx. de Linhas	O número máximo de linhas que você deseja pesquisar.
Resultado Mais Antigo (dias)	Os resultados mais antigos que você deseja ver em número de dias.
Incluir amostras de dados brutos	Selecione esta opção para incluir amostras de dados brutos nos resultados da pesquisa de detecções. A quantidade de dados retornados depende da configuração na

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
nos resultados da pesquisa	propriedade do **número de linhas de dados brutos** nas propriedades do Security Incident Response.
MID Server	Selecione **Qualquer** para usar qualquer MID Server ativo ou selecione um nome de MID Server específico.

Nota:
Configurar esta integração ativa fluxos de trabalho. Para gerenciar os fluxos de trabalho, navegue até o **Editor de fluxo**de trabalho.

6. Clique em **Enviar**.
   O cartão de configuração de integração é exibido.
7. Ao exibir o novo cartão de configuração, você pode clicar em **Configurar** ou **Excluir** para mudar ou excluir a configuração, respectivamente.
8. Para retornar à lista original de cartões de configuração de integração, selecione **Não** na lista suspensa **Mostrar configurações**.

Integração de Plataforma de ponto de extremidade Tanium

O Plataforma de ponto de extremidade Tanium usa um fluxo de trabalho e atividades de fluxo de trabalho para retornar processos em execução para ICs afetados.

Explorar Integrações do Security Incident Response	Configuração • Plataforma de ponto de extremidade Tanium configuração de integração • Ativar e configurar a integração do Security Operations com a Tanium • Configurar para acesso ao MID Server • Atualize seu certificado X.509
Usar • Tanium - Obter fluxo de trabalho de processos em execução • Tanium - Fluxo de trabalho Obter detalhes do arquivo	Desenvolver • ServiceNow Security Operations diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solução de problemas e ajuda adicional • Solução de problemas de integração • Faça ou responda perguntas na comunidade do Security Operations	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Plataforma de ponto de extremidade Tanium configuração de integração

Antes de usar a integração do Tanium, ative o plug-in e configure a integração. Se necessário, você também deve atualizar sua certificação SSL X509.

Sempre que um IC é adicionado a um incidente de segurança aberto em Security Incident Response, o fluxo de trabalho **Tanium - Obter processos em execução** é acionado quando o registro é salvo. A Tanium recebe uma pergunta Obter processos e a Tanium retorna os processos em execução para o IC afetado em uma tabela. Para obter mais informações sobre o fluxo de trabalho e as atividades de fluxo de trabalho associadas, consulte Tanium - Obter fluxo de trabalho de processos em execução.

Ativar e configurar a integração do Security Operations com a Tanium

O recurso Configuração de integração permite que você ative e configure rapidamente integrações de segurança de terceiros, incluindo Tanium integration. Antes de usar a integração Plataforma de ponto de extremidade Tanium, você deve baixá-la do ServiceNow Store.

Antes de Iniciar

Função necessária: sn_si_admin

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Security Operations** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão Tanium, clique em **Configurar**.
4. Preencha os campos no formulário de configuração do Tanium, conforme apropriado.

Campo	Descrição
URL do servidor Tanium	O URL para acessar o endpoint SOAP do servidor Tanium. Normalmente, o URL assume um formato semelhante a https://tanium.server.local/soap. Um endereço IP também pode ser usado. Por exemplo, https//12.13.14.15/soap.
Nome de usuário e senha da Tanium	O nome de usuário e a senha do administrador de integração do Tanium (para o Tanium versão 6.1 e superior).
Sessão do Tanium (pré 6.1)	A chave SOAP da sessão do Tanium (para versões do Tanium anteriores à 6.1). Para instalações do Tanium 6.1 e posteriores, este campo normalmente é deixado em branco.
Sensor de processos em execução	O nome do sensor de processos em execução a ser usado. Por exemplo, **Processos em execução**.
Sensor de endereço IP	O nome do sensor de endereço IP a ser usado para limitar uma consulta a um conjunto de máquinas cliente específicas. Por exemplo, **Endereço IP**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Indexar sensor de arquivos	O nome do sensor usado para obter detalhes do arquivo. O padrão deste campo é Indexar detalhes do arquivo de consulta.
Máximo de entradas de arquivo de índice por IP	O limite do número de arquivos retornados por máquina em uma consulta Obter detalhes do arquivo. O padrão deste campo é 10.
Usar MID Server	Se o servidor Tanium estiver atrás de um MID Server, as credenciais de autenticação deverão ser incluídas no corpo das mensagens SOAP. As credenciais, junto com o restante do corpo da mensagem SOAP, são armazenadas como texto sem formatação no canal de comunicação externo (Fila do ECC).

5. Clique em **Enviar** para armazenar a configuração de integração.

Configurar para acesso ao MID Server

Se o servidor Tanium estiver atrás de um MID Server, execute essas etapas de configuração adicionais para solicitações de proxy por meio do MID Server. Todas as mensagens SOAP enviadas por meio de um MID Server são executadas de forma assíncrona.

Antes de Iniciar

Função necessária: administrador

Deve haver um MID Server em execução associado à sua instância.

No formulário Configuração do Tanium, você deve marcar a caixa de seleção **Usar MID Server**.

Procedimento

1. Navegar até **Todos** > **Serviços web do sistema** > **Saída** > **Mensagem SOAP**.
2. Localize e clique **em Servidor Tanium**.
3. Clique na guia **Funções de Mensagem SOAP**.
4. Para cada uma das três funções a seguir, defina o campo **MID** Server com o MID Server apropriado usado para se comunicar com o servidor Tanium.
   - Obter processos em execução - AddObject
   - Obter dados do resultado
   - ObterInfoResultado
5. Clique em **Atualizar**.

Atualize seu certificado X.509

Se você precisar de uma conexão SSL para a integração, há circunstâncias em que o certificado fornecido pelo fornecedor terceirizado ainda não é confiável em ServiceNow ou expirou. Esta tarefa é opcional.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um Certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

   a. Insira o URL do endpoint na barra de endereço do navegador.
   Por exemplo: `https://<3rdparty>/`.

   b. Clique no ícone de cadeado na linha de endereço.

   c. Clique em **Mais informações** e na guia **Segurança**.

   d. Clique em **Exibir certificado** e na guia **Detalhe**.

   e. Clique em **Exportar** para salvar o PEM em seu sistema de arquivos local.

   f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
   Ele deve começar com `-----BEGIN CERTIFICATE-----` e terminar com `-----END CERTIFICATE-----`.

2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e crie um novo registro para a integração.
4. Em **Certificado PEM**, cole o certificado que você baixou e copiou para a área de transferência anteriormente.
5. Adicione o certificado ao registro do provedor de identidade.
   a. Navegar até **SSO Multiprovedor** > **Provedores de Identidade**.
   b. Selecione o provedor de identidade padrão ativo para o qual você criou o novo certificado.
   c. Role para baixo até a lista relacionada de **certificados X.509** e clique em **Editar**.
   d. Mova o certificado recém-criado para a coluna **Selecionado**.
6. Clique em **Salvar**.
   Os outros campos no registro são gerados automaticamente.

Nota:
Se você tiver um certificado que expirou, será necessário removê-lo. Para obter informações sobre como remover o certificado expirado, consulte KB0691439 Substituir um certificado SAML expirando .

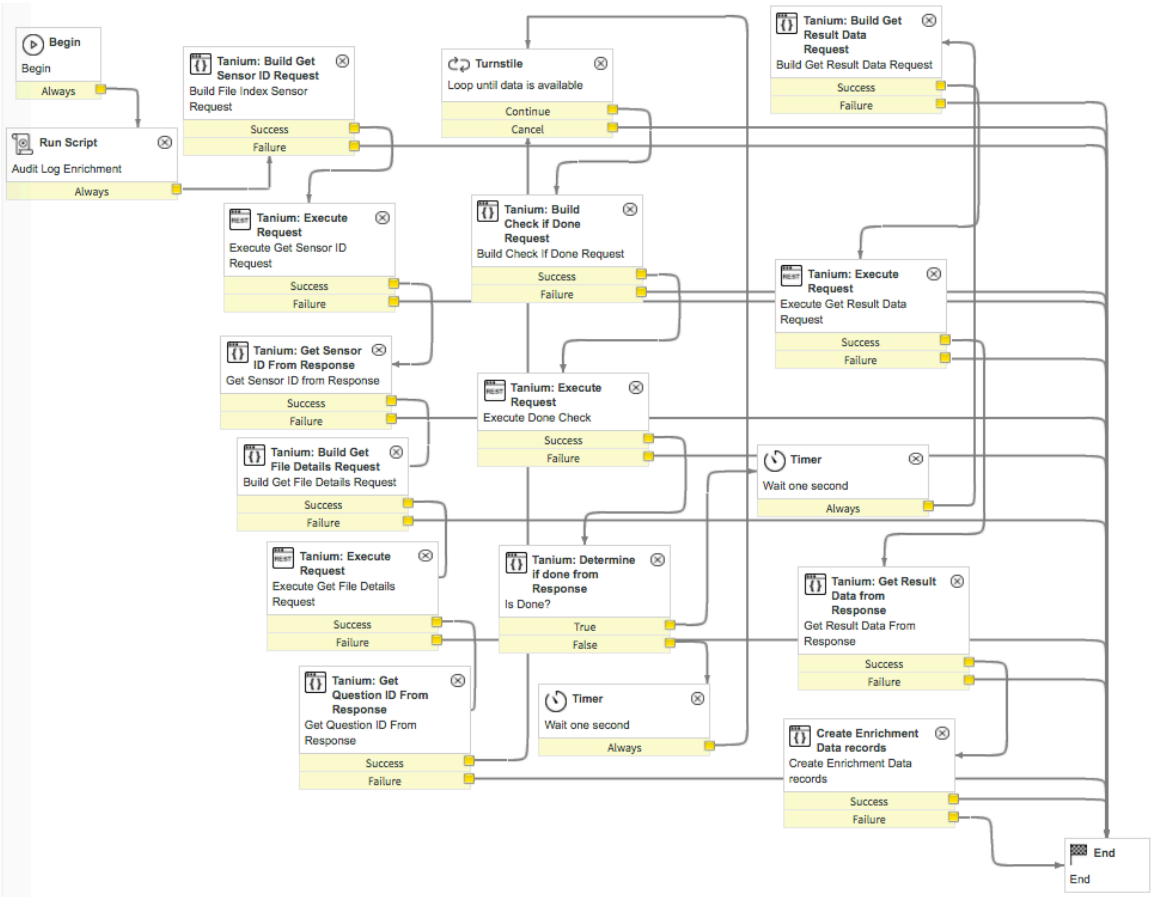
Tanium - Fluxo de trabalho Obter detalhes do arquivo

Este fluxo de trabalho consulta o servidor Tanium em busca da existência de arquivos com um valor de hash ou nome de arquivo específico. As atividades coletam os resultados e os armazenam como dados de aprimoramento em um incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de Integração do Tanium com Security Operations - Obter detalhes do arquivo



Nota:
Este fluxo de trabalho ilustra como você pode consultar o servidor Tanium em busca da existência de arquivos com um valor de hash ou nome de arquivo específico, coletar os dados e armazená-los como dados de aprimoramento em um incidente de segurança. Em sua implementação atual, o fluxo de trabalho não retorna os dados aprimorados para uso pelo sistema. Ele é fornecido para exemplificar o processo que você pode usar para aumentar a eficácia da investigação de incidentes de segurança.

Atividades específicas para esta integração são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Tanium: criar atividade de solicitação de ID de sensor

Esta atividade usa um nome de sensor e cria uma solicitação para executar uma pesquisa no servidor Tanium. Ele retorna um ID de sensor usado por atividades subsequentes.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
sensor_name [cadeia de caracteres]	Uma cadeia de caracteres que identifica o nome do sensor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados.
request_body [Criptografado]	O corpo da solicitação SOAP.
http_timeout [inteiro]	O valor do tempo limite de HTTP, em segundos.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.

Tanium: executar atividade de solicitação

Esta atividade de fluxo de trabalho executa uma solicitação HTTP. As entradas definem o endpoint e o corpo da solicitação esperado. O próprio corpo da solicitação é o envelope SOAP criptografado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
request_body [Criptografado]	O corpo da solicitação SOAP. Este campo de entrada é obrigatório.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados. Este campo de entrada é obrigatório.
http_timeout [integer]	O valor do tempo limite de HTTP, em segundos.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code [integer]	Códigos de status HTTP padrão.
cabeçalho [cadeia de caracteres]	O cabeçalho SOAP.
corpo [cadeia de caracteres]	O corpo SOAP.
erro [cadeia de caracteres]	Quaisquer erros fornecidos pelo servidor.

Tanium: executar atividade de solicitação

Esta atividade de fluxo de trabalho executa uma solicitação HTTP. As entradas definem o endpoint e o corpo da solicitação esperado. O próprio corpo da solicitação é o envelope SOAP criptografado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
request_body [Criptografado]	O corpo da solicitação SOAP. Este campo de entrada é obrigatório.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados. Este campo de entrada é obrigatório.
http_timeout [integer]	O valor do tempo limite de HTTP, em segundos.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code [integer]	Códigos de status HTTP padrão.
cabeçalho [cadeia de caracteres]	O cabeçalho SOAP.
corpo [cadeia de caracteres]	O corpo SOAP.
erro [cadeia de caracteres]	Quaisquer erros fornecidos pelo servidor.

Tanium: obter ID do sensor da atividade de resposta

Esta atividade processa o corpo da resposta SOAP fornecido como entrada e gera o ID do sensor correspondente.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
response_body [cadeia de caracteres]	o corpo da resposta SOAP que retorna do Tanium.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
sensor_id [cadeia de caracteres]	O ID do sensor da cadeia de caracteres associado ao sensor solicitado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tanium: executar atividade de solicitação

Esta atividade de fluxo de trabalho executa uma solicitação HTTP. As entradas definem o endpoint e o corpo da solicitação esperado. O próprio corpo da solicitação é o envelope SOAP criptografado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
request_body [Criptografado]	O corpo da solicitação SOAP. Este campo de entrada é obrigatório.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados. Este campo de entrada é obrigatório.
http_timeout [integer]	O valor do tempo limite de HTTP, em segundos.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code [integer]	Códigos de status HTTP padrão.
cabeçalho [cadeia de caracteres]	O cabeçalho SOAP.
corpo [cadeia de caracteres]	O corpo SOAP.
erro [cadeia de caracteres]	Quaisquer erros fornecidos pelo servidor.

Tanium: obter ID de pergunta da atividade de resposta

Esta atividade de fluxo de trabalho processa o corpo da resposta para obter o ID da pergunta.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
response_body [cadeia de caracteres]	O corpo da resposta SOAP.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
question_id [integer]	O ID da pergunta retornado do servidor Tanium.

Tanium: Criar atividade de solicitação Verificar se concluído

Esta atividade de fluxo de trabalho cria uma solicitação do servidor Tanium para verificar se a coleta de dados para a pergunta foi concluída. Ele retorna a solicitação criptografada e outros componentes necessários para executar a solicitação.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
question_id [integer]	O ID da pergunta retornado do servidor Tanium.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados.
request_body [Criptografado]	O corpo da solicitação SOAP.
http_timeout [Inteiro]	O valor do tempo limite de HTTP, em segundos.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.

Tanium: executar atividade de solicitação

Esta atividade de fluxo de trabalho executa uma solicitação HTTP. As entradas definem o endpoint e o corpo da solicitação esperado. O próprio corpo da solicitação é o envelope SOAP criptografado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
request_body [Criptografado]	O corpo da solicitação SOAP. Este campo de entrada é obrigatório.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados. Este campo de entrada é obrigatório.
http_timeout [integer]	O valor do tempo limite de HTTP, em segundos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code [integer]	Códigos de status HTTP padrão.
cabeçalho [cadeia de caracteres]	O cabeçalho SOAP.
corpo [cadeia de caracteres]	O corpo SOAP.
erro [cadeia de caracteres]	Quaisquer erros fornecidos pelo servidor.

Tanium: determinar se foi concluído a partir da atividade de resposta

Esta atividade de fluxo de trabalho determina se uma solicitação foi concluída com base no corpo da resposta.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
response_body [cadeia de caracteres]	O corpo da solicitação SOAP retornado do Tanium.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
concluído [Booliano]	Retorna verdadeiro se o processamento da solicitação estiver concluído.

Tanium: criar atividade de solicitação de dados de resultado

Este fluxo de trabalho cria uma solicitação para coletar todos os dados retornados do Tanium em resposta a uma pergunta. Ele usa um ID de pergunta como entrada e fornece a saída para executar a solicitação, incluindo uma carga de envelope SOAP criptografada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
question_id [cadeia de caracteres]	O ID da pergunta apresentada ao Tanium.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados.
request_body [Criptografado]	O corpo da solicitação SOAP.
http_timeout [inteiro]	O valor do tempo limite de HTTP, em segundos.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.

Tanium: executar atividade de solicitação

Esta atividade de fluxo de trabalho executa uma solicitação HTTP. As entradas definem o endpoint e o corpo da solicitação esperado. O próprio corpo da solicitação é o envelope SOAP criptografado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
request_body [Criptografado]	O corpo da solicitação SOAP. Este campo de entrada é obrigatório.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados. Este campo de entrada é obrigatório.
http_timeout [integer]	O valor do tempo limite de HTTP, em segundos.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code [integer]	Códigos de status HTTP padrão.
cabeçalho [cadeia de caracteres]	O cabeçalho SOAP.
corpo [cadeia de caracteres]	O corpo SOAP.
erro [cadeia de caracteres]	Quaisquer erros fornecidos pelo servidor.

Tanium: obter dados de resultado da atividade de resposta

A atividade de fluxo de trabalho Tanium: obter dados de resultado da resposta processa o corpo da resposta dos dados de resultado e gera uma matriz de objetos JSON que representa os resultados do Tanium.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A atividade Tanium: obter dados de resultado da resposta pode ser usada com qualquer fluxo de trabalho para recuperar dados de resultado a serem usados no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Sucesso	Dados de resultado recuperados.
Falha	Nenhum dado recuperado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
response_body	Conteúdos de resposta SOAP criptografados
Id_implementação	Identificador de implementação.
afetado_ci	Item de configuração afetado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
data_resultado	Tipo de elemento de matriz de variáveis de API. Cada matriz contém pares de chave-valor compostos pela coluna e valores retornados do servidor. Se nenhum dado for recebido do servidor, a saída será uma matriz vazia.
saída	Dados de retorno formatados em processos em execução usados pelo fluxo de trabalho abstrato.

Tanium - Obter fluxo de trabalho de processos em execução

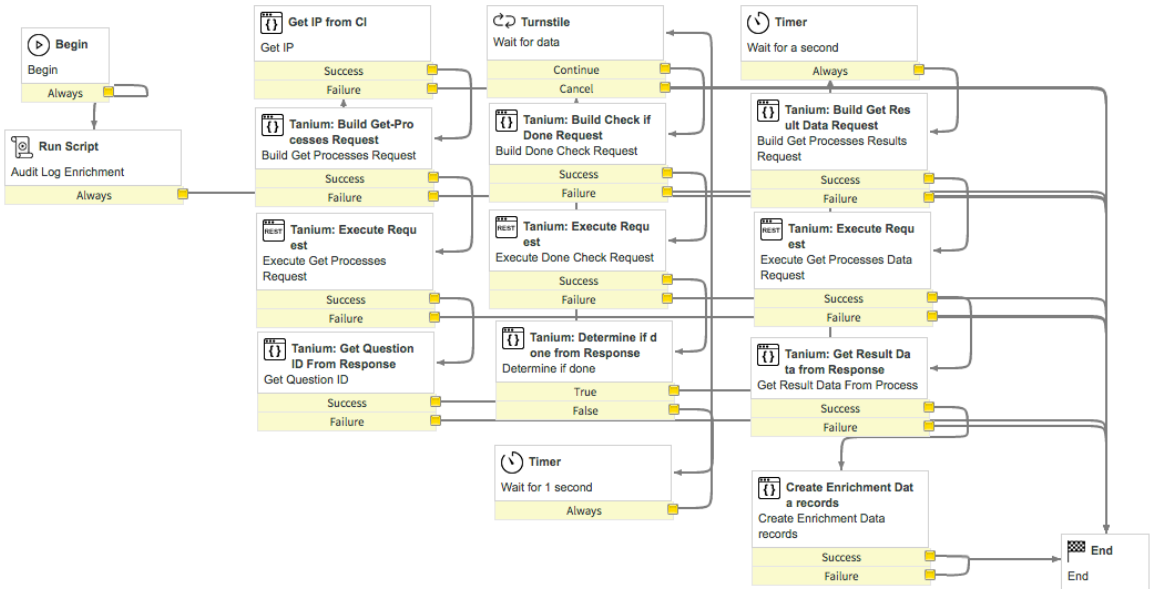
Este fluxo de trabalho cria uma trilha de auditoria e a atividade Tanium: Get-Processs Question usa o endereço IPV4 do IC como entrada e executa uma consulta no servidor Tanium. A saída é uma lista de todos os processos em execução no IC afetado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho do Security Operations Tanium Integration - Obter processos em execução

Quando o campo **Item de configuração** em um incidente de segurança é modificado, este fluxo de trabalho é iniciado.



Como funciona o fluxo de trabalho

Dado um ID de pergunta de cadeia de caracteres (normalmente o resultado de um comando AddObject), a **atividade Tanium: Verificar se concluído** consulta o servidor Tanium para verificar se a coleta de dados foi concluída. Esta atividade usa a inclusão de script **sn_sec_tanium.TaniumEndpointUtil** e se baseia na mensagem SOAP do servidor **Tanium** GetResultInfo.

Quando a **atividade Tanium: Verificar se concluído** retorna verdadeiro, a atividade Tanium: Obter dados de resultado da resposta coleta todos os dados retornados do servidor Tanium em resposta à pergunta Get-Processes. A saída consiste em uma matriz de objetos, cada um contendo pares de chave-valor compostos pela coluna e valores retornados do servidor. Se nenhum dado for recebido do servidor, a saída será uma matriz vazia.

Atividades específicas para esta integração são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Obter IP da atividade de IC

Esta atividade de fluxo de trabalho determina o endereço IPV4 associado a um item de configuração (IC).

A atividade **Obter IP do IC** pode ser usada com qualquer fluxo de trabalho para recuperar o endereço IPv4 de um IC.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
ci_sys_id [cadeia de caracteres]	Identificador do sistema do item de configuração

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ip_addr [cadeia de caracteres]	Endereço IPv4. Se o endereço IP não puder ser determinado, este valor ficará em branco.

Condições de Saída

Os resultados possíveis para esta atividade são:

Condições

Condição	Descrição
Êxito	Um endereço IPv4 foi retornado.
Falha	Não foi possível determinar um endereço IPv4.

Tanium: criar atividade de solicitação Get-Process

Esta atividade de fluxo de trabalho usa o endereço IPV4 de um IC adicionado a um incidente de segurança e cria uma solicitação ao servidor Tanium para todos os processos em execução para esse IC. A saída são os detalhes necessários para executar a solicitação, com a carga criptografada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
ci_ip_address [cadeia de caracteres]	O endereço IPV4 do IC que foi adicionado a um incidente de segurança. Este campo de entrada é obrigatório.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
request_body [Criptografado]	O corpo da solicitação SOAP.
http_timeout [inteiro]	O valor do tempo limite de HTTP, em segundos.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.

Tanium: Criar atividade de solicitação Verificar se concluído

Esta atividade de fluxo de trabalho cria uma solicitação do servidor Tanium para verificar se a coleta de dados para a pergunta foi concluída. Ele retorna a solicitação criptografada e outros componentes necessários para executar a solicitação.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
question_id [integer]	O ID da pergunta retornado do servidor Tanium.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados.
request_body [Criptografado]	O corpo da solicitação SOAP.
http_timeout [Inteiro]	O valor do tempo limite de HTTP, em segundos.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.

Tanium: criar atividade de solicitação de dados de resultado

Este fluxo de trabalho cria uma solicitação para coletar todos os dados retornados do Tanium em resposta a uma pergunta. Ele usa um ID de pergunta como entrada e fornece a saída para executar a solicitação, incluindo uma carga de envelope SOAP criptografada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
question_id [cadeia de caracteres]	O ID da pergunta apresentada ao Tanium.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados.
request_body [Criptografado]	O corpo da solicitação SOAP.
http_timeout [inteiro]	O valor do tempo limite de HTTP, em segundos.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.

Tanium: determinar se foi concluído a partir da atividade de resposta

Esta atividade de fluxo de trabalho determina se uma solicitação foi concluída com base no corpo da resposta.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
response_body [cadeia de caracteres]	O corpo da solicitação SOAP retornado do Tanium.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
concluído [Booliano]	Retorna verdadeiro se o processamento da solicitação estiver concluído.

Tanium: executar atividade de solicitação

Esta atividade de fluxo de trabalho executa uma solicitação HTTP. As entradas definem o endpoint e o corpo da solicitação esperado. O próprio corpo da solicitação é o envelope SOAP criptografado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
request_body [Criptografado]	O corpo da solicitação SOAP. Este campo de entrada é obrigatório.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados. Este campo de entrada é obrigatório.
http_timeout [integer]	O valor do tempo limite de HTTP, em segundos.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code [integer]	Códigos de status HTTP padrão.
cabeçalho [cadeia de caracteres]	O cabeçalho SOAP.
corpo [cadeia de caracteres]	O corpo SOAP.
erro [cadeia de caracteres]	Quaisquer erros fornecidos pelo servidor.

Tanium: obter ID de pergunta da atividade de resposta

Esta atividade de fluxo de trabalho processa o corpo da resposta para obter o ID da pergunta.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
response_body [cadeia de caracteres]	O corpo da resposta SOAP.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
question_id [integer]	O ID da pergunta retornado do servidor Tanium.

Tanium: obter dados de resultado da atividade de resposta

A atividade de fluxo de trabalho Tanium: obter dados de resultado da resposta processa o corpo da resposta dos dados de resultado e gera uma matriz de objetos JSON que representa os resultados do Tanium.

A atividade Tanium: obter dados de resultado da resposta pode ser usada com qualquer fluxo de trabalho para recuperar dados de resultado a serem usados no fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Sucesso	Dados de resultado recuperados.
Falha	Nenhum dado recuperado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
response_body	Conteúdos de resposta SOAP criptografados
Id_implementação	Identificador de implementação.
afetado_ci	Item de configuração afetado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
data_resultado	Tipo de elemento de matriz de variáveis de API. Cada matriz contém pares de chave-valor compostos pela coluna e valores retornados do servidor. Se nenhum dado for recebido do servidor, a saída será uma matriz vazia.
saída	Dados de retorno formatados em processos em execução usados pelo fluxo de trabalho abstrato.

Tradução automática

Experiência Móvel para Security Incident Response

Use seu dispositivo móvel Android ou iOS para gerenciar as tarefas do centro de operações de segurança (SOC).

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Security Incident Response

Se você não estiver familiarizado com os conceitos básicos do produto Security Incident Response (SIR) em sua instância Now Platform®, consulte Visão geral do Security Incident Response para obter mais informações sobre inteligência contra ameaças e como esse produto pode ajudá-lo a priorizar e resolver ameaças cibernéticas à sua organização.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

Como gerente do centro de operações de segurança (SOC) ou usuário com a função de analista de segurança Now Platform (sn_si.analyst), você pode fazer login em uma instância Now Platform diretamente do seu dispositivo móvel. Com o Aplicativo Security Incident Response Mobile, você pode exibir, editar e atribuir seus incidentes de segurança e tarefas de resposta mais atuais e críticos SIR. As notificações informam quando chegam incidentes de segurança críticos atribuídos a você.

Com o Aplicativo Security Incident Response Mobile, você pode executar as seguintes tarefas relacionadas ao SIR no seu dispositivo móvel:

- Exiba uma lista de incidentes de segurança críticos e tarefas de resposta.
- Receba notificações detalhadas de incidentes de segurança e tarefas que atendam aos critérios de notificação predefinidos.
- Exiba agrupamentos de incidentes de segurança ou tarefas que são baseados em um conjunto predefinido de consultas ou filtros.
- Exiba as anotações de trabalho e as listas relacionadas de incidentes de segurança.
- Atualize incidentes de segurança e adicione anotações de trabalho ou anexos.
- Edite os campos em incidentes de segurança.
- Atribua incidentes de segurança a você ou a outros membros de sua equipe de segurança.

Quando eles são preenchidos, você pode exibir as seguintes listas relacionadas em SIR incidentes de segurança com o Aplicativo Security Incident Response Mobile:

- Item de configuração
- Usuário afetado
- Serviços afetados
- Incidentes de segurança secundários
- Incidentes de segurança semelhantes (sem suporte da Now Platform)
- Observáveis
- Tarefas de resposta
- Tarefas
- ANS de tarefa
- Anexos (sem suporte da Now Platform)

A figura a seguir ilustra como você faz login na instância Now Platform do seu dispositivo móvel e a estrutura da tela inicial do Aplicativo Security Incident Response Mobile que é reproduzida após o login.

Para obter instruções passo a passo sobre como configurar sua instância Now Platform e instalar o Aplicativo Security Incident Response Mobile, consulte Configurar check-list para o Aplicativo Security Incident Response Mobile. Para obter instruções sobre como fazer login, consulte Faça login no Aplicativo Security Incident Response Mobile.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicativo Security Incident Response Mobile

Aplicações

As aplicações são os ServiceNow® componentes de software, como Security Incident Response (SIR), Vulnerability Response (VR), Governança, risco e conformidade (GRC) que fornecem recursos e funcionalidades específicos na sua instância Now Platform. Depois de instalar a aplicação principal Security Incident Response e o Aplicativo Security Incident Response Mobile na sua instância Now Platform, o ícone da aplicação principal é exibido na parte inferior do seu dispositivo móvel Android ou iOS após o login.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicativo Security Incident Response Mobile (Incidentes de segurança) ícone

Pastas

Cada aplicação ServiceNow® mobile contém pastas que separam os applets por categoria. Na imagem anterior da página principal, **Incidentes de segurança** e **Tarefas de resposta** a incidentes são pastas.

Applets

Applets são as diferentes opções da aplicação. Os ícones nas seções **Incidentes de segurança** e **Tarefas de resposta** a incidentes são os applets disponíveis do Aplicativo Security Incident Response Mobile.

Configurar check-list para o Aplicativo Security Incident Response Mobile

A check-list a seguir inclui as tarefas de configuração que você deve concluir na instância Now Platform® e no dispositivo móvel antes de usar o Aplicativo Security Incident Response Mobile.

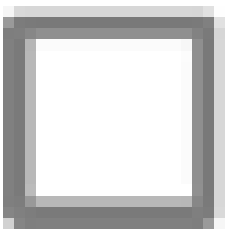
Antes de Iniciar

Como opção, imprima esta check-list e use-a como guia nas tarefas de configuração necessárias para o Aplicativo Security Incident Response Mobile. Verifique se cada item da lista está concluído para que você possa exibir e editar SIR incidentes de segurança no seu dispositivo móvel.

Os itens da check-list são exibidos em texto realçado. Mais informações seguem cada item na coluna à direita. Tempo estimado para concluir esta tarefa: 15 a 20 minutos.

Funções necessárias: admin, sn_si.analyst

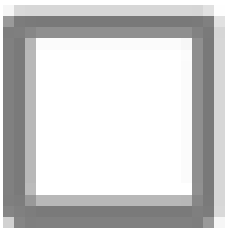
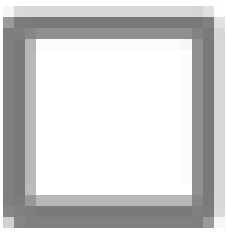
Check-list móvel

Item	Descrição
	Como um usuário com a função de administrador, verifique se você tem a aplicação principal Security Incident Response instalada em uma instância Now Platform. Esta é a instância Now Platform que você exibe no seu dispositivo móvel. **Nota:** A aplicação principal Security Incident Response e a instância Now Platform devem ser da mesma versão da família. 1. Para verificar se a aplicação principal está instalada em sua instância, navegue até Plug- **ins** e pesquise por Security Incident Response. 2. Se a aplicação principal Security Incident Response ainda não estiver instalada, clique em **Instalar** para instalá-la. Para obter mais informações sobre como instalar a aplicação principal Security Incident Response, consulte Instalar e configurar Security Incident Response. Se a aplicação principal Security Incident Response não estiver visível em plug-ins, para obter mais informações sobre como instalar aplicações principais e direitos para aplicações, consulte Security Operations e o ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list móvel

Item	Descrição
	Como um usuário com a função de administrador, verifique se você tem o Aplicativo Security Incident Response Mobile instalado na instância Now Platform que deseja exibir no seu dispositivo móvel. **Nota:** as instâncias Aplicativo Security Incident Response Mobile e Now Platform devem ser da mesma versão da família. Baixe e instale o Aplicativo Security Incident Response Mobile do ServiceNow Store na sua instância Now Platform. Quando você instala o Aplicativo Security Incident Response Mobile, suas dependências, com.glide.sg e com.glide.sg.agent_native_client, também são instaladas. Para verificar se essas dependências estão instaladas: **1.** Navegue até Plug- **ins**. **2.** Pesquise os IDs de plug-in (com.glide.sg e com.glide.sg.agent_native_client). **3.** Se eles não estiverem ativados, ative esses plug-ins. Esses plug-ins são necessários para o Aplicativo Security Incident Response Mobile. Para obter mais informações sobre como instalar aplicações e direitos para aplicações, consulte Security Operations e o ServiceNow Store.
	Como um usuário com a função de administrador Now Platform, verifique se você atribuiu usuários móveis com as funções necessárias em sua instância Now Platform. **1.** Para exibir as funções atribuídas a um usuário, navegue até **Usuários e Grupos** > **Usuários**. **2.** Selecione o nome de usuário seguido pela lista relacionada de funções. Todas as funções atribuídas a este usuário serão exibidas. **3.** Verifique se um usuário está atribuído ou atribua um usuário com a função de biblioteca de infraestrutura de TI (itil). Usuários com a função itil podem criar, abrir, atualizar e fechar incidentes de segurança. Somente usuários com a função itil podem ter tarefas atribuídas a eles. **4.** Verifique se um usuário está atribuído ou atribua um usuário com a função de analista de segurança (sn_si.analyst). Usuários com a função sn_si.analyst podem ler e editar registros de incidentes de segurança. Esta função é adicionada automaticamente quando você atribui a função itil. **5.** Verifique se você criou todos os grupos de atribuição necessários e atribuiu usuários móveis a esses grupos. **Nota:** Se você tiver um grande número de usuários para o aplicativo móvel, como alternativa, poderá atribuir a função sn_si.analyst a um grupo. Cada usuário adicionado ao grupo herda esta função.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list móvel

Item	Descrição
	Para obter mais informações sobre analistas de segurança, consulte Atribuição de analistas de segurança. Para obter mais informações sobre usuários e atribuição de funções a usuários e grupos, consulte Administração de usuários.
☐	Como um usuário com a função sn_si.analyst, baixe o aplicativo Agent ServiceNow® mais atual no seu dispositivo móvel. A versão mais atual do aplicativo Agent está disponível na Apple iOS App Store e na Google Play Store.
☐	Como um usuário com a função sn_si.analyst, verifique se as notificações estão habilitadas no seu dispositivo móvel e na sua instância Now Platform. As notificações informam quando incidentes de segurança críticos são atribuídos a você ou ao seu grupo de atribuição. Para ajudá-lo com a correção oportuna, depois de habilitar as notificações, clique em uma notificação no Aplicativo Security Incident Response Mobile para navegar diretamente para o incidente de segurança. Para habilitar notificações na sua instância Now Platform para que elas sejam exibidas no seu dispositivo móvel, siga estas etapas. **1.** Verifique se você baixou e instalou o Aplicativo Security Incident Response Mobile na sua instância Now Platform. **2.** Em Configurações do sistema na sua instância Now Platform, em Notificações, verifique se você habilitou o **Aplicativo para celular da ServiceNow**. Para obter mais informações sobre como definir notificações, consulte Como definir preferências de notificação do usuário na IU principal.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list móvel

Item	Descrição
	Now Platform As notificações do também são exibidas na tela de mensagens do seu dispositivo móvel. Verifique se as notificações também estão habilitadas nas configurações do seu dispositivo móvel.

Você configurou com sucesso seu dispositivo móvel e o Now Platform para o Aplicativo Security Incident Response Mobile. A próxima etapa é fazer login na sua instância Now Platform com seu dispositivo móvel.

Faça login no Aplicativo Security Incident Response Mobile

Abra o aplicativo Security Incident Response Mobile e adicione uma instância Now Platform® com o Security Incident Response ao seu dispositivo móvel.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

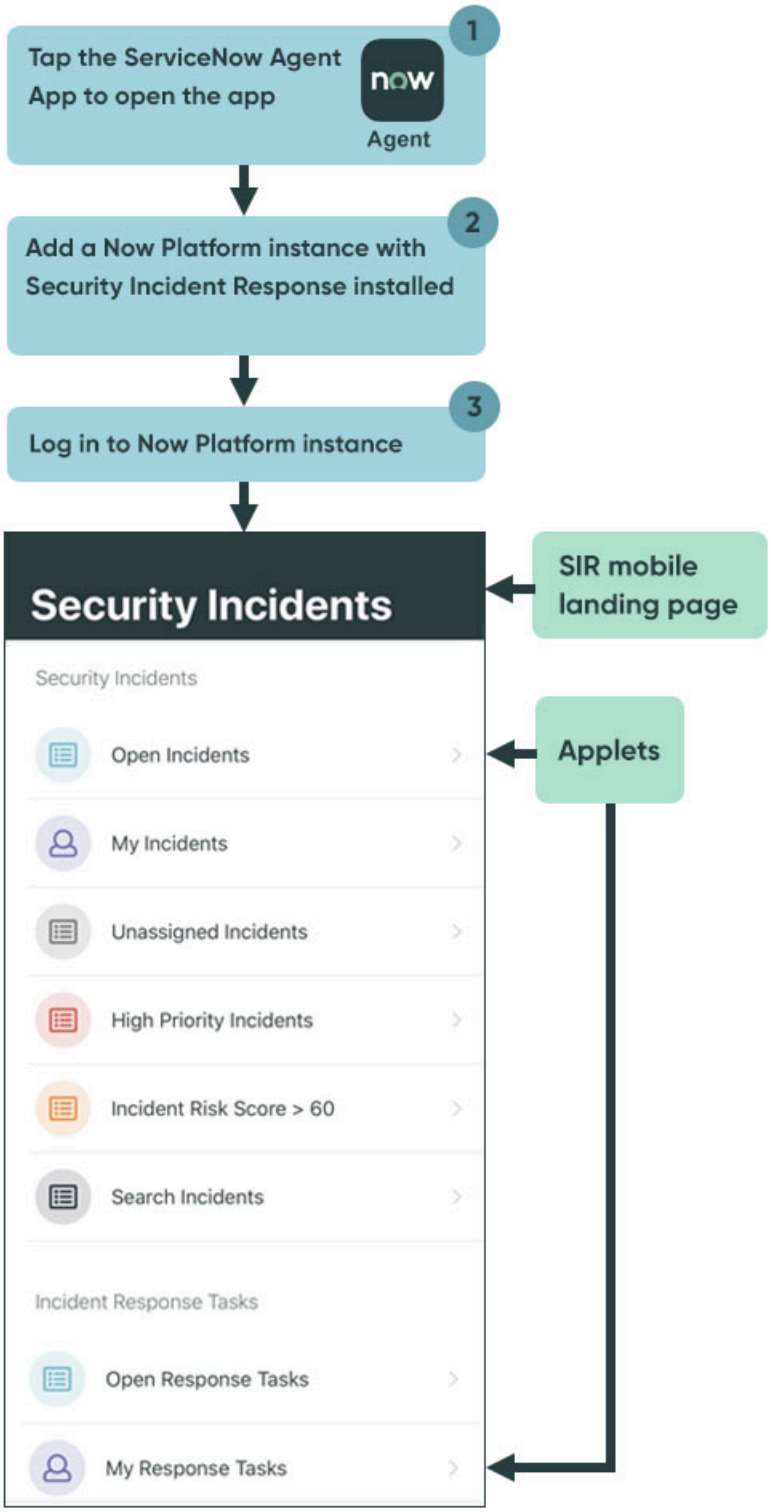
Tempo para concluir esta tarefa: 5 a 10 minutos.

Verifique se você concluiu as etapas de configuração descritas em Configurar check-list para o Aplicativo Security Incident Response Mobile.

Tradução automática

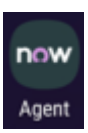
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicativo Security Incident Response Mobile



Procedimento

1. No seu dispositivo móvel, toque no aplicativo **ServiceNow Agent** para abri-lo.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você ainda não estiver conectado a uma instância Now Platform, a tela Instâncias será exibida.

2. Se a instância Now Platform com a aplicação principal Security Incident Response ainda não tiver sido adicionada ao seu dispositivo móvel, siga estas etapas para adicioná-la.

   a. Na tela Instâncias exibida, toque no .
   Uma tela é exibida solicitando que você insira e salve um endereço de uma instância Now Platform.

   b. Preencha os campos.

Campo	Descrição
Insira o endereço da instância ou leia um código QR.	Escolha um para continuar: ▪ Antes de .service-now.com, insira o nome da sua instância Now Platform, por exemplo, sirmobileny. ▪ Insira um endereço. Este endereço é o URL da sua instância Now Platform que você deseja exibir no seu dispositivo móvel, por exemplo, https://sirmobileny.service-now.com. ▪ Digitalize um código QR.
(Opcional) Inserir apelido	Insira um apelido para esta instância. Se você tiver várias instâncias adicionadas ao dispositivo, os apelidos poderão ajudá-lo a localizar rapidamente uma instância do Now Platform.

   c. Toque em **Salvar e fazer login**.

3. Na tela de login ServiceNow exibida, insira o Nome de usuário e a Senha da instância Now Platform que você deseja adicionar e toque em **Login**.
   A tela inicial de Incidentes de segurança é exibida. Você fez login com sucesso em Aplicativo Security Incident Response Mobile.

4. Depois de fazer login, verifique se as notificações estão habilitadas no Aplicativo Security Incident Response Mobile.

   a. Na tela inicial na parte inferior, toque em **Notificação**.

   b. Na tela Notificações, toque em **Habilitar notificações** se não estiver habilitado.
   As notificações do Now Platform são exibidas na tela Notificações no Aplicativo Security Incident Response Mobile.

5. Depois de fazer login em uma instância no seu dispositivo móvel, é a instância padrão Now Platform no dispositivo.
   Se você quiser exibir outro Now Platform no dispositivo, será necessário sair da instância padrão. Para sair:

   a. Toque no ícone de configurações.

   b. Toque **em Logout**.
   A tela Instâncias é exibida com todas as instâncias Now Platform que você adicionou ao dispositivo móvel.

   c. **Opcional:** Toque em outra instância para fazer login nela ou, como alternativa, siga as etapas anteriores para adicionar outra instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se a tela de instâncias do Aplicativo Security Incident Response Mobile não for exibida depois de tocar no aplicativo **ServiceNow Agent** no seu dispositivo, verifique se o **ServiceNow Agent** é permitido como um aplicativo confiável no seu dispositivo. Para permitir o acesso como um aplicativo confiável, navegue até as configurações e gerenciamento geral de dispositivos no seu dispositivo e toque na opção (aplicativo de confiança etc.) para permitir o acesso.

Se uma mensagem de erro for exibida depois de inserir suas credenciais na tela de login, verifique se o nome de usuário e a senha da instância Now Platform estão corretos.

Se você tiver problemas para exibir a tela inicial, verifique sua conexão de rede.

Se você não conseguir exibir a tela Instâncias depois de tocar no aplicativo **ServiceNow Agent**, tente desinstalá-lo do seu dispositivo. Verifique se você tem a versão mais atual do app na App Store da Apple iOS ou na Play Store Google e tente reinstalá-lo.

Exiba, edite e atribua incidentes de segurança em aberto com o Aplicativo Security Incident Response Mobile

Como analista de incidentes de segurança, exiba, edite e atribua incidentes de segurança Security Incident Response (SIR) abertos no seu dispositivo móvel. Exiba as listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre os incidentes.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Na lista de registros, atribua um incidente de segurança em aberto a você ou reatribua-o. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5 a 10 minutos.

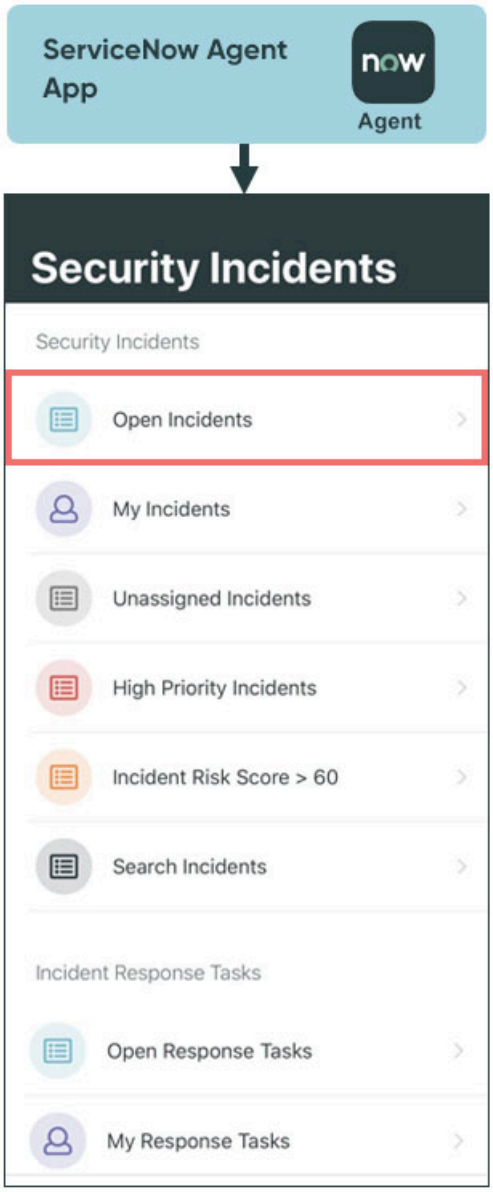
Procedimento

1. Se você não estiver conectado à sua instância Now Platform no seu dispositivo móvel, consulte Faça login no Aplicativo Security Incident Response Mobile.
2. Com a página inicial de Incidentes de segurança exibida, toque **em Abrir incidentes**.

Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

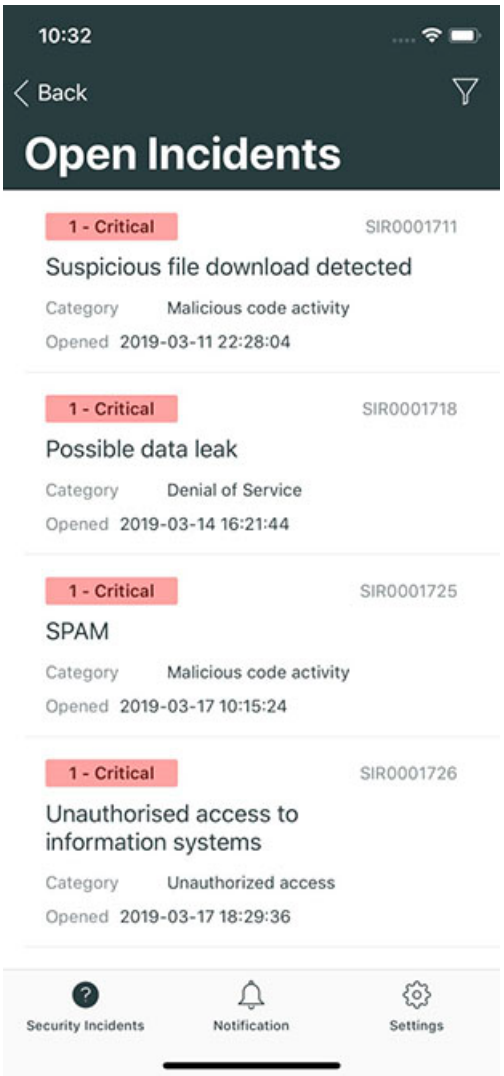
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A tela Incidentes em aberto é exibida com uma lista de registros de incidentes de segurança em aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. **Opcional:** Consulte Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro (ícone de) exibido, defina filtros para limitar o número de registros na lista. A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condição na Now Platform.

4. Para atribuir um incidente a você mesmo ou reatribuí-lo diretamente da lista de incidentes de segurança em aberto, deslize para a esquerda em um registro para abrir o menu.

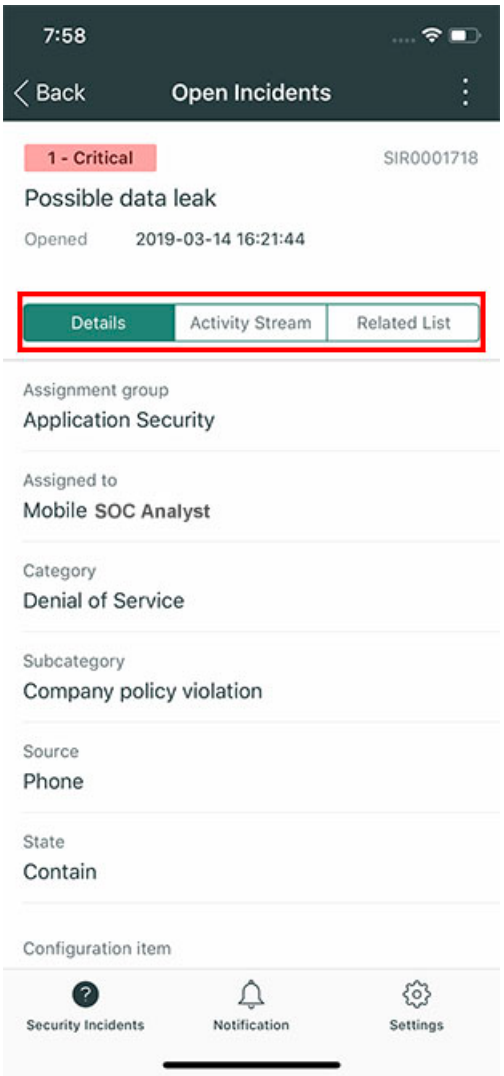
5. Escolha um no menu exibido para continuar.

6. Como alternativa, para exibir os detalhes de um registro de incidente de segurança aberto e para ver mais registros associados e listas relacionadas, com a tela Incidentes em aberto exibida, toque em um registro na lista.

7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exibir, editar e reatribuir incidentes de segurança atribuídos a você com o Aplicativo Security Incident Response Mobile

Como analista de incidentes de segurança, exiba, edite e reatribua Security Incident Response (SIR) incidentes que foram atribuídos a você. Exiba as listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre os incidentes.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Reatribua um incidente de segurança em aberto a outro analista do seu grupo na lista de registros. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5 a 10 minutos.

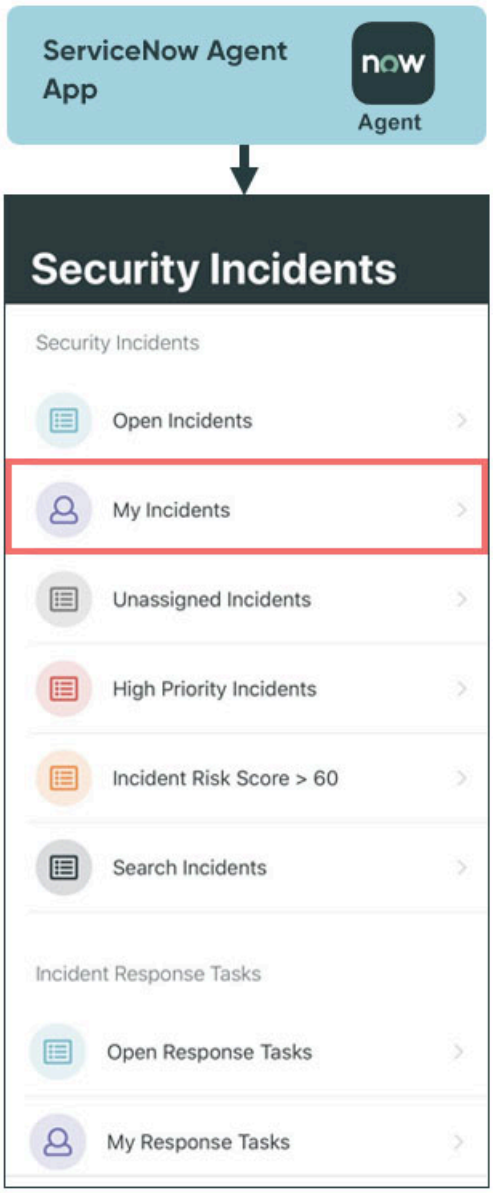
Procedimento

1. Se você não estiver conectado à sua instância Now Platform no seu dispositivo móvel, consulte Faça login no Aplicativo Security Incident Response Mobile.
2. Com a tela inicial de Incidentes de segurança exibida, toque **em Meus incidentes**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

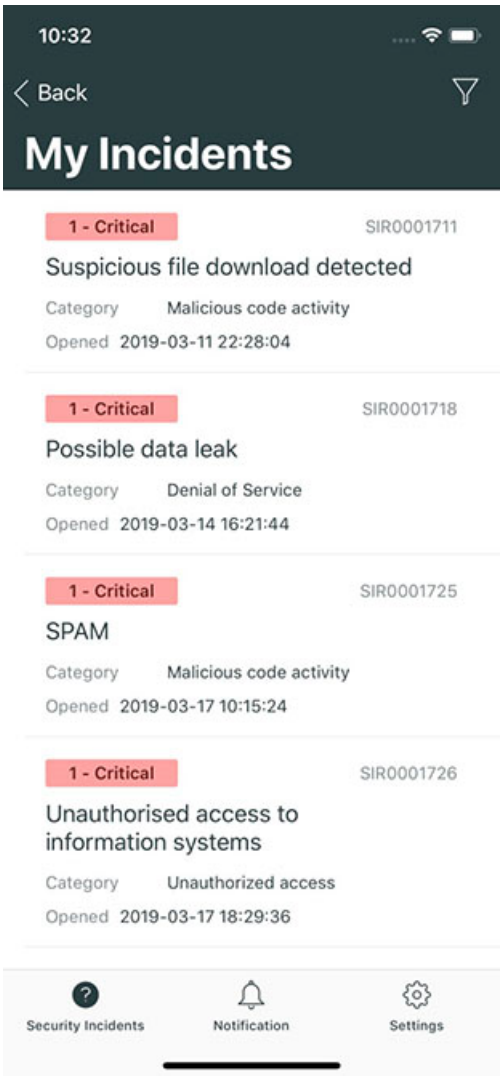
Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



A tela Meus incidentes é exibida com uma lista de registros de incidentes de segurança abertos que são atribuídos a você.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



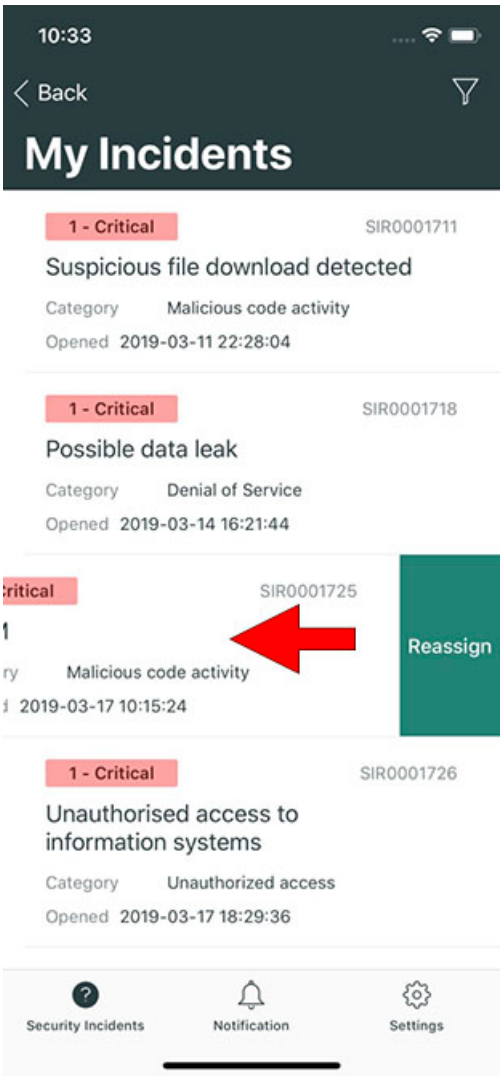
3. **Opcional:** Consulte Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro ( ) exibido, defina filtros para limitar o número de registros na lista. A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condição na Now Platform.

4. Para reatribuir um incidente diretamente da lista, com a lista de registros de incidentes de segurança abertos exibida, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



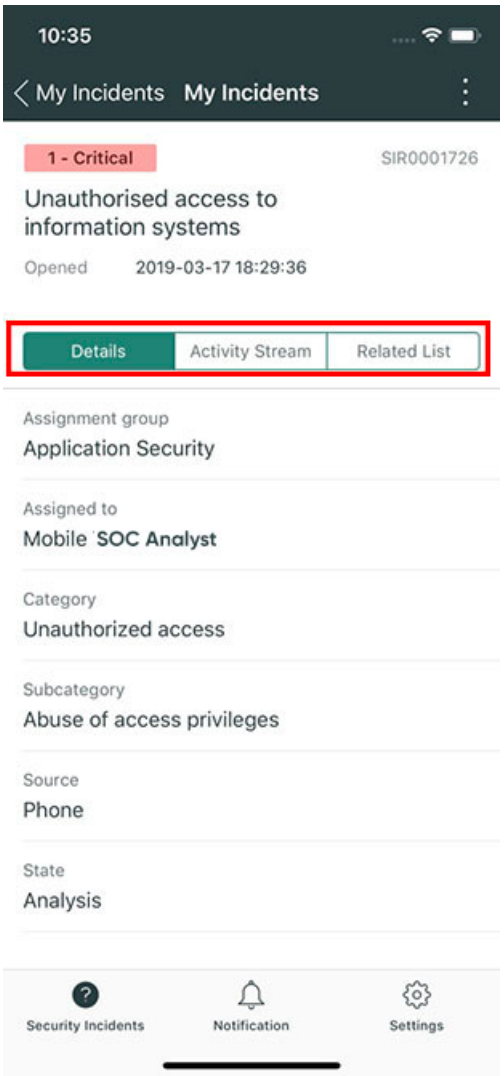
5. Edite o Grupo de atribuição ou os campos Atribuído a no menu exibido.

6. Como alternativa, para exibir os detalhes do registro de incidente de segurança aberto, com a tela Meus incidentes exibida, toque em um registro na lista.

7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exiba, edite e atribua incidentes de segurança não atribuídos com o Aplicativo Security Incident Response Mobile

No seu dispositivo móvel, exiba, edite e atribua Security Incident Response (SIR) incidentes não atribuídos. Exiba as listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre os incidentes.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Na lista de registros, atribua um incidente de segurança aberto e não atribuído a você ou a outro analista do seu grupo. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5 a 10 minutos.

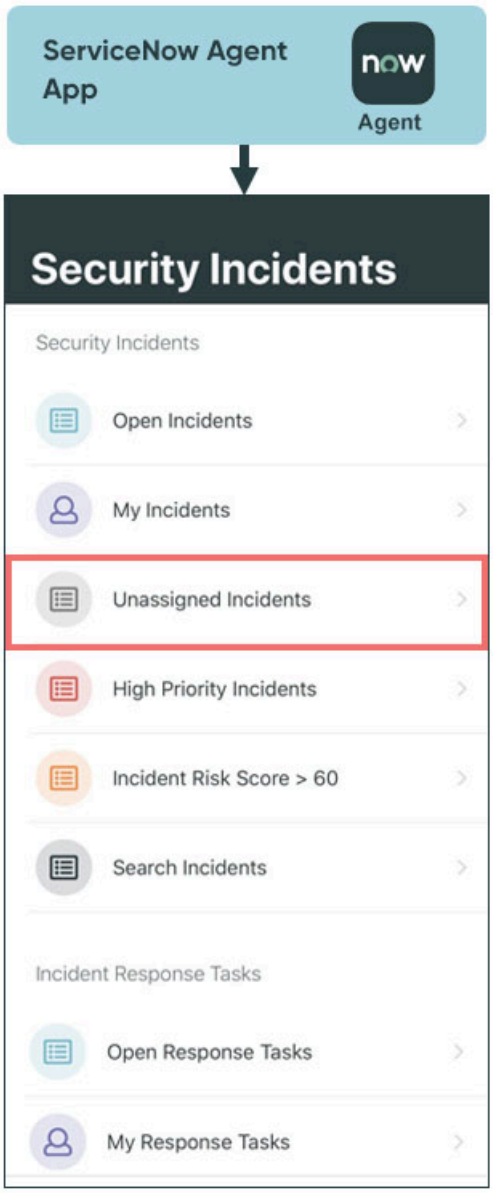
Procedimento

1. Se você não estiver conectado à sua instância da Now Platform em seu dispositivo móvel, consulte Faça login no Aplicativo Security Incident Response Mobilepara obter mais informações.
2. Com a tela inicial de Incidentes de segurança exibida, toque **em Incidentes não atribuídos**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

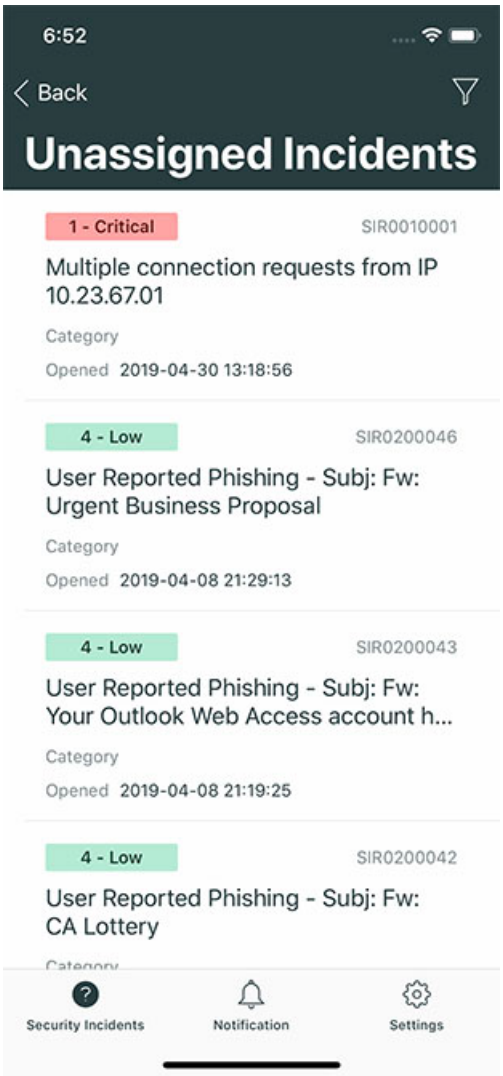
Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



A tela Incidentes não atribuídos é exibida com uma lista de registros de incidentes de segurança não atribuídos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



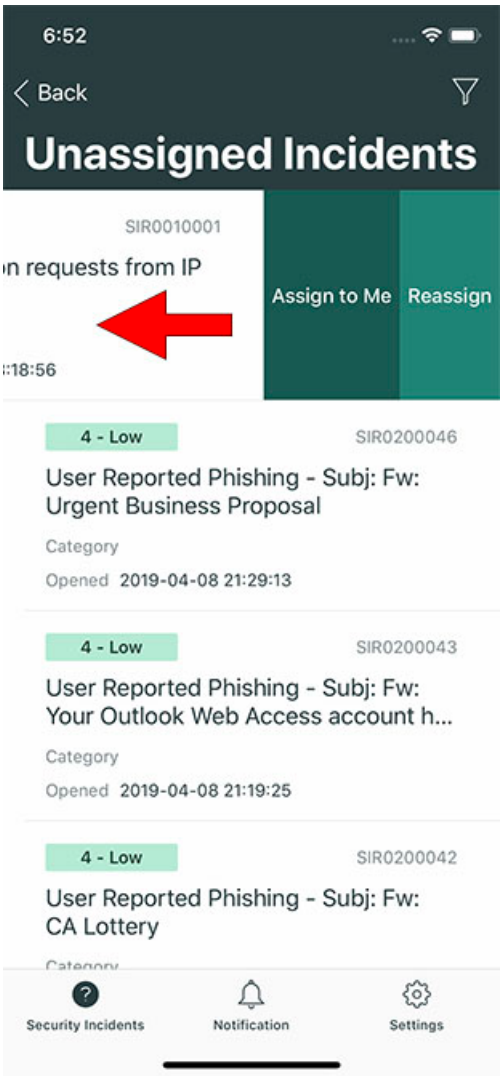
3. **Opcional:** Consulte Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro (ícone de) exibido, defina filtros para limitar o número de registros na lista. A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condição na Now Platform.

4. Para atribuir ou reatribuir um registro de incidente de segurança em aberto diretamente da lista, com a lista de registros de incidentes de segurança não atribuídos em aberto exibida, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



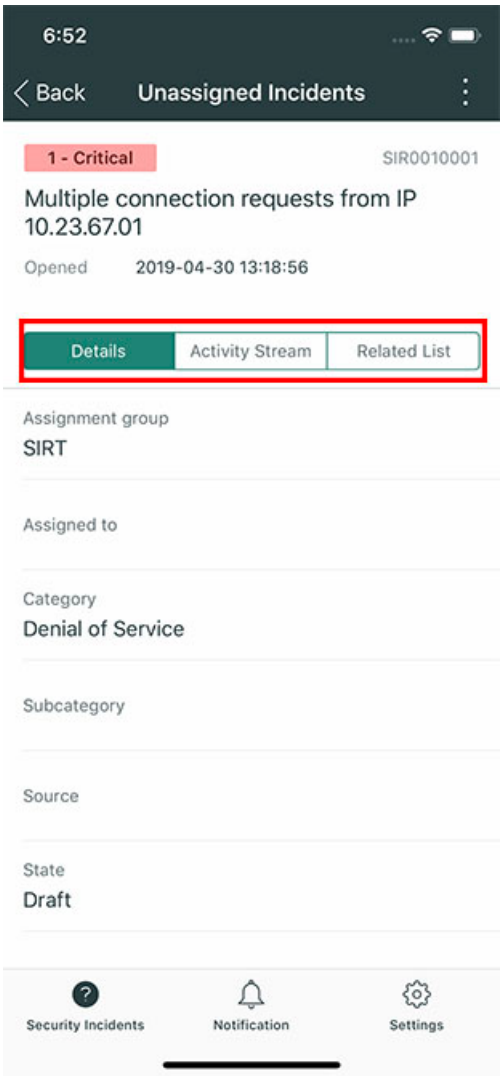
5. Escolha um no menu para continuar.

6. Como alternativa, com a tela Incidentes não atribuídos exibida, toque em um registro na lista.

7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

Exiba, edite e atribua incidentes de alta prioridade com o Aplicativo Security Incident Response Mobile

No seu dispositivo móvel, exiba, edite e atribua incidentes de alta prioridade Security Incident Response (SIR). Exiba as listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre os incidentes.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

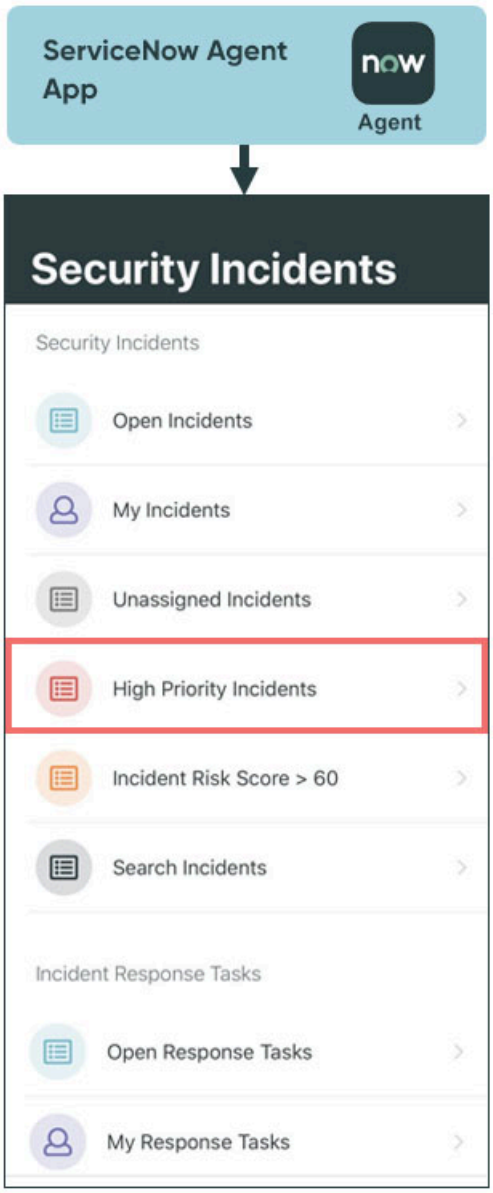
Na lista de registros, atribua um incidente de segurança crítico em aberto a você ou a outro analista do seu grupo. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5 a 10 minutos.

Procedimento

1. Se você não estiver conectado à sua instância da Now Platform em seu dispositivo móvel, consulte Faça login no Aplicativo Security Incident Response Mobilepara obter mais informações.
2. Com a tela inicial de Incidentes de segurança exibida, toque **em Incidentes de alta prioridade**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

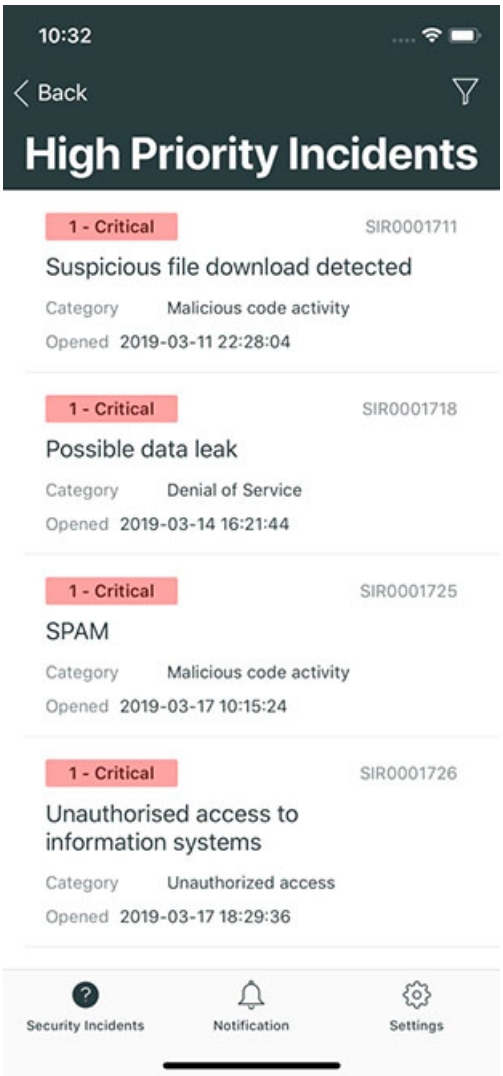
Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



A tela Incidentes de alta prioridade é exibida com uma lista de incidentes de segurança críticos (alta prioridade).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



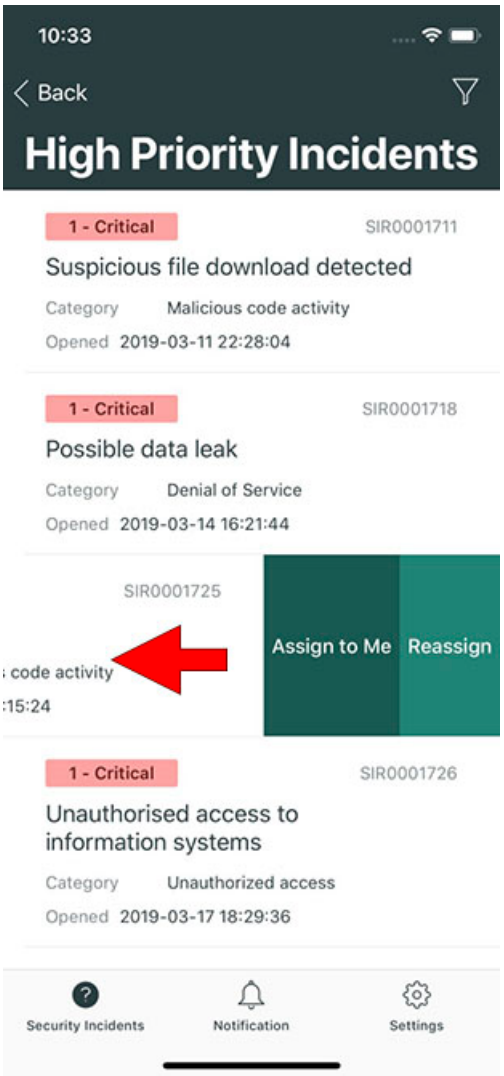
3. **Opcional:** Consulte Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro ( ) exibido, defina filtros para limitar o número de registros na lista. A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condição na Now Platform.

4. Com a lista de registros de incidentes de segurança de alta prioridade abertos exibida, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



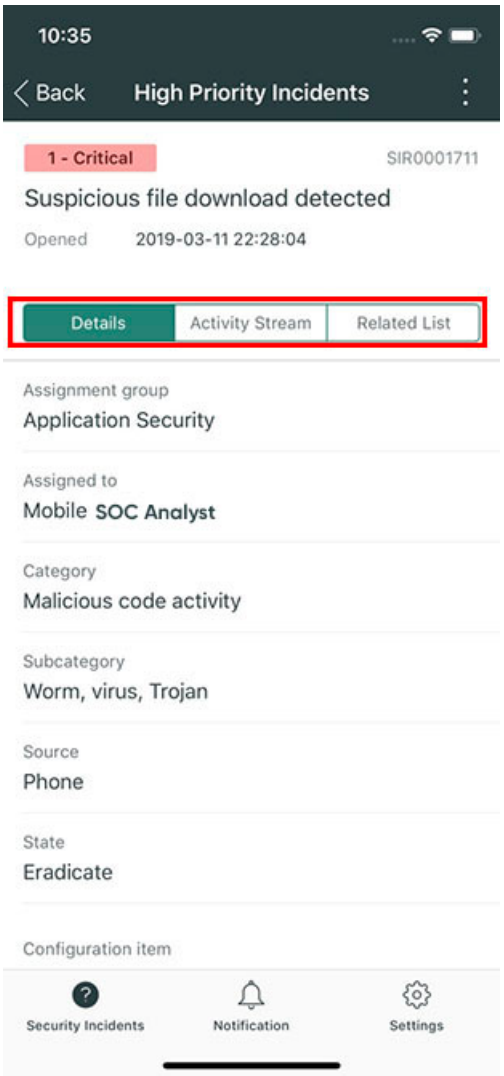
5. Escolha um para continuar.

6. Para exibir os detalhes de um registro de incidente de segurança aberto e ver mais registros associados e listas relacionadas, com a tela Incidentes de alta prioridade exibida, toque em um registro na lista.

7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exiba, edite e atribua incidentes de segurança com uma pontuação de risco maior que 60 com o Aplicativo Security Incident Response Mobile

Em seu dispositivo móvel, exiba e edite Security Incident Response (SIR) incidentes com um valor no campo de pontuação de risco maior que 60. Exiba as listas relacionadas e a trilha de auditoria das anotações de trabalho para obter mais detalhes sobre os incidentes.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Na lista de registros, atribua um incidente de segurança em aberto que tenha uma pontuação de risco maior que 60 a você ou a outro analista do seu grupo. Como alternativa, exiba os detalhes e as listas relacionadas do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5 a 10 minutos.

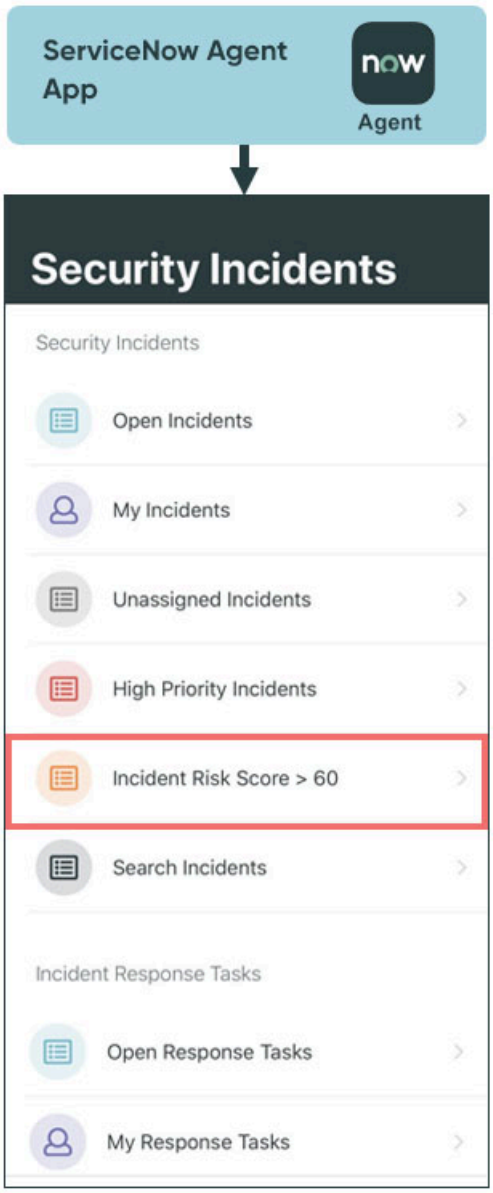
Procedimento

1. Se você não estiver conectado à sua instância da Now Platform em seu dispositivo móvel, consulte Faça login no Aplicativo Security Incident Response Mobilepara obter mais informações.
2. Com a tela inicial de Incidentes de segurança exibida, toque **em Pontuação de risco > 60**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

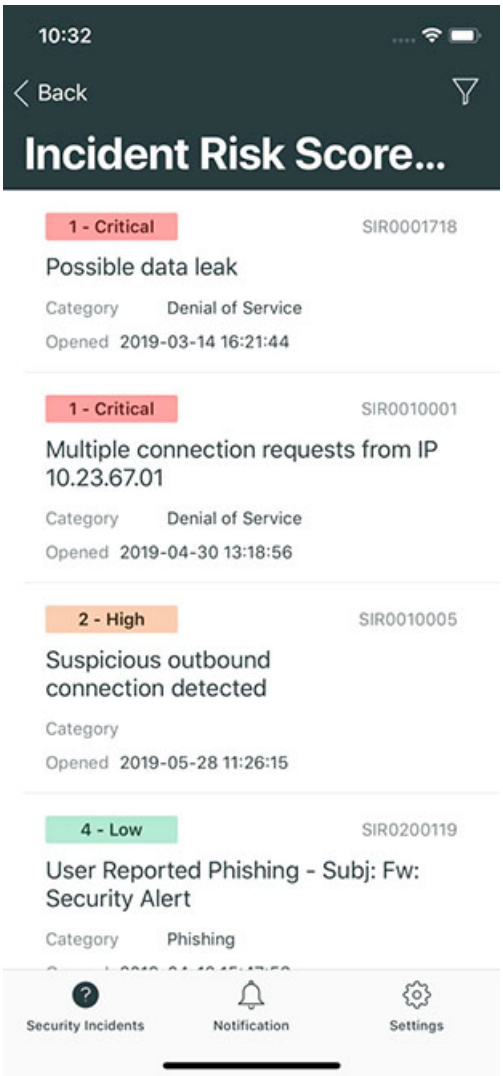
Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



A tela Pontuação de risco de incidente é exibida com uma lista de incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



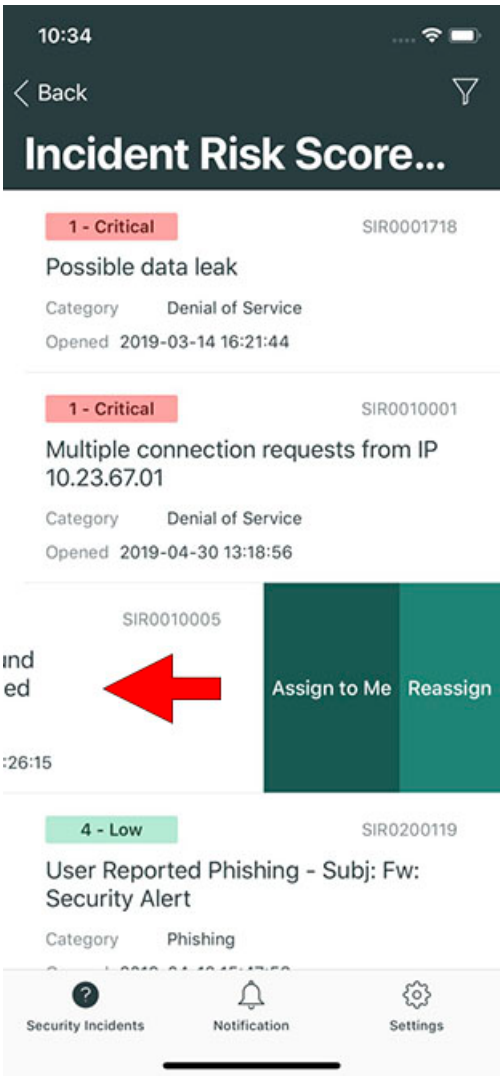
3. **Opcional:** Consulte Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile para pesquisar incidentes de segurança que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro (ícone de) exibido, defina filtros para limitar o número de registros na lista. A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condição na Now Platform.

4. Para atribuir um incidente de segurança a si mesmo ou reatribuí-lo diretamente da lista de registros de incidentes de segurança abertos exibidos, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



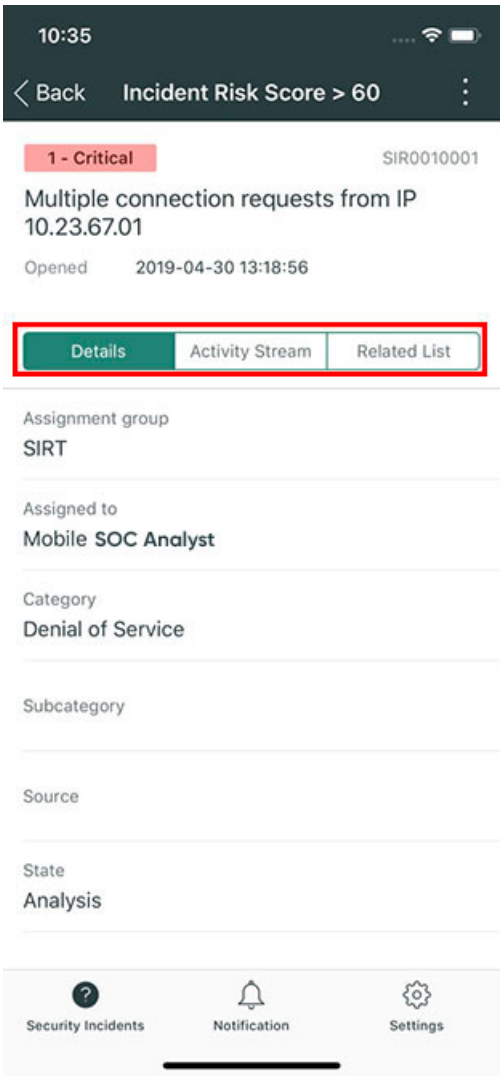
5. Escolha um para continuar.

6. Como alternativa, para exibir os detalhes de um registro de incidente de segurança aberto e ver mais registros associados e listas relacionadas, com a tela Pontuação de risco do incidente exibida, toque em um registro na lista.

7. No registro aberto exibido, escolha uma opção na tabela a seguir para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile

Pesquise incidentes de segurança Security Incident Response (SIR) em uma instância Now Platform®. Somente incidentes que correspondam aos critérios de pesquisa específicos inseridos são exibidos.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Tempo para concluir esta tarefa: 5 a 10 minutos.

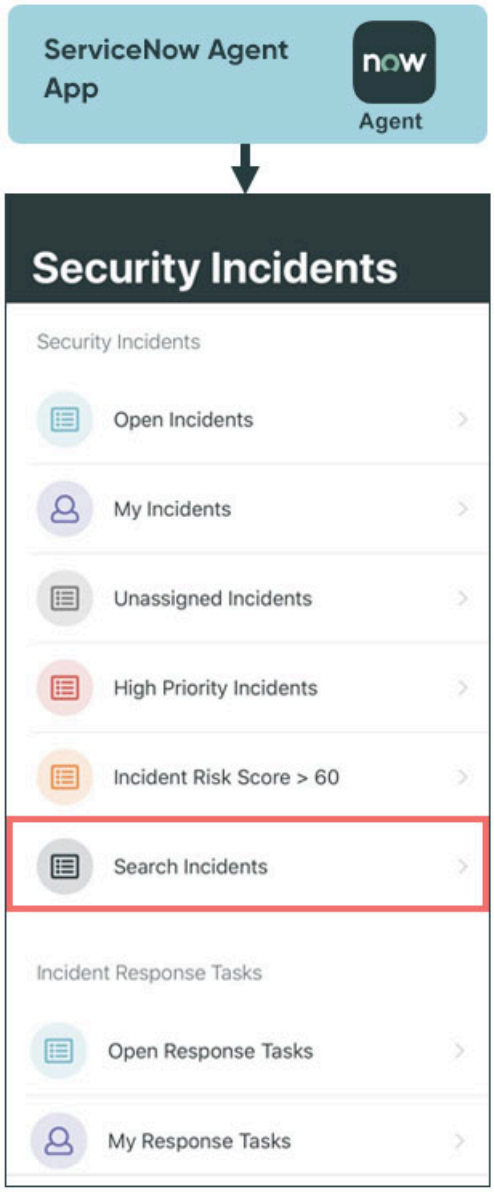
Procedimento

1. Se você não estiver conectado à sua instância da Now Platform em seu dispositivo móvel, consulte Faça login no Aplicativo Security Incident Response Mobilepara obter mais informações.
2. Com a tela inicial de Incidentes de segurança exibida, toque **em Pesquisar incidentes**.

   Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para limitar o número de resultados da pesquisa retornados, preencha o máximo possível de campos no formulário.
Para adicionar critérios de pesquisa, consulte a tabela a seguir. Siga as instruções após a tabela para editar os critérios de pesquisa existentes, limpar os critérios de pesquisa ou enviar uma pesquisa.

Tocar neste campo	Para adicionar uma entrada em Android dispositivos	Para adicionar e entrada em iOS dispositivos
Número	Insira um valor alfanumérico para um incidente de segurança, por exemplo, SIR0010004. Esse número é exibido no canto superior direito do incidente de segurança. O recurso pesquisa cadeias de caracteres numéricas e cadeias numéricas	Insira um valor alfanumérico para um incidente de segurança, por exemplo, SIR0010004. Esse número é exibido no canto superior direito do incidente de segurança. O recurso pesquisa cadeias de caracteres numéricas e cadeias numéricas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tocar neste campo	Para adicionar uma entrada em Android dispositivos	Para adicionar e entrada em iOS dispositivos
	parciais. Para pesquisas mais refinadas, insira mais dígitos. Caracteres curinga (*) não são aceitos. Toque em um novo campo para inserir mais critérios ou para enviar uma pesquisa.	parciais. Para pesquisas mais refinadas, insira mais dígitos. Caracteres curinga (*) não são aceitos. Toque em um novo campo para inserir mais critérios ou em **Pesquisar** para enviar uma pesquisa.
Descrição resumida	Insira o texto no campo, por exemplo, malware. O recurso pesquisa cadeias de caracteres de texto e cadeias de caracteres parciais do campo Descrição resumida. Para pesquisas mais refinadas, insira mais texto. Caracteres curinga (*) não são aceitos. Toque em um novo campo para inserir mais critérios ou para enviar uma pesquisa.	Insira o texto no campo, por exemplo, malware. O recurso pesquisa cadeias de caracteres de texto e cadeias de caracteres parciais do campo Descrição resumida. Para pesquisas mais refinadas, insira mais texto. Caracteres curinga (*) não são aceitos. Toque em um novo campo para inserir mais critérios ou em **Pesquisar** para enviar uma pesquisa.
Prioridade	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque no ícone de marca de seleção para retornar à tela Pesquisar incidentes.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** para retornar à tela Pesquisar incidentes.
Categoria	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque no ícone de marca de seleção para retornar à tela Pesquisar incidentes.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** para retornar à tela Pesquisar incidentes.
Estado	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque no ícone de marca de seleção para retornar à tela Pesquisar incidentes.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** para retornar à tela Pesquisar incidentes.
Atribuído a	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa.	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tocar neste campo	Para adicionar uma entrada em Android dispositivos	Para adicionar e entrada em iOS dispositivos
	Para limpar um valor para os campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.	Para limpar um valor para os campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.
Grupo de atribuição	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor para os campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor para os campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.

Para dispositivos Android, com a tela Pesquisar incidentes exibida e todos os seus critérios inseridos, escolha um para continuar.

4. Para dispositivos iOS, com a tela Pesquisar incidentes exibida, escolha um para continuar.

5. **Opcional:** Se sua pesquisa retornar vários registros, você poderá Filtrar registros com o Aplicativo Security Incident Response Mobile para refinar os resultados da pesquisa.

Exibir, editar e atribuir tarefas de resposta em aberto com o Aplicativo Security Incident Response Mobile

Exiba, edite e atribua tarefas de resposta em aberto. Suas mudanças são salvas na Tarefa do Security Incident Response do incidente de segurança primário.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Na lista de registros, atribua uma tarefa de resposta aberta e não atribuída a você ou a outro analista do seu grupo. Como alternativa, exiba os detalhes do registro ou adicione uma anotação de trabalho antes da atribuição. Tempo para concluir esta tarefa: 5 a 10 minutos.

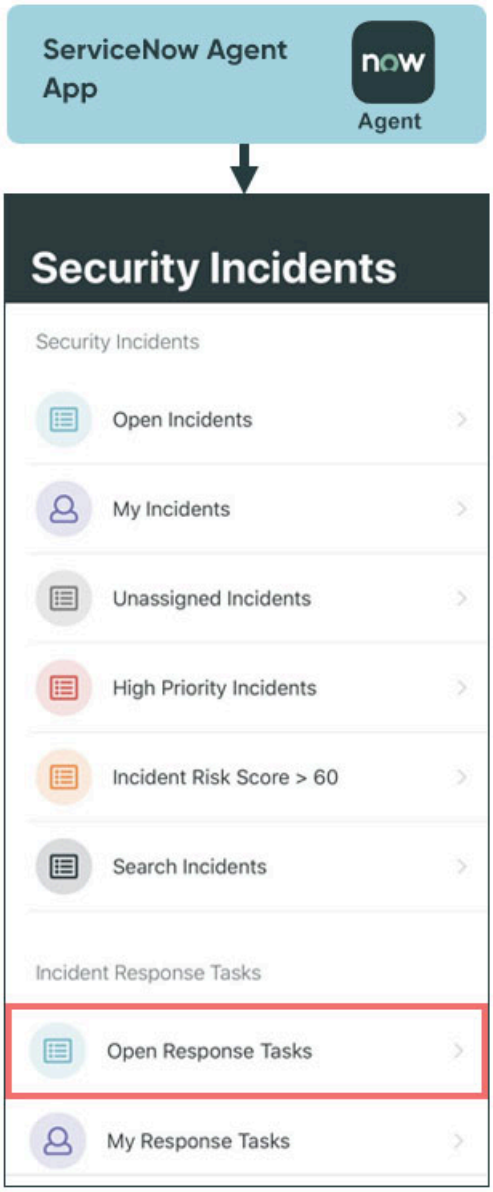
Procedimento

1. Se você não estiver conectado à sua instância da Now Platform em seu dispositivo móvel, consulte Faça login no Aplicativo Security Incident Response Mobilepara obter mais informações.
2. Com a tela inicial de Incidentes de segurança exibida, toque **em Abrir Tarefas de resposta**.

Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.

Tradução automática

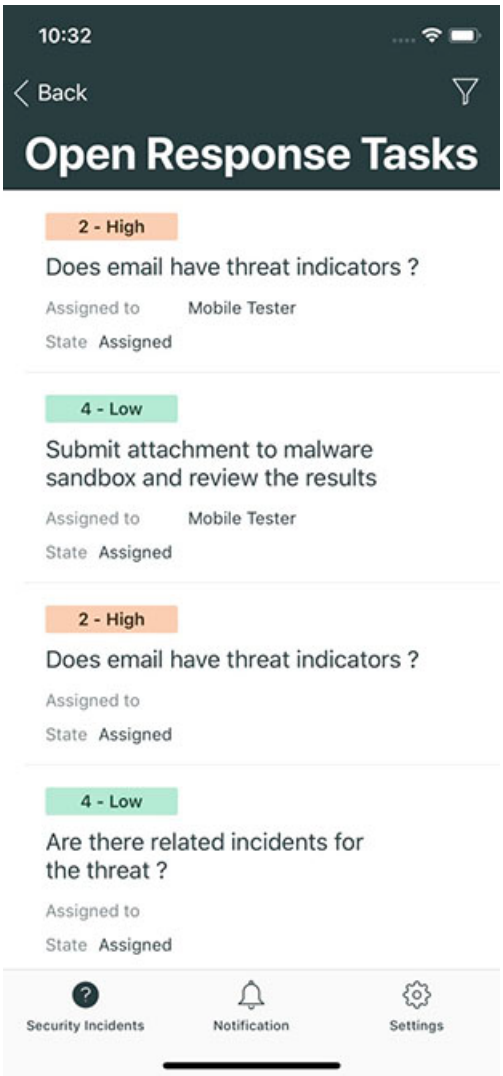
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A tela Tarefas de resposta em aberto é exibida com uma lista de tarefas em aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. **Opcional:** Consulte Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile para pesquisar tarefas que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro (ícone de) exibido, defina filtros para limitar o número de registros na lista. A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condição na Now Platform.

4. Com a lista de tarefas de resposta em aberto exibida, para atribuir ou reatribuir diretamente da lista, deslize para a esquerda em um registro para abrir o menu.

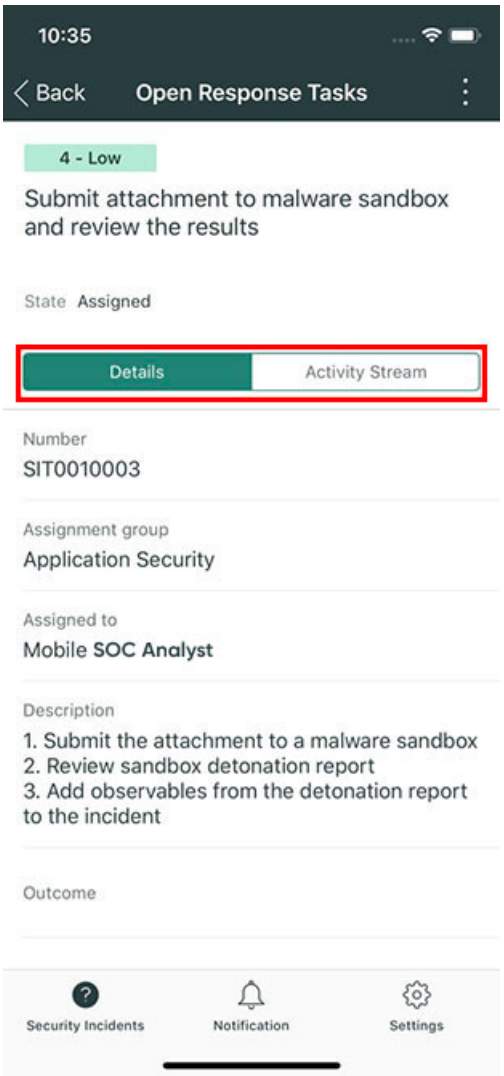
5. Escolha um para continuar.

6. Como alternativa, para exibir os detalhes de um registro de tarefa de resposta em aberto, com a tela Abrir tarefas de resposta exibida, toque em um registro na lista.

7. Com as guias no registro da tarefa de resposta exibidas, escolha uma na tabela a seguir para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exiba, edite e reatribua suas tarefas de resposta com o Aplicativo Security Incident Response Mobile

Exiba, edite e reatribua tarefas de resposta atribuídas a você. Suas mudanças são salvas na Tarefa do Security Incident Response do incidente de segurança primário.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Na lista de registros, reatribua uma tarefa de resposta em aberto que foi atribuída a você a outro analista do seu grupo. Como alternativa, exiba os detalhes do registro ou adicione uma anotação de trabalho antes da reatribuição. Tempo para concluir esta tarefa: 5 a 10 minutos.

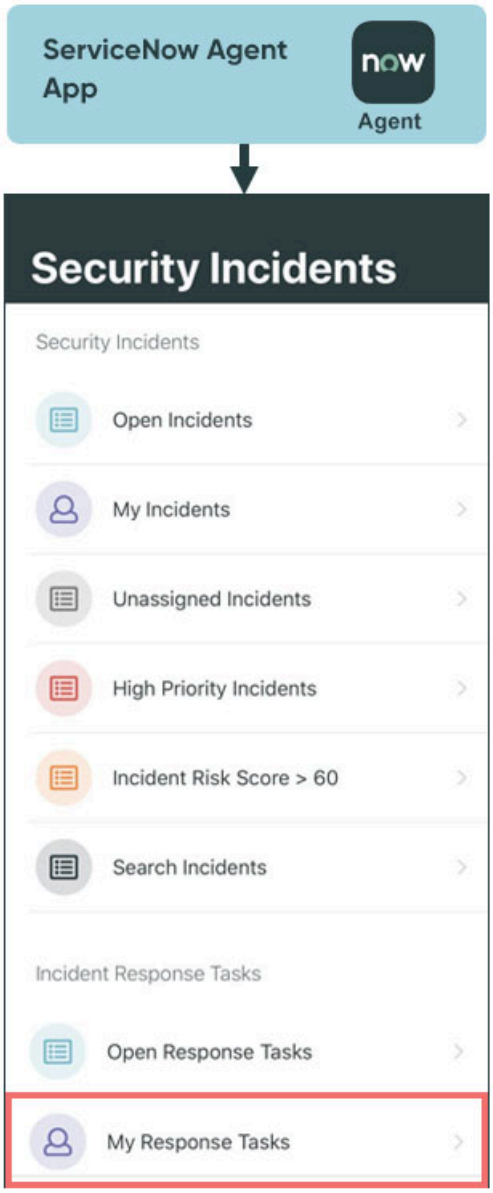
Procedimento

1. Se você não estiver conectado à sua instância da Now Platform em seu dispositivo móvel, consulte Faça login no Aplicativo Security Incident Response Mobilepara obter mais informações.
2. Com a tela inicial de Incidentes de segurança exibida, toque **em Minhas tarefas de resposta**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

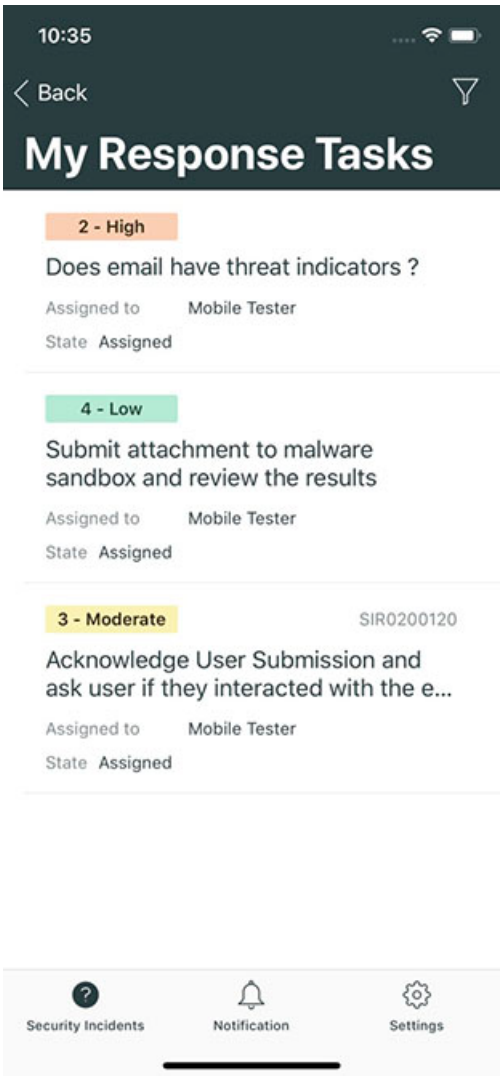
Se você sair de Aplicativo Security Incident Response Mobile depois de fazer login, toque no aplicativo Now Agent (Executante) a qualquer momento para retornar à última tela exibida.



A tela Minhas tarefas de resposta é exibida com uma lista das tarefas de resposta atribuídas a você.

Tradução automática

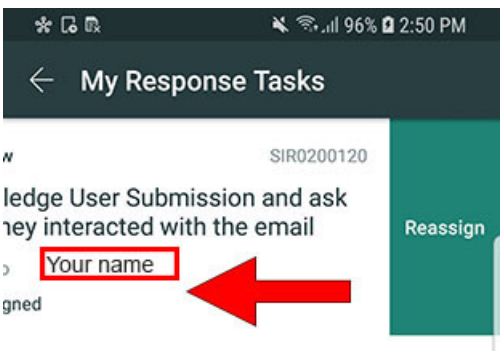
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. **Opcional:** Consulte Pesquisar incidentes de segurança com o Aplicativo Security Incident Response Mobile para pesquisar tarefas que correspondam a critérios específicos.

   Como alternativa, com o ícone de filtro ( ) exibido, defina filtros para limitar o número de registros na lista. A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condição na Now Platform.

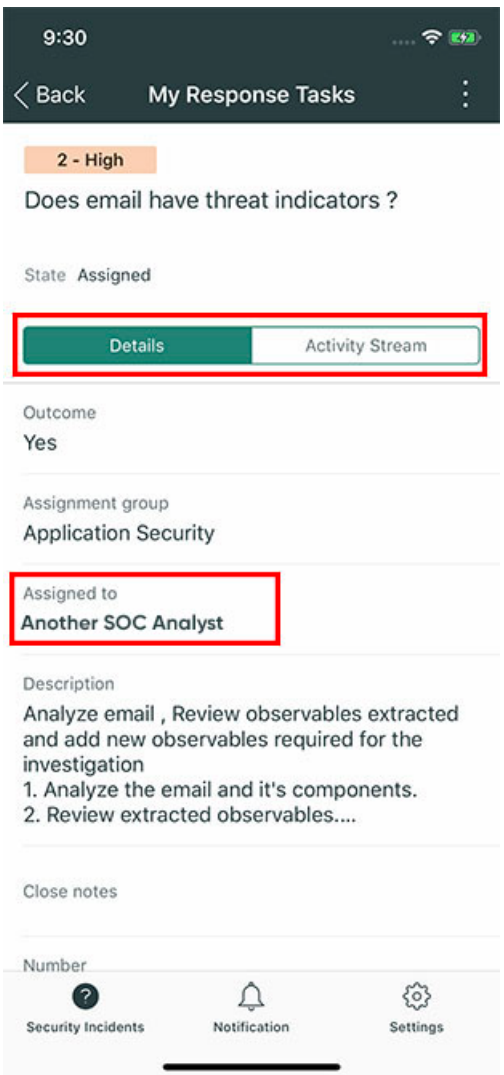
4. Para reatribuir uma tarefa diretamente da lista de registros de tarefa atribuídos a você, deslize para a esquerda em um registro para abrir o menu.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Toque **em Reatribuir**.
6. Na tela Atribuir tarefa de resposta a outro que é exibida, toque em um campo para expandi-lo e selecione outro grupo ou usuário para a tarefa.
7. Toque no ícone enviar ( ) ou **Enviar** para salvar suas mudanças e atualizar a tarefa de resposta. Uma mensagem é exibida confirmando que o registro foi atualizado. A tarefa é atribuída a um novo usuário no incidente de segurança primário e sua instância Now Platform é atualizada.
8. Para exibir os detalhes de uma tarefa de resposta em aberto e as anotações de trabalho, com a tela Minhas tarefas de resposta exibida, toque em um registro na lista.
9. Com os campos na tarefa de resposta exibidos, escolha um na tabela a seguir para continuar.



Tradução automática

Filtrar registros com o Aplicativo Security Incident Response Mobile

Defina filtros adicionais para limitar o número de registros exibidos em uma tela. A filtragem de registros no aplicativo para celular funciona como a filtragem com um construtor de condições na Now Platform.

Antes de Iniciar

Função necessária: sn_si.analyst

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Tempo para concluir esta tarefa: 5 minutos.

Procedimento

1. Para refinar ainda mais os resultados da pesquisa ou para inserir critérios de filtro adicionais em qualquer lista de registros exibida, toque no ícone de filtro (ícone de).
2. Com a tela Filtros exibida, toque em um campo para expandi-lo.
3. Entre as opções exibidas, toque na caixa de seleção ou em um item para o seu filtro.
   Para muitos dos filtros, você pode selecionar mais de uma opção.
4. Toque na seta) ou em **CONCLUÍDO** para salvar as mudanças em um campo.
   Os critérios escolhidos são exibidos na tela Filtros. O número de registros que correspondem aos seus critérios também é exibido na parte superior da tela. Toque em **REDEFINIR** para remover filtros e restaurar a configuração padrão.
5. **Opcional:** Repita as etapas 1 a 4 com a tela Filtros exibida para continuar definindo seus critérios de filtro.
6. Toque no ícone de interseção Ícone para criar condições E.
   Como alternativa, toque no ícone de interseção Ícone para criar condições OR.
7. Depois de adicionar todos os critérios desejados, com a tela Filtros exibida, toque em **FINALIZADO**.
   Na tela, somente os registros que correspondem aos seus critérios de filtro são exibidos.

Orquestração de resposta de incidente de segurança

Orquestração de resposta de incidente de segurança As atividades do permitem que os usuários interajam e recuperem dados de sistemas e ambientes baseados no Windows ou no UNIX usando a orquestração de fluxo de trabalho.

Configurar Orquestração de resposta de incidente de segurança.

Antes de usar Orquestração de resposta de incidente de segurança, execute as etapas para configurar várias partes do sistema, incluindo o preenchimento do CMDB, a configuração do mid-server e a configuração de credenciais.

Antes de Iniciar

Função necessária: administrador

Para usar Security Incident Response, você precisa de um CMDB totalmente preenchido com nomes de domínio. Para obter mais informações, consulte Descoberta .

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Ative o plug-in Security Incident Response.
2. Configurando MID Servers .
3. Configure as credenciais de serviço do Windows MID Server .

Entenda os fluxos de trabalho e os modelos de fluxo de trabalho do Security Incident Response Orchestration

O sistema base Security Incident Response inclui uma série de fluxos de trabalho e modelos de fluxo de trabalho projetados para funcionar com registros de incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.basic

Por Que e Quando Desempenhar Esta Tarefa
Você pode personalizar todos os fluxos de trabalho e modelos de fluxo de trabalho para melhor atender às suas necessidades, desde que tenha a função apropriada: sn_sec_cmn.admin. Fluxos de trabalho são usados em todo o sistema Security Operations para executar uma variedade de tarefas.
Os modelos de fluxo de trabalho, no entanto, são acionados selecionando um valor no campo **Categoria** em um incidente de segurança. Quando isso ocorre, o modelo de fluxo de trabalho associado à seleção inicia um modelo de fluxo de trabalho que instrui os analistas de segurança a lidar com um tipo específico de ameaça.

Por exemplo, se você selecionar **Negação de serviço** no campo **Categoria** em um incidente de segurança, o **Incidente de segurança - Negação de serviço - Modelo** será executado e o analista será orientado a determinar se o destino do DOS é essencial para os negócios. Em caso afirmativo, a próxima tarefa faz com que a prioridade do incidente de segurança seja definida como **1 - Crítico**e, em seguida, executa a próxima tarefa. E assim por diante.

Portanto, Security Incident Response fluxos de trabalho e modelos de fluxo de trabalho são essencialmente os mesmos, exceto que os modelos são usados para um conjunto específico de funções em um incidente de segurança.

Procedimento
1. Navegar até **Todos** > **Security Operations** > **Workflows** > **Exibir Fluxos de Trabalho de Segurança**.
2. Uma lista dos fluxos de trabalho e modelos de fluxo de trabalho enviados no sistema de base é exibida. Todos os novos fluxos de trabalho que você criou no pacote de aplicações Security Operations também são incluídos na lista.
3. Clique no nome do fluxo de trabalho ou do modelo de fluxo de trabalho que você deseja exibir.

Nota:
Os fluxos de trabalho podem ser acionados de várias maneiras diferentes. Esteja ciente de que associar um fluxo de trabalho a um gatilho de fluxo de trabalho não significa necessariamente que o fluxo de trabalho está ativo.

Orquestração de resposta de incidente de segurança fluxos de trabalho e atividades

Vários fluxos de trabalho e atividades estão incluídos com Orquestração de resposta de incidente de segurança.

Somente usuários com a função sn_sec_cmn.admin podem Editor de fluxo de trabalho.

Criar solicitação de pesquisa para fluxo de trabalho de mudanças de IoC

O fluxo de trabalho **Security Incident Response - Criar solicitação de pesquisa para mudanças de IoC** é acionado por uma regra de negócios para ser executado automaticamente quando um IoC é adicionado ou alterado. As verificações de malware são acionadas somente quando novos dados são inseridos e somente os novos dados são verificados.

Antes de Iniciar
Função necessária: sn_si.basic

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

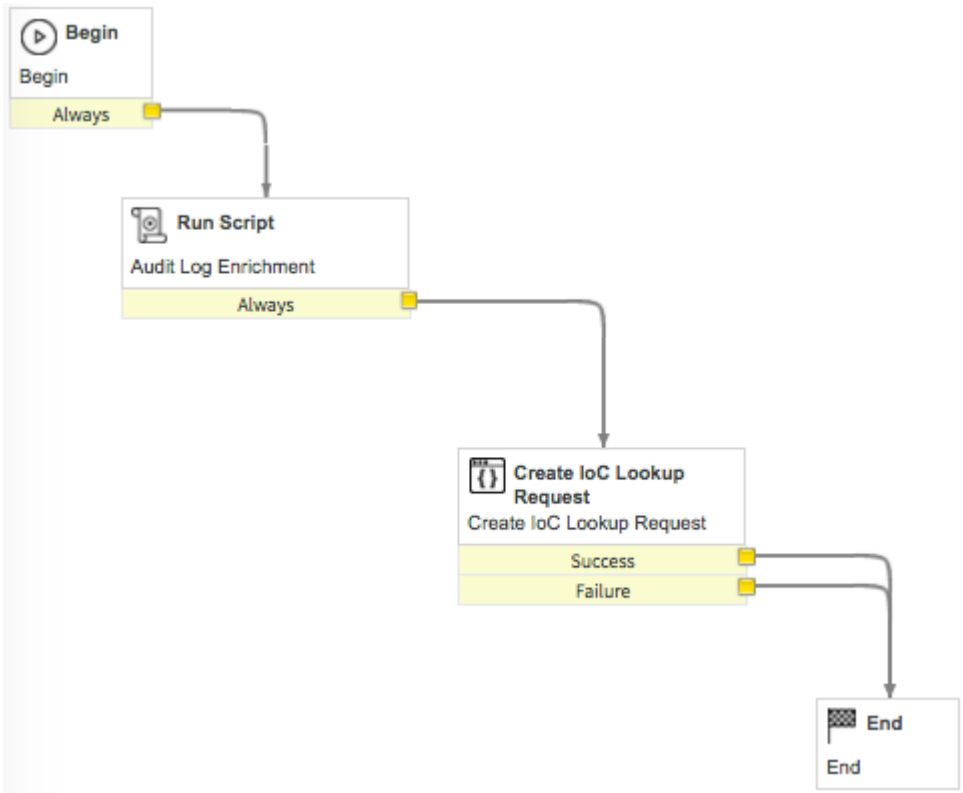
Por Que e Quando Desempenhar Esta Tarefa
Se o IoC estiver vazio, o fluxo de trabalho não será executado. As verificações históricas são retidas e podem ser vistas na guia **Solicitações de verificação de segurança**e nas anotações de trabalho do incidente de segurança.

Os incidentes de segurança existentes são atualizados automaticamente.

As atividades do processo de fluxo de trabalho incluem:

- Execute o script de log de auditoria.
- Atividade Criar solicitação de pesquisa de IoC

Fluxo de trabalho de mudanças de IoC



Atividade Criar solicitação de pesquisa de IoC

A atividade **Criar solicitação de pesquisa de IoC** pode ser usada com qualquer fluxo de trabalho para criar uma solicitação de pesquisa de malware para campos de IoC adicionados ou modificados.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Solicitação de pesquisa criada.
Falha	Solicitação de pesquisa não criada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
Cadeia de caracteres ioc	Informações de IoC no formato JSON. IP, hash, URL.
siId	Identificador do sistema de incidentes de segurança

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
scnReqID	Pesquisar identificador de solicitação

Fluxo de trabalho do Security Incident Response - Obter estatísticas de rede

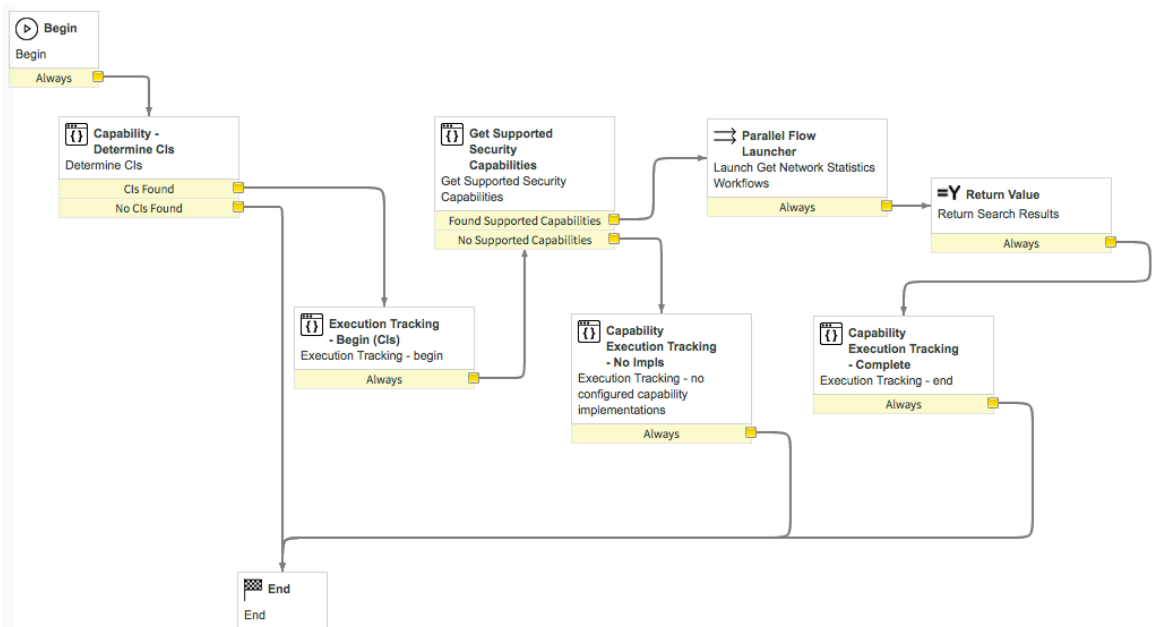
O **Security Incident Response** > **Obter Estatísticas de Rede** O fluxo de trabalho recupera as estatísticas de rede de um recurso baseado no Windows afetado quando adicionado a um incidente de segurança no estado **Análise**.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Para novos incidentes de segurança que contêm itens de configuração, o fluxo de trabalho é executado automaticamente quando o estado muda para **Análise**.

Os incidentes de segurança existentes são atualizados automaticamente quando você está no estado **Análise** e adiciona um novo item de configuração.

Obter Estatísticas de Rede



As atividades do processo de fluxo de trabalho incluem:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade Obter FQDN do item de configuração

Determinar Shell Script por SO

Se a declaração for executada pelo PowerShell

Acompanhamento de execução - Iniciar atividade

Obter estatísticas de rede por meio da atividade netstat

Acompanhamento de execução de capacidade - Atividade com falha

Atividade Criar registros de dados de aprimoramento

Acompanhamento de execução de capacidade - Atividade com falha - Retorna o ID de aprimoramento.

Acompanhamento de execução de capacidade - Concluir atividade

Procedimento

1. Abra um incidente de segurança.
2. Atualize o **Estado** para **Análise**, se necessário.
3. Adicione um item de configuração (computador, servidor ou similar).
4. Clique em **Atualizar**.
   Orquestração de resposta de incidente de segurança fornece informações de estatísticas de rede no **Links relacionados** > **Aprimoramentos de incidente de segurança** guia. Para obter mais informações, consulte Security Operations mapeamento de dados de aprimoramento.

   Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Fluxo de trabalho de integração de comandos do sistema de operações de segurança – Obter processos em execução

O fluxo de trabalho Integração de comandos do sistema de operações de segurança - Obter processos em execução recupera os processos em execução de um item de configuração quando adicionado ou atualizado para um incidente de segurança baseado em Windows ou Unix no estado de **análise**.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Para novos incidentes de segurança, o fluxo de trabalho é executado automaticamente quando você envia o incidente com um item de configuração selecionado, quando o estado muda automaticamente para **Análise**. Se permanecer no estado **Rascunho**, ele não será executado.

Os incidentes de segurança existentes são atualizados automaticamente quando você está no estado **Análise** e adiciona um novo item de configuração.

As atividades do processo de fluxo de trabalho incluem:

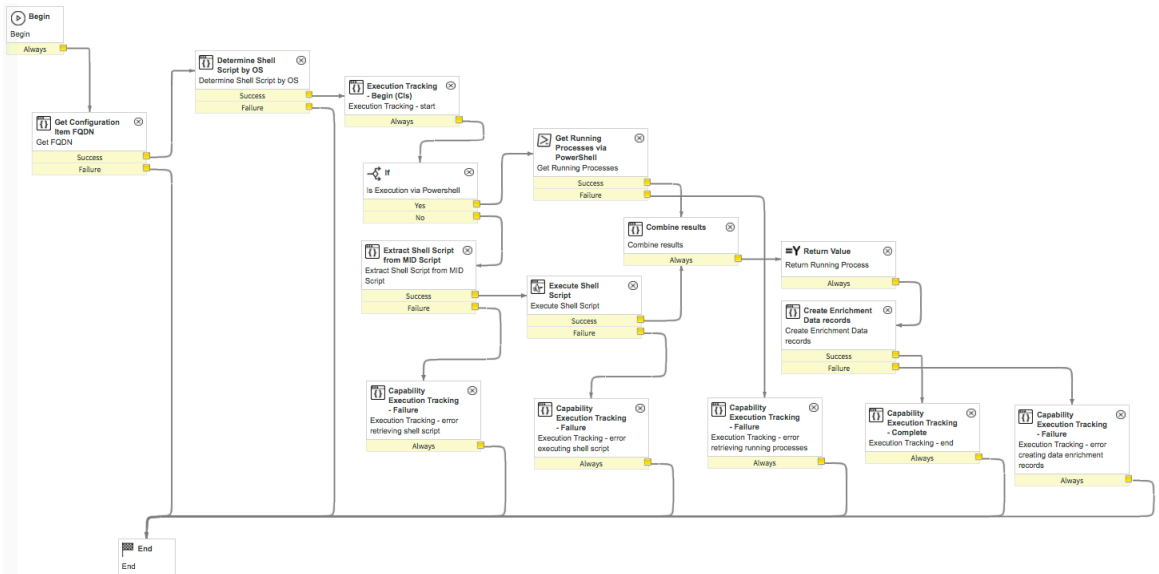
- Atividade Obter FQDN do item de configuração
- Determinar Shell Script por atividade do SO
- Acompanhamento de execução - Iniciar atividade
- Obter processos em execução via PowerShell

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Atividade Executar script de shell
- Acompanhamento de execução de capacidade - Atividade com falha
- Atividade Extrair Shell Script do MID Script
- Combinar resultadose retornar valores em uma matriz
- Atividade Criar registros de dados de aprimoramento
- Acompanhamento de execução de capacidade - Concluir atividade

Obter Processos em Execução



Procedimento

1. Abra um incidente de segurança.
2. Atualize o **Estado** para **Análise**, se necessário.
3. Adicione um item de configuração (computador, servidor ou similar).
4. Clique em **Atualizar**.
   Orquestração de resposta de incidente de segurança fornece informações do processo em execução no **Link relacionados** > **Aprimoramentos de incidente de segurança**guia. Para obter mais informações, consulte Security Operations mapeamento de dados de aprimoramento.

   Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Fluxo de trabalho do Security Incident Response - Obter serviços em execução

O **fluxo de trabalho do Security Incident Response - Obter serviços em execução** recupera uma lista de serviços em execução de itens de configuração (ICs) baseados no Windows, ServiceNow. Este fluxo de trabalho é usado para aprimoramento de incidentes durante as investigações.

Antes de Iniciar

Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

O **fluxo de trabalho do Security Incident Response - Obter serviços em execução** é executado automaticamente quando você adiciona um novo item de configuração a um incidente de segurança do Windows depois que o estado muda para **Análise**. As informações que este fluxo de trabalho obtém aparecem nas guias **Mostrar dados** de aprimoramento do incidente de segurança.

Nota:
Se o incidente de segurança permanecer no estado **Rascunho**, o **fluxo de trabalho do Security Incident Response - Obter serviços em execução** não será executado.

As atividades de fluxo de trabalho incluem:

Atividade de script de aprimoramento de log de auditoria

Atividade Obter FQDN do item de configuração

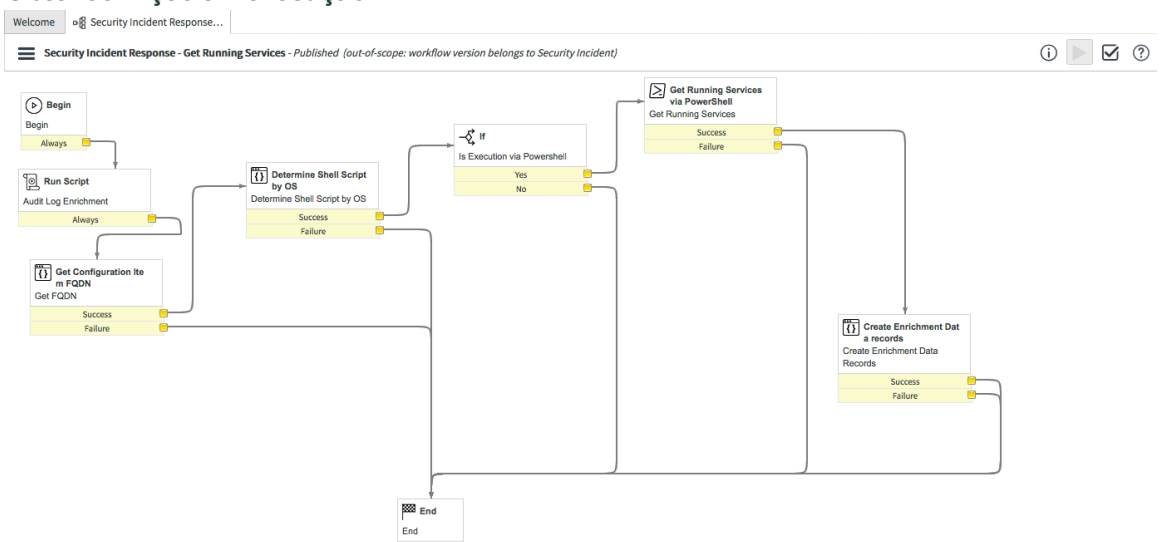
Determinar Shell Script por atividade do SO

É atividade de execução via PowerShell

Obter serviços em execução - Atividade de aprimoramento de WMI

Atividade Criar registros de dados de aprimoramento

Obter serviços em execução



Procedimento

1. Abra um incidente de segurança.
2. Atualize o **Estado** para **Análise**, se necessário.
3. Adicione um item de configuração baseado no Windows (servidor, laptop ou similar).
4. Clique em **Atualizar**.
   Security Incident Response fornece informações de serviços em execução no **Links relacionados** > **Aprimoramentos de incidente de segurança**guia. Para obter mais informações, consulte Security Operations mapeamento de dados de aprimoramento.

Atividade Obter FQDN do item de configuração

O **Orquestração do Security Common** > **Obter FQDN do item de configuração** A atividade de fluxo de trabalho recupera o nome de domínio totalmente qualificado (FQDN) de um item de configuração. Esta atividade pode acelerar o processo de investigação e correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A atividade Obter FQDN do item de configuração pode ser usada com qualquer fluxo de trabalho para recuperar o nome de domínio totalmente qualificado (FQDN) de um item de configuração.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
cmdb_ci.id [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
fqdn [cadeia de caracteres]	O nome de domínio totalmente qualificado (FQDN) do item de configuração.

Anotações Adicionais

O campo fqdn no item de configuração deve ser preenchido.

Determinar Shell Script por atividade do SO

A atividade de fluxo de trabalho Determinar Shell Script por SO determina qual sistema operacional será usado no fluxo de trabalho

A atividade Determinar Shell Script por SO pode ser usada com qualquer fluxo de trabalho para determinar qual script de shell executar com base no sistema operacional em execução no sistema que contém o item de configuração.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Sistema operacional encontrado.
Falha	Nenhum sistema operacional encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
ciSysId	Identificador do sistema do item de configuração.
processType	Identificador interno que define qual script extrair da tabela.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
processScript	Agente de ECC que reúne o processo em execução.
executionTemplate	Determina se o script será executado por meio de um probe ou usando o PowerShell.
richmentMappingId	Identificador do sistema do mapeamento de aprimoramento usado para transformar os dados de resposta.

Obter serviços em execução - Aprimoramento de WMI

O fluxo de trabalho **do Security Incident Response - Obter** serviços em execução reúne serviços em execução em um item de configuração adicionado a um incidente de segurança.

A atividade **Obter serviços em execução - Aprimoramento de WMI** é iniciada automaticamente para recuperar informações de serviços em execução para um host do Windows.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
destino [cadeia de caracteres]	O nome de domínio totalmente qualificado (FQDN) do sistema de destino.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta [cadeia de caracteres]	Uma cadeia de caracteres JSON que representa os serviços em execução no sistema de destino. Os dados JSON incluem: **nome** O nome do serviço **PID**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
	O identificador de processo do serviço em execução **service_type** (Opcional) O tipo de serviço em execução. **start_name** O nome do sistema para o serviço **path** O caminho do arquivo do executável do serviço em execução **start_mode** O modo de início do serviço em execução. **display_name** O nome do serviço em execução como ele aparece para o usuário

Restrições

O MID Server deve oferecer suporte ao **PowerShell**.

O hash SHA-256 requer PowerShell V4.

Atividade Criar registros de dados de aprimoramento

A atividade de fluxo de trabalho **Criar registros de dados de** aprimoramento cria ou atualiza registros de aprimoramento para uso no fluxo de trabalho.

A atividade **Criar registros de dados de aprimoramento** pode ser usada com qualquer fluxo de trabalho para atualizar registros de aprimoramento no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Registro de aprimoramento atualizado.
Falha	Registro de aprimoramento não atualizado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
task_id	Identificador de tarefa.
conteúdo	Conteúdo bruto (dados de processos em execução).
richment_mapping_id	Identificador de mapeamento de aprimoramento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
ci_id	Identificador do item de configuração.
valor_referência	Não utilizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado	GlideRecords criado usando o script richmentUtils.

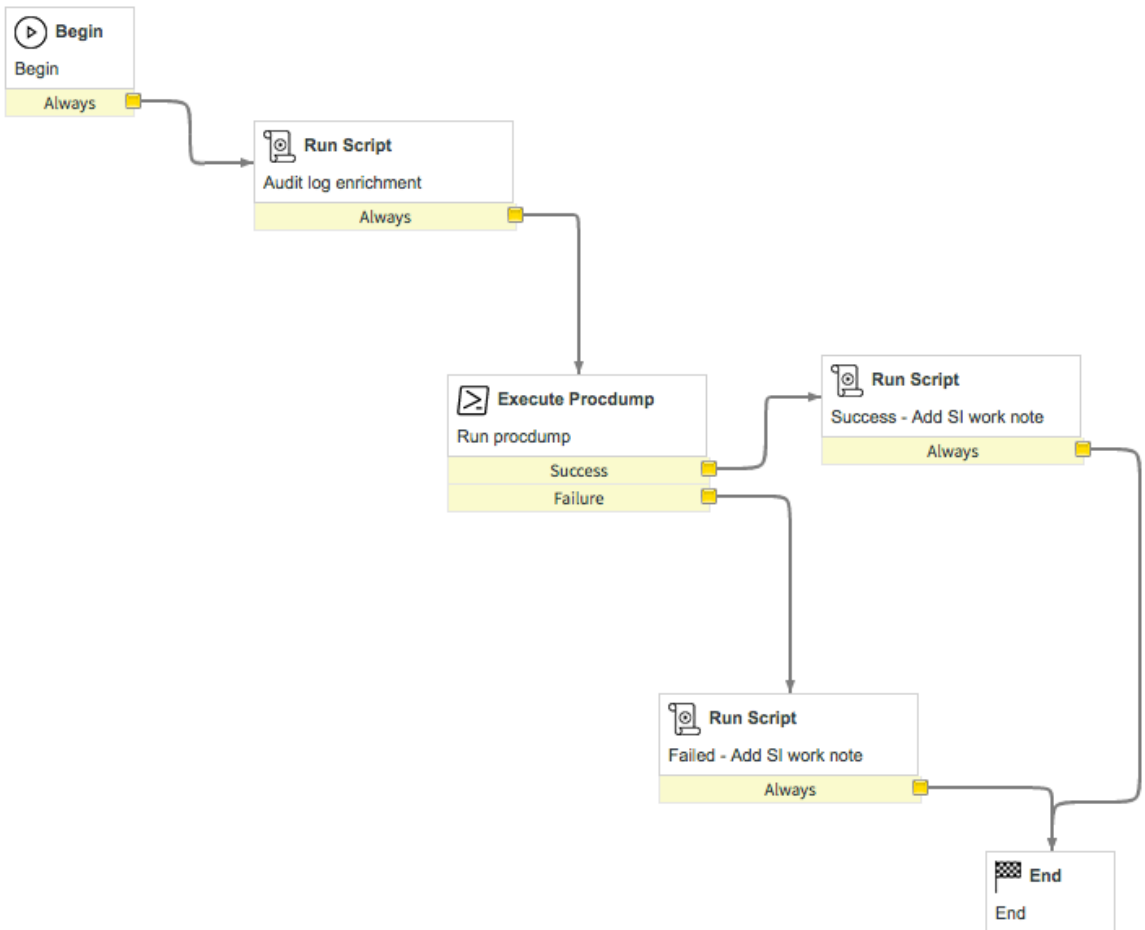
Executar fluxo de trabalho de procdump

O fluxo de trabalho **Executar procdump** executa um despejo de processo em um processo especificado e o salva em um arquivo que pode ser direcionado por analistas de segurança.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado quando processos aprimorados são selecionados e uma ação de IU **Executar procdump** é executada.

Executar procdump



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As atividades do processo de fluxo de trabalho incluem:

- Executar script (enriquecimento de log de auditoria): executa um script para adicionar um log de auditoria ao incidente de segurança.
- Executar atividade de procdump
- Executar script (Êxito – Adicionar anotação de trabalho de SI): executa um script para adicionar uma anotação de trabalho quando o procdump é bem-sucedido.
- Executar script (Falha - Adicionar anotação de trabalho de SI): executa um script para adicionar uma anotação de trabalho quando o procdump falha. Os motivos pelos quais o procdump pode falhar incluem:
  - Caminho de despejo inválido
  - Caminho de compartilhamento de arquivo inválido
  - Não é possível buscar o nome do domínio totalmente qualificado da máquina Windows em que o procdump está sendo executado
  - O nome do processo não foi especificado
  - A variável de ambiente PROCDUMP não foi encontrada
  - Falha ao copiar uma cópia do arquivo de despejo do caminho de despejo para o caminho de compartilhamento do arquivo

Executar atividade de procdump

Executar procdump é uma atividade do PowerShell que executa o procdump nos processos selecionados, despeja os dados em um arquivo e os publica em um site compartilhado em uma rede interna. Um analista pode exibir um processo da lista de proibições, destacado em vermelho em um incidente de segurança, e executar análises adicionais no arquivo.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O procdump foi executado com sucesso no process_name e os detalhes estão disponíveis em activityOutput.response.
Falha	Falha ao executar o procdump no process_name e os detalhes estão disponíveis em activityOutput.response.

Variáveis de entrada

As variáveis de entrada são usadas para criar as saídas solicitadas.

Variáveis de entrada

Variável	Descrição
targetId	[Obrigatório] O ID de destino no qual executar o procdump.
process_name	[Obrigatório] O nome do processo para o procdump.
despejo_path	[Obrigatório] O caminho do arquivo local no qual o arquivo de despejo gerado será salvo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
nome_do_arquivo_despejo	[Obrigatório] O nome do arquivo gerado pelo procdump. Todos os caracteres especiais serão substituídos por hifens (-) do nome do arquivo de despejo quando o arquivo for gerado.
file_share_path	[Obrigatório] O caminho de compartilhamento do arquivo para o qual o arquivo de despejo será copiado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
share_path	O caminho de compartilhamento de arquivos para o qual o arquivo de despejo foi copiado.
resposta	Uma representação JSON do resultado do procdump.
resultado	O resultado do procdump.

Incidente de segurança - Avaliar fluxo de trabalho de resultado da tarefa de resposta

Incidente de segurança - o fluxo de trabalho do resultado da tarefa Avaliar resposta determina a tarefa a ser usada, invoca um fluxo de trabalho escolhido e um script de avaliação com base no registro do avaliador de resultado fornecido como entrada para o fluxo de trabalho escolhido.

Antes de Iniciar
Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho deve ser executado ao mesmo tempo que a atividade de criação de tarefa a ser avaliada. O script de avaliação consulta os artefatos (como registros de pesquisa de detecções ou processos em execução) da capacidade configurada usando informações de contexto da tarefa de resposta (como o incidente de segurança primário) para determinar o resultado apropriado para a tarefa de resposta. O resultado pode ser dependente da atividade do fluxo de trabalho, mas geralmente é **sim** ou **não**. Ao criar um registro de avaliador de resultado, somente as capacidades que têm um fluxo de trabalho configurado, com a caixa **É recurso baseado em tarefa** marcada e um conjunto de variáveis de entrada de tarefa estão disponíveis para seleção.

As atividades do processo de fluxo de trabalho incluem:

Executar script para determinar a tarefa de resposta

Deve executar o fluxo de trabalho

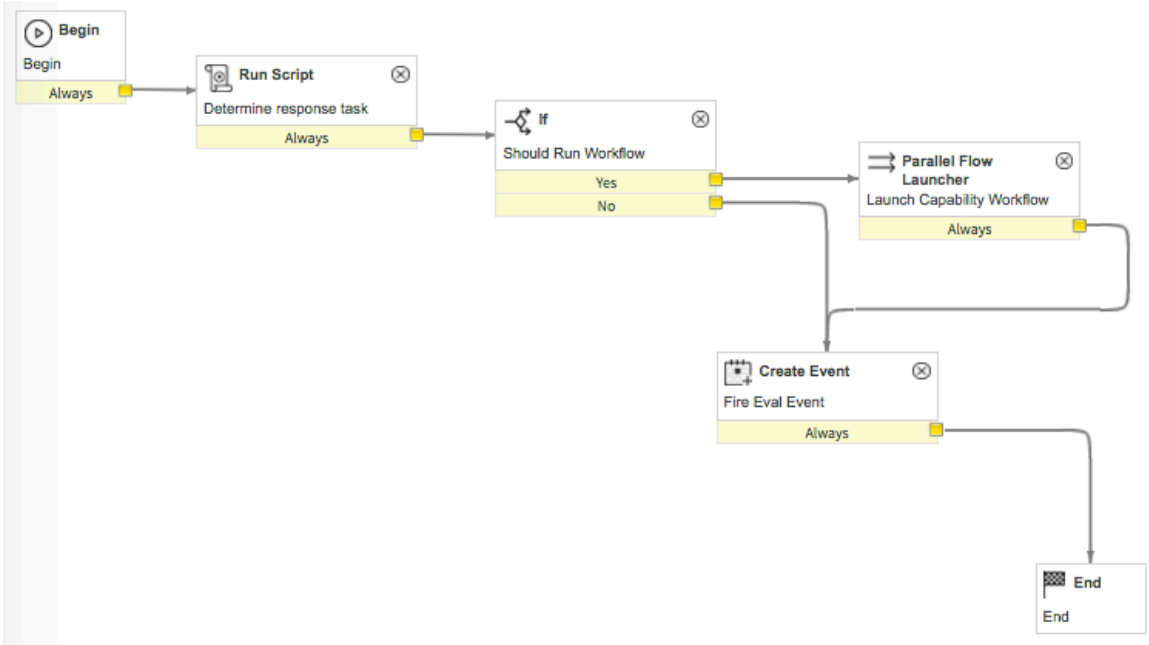
Fluxo de trabalho da capacidade de inicialização do inicializador de fluxo paralelo

Criar evento de avaliação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Avaliar resultado da tarefa de resposta



Modelos de fluxo de trabalho do Security Incident Response

Os modelos de fluxo de trabalho são fornecidos com Orquestração de resposta de incidente de segurança para permitir que você execute procedimentos básicos de análise relacionados à operação de segurança. Os modelos podem ser usados como estão ou você pode personalizá-los para criar fluxos de trabalho que atendam melhor às suas necessidades específicas. Os modelos de fluxo de trabalho são desativados por padrão.

Somente usuários com a função sn_sec_cmn.admin podem editar o Editor de fluxo de trabalho.

Modelo de fluxo de trabalho de Exposição de dados confidenciais de incidente de segurança

O Incidente de segurança - Exposição de dados confidenciais - Modelo permite que você execute uma série de tarefas projetadas para lidar com a exposição de dados confidenciais.

Antes de Iniciar

Função necessária: sn_si.write

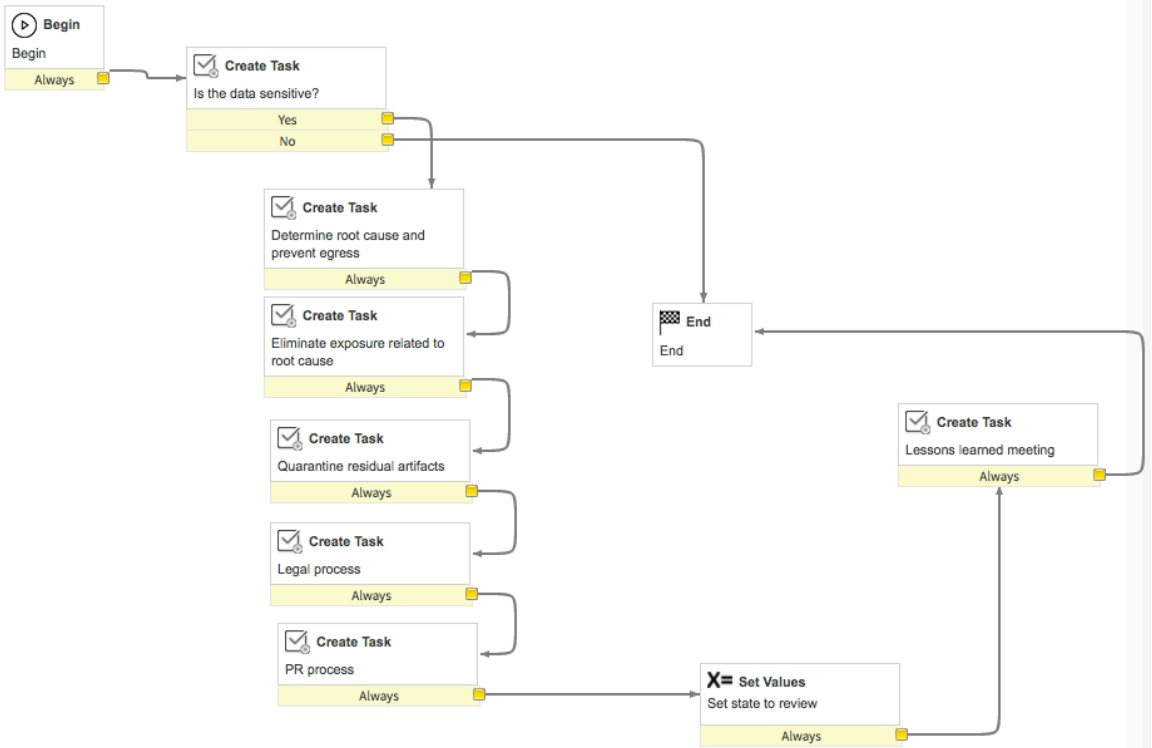
Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida ou alterada para **Exposição de dados de identidade pessoal confidencial**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exposição de dados de identidade pessoal confidencial



Procedimento

1. Abra o incidente de segurança para o qual você deseja lidar com a exposição de dados confidenciais ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Exposição de dados de identidade pessoal confidencial**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tarefas de resposta no modelo de exposição de dados confidenciais

Tarefa de resposta	Descrição	Resultados
Os dados são confidenciais?	Determine se os dados associados a este incidente de segurança são confidenciais. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionou **Sim**, a próxima tarefa de resposta será executada. Se você selecionou **Não**, o fluxo será encerrado.
Determinar a causa raiz e impedir a saída	Determine a causa raiz do ataque e adicione filtragem de saída para parar a exfiltração, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Eliminar exposição relacionada à causa raiz	Com base na causa raiz, execute as etapas para eliminar a exposição, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Descrição	Resultados
Artefatos residuais de quarentena	Execute as etapas para colocar em quarentena quaisquer artefatos residuais, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Processo jurídico	Execute as etapas para atender aos requisitos jurídicos desta análise, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Processo de RC	Execute as etapas para atender aos requisitos de RC desta análise, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**.
Reunião de lições aprendidas	Realize uma reunião de lições aprendidas para fazer a triagem do trabalho realizado nesses dados confidenciais, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, o incidente de segurança permanecerá no estado **Revisar** até que você o feche.

Modelo de fluxo de trabalho de negação de serviço de incidente de segurança

O Incidente de segurança - Negação de serviço - Modelo permite que você execute uma série de tarefas projetadas para lidar com ataques de negação de serviço (DOS).

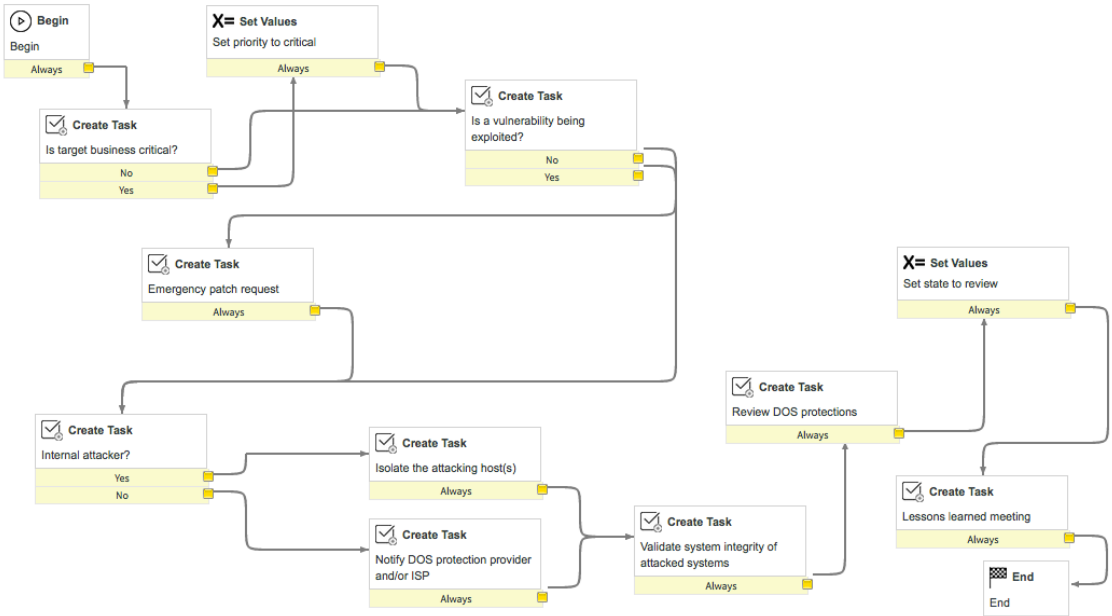
Antes de Iniciar
Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa
O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Negação de serviço**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Negação de serviço (DOS)



Procedimento

1. Abra o incidente de segurança para esta ocorrência de negação de serviço ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Negação de serviço**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tarefas de resposta no modelo de negação de serviço

Tarefa de resposta	Ação	Resultados
A meta é crítica para os negócios?	Determine se o destino deste ataque do DOS é essencial para os negócios. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Definir prioridade como crítica** será executada. Se você selecionar **Não**, **uma vulnerabilidade está sendo explorada?** tarefa é executada.
Definir prioridade como crítica	Nenhuma ação necessária.	A **Prioridade** do incidente de segurança é alterada automaticamente para **Crítica**e a **resposta Uma vulnerabilidade está sendo explorada?** tarefa é executada.
Há uma vulnerabilidade sendo explorada?	Determine se este ataque do DOS explora uma vulnerabilidade de software.	Se você selecionar **Sim**, a tarefa **de solicitação de patch de emergência** será executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
	Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Não**, o **invasor interno?** tarefa é executada.
Solicitação de patch de emergência	Emita uma solicitação de patch de emergência para os sistemas que estão sendo atacados. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Invasor interno?	Determine se a origem deste ataque do DOS é interna à sua organização. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Isolar host(es) de ataque** será executada. Se você selecionar **Não**, o **provedor de proteção Notify DOS e/ou a tarefa do ISP** serão executados.
Isolar os hosts de ataque	Execute as etapas necessárias para isolar os hosts internos responsáveis pelo ataque. Atualize o campo **Estado** na tarefa conforme apropriado.	Depois de concluir esta etapa, a tarefa **Validar a integridade do sistema dos sistemas atacados** será executada.
Notificar provedor de proteção do DOS e/ou ISP	Execute as etapas necessárias para entrar em contato com seu provedor de proteção contra negação de serviço e/ou seu provedor de serviços de Internet para notificá-los sobre o ataque. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Validar a integridade do sistema dos sistemas atacados	Execute as etapas necessárias para avaliar e validar a integridade dos computadores atacados. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Revisar proteções do DOS	Realize uma revisão das proteções e procedimentos existentes do DOS. Faça as alterações necessárias. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**. A tarefa de **reunião de Lições aprendidas** é executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Reunião de lições aprendidas	Realize uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de negação de serviço. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, o fluxo será encerrado.

Modelo de fluxo de trabalho de equipamento perdido de incidente de segurança

O Incidente de segurança - Equipamento perdido - Modelo permite que você execute uma série de tarefas projetadas para lidar com equipamentos perdidos.

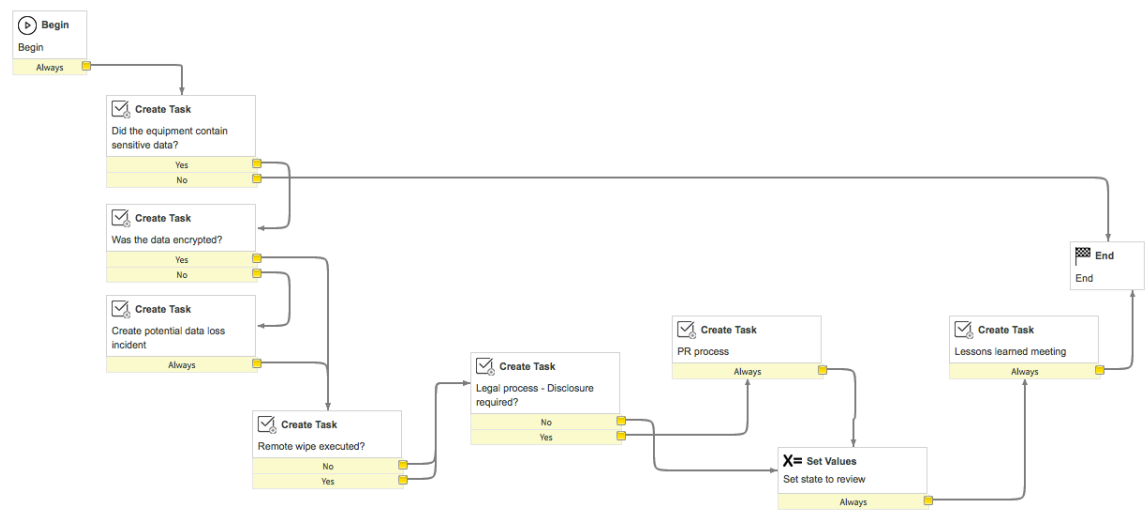
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Perda de equipamento**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Perda de equipamento



Procedimento

1. Abra o incidente de segurança para a perda de equipamento ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Perda de equipamento**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de resposta no modelo de equipamento perdido

Tarefa de resposta	Ação	Resultados
O equipamento continha dados confidenciais?	Determine se o equipamento associado a este incidente de segurança continha informações confidenciais. Na tarefa, selecione **Sim** ou **Não** em **Resultado**, conforme apropriado.	Se você selecionar **Sim**, **os dados foram criptografados?** tarefa é executada. Se você selecionar **Não**, o fluxo será encerrado.
Os dados foram criptografados?	Determine se os dados confidenciais no dispositivo perdido foram criptografados. Na tarefa, selecione **Sim** ou **Não** em **Resultado**, conforme apropriado.	Se você selecionar **Sim**, o **apagamento remoto foi criado?** tarefa de resposta é executada. Se você selecionar **Não**, a tarefa de resposta do **incidente Criar possível perda de dados**será executada.
Criar possível incidente de perda de dados	Execute as etapas necessárias para criar um possível incidente de perda de dados. Depois de terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	O **apagamento remoto foi criado?** tarefa de resposta é executada.
Apagamento remoto criado?	Execute as etapas necessárias para executar um apagamento remoto do equipamento perdido. Na tarefa, selecione **Sim** ou **Não** em **Resultado**, conforme apropriado.	A tarefa de **Processo jurídico - Divulgação necessária** é executada.
Processo jurídico - divulgação necessária?	Execute as etapas para atender aos requisitos jurídicos desta análise. Selecione **Sim** se uma divulgação jurídica for necessária, **Não**se não for.	A tarefa de **reunião de Lições aprendidas** é executada.
Processo de RC	Execute as etapas necessárias para atender aos requisitos de RC desta análise. Depois de terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	A tarefa **Definir estado como revisão** foi executada.
Definir estado como revisão	Nenhuma ação é necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Reunião de lições aprendidas	Realize uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de perda de equipamento. Depois de terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	O fluxo termina.

Modelo de fluxo de trabalho de software malicioso de incidente de segurança

O Incidente de segurança - Software malicioso - Modelo permite que você execute uma série de tarefas projetadas para lidar com software malicioso em sua rede.

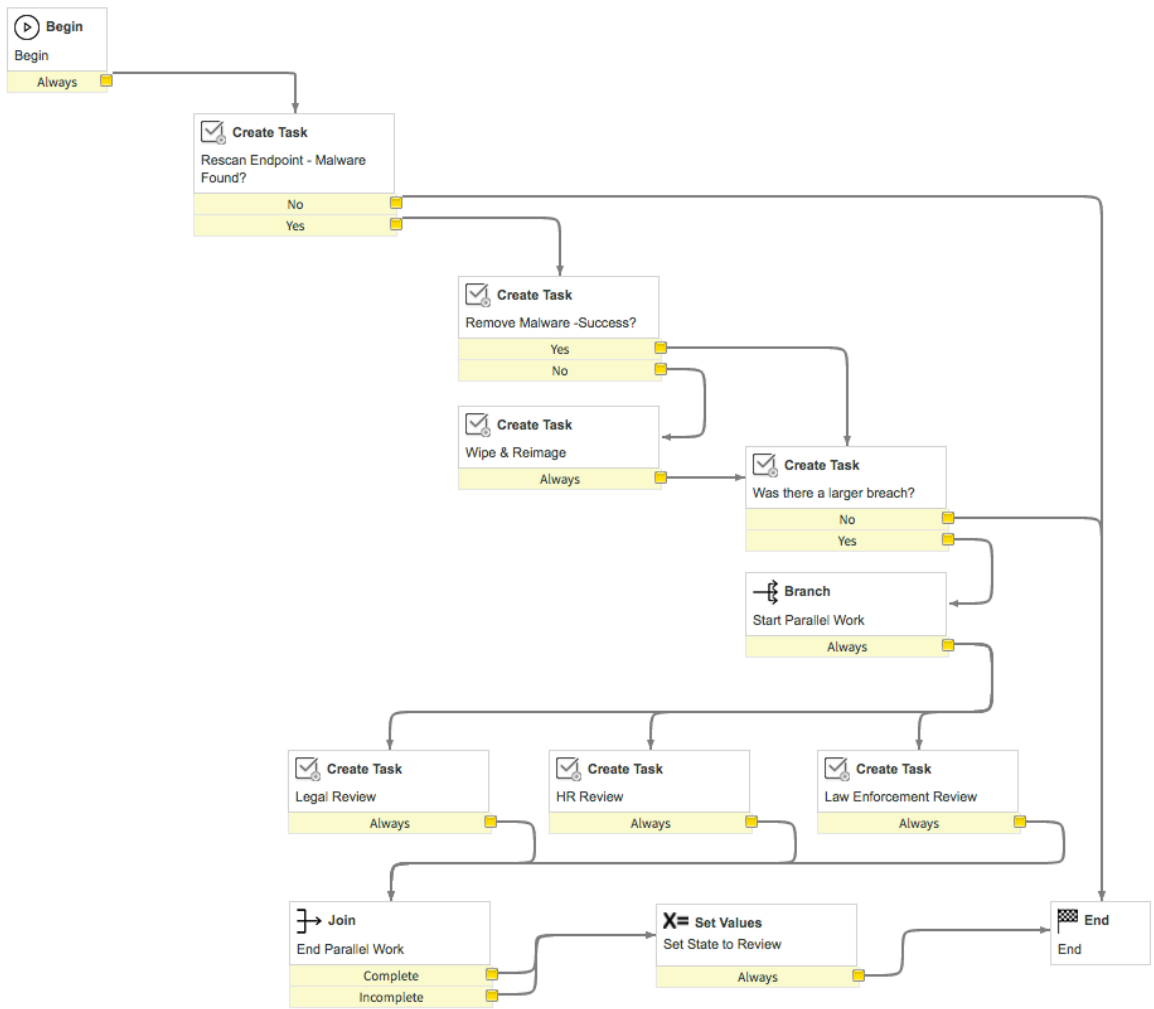
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Software mal**-intencionado. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Software malicioso



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o incidente de segurança para este possível ataque ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Atividade de código malicioso**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no modelo de software malicioso

Tarefa de resposta	Ação	Resultados
Endpoint de verificação - Malware encontrado?	Depois de executar uma verificação, determine se o malware foi encontrado. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a **mensagem Remover malware - Sucesso?** tarefa é executada. Se você selecionar **Não**, o fluxo será encerrado.
Remover malware - Sucesso?	Determine se o malware foi removido com sucesso. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a **mensagem Houve uma violação maior?** tarefa é executada. Se você selecionar **Não**, a tarefa de **limpeza e recriação** de imagens será executada.
Limpar e recriar imagem	Se você não removeu com sucesso o malware encontrado, esta tarefa instrui você a executar um apagamento e recriação de imagens nos computadores infectados com o malware.	Depois que a tarefa for concluída, a tarefa **Definir estado como revisão** será executada.
Houve uma violação maior?	Determine se a violação causada pelo software mal-intencionado é maior do que se acredita. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as seguintes tarefas serão executadas em paralelo: ○ Revisão jurídica ○ Revisão de RH ○ Revisão da aplicação da lei Se você selecionar **Não**, o fluxo será encerrado.
Revisão jurídica Revisão de RH	Execute as etapas necessárias para que cada um desses departamentos revise o processo que você seguiu para erradicar o software mal-intencionado.	Quando as tarefas forem concluídas, a tarefa **Definir estado como revisão** será executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Revisão da aplicação da lei		
Definir Estado como Revisar	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**e o fluxo termina.

Modelo de fluxo de trabalho de phishing de incidente de segurança

O Incidente de segurança - Phishing - Modelo permite que você execute uma série de tarefas projetadas para lidar com e-mails de phishing na sua rede.

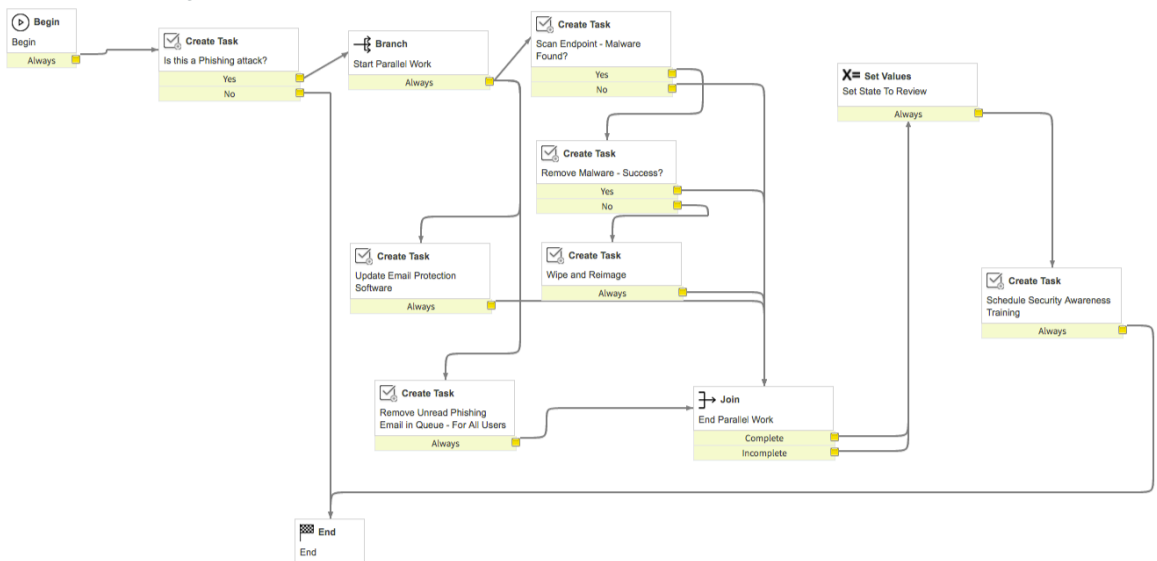
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Spear Phishing**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Spear Phishing



Procedimento

1. Abra o incidente de segurança para este possível ataque de phishing ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Spear Phishing**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de resposta no modelo de Spear Phishing

Tarefa de resposta	Ação	Resultados
Isso é um ataque de phishing?	Determine se este é um ataque de phishing. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as seguintes tarefas serão executadas em paralelo: ◦ Endpoint de verificação - Malware encontrado? ◦ Atualizar software de proteção de e-mail ◦ Remover e-mail de phishing não lido da fila - Para todos os usuários Se você selecionar **Não**, o fluxo será encerrado.
Endpoint de verificação - Malware encontrado?	Depois de executar uma verificação, determine se o malware foi encontrado. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a **mensagem Remover malware - Sucesso?** tarefa é executada. Se você selecionar **Não**, a tarefa **Definir estado como revisão** será executada.
Remover malware - Sucesso?	Determine se o malware foi removido com sucesso. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Definir estado como revisão** será executada. Se você selecionar **Não**, a tarefa **de limpeza e recriação de imagem** será executada.
Limpar e recriar imagem	Se você não removeu com sucesso o malware encontrado, esta tarefa instrui você a executar um apagamento e recriação de imagens nos computadores infectados com o malware.	Depois que a tarefa for concluída, a tarefa **Definir estado como revisão** será executada.
Atualizar software de proteção de e-mail	Se for determinado que se trata de um ataque de phishing, você será solicitado a atualizar o software de proteção de e-mail de acordo.	Quando a tarefa for concluída, a tarefa **Definir estado como revisão** será executada.
Remover e-mail de phishing não lido da fila - Para todos os usuários	Execute as etapas necessárias para remover o e-mail de phishing ainda na fila para todos os usuários.	Quando a tarefa for concluída, a tarefa **Definir estado como revisão** será executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Definir Estado como Revisar	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**. A tarefa **Programar treinamento de conscientização de segurança** é executada.
Programar treinamento de conscientização de segurança	Programe treinamento para aumentar a conscientização de segurança de seus funcionários. Atualize o campo **Estado** na tarefa conforme apropriado.	Quando a tarefa é concluída, o fluxo termina.

Modelo de fluxo de trabalho de violação de política de incidente de segurança

O modelo Incidente de segurança - Violação de política - permite que você execute uma série de tarefas projetadas para lidar com violações de política de segurança.

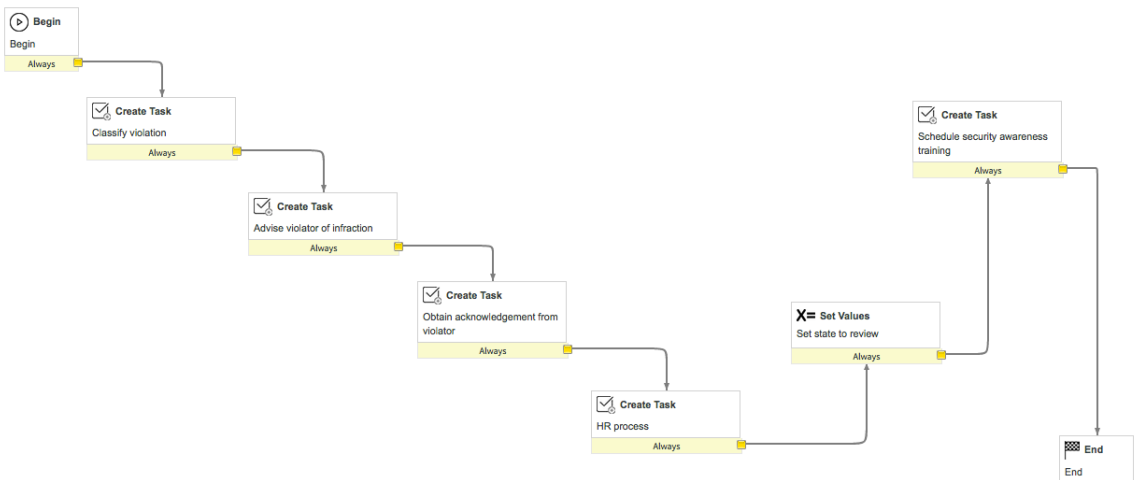
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Violação de política**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Violação de política



Procedimento

1. Abra o incidente de segurança para a violação de política ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Violação de política**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no modelo de violação de política

Tarefa de resposta	Ação	Resultados
Classificar violação	Classifique como esta infração viola as políticas de segurança da sua organização. Atualize o campo **Estado** na tarefa depois de concluí-la.	A tarefa **Aconselhar o infrator sobre a resposta de infração** é executada.
Avisar infrator sobre infração	Comunique a natureza da infração ao violador. Atualize o campo **Estado** na tarefa depois de comunicá-lo.	A tarefa de resposta **Obter confirmação do violador** foi executada.
Obter confirmação do violador	Obter uma confirmação do violador da infração. Atualize o campo **Estado** na tarefa conforme apropriado.	A tarefa de resposta do **processo de RH** é executada.
Processo de RH	Comunique todas as informações necessárias sobre esta violação ao RH. Atualize o campo **Estado** na tarefa conforme apropriado.	A tarefa **Definir estado para revisar a** resposta é executada.
Definir estado como revisão	Nenhuma ação é necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**.
Programar treinamento de conscientização de segurança	Realize um treinamento de conscientização de segurança para educar a equipe sobre como evitar violações de segurança semelhantes no futuro. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, o fluxo será encerrado.

Tradução automática

Modelo de fluxo de trabalho de reconhecimento de incidente de segurança

O reconhecimento geralmente é uma etapa preliminar em direção a um novo ataque que busca explorar um dispositivo ou sistema. O Incidente de segurança - Reconhecimento - Modelo permite que você execute uma série de tarefas projetadas para lidar com o reconhecimento em sua rede.

Antes de Iniciar

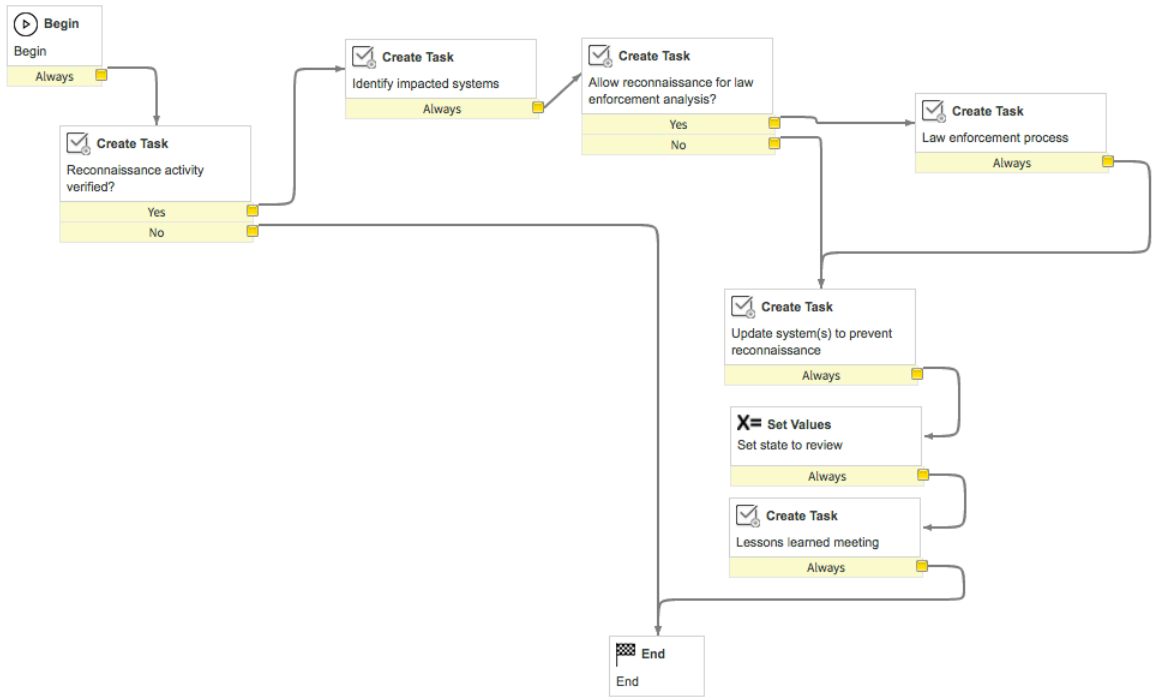
Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Atividade de reconhecimento**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade de reconhecimento



Procedimento

1. Abra o incidente de segurança para este possível ataque ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Atividade de reconhecimento**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no modelo de reconhecimento

Tarefa de resposta	Ação	Resultados
Atividade de reconhecimento verificada?	Determine se algum reconhecimento observado foi verificado. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Identificar sistemas afetados** será executada. Se você selecionar **Não**, o fluxo será encerrado.
Identificar sistemas afetados	Determine os sistemas afetados pelo reconhecimento.	Quando esta tarefa estiver concluída, a **mensagem Permitir reconhecimento para análise de aplicação da lei?** tarefa é executada.
Permitir reconhecimento para análise de aplicação da lei?	Determine se você deseja que o reconhecimento seja analisado pelas agências de segurança pública. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa do **processo de aplicação da lei** será executada. Se você selecionar **Não**, a tarefa **Atualizar sistema(s) para impedir o reconhecimento** será executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Processo de aplicação da lei	Execute o processo de aplicação da lei conforme definido pela sua empresa.	Quando esta tarefa estiver concluída, a tarefa de **atualização de sistema(s) para impedir o reconhecimento** será executada.
Atualizar sistema(s) para impedir reconhecimento	Execute as etapas necessárias para atualizar os sistemas afetados pelo reconhecimento.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**e a tarefa de **reunião de Lições aprendidas** é executada.
Reunião de lições aprendidas	Realize uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de reconhecimento. Atualize o campo **Estado** na tarefa conforme apropriado.	Quando esta tarefa for concluída, o fluxo será encerrado.

Modelo de fluxo de trabalho de servidor ou serviço invasor de incidente de segurança

O Incidente de segurança - Servidor ou serviço invasor - permite que você execute uma série de tarefas projetadas para lidar com atividades de servidores ou serviços invasores que afetam sua rede.

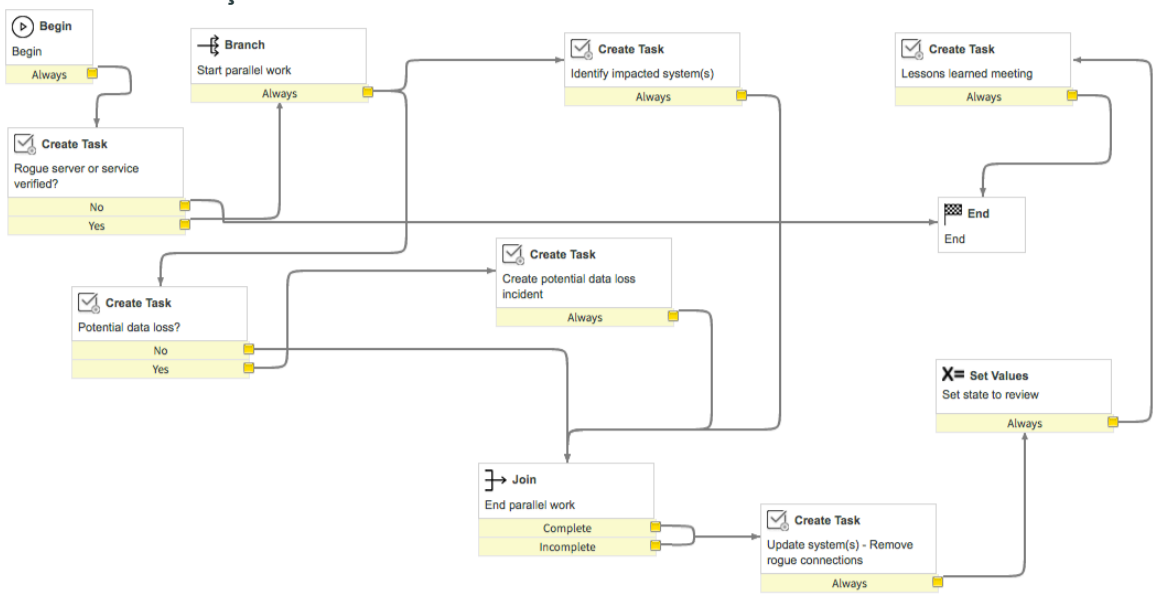
Antes de Iniciar
Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa
O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Servidor ou serviço invasor**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Servidor ou serviço invasor



Procedimento

1. Abra o incidente de segurança para este possível ataque ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Servidor invasor ou atividade de serviço**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no servidor invasor ou no modelo de serviço

Tarefa de resposta	Ação	Resultados
Servidor ou serviço invasor verificado?	Determine se uma conexão com um servidor ou serviço invasor foi verificada em sua rede. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as duas tarefas a seguir serão executadas em paralelo: ○ **Identificar sistema(s) afetado(s)** ○ **Possível perda de dados?** Se você selecionar **Não**, o fluxo será encerrado.
Identificar sistema(s) afetado(s)	Determine os sistemas afetados pelo contato com o servidor ou serviço invasor.	Quando esta tarefa estiver concluída, a tarefa **Atualizar sistema(s) - Remover conexões** não autorizadas será executada.
Possível perda de dados?	Determine se a conexão com o servidor ou serviço invasor causou possível perda de dados. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Criar possível incidente de perda de dados** será executada. Se você selecionar **Não**, a tarefa **Atualizar sistema(s) - Remover conexões** não autorizadas será executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Criar possível incidente de perda de dados	Execute as etapas necessárias para criar um incidente de segurança para a possível perda de dados.	Quando esta tarefa estiver concluída, a tarefa **Atualizar sistema(s) - Remover conexões** não autorizadas será executada.
Atualizar sistema(s) - Remover conexões invasoras	Execute as etapas necessárias para remover as conexões não autorizadas.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**e a tarefa de **reunião de Lições aprendidas** é executada.
Reunião de lições aprendidas	Realize uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este servidor invasor ou incidente de serviço. Atualize o campo **Estado** na tarefa conforme apropriado.	Quando esta tarefa for concluída, o fluxo será encerrado.

Modelo de fluxo de trabalho de spam de incidente de segurança

O Incidente de segurança - Spam - Modelo permite que você execute uma série de tarefas projetadas para lidar com spam de e-mail em sua rede.

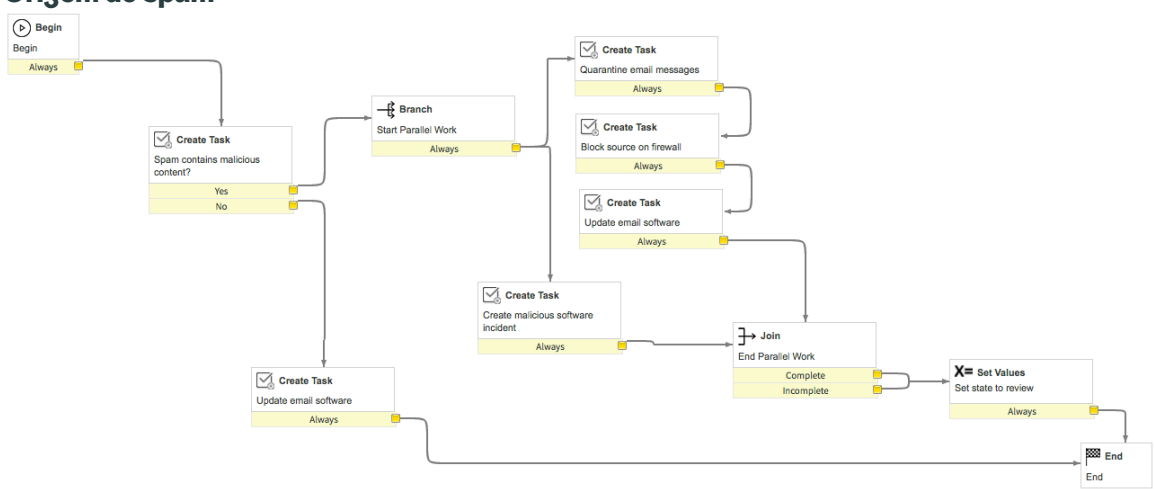
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida ou alterada para **Origem de spam**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Origem do spam



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o incidente de segurança para o qual você deseja lidar com spam de e-mail ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Origem de spam**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no modelo de spam

Tarefa de resposta	Ação	Resultados
O spam contém conteúdo malicioso?	Determine se o spam contém software mal-intencionado. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionou **Sim**, as seguintes tarefas de resposta serão executadas: ○ **Mensagem de e-mail de quarentena** ○ **Criar incidente de software malicioso** Se você selecionou **Não**, a **atualização do software de e-mail** será executada.
Criar incidente de software malicioso	Execute as etapas para criar um incidente de segurança, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, essa tarefa de resposta aguardará até que as próximas três tarefas de resposta sejam concluídas. O estado do incidente de segurança muda para **Revisão**.
Mensagem de e-mail de quarentena	Execute as etapas para colocar o spam em quarentena, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Bloquear origem no firewall	Execute as etapas para bloquear o endereço de e-mail no firewall, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Atualizar software de e-mail	Adicione o endereço de e-mail à sua lista de bloqueios, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada. **Nota:** Esta tarefa de resposta também será executada se você respondeu **Não** para a pergunta O **spam contém conteúdo malicioso?** tarefa de resposta.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modelo de fluxo de trabalho de acesso não autorizado de incidente de segurança

O Incidente de segurança - Acesso não autorizado - Modelo permite que você execute uma série de tarefas projetadas para lidar com o acesso não autorizado à sua rede.

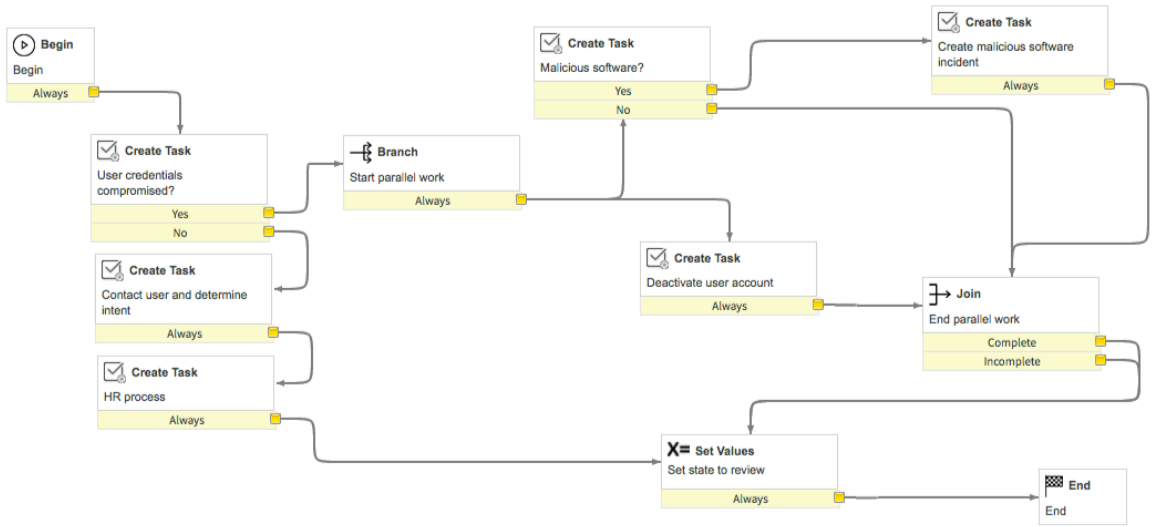
Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como **Acesso não autorizado**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Acesso não autorizado



Procedimento

1. Abra o incidente de segurança para este possível ataque ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Acesso não autorizado**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no modelo de acesso não autorizado

Tarefa de resposta	Ação	Resultados
Credenciais de usuário comprometidas?	Determine se alguma credencial de usuário foi comprometida. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as duas tarefas a seguir serão executadas em paralelo: ○ **Software malicioso?** ○ **Desativar conta do usuário** Se você selecionar **Não**, a tarefa **Entrar em contato com o usuário e determinar a intenção** será executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Software malicioso?	Determine se o acesso não autorizado resultou na introdução de software mal-intencionado. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Criar incidente de software mal-intencionado** será executada. Se você selecionar **Não**, a tarefa **Definir estado para revisão** será executada.
Criar incidente de software malicioso	Execute as etapas necessárias para criar um incidente de segurança para o acesso não autorizado.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Desativar conta do usuário	Execute as etapas necessárias para desativar a conta do usuário comprometida.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Entre em contato com o usuário e determine a intenção	Execute as etapas necessárias para entrar em contato com o usuário responsável pelo acesso não autorizado e determinar o motivo da tentativa de acesso.	Quando esta tarefa é concluída, a tarefa de **processo de RH** é executada.
Processo de RH	Execute as etapas necessárias para entrar em contato com os recursos humanos para implementar a ação disciplinar, se necessário.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**e o fluxo termina.

Modelo de fluxo de trabalho de Desfiguração de Web/BBS de incidente de segurança

O Incidente de segurança - Web/Destruição de BBS - Modelo permite que você execute uma série de tarefas projetadas para lidar com o vandalismo direcionado contra um dos BBS ou sites da Web da sua organização.

Antes de Iniciar

Função necessária: sn_si.write

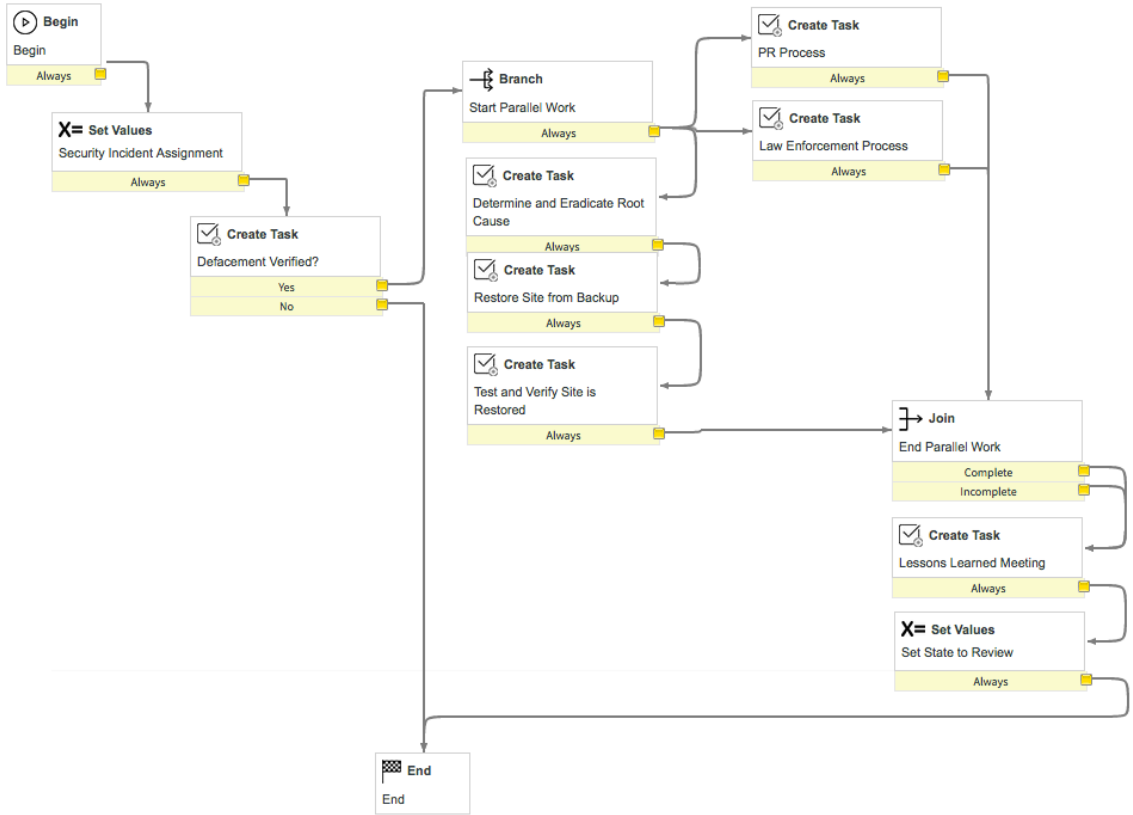
Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho é acionado quando a **Categoria** em um incidente de segurança é definida como Desfiguração da **Web/BBS**. Esta ação faz com que uma tarefa de resposta seja criada para a primeira atividade no fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Destruição da web/BBS



Procedimento

1. Abra o incidente de segurança para esta ocorrência de desfiguração da Web ou de BBS ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione Desfiguração de **Web/BBS**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tarefas de resposta no modelo de desfiguração da Web/BBS

Tarefa de resposta	Ação	Resultados
Atribuição de incidente de segurança	Crie um incidente de segurança para cada incidente relatado de desfiguração de site ou BBS.	A próxima tarefa de resposta é executada.
Desfiguração verificada?	Determine se o site ou o BBS foram de fato desfigurados. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as seguintes tarefas de resposta serão executadas: ○ **Processo de RC** ○ **Processo de aplicação da lei** ○ **Determinar e erradicar a causa raiz** Se você selecionar **Não**, o fluxo será encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Processo de RC	Execute as etapas necessárias para notificar o público de que o site ou o BBS foi desfigurado. Quando terminar o processo de RC, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	A tarefa de **reunião de Lições aprendidas** é executada.
Processo de aplicação da lei	Execute as etapas necessárias para envolver as agências de aplicação da lei apropriadas em relação ao ataque. Ao terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	A tarefa de **reunião de Lições aprendidas** é executada.
Determinar e erradicar a causa raiz	Execute as etapas necessárias para descobrir e eliminar a causa raiz da desfiguração. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Restaurar site a partir do backup	Execute as etapas necessárias para fazer backup e restaurar o site ou o BBS. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Testar e verificar se o site foi restaurado	Verifique se o site foi restaurado. Ao terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	A tarefa de **reunião de Lições aprendidas** é executada.
Reunião de lições aprendidas	Realize uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de desfiguração de site/BBS. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a tarefa **Definir estado para revisão** será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**. O fluxo termina.

Modelos de fluxo do Security Incident Response

O sistema base Security Incident Response inclui uma série de modelos de fluxo de trabalho criados usando o Flow Designer que funcionam com registros de incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Somente usuários com a função sn_sec_cmn.admin podem adicionar ou editar modelos de fluxo de trabalho do Security Operations, e o usuário com a função sn_si_admin é necessário para atualizar os modelos de fluxo.

Informações importantes de ativação

Os modelos de fluxo de trabalho criados com o Editor de fluxo de trabalho e os modelos de fluxo criados com o Flow Designer são desativados por padrão. Os modelos de fluxo de trabalho podem ser ativados usando gatilhos de fluxode trabalho. Os modelos do Flow Designer podem ser ativados usando o Flow Designer.

Nota:
Você deve ter cuidado para não ativar o mesmo modelo de cada tipo. Por exemplo, evite ativar o Modelo de fluxo de trabalho de Exposição de dados confidenciais de incidente de segurança e o Modelo de fluxo de exposição de dados confidenciais de incidente de segurança. Isso pode causar a execução do fluxo de trabalho e do fluxo e a criação de informações duplicadas.

Modelo de fluxo de exposição de dados confidenciais de incidente de segurança

O Incidente de segurança - Exposição de dados confidenciais - Modelo permite que você execute uma série de tarefas projetadas para lidar com a exposição de dados confidenciais.

Antes de Iniciar
Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo é acionado quando a **Categoria** em um incidente de segurança é definida ou alterada para **Exposição de dados de identidade pessoal confidencial**.

Procedimento

1. Abra o incidente de segurança para o qual você deseja lidar com a exposição de dados confidenciais ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Exposição de dados de identidade pessoal confidencial**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja executada ou o fluxo seja encerrado.

Tarefas de resposta no modelo de exposição de dados confidenciais

Tarefa de resposta	Descrição	Resultados
Os dados são confidenciais?	Determine se os dados associados a este incidente de segurança são confidenciais. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionou **Sim**, a próxima tarefa de resposta será executada. Se você selecionou **Não**, o fluxo será encerrado.
Determinar a causa raiz e impedir a saída	Determine a causa raiz do ataque e adicione filtragem de saída para parar a exfiltração, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Descrição	Resultados
Eliminar exposição relacionada à causa raiz	Com base na causa raiz, execute as etapas para eliminar a exposição, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Artefatos residuais de quarentena	Execute as etapas para colocar em quarentena quaisquer artefatos residuais, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Processo jurídico	Execute as etapas para atender aos requisitos jurídicos desta análise, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Processo de RC	Execute as etapas para atender aos requisitos de RC desta análise, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**.
Reunião de lições aprendidas	Realize uma reunião de lições aprendidas para fazer a triagem do trabalho realizado nesses dados confidenciais, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, o incidente de segurança permanecerá no estado **Revisar** até que você o feche.

Modelo de fluxo de negação de serviço de incidente de segurança

O Incidente de segurança - Negação de serviço - Modelo permite que você execute uma série de tarefas projetadas para lidar com ataques de negação de serviço (DOS).

Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo é acionado quando a **Categoria** em um incidente de segurança é definida como **Negação de serviço**.

Procedimento

1. Abra o incidente de segurança para esta ocorrência de negação de serviço ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Negação de serviço**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo de trabalho seja encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de resposta no modelo de negação de serviço

Tarefa de resposta	Ação	Resultados
A meta é crítica para os negócios?	Determine se o destino deste ataque do DOS é essencial para os negócios. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Definir prioridade como crítica** será executada. Se você selecionar **Não**, **uma vulnerabilidade está sendo explorada?** tarefa é executada.
Definir prioridade como crítica	Nenhuma ação necessária.	A **Prioridade** do incidente de segurança é alterada automaticamente para **Crítica**e a **resposta Uma vulnerabilidade está sendo explorada?** tarefa é executada.
Há uma vulnerabilidade sendo explorada?	Determine se este ataque do DOS explora uma vulnerabilidade de software. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **de solicitação de patch de emergência** será executada. Se você selecionar **Não**, o **invasor interno?** tarefa é executada.
Solicitação de patch de emergência	Emita uma solicitação de patch de emergência para os sistemas que estão sendo atacados. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Invasor interno?	Determine se a origem deste ataque do DOS é interna à sua organização. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Isolar host(es) de ataque** será executada. Se você selecionar **Não**, o **provedor de proteção Notify DOS e/ou a tarefa do ISP** serão executados.
Isolar os hosts de ataque	Execute as etapas necessárias para isolar os hosts internos responsáveis pelo ataque. Atualize o campo **Estado** na tarefa conforme apropriado.	Depois de concluir esta etapa, a tarefa **Validar a integridade do sistema dos sistemas atacados** será executada.
Notificar provedor de proteção do DOS e/ou ISP	Execute as etapas necessárias para entrar em contato com seu provedor de proteção contra negação de serviço e/ou seu provedor de serviços de Internet para notificá-los sobre o ataque. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Validar a integridade do sistema dos sistemas atacados	Execute as etapas necessárias para avaliar e validar a integridade dos computadores atacados. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Revisar proteções do DOS	Realize uma revisão das proteções e procedimentos existentes do DOS. Faça as alterações necessárias. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**. A tarefa de **reunião de Lições aprendidas** é executada.
Reunião de lições aprendidas	Realize uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de negação de serviço. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, o fluxo será encerrado.

Modelo de fluxo de equipamento perdido de incidente de segurança

O Incidente de segurança - Equipamento perdido - Modelo permite que você execute uma série de tarefas projetadas para lidar com equipamentos perdidos.

Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo é acionado quando a **Categoria** em um incidente de segurança é definida como **Perda de equipamento**.

Procedimento

1. Abra o incidente de segurança para esta ocorrência de negação de serviço ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Perda de equipamento**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de resposta no modelo de equipamento perdido

Tarefa de resposta	Ação	Resultados
O equipamento continha dados confidenciais?	Determine se o equipamento associado a este incidente de segurança continha informações confidenciais. Na tarefa, selecione **Sim** ou **Não** em **Resultado**, conforme apropriado.	Se você selecionar **Sim**, **os dados foram criptografados?** tarefa é executada. Se você selecionar **Não**, o fluxo será encerrado.
Os dados foram criptografados?	Determine se os dados confidenciais no dispositivo perdido foram criptografados. Na tarefa, selecione **Sim** ou **Não** em **Resultado**, conforme apropriado.	Se você selecionar **Sim**, o **apagamento remoto foi criado?** tarefa de resposta é executada. Se você selecionar **Não**, a tarefa de resposta do **incidente Criar possível perda de dados**será executada.
Criar possível incidente de perda de dados	Execute as etapas necessárias para criar um possível incidente de perda de dados. Depois de terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	O **apagamento remoto foi criado?** tarefa de resposta é executada.
Apagamento remoto criado?	Execute as etapas necessárias para executar um apagamento remoto do equipamento perdido. Na tarefa, selecione **Sim** ou **Não** em **Resultado**, conforme apropriado.	A tarefa de **Processo jurídico - Divulgação necessária** é executada.
Processo jurídico - divulgação necessária?	Execute as etapas para atender aos requisitos jurídicos desta análise. Selecione **Sim** se uma divulgação jurídica for necessária, **Não**se não for.	A tarefa de **reunião de Lições aprendidas** é executada.
Processo de RC	Execute as etapas necessárias para atender aos requisitos de RC desta análise. Depois de terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	A tarefa **Definir estado como revisão** foi executada.
Definir estado como revisão	Nenhuma ação é necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Reunião de lições aprendidas	Realize uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de perda de equipamento. Depois de terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	O fluxo termina.

Modelo de fluxo de Software mal-intencionado de incidente de segurança

O Incidente de segurança - Software malicioso - Modelo permite que você execute uma série de tarefas projetadas para lidar com software malicioso em sua rede.

Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo é acionado quando a **Categoria** em um incidente de segurança é definida como **Atividade de código malicioso**.

Procedimento

1. Abra o incidente de segurança para este possível ataque ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Atividade de código malicioso**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tarefas de resposta no modelo de software malicioso

Tarefa de resposta	Ação	Resultados
Endpoint de verificação - Malware encontrado?	Depois de executar uma verificação, determine se o malware foi encontrado. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a **mensagem Remover malware - Sucesso?** tarefa é executada. Se você selecionar **Não**, o fluxo será encerrado.
Remover malware - Sucesso?	Determine se o malware foi removido com sucesso. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a **mensagem Houve uma violação maior?** tarefa é executada. Se você selecionar **Não**, a tarefa de **limpeza e recriação** de imagens será executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Limpar e recriar imagem	Se você não removeu com sucesso o malware encontrado, esta tarefa instrui você a executar um apagamento e recriação de imagens nos computadores infectados com o malware.	Depois que a tarefa for concluída, a tarefa **Definir estado como revisão** será executada.
Houve uma violação maior?	Determine se a violação causada pelo software mal-intencionado é maior do que se acredita. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as seguintes tarefas serão executadas em paralelo: ○ Revisão jurídica ○ Revisão de RH ○ Revisão da aplicação da lei Se você selecionar **Não**, o fluxo será encerrado.
Revisão jurídica Revisão de RH Revisão da aplicação da lei	Execute as etapas necessárias para que cada um desses departamentos revise o processo que você seguiu para erradicar o software mal-intencionado.	Quando as tarefas forem concluídas, a tarefa **Definir estado como revisão** será executada.
Definir Estado como Revisar	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**e o fluxo termina.

Modelo de fluxo de phishing de incidente de segurança

O Incidente de segurança - Phishing - Modelo permite que você execute uma série de tarefas projetadas para lidar com e-mails de phishing na sua rede.

Antes de Iniciar
Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo é acionado quando a **Categoria** em um incidente de segurança é definida como **Spear Phishing**.

Procedimento

1. Abra o incidente de segurança para este possível ataque de phishing ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Spear Phishing**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de resposta no modelo de Spear Phishing

Tarefa de resposta	Ação	Resultados
Isso é um ataque de phishing?	Determine se este é um ataque de phishing. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as seguintes tarefas serão executadas em paralelo: ◦ Endpoint de verificação - Malware encontrado? ◦ Atualizar software de proteção de e-mail ◦ Remover e-mail de phishing não lido da fila - Para todos os usuários Se você selecionar **Não**, o fluxo será encerrado.
Endpoint de verificação - Malware encontrado?	Depois de executar uma verificação, determine se o malware foi encontrado. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a **mensagem Remover malware - Sucesso?** tarefa é executada. Se você selecionar **Não**, a tarefa **Definir estado como revisão** será executada.
Remover malware - Sucesso?	Determine se o malware foi removido com sucesso. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Definir estado como revisão** será executada. Se você selecionar **Não**, a tarefa **de limpeza e recriação de imagem** será executada.
Limpar e recriar imagem	Se você não removeu com sucesso o malware encontrado, esta tarefa instrui você a executar um apagamento e recriação de imagens nos computadores infectados com o malware.	Depois que a tarefa for concluída, a tarefa **Definir estado como revisão** será executada.
Atualizar software de proteção de e-mail	Se for determinado que se trata de um ataque de phishing, você será solicitado a atualizar o software de proteção de e-mail de acordo.	Quando a tarefa for concluída, a tarefa **Definir estado como revisão** será executada.
Remover e-mail de phishing não lido da fila - Para todos os usuários	Execute as etapas necessárias para remover o e-mail de phishing ainda na fila para todos os usuários.	Quando a tarefa for concluída, a tarefa **Definir estado como revisão** será executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Definir Estado como Revisar	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**. A tarefa **Programar treinamento de conscientização de segurança** é executada.
Programar treinamento de conscientização de segurança	Programe treinamento para aumentar a conscientização de segurança de seus funcionários. Atualize o campo **Estado** na tarefa conforme apropriado.	Quando a tarefa é concluída, o fluxo termina.

Modelo de fluxo de violação de política de incidente de segurança

O modelo Incidente de segurança - Violação de política - permite que você execute uma série de tarefas projetadas para lidar com violações de política de segurança.

Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo é acionado quando a **Categoria** em um incidente de segurança é definida como **Violação de política**.

Procedimento

1. Abra o incidente de segurança para a violação de política ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Violação de política**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tarefas de resposta no modelo de violação de política

Tarefa de resposta	Ação	Resultados
Classificar violação	Classifique como esta infração viola as políticas de segurança da sua organização. Atualize o campo **Estado** na tarefa depois de concluí-la.	A tarefa **Aconselhar o infrator sobre a resposta de infração** é executada.
Avisar infrator sobre infração	Comunique a natureza da infração ao violador. Atualize o campo **Estado** na tarefa depois de comunicá-lo.	A tarefa de resposta **Obter confirmação do violador** foi executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Obter confirmação do violador	Obter uma confirmação do violador da infração. Atualize o campo **Estado** na tarefa conforme apropriado.	A tarefa de resposta do **processo de RH** é executada.
Processo de RH	Comunique todas as informações necessárias sobre esta violação ao RH. Atualize o campo **Estado** na tarefa conforme apropriado.	A tarefa **Definir estado para revisar a** resposta é executada.
Definir estado como revisão	Nenhuma ação é necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**.
Programar treinamento de conscientização de segurança	Realize um treinamento de conscientização de segurança para educar a equipe sobre como evitar violações de segurança semelhantes no futuro. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, o fluxo será encerrado.

Modelo de fluxo de reconhecimento de incidente de segurança

O reconhecimento geralmente é uma etapa preliminar em direção a um novo ataque que busca explorar um dispositivo ou sistema. O Incidente de segurança - Reconhecimento - Modelo permite que você execute uma série de tarefas projetadas para lidar com o reconhecimento em sua rede.

Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo é acionado quando a **Categoria** em um incidente de segurança é definida como **Atividade de reconhecimento**.

Procedimento

1. Abra o incidente de segurança para este possível ataque ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Atividade de reconhecimento**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tarefas de resposta no modelo de reconhecimento

Tarefa de resposta	Ação	Resultados
Atividade de reconhecimento verificada?	Determine se algum reconhecimento observado foi verificado.	Se você selecionar **Sim**, a tarefa **Identificar sistemas afetados** será executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
	Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Não**, o fluxo será encerrado.
Identificar sistemas afetados	Determine os sistemas afetados pelo reconhecimento.	Quando esta tarefa estiver concluída, a **mensagem Permitir reconhecimento para análise de aplicação da lei?** tarefa é executada.
Permitir reconhecimento para análise de aplicação da lei?	Determine se você deseja que o reconhecimento seja analisado pelas agências de segurança pública. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa do **processo de aplicação da lei** será executada. Se você selecionar **Não**, a tarefa **Atualizar sistema(s) para impedir o reconhecimento** será executada.
Processo de aplicação da lei	Execute o processo de aplicação da lei conforme definido pela sua empresa.	Quando esta tarefa estiver concluída, a tarefa de **atualização de sistema(s) para impedir o reconhecimento** será executada.
Atualizar sistema(s) para impedir reconhecimento	Execute as etapas necessárias para atualizar os sistemas afetados pelo reconhecimento.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**e a tarefa de **reunião de Lições aprendidas** é executada.
Reunião de lições aprendidas	Realize uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de reconhecimento. Atualize o campo **Estado** na tarefa conforme apropriado.	Quando esta tarefa for concluída, o fluxo será encerrado.

Tradução automática

Servidor invasor de incidente de segurança ou modelo de fluxo de serviço

O Incidente de segurança - Servidor ou serviço invasor - permite que você execute uma série de tarefas projetadas para lidar com atividades de servidores ou serviços invasores que afetam sua rede.

Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo é acionado quando a **Categoria** em um incidente de segurança é definida como **Servidor ou serviço invasor**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o incidente de segurança para este possível ataque ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Servidor invasor ou atividade de serviço**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tarefas de resposta no servidor invasor ou no modelo de serviço

Tarefa de resposta	Ação	Resultados
Servidor ou serviço invasor verificado?	Determine se uma conexão com um servidor ou serviço invasor foi verificada em sua rede. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as duas tarefas a seguir serão executadas em paralelo: ○ **Identificar sistema(s) afetado(s)** ○ **Possível perda de dados?** Se você selecionar **Não**, o fluxo será encerrado.
Identificar sistema(s) afetado(s)	Determine os sistemas afetados pelo contato com o servidor ou serviço invasor.	Quando esta tarefa estiver concluída, a tarefa **Atualizar sistema(s) - Remover conexões** não autorizadas será executada.
Possível perda de dados?	Determine se a conexão com o servidor ou serviço invasor causou possível perda de dados. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Criar possível incidente de perda de dados** será executada. Se você selecionar **Não**, a tarefa **Atualizar sistema(s) - Remover conexões** não autorizadas será executada.
Criar possível incidente de perda de dados	Execute as etapas necessárias para criar um incidente de segurança para a possível perda de dados.	Quando esta tarefa estiver concluída, a tarefa **Atualizar sistema(s) - Remover conexões** não autorizadas será executada.
Atualizar sistema(s) - Remover conexões invasoras	Execute as etapas necessárias para remover as conexões não autorizadas.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar** e a tarefa de **reunião de Lições aprendidas** é executada.
Reunião de lições aprendidas	Realize uma reunião de lições aprendidas para fazer a triagem do trabalho realizado	Quando esta tarefa for concluída, o fluxo será encerrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
	para este servidor invasor ou incidente de serviço. Atualize o campo **Estado** na tarefa conforme apropriado.	

Modelo de fluxo de spam de incidente de segurança

O Incidente de segurança - Spam - Modelo permite que você execute uma série de tarefas projetadas para lidar com spam de e-mail em sua rede.

Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo é acionado quando a **Categoria** em um incidente de segurança é definida ou alterada para **Origem de spam**.

Procedimento

1. Abra o incidente de segurança para o qual você deseja lidar com spam de e-mail ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Origem de spam**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tarefas de resposta no modelo de spam

Tarefa de resposta	Ação	Resultados
O spam contém conteúdo malicioso?	Determine se o spam contém software mal-intencionado. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionou **Sim**, as seguintes tarefas de resposta serão executadas: ○ **Mensagem de e-mail de quarentena** ○ **Criar incidente de software malicioso** Se você selecionou **Não**, a **atualização do software de e-mail** será executada.
Criar incidente de software malicioso	Execute as etapas para criar um incidente de segurança, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, essa tarefa de resposta aguardará até que as próximas três tarefas de resposta sejam concluídas. O estado do incidente de segurança muda para **Revisão**.
Mensagem de e-mail de quarentena	Execute as etapas para colocar o spam em quarentena, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Bloquear origem no firewall	Execute as etapas para bloquear o endereço de e-mail no firewall, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Atualizar software de e-mail	Adicione o endereço de e-mail à sua lista de bloqueios, atualizando o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada. **Nota:** Esta tarefa de resposta também será executada se você respondeu **Não** para a pergunta O **spam contém conteúdo malicioso?** tarefa de resposta.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**.

Modelo de fluxo de acesso não autorizado de incidente de segurança

O Incidente de segurança - Acesso não autorizado - Modelo permite que você execute uma série de tarefas projetadas para lidar com o acesso não autorizado à sua rede.

Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo é acionado quando a **Categoria** em um incidente de segurança é definida como **Acesso não autorizado**.

Procedimento

1. Abra o incidente de segurança para este possível ataque ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione **Acesso não autorizado**.
3. Salve o registro.
4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tarefas de resposta no modelo de acesso não autorizado

Tarefa de resposta	Ação	Resultados
Credenciais de usuário comprometidas?	Determine se alguma credencial de usuário foi comprometida. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as duas tarefas a seguir serão executadas em paralelo: ○ **Software malicioso?** ○ **Desativar conta do usuário**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
		Se você selecionar **Não**, a tarefa **Entrar em contato com o usuário e determinar a intenção** será executada.
Software malicioso?	Determine se o acesso não autorizado resultou na introdução de software mal-intencionado. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, a tarefa **Criar incidente de software mal-intencionado** será executada. Se você selecionar **Não**, a tarefa **Definir estado para revisão** será executada.
Criar incidente de software malicioso	Execute as etapas necessárias para criar um incidente de segurança para o acesso não autorizado.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Desativar conta do usuário	Execute as etapas necessárias para desativar a conta do usuário comprometida.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Entre em contato com o usuário e determine a intenção	Execute as etapas necessárias para entrar em contato com o usuário responsável pelo acesso não autorizado e determinar o motivo da tentativa de acesso.	Quando esta tarefa é concluída, a tarefa de **processo de RH** é executada.
Processo de RH	Execute as etapas necessárias para entrar em contato com os recursos humanos para implementar a ação disciplinar, se necessário.	Quando esta tarefa for concluída, a tarefa **Definir estado para revisão** será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**e o fluxo termina.

Modelo de fluxo de desfiguração de Web/BBS de incidente de segurança

O Incidente de segurança - Web/Destruição de BBS - Modelo permite que você execute uma série de tarefas projetadas para lidar com o vandalismo direcionado contra um dos BBS ou sites da Web da sua organização.

Antes de Iniciar

Função necessária: sn_si.write

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo é acionado quando a **Categoria** em um incidente de segurança é definida como Desfiguração da **Web/BBS**.

Procedimento

1. Abra o incidente de segurança para esta ocorrência de desfiguração da Web ou de BBS ou crie um novo incidente de segurança.
2. Em **Categoria**, selecione Desfiguração de **Web/BBS**.
3. Salve o registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Role para baixo e abra a lista relacionada **Tarefas de resposta**.
   A primeira de uma série de tarefas de resposta é exibida. Cada vez que o registro é salvo, sua resposta à tarefa anterior faz com que a próxima tarefa de resposta seja criada ou o fluxo seja encerrado.

Tarefas de resposta no modelo de desfiguração da Web/BBS

Tarefa de resposta	Ação	Resultados
Atribuição de incidente de segurança	Crie um incidente de segurança para cada incidente relatado de desfiguração de site ou BBS.	A próxima tarefa de resposta é executada.
Desfiguração verificada?	Determine se o site ou o BBS foram de fato desfigurados. Na tarefa, selecione **Sim** ou **Não** em **Resultado**.	Se você selecionar **Sim**, as seguintes tarefas de resposta serão executadas: ○ **Processo de RC** ○ **Processo de aplicação da lei** ○ **Determinar e erradicar a causa raiz** Se você selecionar **Não**, o fluxo será encerrado.
Processo de RC	Execute as etapas necessárias para notificar o público de que o site ou o BBS foi desfigurado. Quando terminar o processo de RC, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	A tarefa de **reunião de Lições aprendidas** é executada.
Processo de aplicação da lei	Execute as etapas necessárias para envolver as agências de aplicação da lei apropriadas em relação ao ataque. Ao terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	A tarefa de **reunião de Lições aprendidas** é executada.
Determinar e erradicar a causa raiz	Execute as etapas necessárias para descobrir e eliminar a causa raiz da desfiguração. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Restaurar site a partir do backup	Execute as etapas necessárias para fazer backup e restaurar o site ou o BBS. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterou o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a próxima tarefa de resposta será executada.
Testar e verificar se o site foi restaurado	Verifique se o site foi restaurado. Ao terminar, defina o estado da tarefa como **Concluído** ou **Incompleto**, conforme apropriado.	A tarefa de **reunião de Lições aprendidas** é executada.

Tradução automática

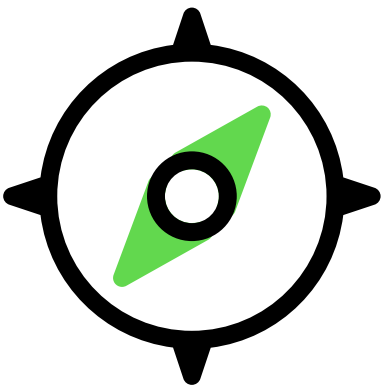
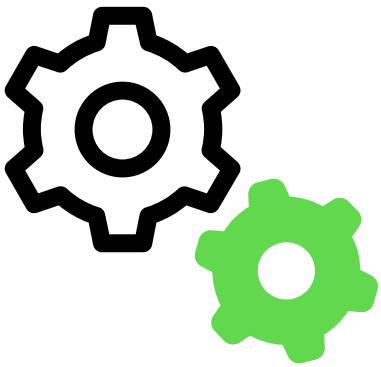
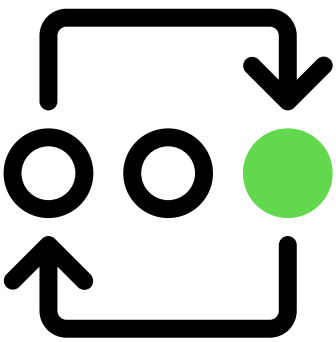
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de resposta	Ação	Resultados
Reunião de lições aprendidas	Realize uma reunião de lições aprendidas para fazer a triagem do trabalho realizado para este incidente de desfiguração de site/BBS. Atualize o campo **Estado** na tarefa conforme apropriado.	Se você alterar o estado da tarefa para **Encerrado concluído** ou **Cancelado**, a tarefa **Definir estado para revisão** será executada.
Definir estado como revisão	Nenhuma ação necessária.	O **Estado** do incidente de segurança é alterado automaticamente para **Revisar**. O fluxo termina.

Controle de posturas de segurança

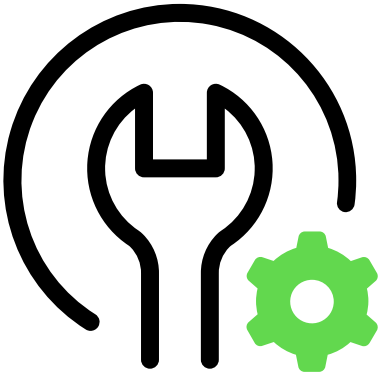
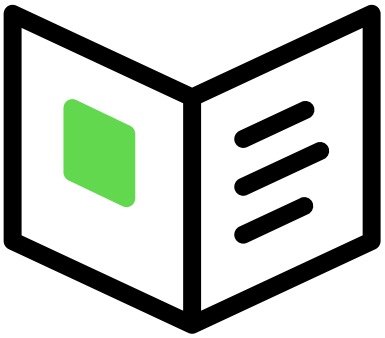
Obtenha visibilidade do inventário de ativos da sua empresa e da cobertura da ferramenta de segurança. Use as políticas fornecidas com o produto ou crie a sua própria para identificar ativos que não tenham as principais ferramentas de segurança, como proteção de endpoint, gestão de configuração e verificação de vulnerabilidades. Monitore ativos em busca de configurações de ferramentas de segurança específicas para seu ambiente e automatize o fluxo de trabalho de correção de lacunas de segurança na aplicação Configuration Compliance.

Iniciar

Explorar	Instalar	Integrar
		
Conheça os conceitos e recursos do Security Posture Control	Instalar aplicações do Security Posture Control	Integrar os Conectores do Service Graph com o Security Posture Control

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usar		Referência
		
Saiba como usar o espaço para pesquisar seus ativos e identificar lacunas de segurança		Obtenha detalhes sobre cenários que ajudam a identificar tipos específicos de lacunas de cobertura da ferramenta

Solucionar problemas e obter ajuda

- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Explorar o Controle de posturas de segurança

O Security Posture Control permite que as equipes de segurança cibernética tenham visibilidade de todo o inventário de ativos empresariais e determinem sua postura geral de segurança.

Os analistas de segurança obtêm informações sobre o desempenho das ferramentas de segurança e a cobertura de seus ativos com base no inventário de ativos e nos dados importados dos Service Graph Connectors. Os gerentes de vulnerabilidade podem usar informações do Security Posture Control (SPC) para priorizar a correção de combinações de alto risco para exposição e vulnerabilidades na Internet e criar políticas e informações personalizadas para monitorar a conformidade dos ativos com os padrões de configuração da ferramenta de segurança interna.

Controle de posturas de segurança consiste em duas aplicações que estão disponíveis por assinatura separada do ServiceNow® Store:

- Núcleo de postura de segurança
- Gestão de posturas de segurança para ativos- (ASPM)

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

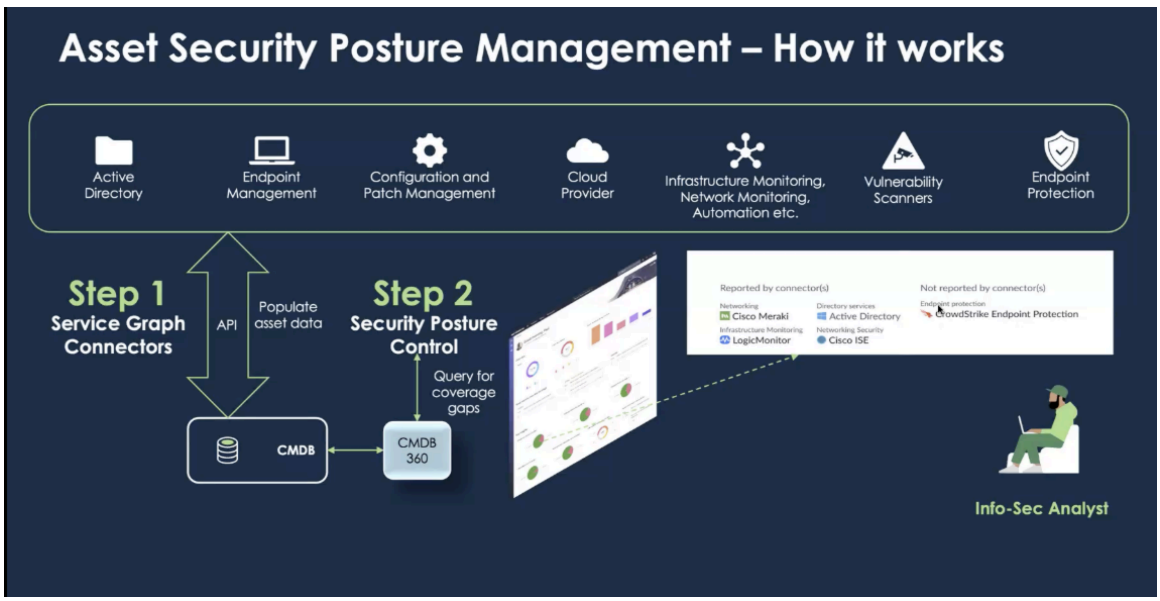
Com o produto SPC, as equipes de Info-Sec podem executar as seguintes tarefas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Exiba informações de postura de segurança para ativos no local e na nuvem.
- Monitore a conformidade dos ativos com os padrões de configuração da ferramenta de segurança interna, por exemplo, verificando se a versão mais recente de um produto de proteção de endpoint está sendo usada.
- Automatize o fluxo de trabalho de correção das lacunas de postura de segurança que você encontrar com a aplicação Configuration Compliance.
- Verifique o status de conformidade do seu ambiente de nuvem para os ambientes de nuvem do Azure e AWS em relação aos padrões de parâmetro de comparação de organizações como o Center for Internet Security (CIS).
- Crie políticas e informações personalizadas com base em metadados de ativos, dados de cobertura da ferramenta de segurança e dados de vulnerabilidade.

Como o Gestão de posturas de segurança para ativos funciona



Gestão de posturas de segurança para ativos identifica lacunas na cobertura da ferramenta de segurança em ativos usando integrações de API com várias ferramentas (Conectores do Service Graph). As categorias incluem, entre outras:

- Experiência do Funcionário Digital
- Gestão de endpoint
- Gestão de superfície de ataque externo
- IT Asset Management
- Monitoramento de infraestrutura
- Rede
- Segurança de rede
- Monitoramento de desempenho de rede
- Configuration and Patch Management
- Proteção de endpoint
- Provedor de Nuvem
- Monitoramento de desempenho da aplicação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Serviços de diretório
- Avaliação de vulnerabilidade

Para obter mais informações sobre os conectores do Service Graph compatíveis, consulte Service Graph Connectors . Os Conectores do Service Graph compatíveis estão disponíveis na ServiceNow® Store com assinaturas separadas.

A ServiceNow Gestão de posturas de segurança para ativos depende dos dados de ativos preenchidos a partir de várias categorias de ferramentas no seu CMDB. Os dados do ativo de diferentes fontes são comparados para identificar possíveis lacunas de segurança. Por exemplo, digamos que haja dados de ativo preenchidos no CMDB que sejam relatados pelo monitoramento de infraestrutura e produtos de rede. No entanto, digamos que os dados desses mesmos ativos não sejam relatados por produtos de proteção de endpoint. A comparação dos dados de ativos relatados no CMDB, neste caso, mostra que os ativos não têm um agente de proteção de endpoint.

O produto Controle de posturas de segurança encontra lacunas na ferramenta de segurança executando as tarefas a seguir.

1. Identifica a lista de todos os ativos exclusivos preenchidos por vários Conectores do Service Graph no CMDB.
2. Avalia os ativos do inventário e identifica aqueles não relatados por categorias específicas, por exemplo, proteção de endpoint. Os ativos são identificados no inventário com base em uma política ativada.
3. Relata ativos que são identificados como "relatados" ou "não relatados" como "Descobertas" (Resultados de testes) na aplicação Configuration Compliance.
4. Prioriza, agrupa e atribui descobertas a diferentes equipes para correção na aplicação Configuration Compliance.

Identificar lacunas da ferramenta de segurança requer que você execute as etapas a seguir.

1. Configure e ative conexões de API com qualquer uma das ferramentas que você está usando em várias categorias.
2. Realize uma ou mais pesquisas de ativo com base em critérios específicos para obter um inventário.
3. Ative as políticas enviadas com a aplicação Controle de posturas de segurança ou crie suas próprias políticas e ative-as com base nos resultados de suas pesquisas de ativo.
4. Ative informações personalizadas ou crie e ative suas próprias informações para ajudá-lo a monitorar seus ativos.
5. Configure regras para automatizar o fluxo de trabalho de correção na aplicação Configuration Compliance.

Com Gestão de posturas de segurança para ativos, você também pode identificar ativos que não têm ferramentas de segurança em combinação com vulnerabilidades críticas e exposição na Internet. Atualmente, somente a exposição na Internet para Amazon Web Services (AWS) é compatível. Algumas das políticas enviadas com a aplicação Controle de posturas de segurança procuram combinações de alto risco de vulnerabilidades críticas e lacunas na cobertura da ferramenta de segurança. No entanto, para que essas políticas de combinação funcionem, você deve ter a aplicação Vulnerability Response e pelo menos um produto de integração de scanner de vulnerabilidade, como Qualys, Rapid7ou Tenable Vulnerability Integration instalado. Essas aplicações estão disponíveis com assinaturas separadas do ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instalar as aplicações compatíveis com o Security Posture Control

As aplicações necessárias para esta integração estão disponíveis no ServiceNow Store. Algumas aplicações têm dependências que você deve baixar e instalar separadamente.

Antes de Iniciar

Função necessária: administrador para download, instalação e ativação de todas as aplicações.

Procedimento

1. Baixe as aplicações necessárias da instância ServiceNow Store para sua instância ServiceNow.

   A aplicação Security Posture Control (SPC Core) fornece a estrutura principal e é necessária para o ASPM (Asset Security Posture Management). A aplicação Configuration Compliance e suas dependências permitem que você crie tarefas de correção para as vulnerabilidades encontradas usando a ASPM (Asset Security Posture Management) e a CSPM (Cloud Security Posture Management).

Aplicação	ID de Aplicativo
Gestão de posturas de segurança de ativos	(ID do plug-in: sn_sec_caasm)
Licença do ITOM Discovery	(ID do plug-in: com.snc.itom.discovery.license)
Núcleo de controle de postura de segurança	(ID do plug-in: sn_sec_spc_core)
Configuration Compliance (inclui app secundário seps_shared_components)	(ID do plug-in: sn_vulc)
Uso e licenciamento do Vulnerability Response	(ID do plug-in: sn_vul_licensing)
Aplicações do Cloud Security Posture Management	
Plug-in Descoberta	(ID do plug-in: com.snc.discovery)
Cloud Configuration Governance	(ID do plug-in: sn_itom_ccg)
Pacote de conteúdo CCG	(ID do plug-in: sn_itom_ccg_cp)
CMDB CI Class Models	(ID do plug-in: sn_cmdb_ci_class)
Biblioteca de ações na nuvem	(ID do plug-in: com.sn.itom.cal)

   Para obter mais informações sobre como baixar e ativar aplicações, consulte os seguintes tópicos:

   - Baixe uma aplicação de ServiceNow Store pela primeira vez.
   - Ativar uma aplicação ServiceNow Store.

2. Depois de baixar as aplicações, navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
3. Localize as aplicações que você baixou e selecione **Instalar** para ativá-las junto com suas dependências. Todas as aplicações de dependência que também são instaladas automaticamente junto com uma aplicação são exibidas na caixa de diálogo de instalação da aplicação. No entanto, se você for solicitado a instalar plug-ins de dependência durante a instalação, siga os prompts fornecidos. Verifique se você tem todas as aplicações e dependências listadas na tabela anterior instaladas e ativadas.

   Uma caixa de diálogo é exibida depois que uma aplicação é ativada com sucesso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Depois de instalar e ativar as aplicações, atribua usuários aos seguintes grupos de controle de postura de segurança:

   Esses grupos herdam todas as funções necessárias para ler e editar registros SPC.

   Grupo de administradores de SPC

   Os usuários neste grupo têm acesso total de leitura e gravação a todos os registros do produto, incluindo informações de licenciamento.

   Grupo de analistas do SPC

   Os usuários neste grupo têm acesso total de leitura e gravação a todos os registros do produto, mas não têm permissão de gravação. Eles não podem exibir informações de licenciamento.

   Grupo Somente leitura de analistas do SPC

   Os usuários neste grupo podem exibir todos os registros do produto, mas não têm permissão de gravação e não podem exibir informações de licenciamento.

O espaço do Security Posture Control

O espaço do Security Posture Control contém os módulos que você usa para configurar, usar e monitorar os dados importados sobre seus ativos.

Os módulos do espaço

Para acessar o espaço, navegue até **Espaços** > **Controle de posturas de segurança** A página inicial (página principal) será exibida. O espaço do Security Posture Control contém os seguintes módulos:

Módulos

Módulo	Descrição
Página inicial	As seções Visão geral, Principais informações e Principais coberturas de caso de uso incluem visualizações de dados que relatam e monitoram informações sobre seus ativos. Esses dados são criados e atualizados pelas políticas incluídas com a aplicação depois de ativá-las. Consulte Informações principais e informações personalizadas para Controle de postura de segurança e Políticas para controle de postura de segurança.
Informações personalizadas	Visualizações de dados sobre seus ativos que você cria com suas próprias políticas ou com as políticas incluídas com o aplicativo. Consulte Informações principais e informações personalizadas para Controle de postura de segurança.
Pesquisa de ativos	Pesquise rapidamente ativos em seu ambiente com base nas condições definidas. Verifique se você pode localizar ativos com um conjunto de condições antes de confirmar essas condições em uma política. Você pode refinar essas pesquisas para obter uma visualização dos ativos que atendem aos seus critérios de pesquisa. Quando estiver pronto, você poderá salvar suas condições como uma política. Consulte Criar uma pesquisa de ativo no Security Posture Control.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulos

Módulo	Descrição
Políticas e descobertas	As políticas auditam seus ativos para encontrar correspondências para possíveis violações. Informações, visualizações e casos de uso dependem de políticas. Consulte Políticas para controle de postura de segurança. As descobertas correspondem às suas políticas mapeadas para a aplicação Configuration Compliance para correção. Consulte Como configurar e exibir suas descobertas para o Security Posture Control.
Configuração de conectores e casos de uso	Casos de uso são cenários diferentes que você configura para ajudá-lo a identificar tipos específicos de lacunas de cobertura da ferramenta. Cada caso de uso requer uma política ou políticas para auditar seus ativos em busca de possíveis violações. Você também pode definir suas próprias políticas para ajudá-lo a atender aos requisitos de seus padrões de segurança interna específicos. Consulte Casos de uso no Security Posture Control.
Configuração de informações personalizadas	Você pode criar suas próprias informações se quiser mais informações não encontradas nas principais informações incluídas com a aplicação. Você pode usar políticas existentes ou suas próprias políticas personalizadas para avaliação. Suas informações personalizadas são exibidas no painel Informações personalizadas. Consulte Criar e ativar uma informação personalizada para o controle de postura de segurança.

Conectores do Service Graph para controle de postura de segurança

O Security Posture Control depende de integrações de API ou Conectores do Service Graph (SGCs) como uma fonte de chave para os dados de ativos usados para identificar lacunas de segurança.

No momento, o Security Posture Control oferece suporte a uma ampla variedade de conectores que estão disponíveis na ServiceNow Store. Escolha os conectores que deseja usar, baixe as aplicações e ative-as. Como o Security Posture Control oferece suporte a mais conectores, a lista de conectores compatíveis que estão disponíveis na Store aumentará.

Para obter mais informações sobre como baixar, configurar e ativar aplicações compatíveis com Service Graph Connectors, consulte os seguintes tópicos:

- Service Graph Connectors .
- Baixe uma aplicação de ServiceNow Store pela primeira vez.
- Ativar uma aplicação ServiceNow Store.

O Security Posture Control fornece duas classes de ativos de nível superior que podem ser consultadas ou avaliadas como parte das políticas.

Ativo de hardware

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta classe é uma abstração que representa qualquer dispositivo IP no local que inclui dispositivos de computação pessoal, servidores, dispositivos de rede e outro hardware.

Máquina Virtual em Nuvem

Esta classe representa uma máquina virtual no ambiente de nuvem pública como AWS, Azure ou GCP. Um exemplo são as instâncias do EC2 na AWS.

As políticas auditam seus ativos em busca de possíveis violações com base nos dados importados dos SGCs.

Se uma política tentar recuperar uma classe de ativo que seja relatada ou não por um Conector do Service Graph específico, o Security Posture Control mapeia todas as classes de item de configuração (IC) relevantes que estão relacionadas a essa classe de ativo no CMDB que são preenchidas ou não preenchido por esse Conector do Service Graph.

Por exemplo, digamos que uma política procure todos os ativos de hardware relatados pelo Service Graph Connector Jamf Pro. A lógica a seguir se aplica.

1. O Security Posture Control identifica quais classes de IC no CMDB são mapeadas para a classe "Ativo de hardware" do Jamf Pro.

   Nota:
   Diferentes Conectores do Service Graph preenchem diferentes classes de IC no CMDB, e o mapeamento para classes de IC de "Ativo de hardware" varia de um Conector do Service Graph para outro.

2. O controle de postura de segurança determina que as classes de IC, Computador, Servidor e Impressora no CMDB sejam mapeadas para a classe de ativo "Ativo de hardware" para o Service Graph Connector Jamf Pro.
3. O Security Posture Control consulta todos os registros de ativo preenchidos em qualquer uma dessas três classes de IC: Servidor, Computador, Impressora pelo Conector do Service Graph Jamf Pro no CMDB e retorna esses ativos.

   Você também pode exibir os conectores e suas categorias na tabela de conectores [sn_sec_spc_core_connector] em sua instância.

   Você pode exibir os tipos de ativo e como eles são mapeados para classes de IC e conectores na tabela [sn_sec_spc_core_asset_type_connector].

   Para exibir os conectores compatíveis no espaço, verificar o status on-line e exibir a Configuração de caso de uso de chave, navegue até **Espaços** > **Controle de posturas de segurança** > **Configuração de conectores e casos de uso** > **Guia Conectores do Service Graph compatíveis**.

Cada Conector do Service Graph compatível se enquadra em uma das categorias a seguir.

- Experiência do Funcionário Digital
- Gestão de endpoint
- Gestão de superfície de ataque externo
- IT Asset Management
- Monitoramento de infraestrutura
- Rede
- Segurança de rede
- Monitoramento de desempenho de rede

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Configuration and Patch Management
- Proteção de endpoint
- Provedor de Nuvem
- Monitoramento de desempenho da aplicação
- Serviços de diretório
- Avaliação de vulnerabilidade

A coluna "Classes de IC compatíveis com o SPC" na tabela a seguir indica quais classes de registros de IC são consideradas durante uma consulta pelo produto Security Posture Control como parte de uma avaliação de política. Esta tabela não é uma lista abrangente, mas você pode usá-la para ver como os dados ingeridos de várias categorias e origens geralmente são mapeados e consultados.

SGCs compatíveis

Conector e tipo de ativo	Classes de IC compatíveis com SPC	Categoria do conector	Origem da descoberta
Dynatrace Ativo de hardware	cmdb_ci_server cmdb_ci_computer	Monitoramento de desempenho da aplicação	SGO-Dynatrace
New Relic Ativo de hardware	cmdb_ci_server	Monitoramento de desempenho da aplicação	SG-NewRelic
AppDynamics Ativo de hardware	cmdb_ci_server	Monitoramento de desempenho da aplicação	SG-AppDynamics
Azure CloudVM	cmdb_ci_server cmdb_ci_vm_instance	Provedor de Nuvem	SG-Azure
AWS CloudVM	cmdb_ci_server cmdb_ci_vm_instance	Provedor de Nuvem	SG-AWS
GCP CloudVM	cmdb_ci_server cmdb_ci_vm_instance	Provedor de Nuvem	SG-GCP
SCCM Ativo de hardware	cmdb_ci_computer cmdb_ci_server	Configuração e gestão de patches	SG-SCCM
Puppet Ativo de hardware	cmdb_ci_server cmdb_ci_computer	Configuração e gestão de patches	Servidor SG-Puppet

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conector e tipo de ativo	Classes de IC compatíveis com SPC	Categoria do conector	Origem da descoberta
BigFix Ativo de hardware	cmdb_ci_computer cmdb_ci_server	Configuração e gestão de patches	SG-BigFix
Espaço da VMWare ONE UEM Ativo de hardware	cmdb_ci_computer cmdb_ci_server cmdb_ci_printer	Gestão de endpoint	SG-Workspace ONE UEM
CrowdStrike Ativo de hardware	cmdb_ci_server	Proteção de endpoint	SG-CrowdStrike
ScienceLogic Ativo de hardware	cmdb_ci_server cmdb_ci_hc_device cmdb_ci_computer cmdb_ci_vm_instance cmdb_ci_printer cmdb_ci_iot	Monitoramento de infraestrutura	SG-ScienceLogic
Datadog Ativo de hardware	cmdb_ci_server	Monitoramento de infraestrutura	SGO-Datadog
Monitor de Lógica Ativo de hardware	cmdb_ci_hc_device cmdb_ci_printer cmdb_ci_vm_instance cmdb_ci_computer cmdb_ci_server cmdb_ci_iot	Monitoramento de infraestrutura	SG-LogicMonitor
Prognóstico Ativo de hardware	cmdb_ci_computer cmdb_ci_server cmdb_ci_hc_device cmdb_ci_printer cmdb_ci_iot	Segurança de rede	SG-Forescout
Revelação de ExtraHop(x)	cmdb_ci_printer	Segurança de rede	SG-ExtraHop

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conector e tipo de ativo	Classes de IC compatíveis com SPC	Categoria do conector	Origem da descoberta
Ativo de hardware	cmdb_ci_server cmdb_ci_computer cmdb_ci_iot cmdb_ci_hc_device		
Cisco Merak Ativo de hardware	cmdb_ci_computer cmdb_ci_iot cmdb_ci_hc_device cmdb_ci_printer cmdb_ci_server	Rede	SG-Meraka
Rapid7 Ativo de hardware	cmdb_ci_hardware	Avaliação de vulnerabilidade	SG-Rapid7
Tenable Ativo de hardware	cmdb_ci_ot_control cmdb_ci_ot_industrial_robot cmdb_ci_hardware cmdb_ci_hub_network cmdb_ci_printer cmdb_ci_ot_hmi cmdb_ci_ot_industrial_actuator cmdb_ci_storage_server cmdb_ci_ot_plc cmdb_ci_ot_histórico cmdb_ci_ot_rtu cmdb_ci_ot_cnc cmdb_ci_computer cmdb_ci_ip_firewall cmdb_ci_iot cmdb_ci_ot_ie cmdb_ci_ot_industrial_drive cmdb_ci_ot_ews	Avaliação de vulnerabilidade	SG-TenableForAssets

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Conector e tipo de ativo	Classes de IC compatíveis com SPC	Categoria do conector	Origem da descoberta
	cmdb_ci_securitycmbd_ci_ip_switch cmdb_ci_ups cmbd_ci_server		
Qualys Ativo de hardware	cmdb_ci_computer cmdb_ci_server	Avaliação de vulnerabilidade	SG-Qualys

Políticas para controle de postura de segurança

Cada caso de uso depende de uma ou mais políticas que auditam seus ativos para encontrar possíveis violações.

Visão geral

As políticas de controle de postura de segurança são criadas em um modelo de dados entity-relationships-properties. Você pode definir políticas para procurar uma entidade ou ativo que corresponda a um critério específico. O critério pode ser especificado na forma de condições nas propriedades dessa entidade ou nas propriedades de uma entidade relacionada.

Atualmente, as seguintes entidades ou tipos de ativo primários ou de nível superior podem ser usados como ponto de partida na definição das políticas. Existem outras entidades compatíveis no esquema da política de controle de postura de segurança, como "Vulnerabilidade" ou "Metadados", mas essas entidades não podem ser o ponto de partida. Você pode navegar até essas entidades secundárias usando um relacionamento das entidades primárias ou de suas entidades relacionadas.

Entidades primárias:

- Ativo de hardware
- Máquina Virtual em Nuvem

Entidades e seus relacionamentos com entidades secundárias

Entidade	Relacionamento	Entidade de destino	Descrição
Ativo de hardware	Da classe de IC	Campos do CMDB	Representa classes padrão no CMDB ou suas classes de IC personalizadas no CMDB.
Ativo de hardware	Relatado por conector	Conector	Representa um Conector do Service Graph que relatou ou não relatou esta entidade.
Ativo de hardware	Não relatado por	Conector	Representa um Conector do Service Graph que relatou ou não relatou esta entidade.
Ativo de hardware	Com dados do conector	Detalhes do conector	Representa todas as propriedades disponíveis neste ativo que são específicas do Service Graph Connector.
Ativo de hardware	Com metadados do CMDB	Metadados do CMDB	Representa a coleção de propriedades de IC do CMDB neste ativo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Entidades e seus relacionamentos com entidades secundárias

Ativo de hardware	Com vulnerabilidade	Registro de vulnerabilidade	Representa um item vulnerável presente neste ativo.
Máquina Virtual em Nuvem			
Máquina Virtual em Nuvem	Da classe de IC	Campos do CMDB	Representa classes padrão no CMDB ou suas classes de IC personalizadas no CMDB.
Máquina Virtual em Nuvem	Relatado por	Conector	Representa um Conector do Service Graph que relatou este ativo de nuvem.
Máquina Virtual em Nuvem	Não relatado por	Conector	Representa um Conector do Service Graph que não relatou este ativo de nuvem.
Máquina Virtual em Nuvem	Com dados do conector	Conector	Representa todas as propriedades disponíveis neste ativo de nuvem que são específicas de um conector do Service Graph.
Máquina Virtual em Nuvem	Com metadados do CMDB	CMDBMetadata	Representa a coleção de propriedades de IC do CMDB neste ativo de nuvem.
Máquina Virtual em Nuvem	Com vulnerabilidade	Registro de vulnerabilidade	Representa um item vulnerável presente neste ativo de nuvem.
Máquina Virtual em Nuvem	Tem metadados de nuvem	Metadados em nuvem	Representa a coleção de propriedades de nuvem neste ativo de nuvem.
Máquina Virtual em Nuvem	Tem porta exposta à Internet	Abrir porta	Representa uma porta neste ativo de nuvem que está aberta à Internet.

Todas as entidades e propriedades compatíveis com essas entidades

Entidade	Propriedades
Ativo de hardware	Nenhum(a)
Máquina Virtual em Nuvem	• ID da conta de nuvem • Nuvem - região • provedor de nuvem
Máquina virtual em nuvem - Conector do Service Graph	• Categoria: categoria ou tipo do Conector do Service Graph, por exemplo, proteção de endpoint. • Nome do produto: o nome do produto que relata os ativos por meio do Conector do Service Graph.
Máquina virtual em nuvem - Dados do conector	Detalhes específicos a categorias e tipos de conectores, por exemplo, Detalhes de software, Detalhes de ativo, Detalhes de interface de rede

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Todas as entidades e propriedades compatíveis com essas entidades	
Metadados do CMDB – Conexão	• Tem informações do modelo: nome do modelo, nome de exibição, fabricante. • Com o software instalado - Cadeia de caracteres de desinstalação, versão, nome.
Metadados do CMDB - Propriedade	Propriedades de nuvem, como nome do host, número de série, domínio do SO.
Metadados em nuvem	• Cloud-region • Internet - exposição • provedor de nuvem • ID da conta de nuvem
Vulnerabilidade	• Has-exploit • Gravidade • ID de CVE
Abrir Porta	• Porta (porta que está aberta, por exemplo, 22). • Protocolo (por exemplo, TCP).

Políticas incluídas com a aplicação

Existem algumas políticas incluídas com a aplicação Security Posture Control que estão vinculadas a casos de uso importantes e são mostradas como informações importantes no painel na página principal (módulo inicial) no espaço de SPC. Para exibir essas políticas, navegue até **Espaços** > **Controle de posturas de segurança** > **Lista** > **Todos**.

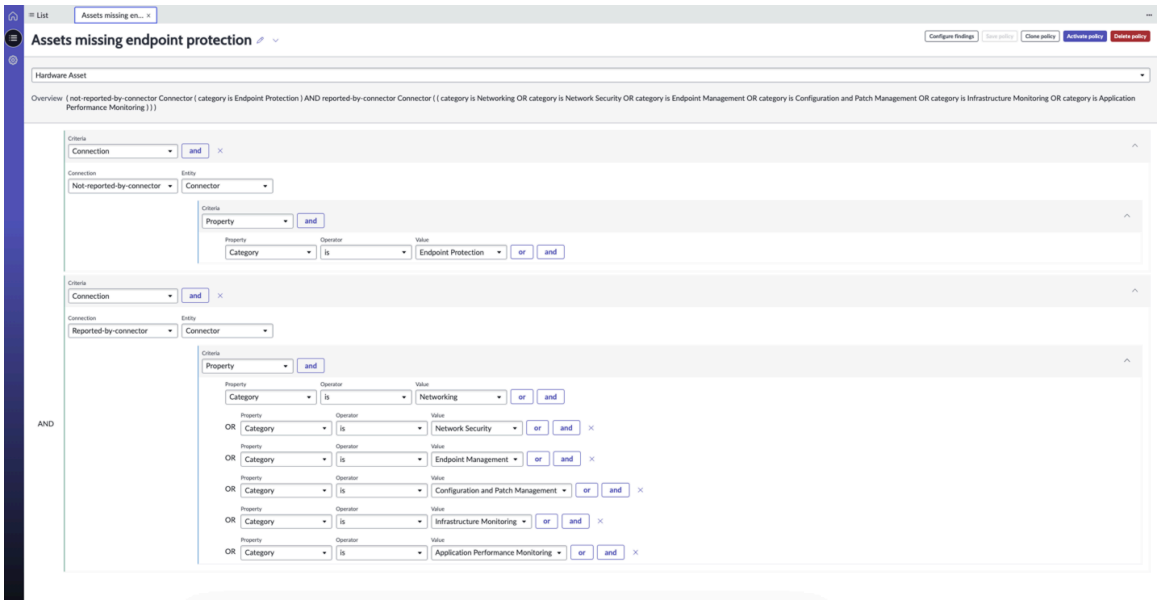
Essas políticas não podem ser editadas. No entanto, você pode alterar os metadados. Você pode clonar essas políticas para criar suas próprias políticas personalizadas, mas observe que as políticas clonadas não são refletidas como informações importantes no painel na página inicial do com as outras informações importantes.

Depois de clonar e ativar as políticas criadas, você cria seu próprio registro de informações personalizadas no módulo do Construtor de informações personalizadas no espaço de trabalho (o último módulo no painel do navegador) e exibe os dados no painel Informações personalizadas (o segundo ícone de na parte superior do espaço).

A imagem a seguir mostra uma política incluída com o produto que procura ativos sem proteção de endpoint. As condições desta política procuram ativos que não são relatados pelo Conector do Service Graph da categoria "Proteção de endpoint" e são relatados pelos Conectores do Service Graph em qualquer uma das categorias: Rede, Monitoramento de infraestrutura ou Provedor de nuvem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Como criar suas próprias políticas

Você pode criar suas próprias políticas para monitorar seus ativos. Essas políticas são baseadas em dados dos vários Conectores do Service Graph instalados e ativados, que incluem metadados específicos do conector para os ativos, como:

- Versão do agente do CrowdStrike
- Exposto à internet
- Vulnerabilidades críticas

Você pode clonar uma política existente e adicionar condições a ela ou criar uma política do zero. Para suas políticas personalizadas, você pode incluir condições para metadados, como SO, versão do SO e FQDN, por exemplo, para ajudá-lo a monitorar ativos com software mais antigo. Observe que essas propriedades são comuns do CMDB preenchidas por vários Conectores do Service Graph para qualquer ativo.

Você também pode adicionar uma condição para exceções aprovadas com a aplicação de Governança, risco e conformidade (GRC) que não deseja monitorar e incluir em suas contagens de ativos.

Políticas de base e políticas secundárias

Você pode usar várias políticas para avaliar seus ativos e criar suas próprias informações personalizadas. Você pode usar mais de uma política se quiser reduzir o número de ativos correspondentes de um tamanho de amostra grande ou se concentrar em mais de uma condição correspondente. Como exemplo, digamos que você queira criar um gráfico de comparação que mostre quantos de seus ativos totais, no local e na nuvem, não foram verificados quanto a vulnerabilidades.

Você também pode criar políticas secundárias a partir de qualquer registro de política para ajudar a refinar ainda mais seus critérios de pesquisa e retornar correspondências mais específicas. Todas as condições na política base também são herdadas na política secundária.

Se você adicionar mais de uma política:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O nível 1 é a base. Esta política consulta um tamanho de amostra extensivo em (N), por exemplo, todos os ativos no Active Directory relatados pelo conector do Active Directory Service Graph.
- O nível 2 avalia os resultados da primeira política. Esta política avalia somente um subconjunto de (N). Por exemplo, de todos os ativos no Active Directory, retorne somente os ativos com ferramentas de avaliação de vulnerabilidade que não sejam verificados quanto a vulnerabilidades.
- O nível 3 avalia os resultados das políticas 1 e 2 e assim por diante. Por exemplo, de todos os ativos no seu Active Directory com ferramentas de avaliação de vulnerabilidade que não são verificadas quanto a vulnerabilidades, retorne somente os agentes de proteção de endpoint ausentes.
- Observação: é possível ter várias políticas em uma hierarquia. Com a hierarquia, você pode exibir as diferentes classificações de como seus ativos correspondem a cada nível na hierarquia.

Para criar uma política secundária, em um registro de política, selecione **Nova política** e defina as condições desejadas. Você tem a opção de usar as condições de uma política existente como início e excluir resultados de políticas existentes e exceções aprovadas. Para obter mais informações, consulte Criar, clonar e ativar uma política para o Security Posture Control.

Ao selecionar políticas para informações personalizadas, você não pode escolher uma política secundária no mesmo nível de uma política primária, a menos que altere a hierarquia.

Filtragem de metadados e CMDB

Pode ser importante para suas equipes de segurança monitorar ativos com software mais antigo. Você pode especificar critérios de política para incluir as propriedades comuns listadas abaixo.

- SO
- Versão do SO
- Nome do host
- FQDN
- Endereço IP
- Versão do IP
- Máscara de rede
- Endereço MAC
- Fabricante do MAC
- Software
- RAM
- Número de Série
- NIC
- Tipo de Número de Série
- Localização

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Contagem de CPUs
- Espaço em Disco

Nota:
Para coletar esses metadados, as propriedades a seguir devem estar disponíveis na conexão de metadados do CMDB preenchida pelos conectores do Service Graph.

Exceções com a aplicação Governance, Risk, and Compliance (GRC)

Uma exceção de Gestão de riscos integrada (IRM) é um ativo com uma exceção aprovada do produto de Governança, risco e conformidade (GRC). Você tem a opção em uma política de adicionar uma condição para uma exceção para não monitorar esses ativos e incluí-los em suas contagens.

Por exemplo, alguns ativos podem ter exceções aprovadas para determinados objetivos de controle com IRM. Para reduzir as correspondências retornadas, as equipes de segurança da informação podem excluir esses ativos do monitoramento de controles de segurança com exceções de IRM que já foram aprovadas.

Ativar uma política para um caso de uso no Security Posture Control

As políticas incluídas com a aplicação devem ser ativadas antes que o Security Posture Control possa monitorar os ativos que correspondem a essa política. Por padrão, nenhuma das políticas incluídas com a aplicação está ativada.

Antes de Iniciar
Você deve ativar as políticas manualmente depois de verificar se todos os pré-requisitos necessários foram atendidos:

- Conectores do Service Graph ativados.
- Todas as aplicações necessárias, como Vulnerability Response, são instaladas e ativadas, se aplicável para casos de uso.

Nota:
Você não pode editar uma política incluída com a aplicação. No entanto, você pode editar os metadados (ícone de lápis próximo ao nome da política no registro) e clonar ou criar uma nova política com base nas condições de uma política existente.

Funções necessárias:

- Grupo de administradores de SPC
- Grupo de analistas do SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Lista** > **Políticas** > **Todos**.
2. Selecione um registro de política para abri-lo.
3. Você tem as seguintes opções em um registro de política que não está ativado:

Opção	Descrição
Desativar política	Desative uma política ativa se você não quiser que nenhum ativo seja monitorado ou avaliado em relação a essa política ou se quiser editar suas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	condições. Esta opção de edição só está visível em registros de política ativos.
Salvar política	Salve as condições da política.
Configurar descobertas	○ Selecione **Sim** se quiser que suas descobertas sejam agrupadas e atribuídas para correção de acordo com as regras configuradas na aplicação Configuration Compliance. Essas descobertas podem ser resultados que revelam falhas de segurança. ○ Selecione **Não** se quiser que suas descobertas sejam encerradas automaticamente. Essas descobertas podem ser resultados que não revelam falhas de segurança. ○ Selecione o link **Configurar regras de atribuição** para configurar regras de atribuição na aplicação Configuration Compliance para atribuir quaisquer descobertas da sua política para resolução.
Clonar política	Crie uma nova política com as mesmas condições desta política como ponto de partida. Para obter mais informações, consulte Criar, clonar e ativar uma política para o Security Posture Control.
Criar uma política secundária	Crie uma política secundária que herde as condições da política atual. As condições de política atuais são exibidas no campo "Política de base" no novo registro e você adiciona mais condições.
Ativar política	Ative esta política para que ela pesquise ativos, encontre correspondências e gere descobertas.
Excluir política	Exclua esta política. A opção de exclusão não é compatível com políticas que já tenham gerado descobertas. Você só pode desativar essas políticas com descobertas.

Para determinar se uma política está ativada, confirme seu status (verdadeiro ou falso) na coluna Ativa **Todos** > **Espaços** > **Controle de posturas de segurança** > **Lista** > **Políticas** > **Todos**.

Criar, clonar e ativar uma política para o Security Posture Control

Crie suas próprias políticas personalizadas para monitorar ativos para cobertura de ferramenta e outras combinações de alto risco.

Antes de Iniciar

Antes de começar, consulte o caso de uso para Detectar ativos com vulnerabilidades e lacunas na cobertura da ferramenta de segurança descrito em Casos de uso no Security Posture Control para garantir que você ativou o Conector do Service Graph para o produto CrowdStrike e instalou a aplicação Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para entender as etapas necessárias para criar uma política, siga o exemplo fornecido abaixo. Para esta política, digamos que você queira criar uma política que encontre todos os ativos que não sejam vistos ou relatados pelo produto CrowdStrike e tenham uma vulnerabilidade log4shell, "CVE-2021-44228".

Funções necessárias:

- Grupo de administradores de SPC
- Grupo de analistas do SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Lista** > **Políticas** > **Todos**.
2. Selecione **Nova política**.
3. Selecione o ícone de lápis ao lado do nome na parte superior para modificar os metadados.

   Preencha os campos.

Campo	Descrição
Nome	Um nome exclusivo para sua política.
Criticidade	Selecione um na lista.
Descrição resumida	Uma descrição exclusiva da sua apólice.

4. Selecione **Salvar metadados**.
5. No primeiro campo do formulário, selecione **Ativo de hardware** na lista.

   Observe as opções de Política de base e Política de exclusão à direita da página.

   - Política de base: você pode herdar as condições de uma política existente para usar como base para esta política como ponto de partida.
   - Políticas de exclusão: você pode excluir ativos correspondentes de uma ou mais políticas existentes para que seus resultados sejam ignorados nesta política. Esta opção pode ajudar a refinar ainda mais os resultados retornados para esta política ou permitir que você ignore quaisquer exceções aprovadas para ativos.

   Os campos Conexão e Entidade são exibidos.

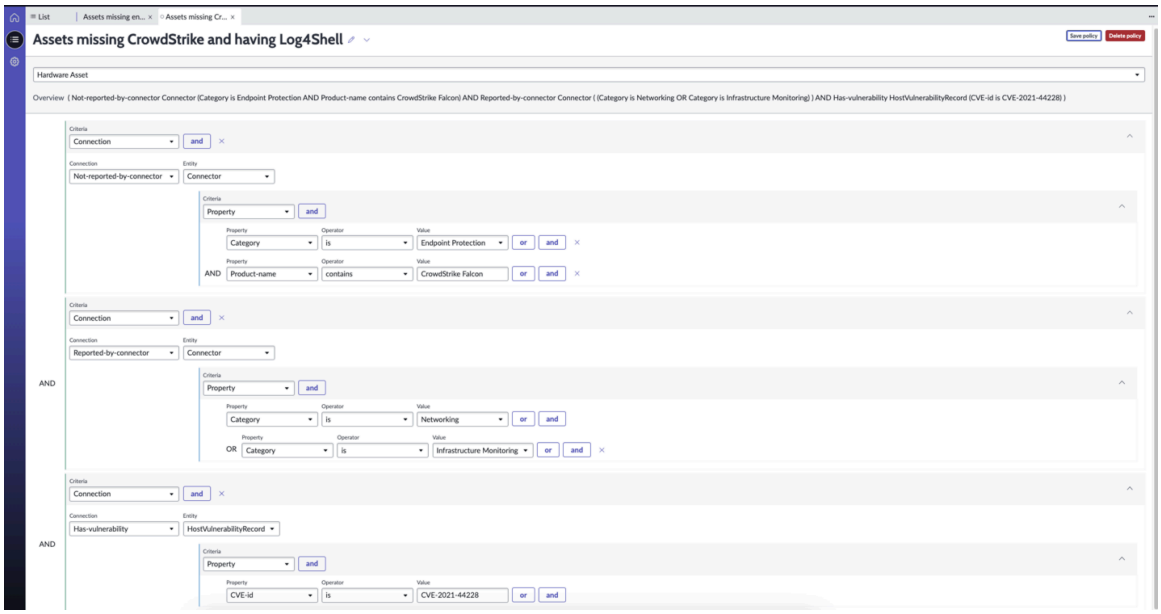
6. Selecione **Não relatado por** na lista do campo Conexão.
   O campo Entidade de destino é preenchido automaticamente com o Conector do Service Graph.
   Uma nova condição com o campo Critérios é exibida com os campos Propriedade, Operador e Valor. A propriedade é exibida no campo Critérios.
7. Selecione **[Categoria][é][Proteção de endpoint]** na lista de valores exibida.
8. Selecione o operador **e** à direita do campo Valor preenchido com Endpoint Protection.
9. No próximo conjunto de campos, selecione **[Product-name][is][CrowdStrike]**.
10. Selecione o operador **e** na parte superior do primeiro campo Entidade preenchido com o Conector do Service Graph para exibir os novos campos Conexão e Entidade.
11. Selecione **Relatado por**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O campo Entidade é preenchido automaticamente (Conector do Service Graph). Uma nova condição (Critérios) é exibida com campos para Propriedade, Operador e Valor. **A propriedade** é exibida no campo Critérios.

12. Selecione **[Categoria][é][Rede]**.
13. Selecione o operador **e** ao lado do campo Valor preenchido com Rede.
14. Selecione **[Categoria][é][Monitoramento de infraestrutura]**.
15. Selecione o operador **e** pelo segundo do campo Entidade preenchido com o Conector do Service Graph.
16. No novo campo Conexão, selecione **Com vulnerabilidade**.
    O campo Entidade é preenchido automaticamente com Vulnerabilidade.
17. Selecione **[CVE-id][is]** e insira **CVE-2021-44228**.
    As condições da política devem corresponder à imagem.



18. Selecione **Salvar política**, configure as descobertas e ative a política.

    Depois de salvar e ativar uma política, ela avalia os dados importados do SGC programados na próxima execução. Se você quiser exibir os dados no painel de informações personalizadas no espaço de trabalho, deverá criar uma nova informação no módulo de configuração de informações personalizadas no painel (último ícone no espaço de trabalho). Depois de ativar a informação personalizada, seus dados são exibidos no painel Informações personalizadas no espaço de trabalho (segundo ícone).

19. No menu à direita de Salvar política, selecione **Configurar descobertas**.
20. Preencha os campos.
21. Selecione **Salvar configuração**.
22. **Opcional:** Se você quiser clonar esta política ou qualquer política existente, selecione **Clonar política** no menu ao lado de **Ativar política**.

    (Optional) Você pode criar uma política secundária usando qualquer política como base para ajudá-lo a estender as políticas existentes sem precisar inserir as condições novamente. Todas as condições na política base também são herdadas na política

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

secundária. Um novo registro de política é aberto com o nome da política clonada seguido por "cópia".

Selecione **Políticas de exclusão** e selecione as políticas que você deseja excluir das descobertas desta política. Quaisquer descobertas em sua nova política que correspondam a qualquer política ou políticas existentes não serão incluídas em suas descobertas.

23. Selecione **a Política base** e selecione qualquer política ativa como a política primária.

    Você pode escolher esta opção se quiser usar as condições de uma política existente como ponto de partida para sua nova política.

    Se você adicionar mais de uma política, observe a seguinte hierarquia. Você pode ter várias políticas em uma hierarquia de políticas. Com cada política, você pode exibir as diferentes classificações de como seus ativos correspondem a cada nível.

    - O nível 1 é a base. Esta política consulta um tamanho de amostra extensivo em (N), por exemplo, todos os ativos no Active Directory relatados pelo conector do Active Directory Service Graph.
    - O nível 2 avalia os resultados da primeira política. Esta política avalia somente um subconjunto de (N). Por exemplo, de todos os ativos no Active Directory, retorne somente os ativos com ferramentas de avaliação de vulnerabilidade que não sejam verificados quanto a vulnerabilidades.
    - O nível 3 avalia os resultados das políticas 1 e 2 e assim por diante. Por exemplo, de todos os ativos no seu Active Directory com ferramentas de avaliação de vulnerabilidade que não são verificadas quanto a vulnerabilidades, retorne somente os agentes de proteção de endpoint ausentes.

    Nota:
    Você pode ter várias políticas em uma hierarquia. Com a hierarquia, você pode exibir as diferentes classificações de como seus ativos correspondem a cada nível na hierarquia.

24. Salve sua política.
    Sua política é exibida na lista Todos no módulo Lista no espaço.

25. Para ativar uma política, abra o registro da política e selecione **Ativar política**.

Informações principais e informações personalizadas para Controle de postura de segurança

As informações principais e personalizadas fornecem relatórios visuais que são criados e atualizados pelos critérios de avaliação que correspondem aos seus ativos.

Informações principais

Os critérios usados para as avaliações de seus ativos são fornecidos pelas políticas incluídas com o aplicativo.

- As informações principais usam as políticas incluídas com a aplicação.
- Informações personalizadas podem ser criadas usando as políticas incluídas na aplicação, suas próprias políticas personalizadas ou uma combinação de ambas.

Na página inicial (página principal) do espaço do Security Posture Control, a seção Informações principais abaixo da Visão geral exibe relatórios visuais que são criados e atualizados pelas políticas incluídas com a aplicação. Essas informações também estão incluídas com a aplicação e exibem as seguintes informações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Agente de proteção de endpoint instalado: número total de ativos que têm ou não proteção de endpoint.
- Cobertura de dispositivo gerenciado: número de ativos gerenciados comparados aos não gerenciados.
- Cobertura de verificação de vulnerabilidades: número total de ativos verificados em comparação com aqueles que não foram verificados quanto a vulnerabilidades conhecidas por um verificador de vulnerabilidades de terceiros.
- Ativos com vulnerabilidades críticas: número de ativos do número total de ativos que têm vulnerabilidades críticas.
- Itens vulneráveis por criticidade: número total de itens vulneráveis divididos por severidade. Uma vulnerabilidade conhecida que corresponde a um ativo no seu CMDB resulta em um item vulnerável. Esta informação requer que você instale a aplicação Vulnerability Response e pelo menos uma integração de scanner: Qualys, Rapid7 ou Tenable Vulnerability Integration. Todas essas aplicações estão disponíveis na ServiceNow® Store.
- 3 principais políticas por descobertas: políticas que retornam a maioria das descobertas (correspondências) em seus ativos.

Informações personalizadas

Você pode criar suas próprias informações se quiser mais informações não encontradas nas principais informações. Você pode criar essas informações personalizadas e usar as políticas existentes ou suas próprias políticas personalizadas para avaliação. Suas informações personalizadas são exibidas no módulo do painel Informações personalizadas, o segundo ícone de cima para baixo no espaço.

Criar e ativar uma informação personalizada para o controle de postura de segurança

Você pode criar suas próprias informações. Informações personalizadas são informações que você pode criar usando políticas existentes ou suas próprias políticas personalizadas.

Antes de Iniciar
Você deve criar um registro de informações e ativá-lo antes de exibir seus dados no painel Informações personalizadas. Você pode ter até seis informações e 21 gráficos no módulo do painel Informações personalizadas no espaço de trabalho.

Todas as políticas usadas para uma informação personalizada devem ser ativadas.

Funções necessárias:

- Grupo de administradores de SPC
- Grupo de analistas do SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Construtor de informações personalizadas** (último ícone no espaço).

   Nesta página principal, há três guias:

   Ativo

   Suas informações personalizadas ativadas. As informações personalizadas ativadas são exibidas na página principal de Informações personalizadas (segundo ícone de cima para baixo no espaço).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Inativo

Suas informações personalizadas inativas. As informações desativadas não são exibidas na página principal de informações personalizadas até que as informações e suas políticas de suporte que as suportam sejam ativadas.

Todos

Todas as suas informações personalizadas ativas e inativas.

2. Selecione **Nova informação** à direita da página para criar um novo registro.
3. No campo Tipo, selecione uma informação na lista de seleção.

Opção	Descrição
Gráfico de comparação	Compare as contagens de ativos correspondentes para até cinco apólices.
Widget de contagem de correspondência de política	O número total de ativos que correspondem a uma ou mais políticas.
Gráfico de porcentagem de correspondência de política	A porcentagem do total de ativos que correspondem ou não a uma política.
Gráfico de tendências de correspondência de política	Tendência histórica de ativos que correspondem a uma ou mais políticas.

4. Selecione as políticas e os rótulos de informações desejados para seus dados de informações.
5. Selecione **Salvar**.
   Sua informação é salva na guia Informação inativa.
6. Para ativar sua nova informação, abra o registro na lista de inativos e selecione **Ativar**.
   Os dados são coletados da próxima importação programada dos Conectores do Service Graph que estão associados às políticas de informações e são exibidos no módulo do Painel de informações personalizadas no espaço.

Como configurar e exibir suas descobertas para o Security Posture Control

Você pode exibir as descobertas geradas pela avaliação de políticas no Security Posture Control no espaço do Security Posture Control.

Visão geral

Todos os ativos correspondentes são relatados como "Descobertas". Você pode configurar as descobertas a serem geradas a partir da execução de políticas para que essas descobertas possam ser atribuídas a várias equipes para correção ou usadas para geração de relatórios. O Security Posture Control publica essas descobertas como "Resultados de testes" no módulo Configuration Compliance. Todos os controles administrativos na aplicação Configuration Compliance que estão relacionados à atribuição, agrupamento, ou seja, geração de tarefa de correção, destinos de correção e exceções são compatíveis com as descobertas geradas pelo Security Posture Control.

Os tipos de descobertas:

Cobertura da ferramenta

Este tipo representa uma lacuna de cobertura da ferramenta de segurança. Este tipo de descoberta é aplicável a políticas que usam relacionamentos de conector "Relatado por" e "Não relatado".

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exposição na Internet

Este tipo representa a exposição na Internet de um ativo de nuvem. Este tipo de descoberta é aplicável a políticas que usam o relacionamento "Tem porta exposta à Internet" em máquinas virtuais em nuvem.

Combinação de alto risco

Este tipo representa um problema com mais de um fator de risco associado, por exemplo, ativos com vulnerabilidades críticas e um agente de proteção de endpoint ausente.

Exceção da Gestão de riscos integrados (IRM)

Este tipo representa um ativo com uma exceção aprovada do produto de Governança, risco e conformidade (GRC). Se indicado, essas exceções não serão incluídas nas contagens de descobertas.

Rótulos de postura de segurança são gerados e anexados aos resultados de testes. Um rótulo de um tipo apropriado, "cobertura da ferramenta", por exemplo, é atribuído automaticamente aos resultados de testes com base no tipo de política.

Ao usar rótulos de postura de segurança associados às descobertas, você pode escrever regras de atribuição no Configuration Compliance para rotear esses problemas para as respectivas equipes para correção. Por exemplo, você pode enviar descobertas de "Cobertura da ferramenta" para uma equipe de operações de TI e "Exposição na Internet" para uma equipe de aplicações.

No entanto, se um dos responsáveis pela correção corrigir o problema em uma combinação, a outra descoberta será encerrada automaticamente, pois essas descobertas são geradas a partir de uma política que procura a combinação. Por exemplo, se a equipe de operações de TI fechar a descoberta "Cobertura da ferramenta" instalando o agente de proteção de endpoint, a descoberta "Exposição na Internet" gerada a partir desta política será fechada automaticamente, mesmo que o ativo seja voltado para a Internet, já que esta descoberta é gerada de uma política que procura uma combinação de problemas. Se você quiser rastrear o problema de exposição na Internet nos ativos, é recomendável criar outra política que procure somente a exposição na Internet nos ativos sem outros fatores de risco.

Onde exibir as descobertas

Você tem essas opções para exibir as descobertas geradas pela avaliação de políticas.

- Navegar até **Espaço do Security Posture Control** > **Listas** > **Descobertas** > **Todos.**
- Em um registro de política, selecione **Exibir descobertas**. A lista exibe grupos de descobertas que as organizam em categorias gerais, como "Combinação de alto risco", "Exposição na Internet" e assim por diante, mas esses grupos não são agrupamentos formais que podem ser usados para correção. Você precisa configurar regras de correção e atribuição no Configuration Compliance para descobertas.
- Na aplicação Configuration Compliance, selecione **Resultados de testes** e filtre os registros por **Origem que seja ServiceNow SPC**.

O painel

No espaço do Security Posture Control, a página inicial (página principal) exibe estas visualizações:

Visão geral

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Ativos: número de ativos monitorados no local e na nuvem.
- Descobertas por criticidade: número de descobertas críticas do total de ativos.
- Ativos monitorados pelas 5 principais origens: os 5 principais Conectores do Service Graph que geram relatórios sobre ativos.
- Contas de nuvem: número de contas de nuvem monitoradas pela AWS e pelo Azure.
- Descobertas abertas versus encerradas: comparação de registros ainda em processo ou aguardando resolução e aqueles que foram resolvidos.

Informações principais

- Agente de proteção de endpoint instalado: número total de ativos que têm ou não proteção de endpoint.
- Cobertura de dispositivo gerenciado: número de ativos gerenciados comparados aos não gerenciados.
- Cobertura de verificação de vulnerabilidades: número total de ativos verificados em comparação com o número que não é verificado quanto a vulnerabilidades conhecidas por um scanner de vulnerabilidade de terceiros.
- Ativos com vulnerabilidades críticas: número de ativos do número total de ativos que têm vulnerabilidades críticas.
- Itens vulneráveis por criticidade: número total de itens vulneráveis divididos por severidade. Uma vulnerabilidade conhecida que corresponde a um ativo no seu CMDB resulta em um item vulnerável.
- 3 principais políticas por descobertas: políticas que retornam a maioria das descobertas (correspondências) em seus ativos.

Cobertura de caso de uso principal

Selecione um caso de uso e selecione **Ajudar a ativar** ou **Ajudar a melhorar** para exibir quais conectores do Service Graph e políticas devem ser ativados para os principais casos de uso.

Criar uma pesquisa de ativo no Security Posture Control

Defina suas condições e pesquise ativos por produtos específicos do Service Graph Connector ou ativos que tenham dados específicos relatados por um conector.

Antes de Iniciar
Como exemplo de pesquisa, digamos que você queira identificar seus ativos que têm servidores Windows e uma versão específica encontrada nos detalhes de metadados do CrowdStrike.

Funções necessárias:

- Grupo de administradores de SPC
- Grupo de analistas do SPC

Procedimento

1. Navegar até **Espaços** > **Controle de posturas de segurança** > **Pesquisa de ativos**.
2. Escolha um.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Opção	Descrição
Ativo de hardware	Pesquisar ativos no local
Máquina Virtual em Nuvem	Pesquisar ativos de nuvem

Para este exemplo, selecione **Ativo de hardware** para o tipo de ativo.

3. **Opcional:** Selecione **Política de base e Políticas** de **exclusão** se quiser usar as condições de uma política existente como início e excluir ativos que correspondam às políticas existentes, respectivamente. As políticas selecionadas são exibidas.
4. Selecione **Com dados do conector** para o campo Conexão.
5. Selecione **Detalhes do dispositivo do CrowdStrike** para a entidade.
6. Em Propriedade, Operador e Valor, selecione **[Versão do agente][é]** e insira a versão, por exemplo, **6.26.14003.0**.
7. Selecione o operador e à direita do campo Entidade com Detalhes do dispositivo CrowdStrike como o valor para outra condição.
8. Selecione **Com metadados do CMDB** para o campo Conexão.
   O campo Entidade é preenchido com Metadados do CMDB.
9. Selecione **Propriedade** para o campo Critérios.
10. Em Propriedade, Operador e Valor, selecione **[SO][contém]** e insira **Servidor Windows**.
11. Selecione **Exibir ativos**.
    Após alguns momentos, os resultados serão exibidos na guia Ativos correspondentes. Se você não encontrar correspondências, poderá refinar a pesquisa. Quando estiver satisfeito com a definição das condições corretamente, você poderá salvar a pesquisa como uma política e ativá-la. Como outras políticas, ela pesquisa seus ativos com um trabalho em segundo plano continuamente depois que você a ativa.

Casos de uso no Security Posture Control

Casos de uso são cenários diferentes que você configura para ajudá-lo a identificar tipos específicos de lacunas de cobertura da ferramenta. Cada caso de uso requer uma política ou políticas para auditar seus ativos em busca de possíveis violações. Você também pode definir suas próprias políticas para ajudá-lo a atender aos requisitos de seus padrões de segurança interna específicos.

Casos de uso

A aplicação Security Posture Control oferece suporte a vários casos de uso que estão incluídos com a aplicação. Os casos de uso ajudam a identificar tipos específicos de lacunas de cobertura de ferramenta em seus ativos, exposição de ativos de nuvem na Internet e combinações com vulnerabilidades. As políticas necessárias para os casos de uso compatíveis também estão incluídas no produto.

Você pode exibir o status de cobertura de alguns dos principais casos de uso na página inicial (inicial) do espaço do Security Posture Control em **Espaços** > **Controle de posturas de segurança** > **Página inicial** no módulo inicial (página principal).

Como alternativa, você pode exibir os conectores do Service Graph compatíveis e o status de cobertura de alguns dos principais casos de uso nas guias "Conectores do Service Graph compatíveis" e "Configuração de caso de uso principal" em **Todos** > **Espaços** >

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Controle de posturas de segurança > **Configuração de conectores e casos de uso** (ícone de engrenagem).

Nota:

A guia "Casos de uso principais" nas páginas iniciais não lista todos os casos de uso possíveis. Ele fornece alguns casos de uso importantes que você ativa para ajudá-lo a começar a implantar o produto Security Posture Control.

Antes de ativar as políticas para os casos de uso compatíveis fornecidos com a aplicação, verifique se você concluiu as tarefas a seguir.

- Você instalou e configurou todas as aplicações necessárias descritas em Instalar as aplicações compatíveis com o Security Posture Control.
- Você atendeu a um ou mais dos seguintes pré-requisitos para cada caso de uso.

1. Você está usando ou instala e ativa os Service Graph Connectors para várias categorias.

   As categorias para os casos de uso incluem Service Graph Connectors que você deve ativar para obter informações iniciais e Service Graph Connectors que você tem a opção de ativar para melhorar a cobertura dos ativos que o Security Posture Control está monitorando.

2. Você está usando ou instala e ativa a aplicação Vulnerability Response.
3. Você está usando ou configura a Verificação de conta de nuvem para suas contas da AWS e do Azure em "Gestão de postura de segurança na nuvem".

Os requisitos específicos para cada caso de uso compatível são descritos nas seções a seguir. Além disso, você deve ativar uma ou mais das políticas enviadas com o Security Posture Control para um caso de uso. Esse conceito também é abordado nas seções a seguir.

Caso de uso de controle de postura de segurança: detecção de ativos sem proteção de endpoint

Para detectar ativos sem um agente de proteção de endpoint, os pré-requisitos a seguir são necessários.

Para cada Conector do Service Graph na lista, você pode ver se esse conector é necessário para monitorar ativos no local ou ativos na nuvem. Dependendo do caso de uso, você pode optar por ativar somente os conectores necessários.

Por exemplo, se o seu objetivo é monitorar somente os ativos de nuvem sem proteção de endpoint, você só precisará ativar um Conector do Service Graph para Endpoint Protection e pelo menos um provedor de nuvem: AWS, Azure ou GCP. Você não precisa habilitar Conectores do Service Graph separados para Rede, Monitoramento de infraestrutura e assim por diante.

1. Ative pelo menos um Conector do Service Graph da categoria Proteção de endpoint.
2. Ative pelo menos um Conector do Service Graph para UMA das categorias a seguir.
   a. Rede (necessário somente para ativos no local) .
   b. Monitoramento de infraestrutura (necessário somente para ativos no local) .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Serviços de diretório (necessário somente para ativos no local. Esta categoria cobre o Active Directory).

d. Provedor de nuvem (necessário para monitorar ativos de nuvem para este caso de uso) .

3. [Opcional] Você pode ativar os Conectores do Service Graph para qualquer uma das categorias a seguir para melhorar a cobertura geral, ou seja, o número de ativos que são relatados e monitorados pelo Security Posture Control.

a. Segurança de rede.

b. Gestão de endpoints.

c. Configuration and Patch Management.

d. Monitoramento de desempenho da aplicação .

Depois de verificar se atendeu a esses pré-requisitos, você deve ativar pelo menos uma das políticas. Para qualquer política que comece com "Ativos de nuvem", os Conectores do Service Graph na categoria "Provedor de nuvem" devem ser habilitados. Para obter mais informações sobre políticas, consulte Políticas para controle de postura de segurança.

- Ativos sem proteção de endpoint
- Ativos de nuvem sem proteção de endpoint

Caso de uso de controle de postura de segurança: detecção de ativos perdidos por ferramentas de avaliação de vulnerabilidade

Para detectar ativos perdidos pelas ferramentas de avaliação de vulnerabilidade, os seguintes pré-requisitos são necessários.

Para cada Conector do Service Graph na lista, você pode ver se esse conector é necessário para monitorar ativos no local ou ativos na nuvem. Dependendo do caso de uso, você pode optar por ativar somente os conectores necessários.

Por exemplo, se o seu objetivo é monitorar somente os ativos de nuvem não detectados pelas ferramentas de verificação de vulnerabilidades, você só precisará ativar um Conector do Service Graph para proteção de endpoint e pelo menos um provedor de nuvem: AWS, Azure ou GCP. Você não precisa habilitar Conectores do Service Graph separados para Rede, Monitoramento de infraestrutura e assim por diante.

1. Ative pelo menos um Conector do Service Graph da categoria Avaliação de vulnerabilidade.
2. Ative pelo menos um Conector do Service Graph para UMA das categorias a seguir.

a. Rede (necessário somente para ativos no local) .

b. Monitoramento de infraestrutura (necessário somente para ativos no local) .

c. Serviços de diretório (necessário somente para ativos no local. Esta categoria cobre o Active Directory).

d. Provedor de nuvem (necessário para monitorar ativos de nuvem para este caso de uso) .

3. [Opcional] Você pode ativar os Conectores do Service Graph para qualquer uma das categorias a seguir para melhorar a cobertura geral, ou seja, o número de ativos que são relatados e monitorados pelo Security Posture Control.

a. Segurança de rede.

b. Gestão de endpoints.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Configuration and Patch Management.

d. Monitoramento de desempenho da aplicação .

Depois de verificar se atendeu a esses pré-requisitos, você deve ativar pelo menos uma das políticas. Para qualquer política que comece com "Ativos de nuvem", os Conectores do Service Graph na categoria "Provedor de nuvem" devem ser habilitados. Para obter mais informações sobre políticas, consulte Políticas para controle de postura de segurança.

- Ativos não verificados quanto a vulnerabilidades.
- Ativos em nuvem não verificados quanto a vulnerabilidades.

Caso de uso do Security Posture Control: detecção de ativos não gerenciados

Este caso de uso inclui duas partes, detecção de ativos que não têm configuração e agentes de gestão de patches.

Para detectar ativos sem configuração e ferramentas de gestão de patches, os pré-requisitos a seguir são necessários.

Para cada Conector do Service Graph na lista, você pode ver se esse conector é necessário para monitorar ativos no local ou ativos na nuvem.

Dependendo do caso de uso, você pode optar por ativar somente os conectores necessários. Por exemplo, se o seu objetivo é monitorar somente os ativos de nuvem que não têm ferramentas de configuração e gestão de patches,você só precisa ativar um Conector do Service Graph para proteção de endpoint e pelo menos um provedor de nuvem: AWS, Azure ou GCP. Você não precisa habilitar Conectores do Service Graph separados para Rede, Monitoramento de infraestrutura e assim por diante.

1. Ative pelo menos um Conector do Service Graph nas categorias Configuração e Gestão de patches.
2. Pelo menos um Conector do Service Graph deve estar habilitado para UMA das categorias a seguir.
   a. Rede (necessário somente para ativos no local) .
   b. Monitoramento de infraestrutura (necessário somente para ativos no local) .
   c. Serviços de diretório (necessário somente para ativos no local. Esta categoria cobre o Active Directory).
   d. Provedor de nuvem (necessário para monitorar ativos de nuvem para este caso de uso) .
3. [Opcional] Você pode ativar os Conectores do Service Graph para qualquer uma das categorias a seguir para melhorar a cobertura geral, ou seja, o número de ativos que são relatados e monitorados pelo Security Posture Control.
   a. Segurança de rede.
   b. Gestão de endpoints.
   c. Proteção de endpoint
   d. Avaliação de vulnerabilidade
   e. Monitoramento de desempenho da aplicação .

Depois de verificar se atendeu a esses pré-requisitos, você deve ativar pelo menos uma das políticas. Para qualquer política que comece com "Ativos de nuvem", os Conectores do

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Service Graph na categoria "Provedor de nuvem" devem ser habilitados. Para obter mais informações sobre políticas, consulte Políticas para controle de postura de segurança.

- Configuração e gestão de patches ausentes nos ativos.
- Ativos de nuvem sem configuração e gestão de patches.

Caso de uso de controle de postura de segurança: detecção de ativos sem uma solução de gestão de endpoint

Para detectar ativos sem uma solução de gerenciamento de endpoint, os pré-requisitos a seguir são necessários.

Para cada Conector do Service Graph na lista, você pode ver se esse conector é necessário para monitorar ativos no local ou ativos na nuvem.

Dependendo do caso de uso, você pode optar por ativar somente os conectores necessários. Por exemplo, se o seu objetivo é monitorar somente os ativos de nuvem sem ferramentas de gestão de endpoint, você só precisará ativar um Conector do Service Graph para proteção de endpoint e pelo menos um provedor de nuvem: AWS, Azure ou GCP. Você não precisa habilitar Conectores do Service Graph separados para Rede, Monitoramento de infraestrutura e assim por diante.

1. Ative pelo menos um Conector do Service Graph na categoria Gestão de endpoints.
2. Pelo menos um Conector do Service Graph deve estar habilitado para UMA das categorias a seguir.
   a. Rede (necessário somente para ativos no local) .
   b. Monitoramento de infraestrutura (necessário somente para ativos no local) .
   c. Serviços de diretório (necessário somente para ativos no local. Esta categoria cobre o Active Directory).
   d. Provedor de nuvem (necessário para monitorar ativos de nuvem para este caso de uso) .
3. [Opcional] Você pode ativar os Conectores do Service Graph para qualquer uma das categorias a seguir para melhorar a cobertura geral, ou seja, o número de ativos que são relatados e monitorados pelo Security Posture Control.
   a. Segurança de rede.
   b. Gestão de endpoints.
   c. Proteção de endpoint
   d. Avaliação de vulnerabilidade
   e. Monitoramento de desempenho da aplicação .

Depois de verificar se atendeu a esses pré-requisitos, você deve ativar pelo menos uma das políticas. Para qualquer política que comece com "Ativos de nuvem", os Conectores do Service Graph na categoria "Provedor de nuvem" devem ser habilitados. Para obter mais informações sobre políticas, consulte Políticas para controle de postura de segurança.

- Ativos sem solução de gerenciamento de endpoint.
- Ativos em nuvem sem solução de gestão de endpoint.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caso de uso de controle de postura de segurança: detecção de ativos com vulnerabilidades e lacunas na cobertura da ferramenta de segurança

Você pode identificar ativos com vulnerabilidades críticas e ferramentas de segurança críticas ausentes, como proteção de endpoint, para priorizar esses ativos para correção. O Security Posture Control envia algumas políticas incluídas com o produto para oferecer suporte a este caso de uso.

Este caso de uso requer que você instale a aplicação Vulnerability Response e uma integração com pelo menos um produto de avaliação de vulnerabilidade, como Qualys, Rapid7 ou Tenable.

As políticas a seguir estão incluídas com o produto Security Posture Control para oferecer suporte a este caso de uso para ativos com vulnerabilidades críticas que também não têm cobertura da ferramenta de segurança.

1. Ativos com vulnerabilidades críticas e proteção de endpoint ausente
2. Ativos com vulnerabilidades críticas e sem configuração e gestão de patches
3. Ativos com vulnerabilidades críticas e gestão de endpoint ausente
4. Ativos de nuvem com vulnerabilidades críticas e proteção de endpoint ausente
5. Ativos de nuvem com vulnerabilidades críticas e configuração ausente e gestão de patches
6. Ativos de nuvem com vulnerabilidades críticas e gestão de endpoint ausente

1. Ative pelo menos um Conector do Service Graph na categoria Gestão de endpoints.
   - Endpoint Protection (necessário para as políticas 1 e 4).
   - Configuration and Patch Management (necessário para as políticas 2 e 4).
   - Endpoint Management (necessário para as políticas 3 e 6).
2. Pelo menos um Conector do Service Graph deve estar habilitado para UMA das categorias a seguir.
   a. Rede (necessário somente para ativos no local) .
   b. Monitoramento de infraestrutura (necessário somente para ativos no local) .
   c. Serviços de diretório (necessário somente para ativos no local. Esta categoria cobre o Active Directory).
   d. Provedor de nuvem (necessário para monitorar ativos de nuvem para este caso de uso) .
3. [Opcional] Você pode ativar os Conectores do Service Graph para qualquer uma das categorias a seguir para melhorar a cobertura geral, ou seja, o número de ativos que são relatados e monitorados pelo Security Posture Control.
   a. Segurança de rede.
   b. Gestão de endpoints.
   c. Proteção de endpoint
   d. Avaliação de vulnerabilidade
   e. Monitoramento de desempenho da aplicação .

Depois de verificar se atendeu a esses pré-requisitos, você deve ativar pelo menos uma das políticas. Para qualquer política que comece com "Ativos de nuvem", os Conectores do

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Service Graph na categoria "Provedor de nuvem" devem ser habilitados. Para obter mais informações sobre políticas, consulte Políticas para controle de postura de segurança.

Caso de uso de controle de postura de segurança: detecção de exposição na Internet de ativos de nuvem e combinações de alto risco

É essencial monitorar a possível exposição na Internet de ativos em nuvem (máquinas virtuais) em várias portas para garantir que as vulnerabilidades desses ativos não sejam exploradas remotamente. Este caso de uso ajuda a identificar esses ativos.

O Security Posture Control permite que você avalie a configuração de ativos de nuvem para ajudá-lo a identificar os ativos que são voltados para a internet, ou seja, quais ativos podem ser acessados de qualquer lugar na internet e em quais portas eles existem.

O Security Posture Control combina essas informações com lacunas de cobertura da ferramenta de segurança e dados de vulnerabilidade de scanners de terceiros, como Qualys, Rapid7 e Tenable para identificar combinações de alto risco.

Atualmente, este caso de uso oferece suporte à AWS e requer os seguintes pré-requisitos.

1. O Conector do Service Graph para AWS é ativado para as contas da AWS que você configurou.
2. Você ativou uma ou mais das políticas incluídas com o produto no Security Posture Control.
   - Ativos de nuvem com porta SSH 22 aberta para a Internet.
   - Ativos de nuvem com porta SSH 22 aberta para a Internet e proteção de endpoint ausente.
   - Ativos de nuvem com porta HTTP 80 aberta para a Internet e proteção de endpoint ausente.
   - Ativos de nuvem com vulnerabilidades críticas e porta SSH 22 aberta para a Internet (requer Vulnerability Response).
   - Ativos de nuvem com vulnerabilidades críticas, proteção de endpoint ausente e porta SSH 22 aberta para a Internet (requer Vulnerability Response).
   - Ativos de nuvem com portas HTTP abertas para a Internet, vulnerabilidades críticas e proteção de endpoint ausente (requer Vulnerability Response).

[store-future: BEGIN review]

Integração do Cloud Security Posture Management com Amazon Web Services

A aplicação Cloud Security Posture Management (CSPM) desenvolvida por ServiceNow verifica continuamente seu ambiente de nuvem para identificar qualquer não conformidade ou violação de configuração em relação a estruturas de conformidade, como o CIS.

Principais termos e conceitos

Atualmente, o CSPM de ServiceNow oferece suporte ao CIS AWS Foundations Benchmark v1.4.0. Este módulo coleta os dados de configuração de ativos de nuvem em seu ambiente AWS diretamente da nuvem, os importa para sua instância da Now Platform e os audita para conformidade.

Região

As regiões se referem a uma área geográfica compatível com os serviços em nuvem da AWS. As regiões têm endpoints padrão que permitem acessar os serviços compatíveis com essa região.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplos de regiões podem ser Virgínia ou Utah nos Estados Unidos ou outros locais de DATACENTER fora dos EUA.

Recurso

Recurso é um termo usado no ambiente da AWS que descreve os ativos da AWS e suas definições de configuração. Recursos são os serviços em seus ambientes da AWS. Em sua instância Now Platform, os recursos são chamados de ativos ou itens de configuração (ICs).

Centro de Segurança na Internet (CIS)

O CIS é uma organização sem fins lucrativos orientada pela comunidade que é responsável pelos controles CIS ® e Benchmarks CIS ™, processos reconhecidos globalmente para proteger sistemas e dados de TI. Atualmente, a aplicação ServiceNow CSPM usa as diretrizes publicadas no CIS AWS Foundations 1.4.0 para auditar a conformidade dos ativos de nuvem.

Política (políticas de configuração)

Políticas são diretrizes de governança. No Now Platform, as políticas são chamadas de Políticas de configuração. A aplicação CSPM desenvolvida por ServiceNow fornece políticas de configuração de linha de base para avaliar seu ambiente de nuvem em relação aos padrões de parâmetro de comparação, como CIS. Há um mapeamento um para um entre as políticas de configuração e as diretrizes fornecidas nas estruturas de conformidade.

Conjunto de políticas (configuração de grupos de políticas)

Os conjuntos de políticas são grupos de políticas individuais. No Now Platform, os conjuntos de políticas são chamados de Grupos de políticas de configuração.

Gestão de posturas de segurança para nuvem

As políticas (Políticas de**configuração**) e os conjuntos de políticas (**Grupos de políticas de configuração**) estão localizados no módulo **Cloud Security Posture Management** criado em sua instância para esta integração.

Testar

Testes são bibliotecas de registros de dados que organizam verificações de seus ativos. Os testes de configuração definem como uma classe de ativos de tecnologia deve ser controlada para atender à conformidade. Os testes são usados na aplicação Configuration Compliance para agrupar ativos para correção.

Resultados de testes

Os resultados de testes (TR) são criados em sua instância quando uma auditoria descobre que um recurso em seu ambiente de nuvem não está em conformidade. Os resultados do teste são armazenados na aplicação Configuration Compliance em seu Now Platform. Esses registros exibem os resultados (aprovação/reprovação) das auditorias executadas em seus recursos.

Grupos de resultado do teste

Os grupos de resultados de testes ajudam a organizar os resultados de testes em grupos lógicos e a priorizar suas tarefas de correção.

Funções necessárias de Now Platform

Os administradores de segurança com a função sn_vul.cspm_security_admin podem usar este produto. As verificações de conta em nuvem também podem ser configuradas por usuários com a função sn_vul.cspm_cloud_account_admin.

Para obter uma lista completa das funções necessárias para esta integração, consulte .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho

- Os conjuntos de políticas (**Grupos de políticas de configuração**) incluídos com a aplicação definem quais dados você importa.
- Os dados de configuração de recurso importados são armazenados em tabelas temporárias na sua instância Now Platform. Esses dados armazenados são auditados quanto à conformidade com as políticas listadas no CIS Amazon Web Services Foundations Benchmark v1.4.0 .
- Os resultados das auditorias são criados como resultados de testes e grupos de resultados de testes na aplicação Configuration Compliance em sua instância da plataforma.
- Você pode exibir resultados de testes, grupos de resultados de testes e outros dados Configuration Compliance em painéis e em registros na aplicação Configuration Compliance. Gerentes de segurança, gerentes de vulnerabilidade e analistas de vulnerabilidade podem usar esses dados para identificar, priorizar e responder às vulnerabilidades relacionadas à configuração em seus ativos.

Coleta de dados

Para coletar os dados de configuração do AWS Cloud em seu ambiente, chame a API Cloud AWS por meio de um MID Server da sua instância Now Platform®. Você extrai os dados dos recursos da AWS em seu ambiente empresarial. Os dados em seus recursos podem incluir o seguinte escopo amplo de informações que você pode importar para auditoria:

- Gestão de identidade e acesso (IAM)
- Armazenamento
- Registro em Log
- Monitoramento
- Rede

Exemplos de não conformidade de segurança e configuração em seus dados importados

A lista a seguir inclui alguns exemplos de recursos fora de conformidade ou desvio da prática de segurança sólida na configuração de ativos:

- Verifique os buckets do S3 que estão abertos para exibição pública.
- Verifique se há buckets do S3 que não estejam criptografados.
- As chaves de usuário do IAM não são giradas.
- Verifique se há acesso restrito a imagens de máquina virtual (VM) de determinados fornecedores.
- Verifique quais dos seus endereços IP são públicos.
- Verifique se a autenticação multifator (MFA) está habilitada para buckets S3.

Políticas e padrões de parâmetro de comparação

Existem 58 políticas definidas no CIS Amazon Web Services Foundations Benchmark v1.4.0 . 47 dessas políticas estão codificadas em sua instância como parte desta aplicação. As 11 políticas manuais também listadas no parâmetro de comparação não são compatíveis com esta aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

[End]
[store-future: BEGIN review]

Instalar e ativar a aplicação CSPM Innovation Lab para AWS

As aplicações necessárias para esta integração estão disponíveis no ServiceNow® Store e listadas no link Exibir dependências e licenciamento na página de listagem da aplicação. Algumas aplicações têm dependências que você deve baixar e instalar separadamente.

Antes de Iniciar

Função necessária: administrador para download, instalação e ativação de todas as aplicações.

O administrador atribui as funções a seguir. Essas funções Now Platform® são necessárias para a aplicação.

Para obter mais informações sobre como baixar e ativar aplicações, consulte os seguintes tópicos:

-
- Ativar uma aplicação ServiceNow Store

Procedimento

1. Clique no link fornecido no e-mail recebido para acessar as aplicações desta integração no ServiceNow Store.

   Para exibir as dependências de uma aplicação, na página da aplicação no ServiceNow Store, clique em **Exibir dependências e requisitos de licenciamento** em Dependências e licenciamento.

   Nota:
   A aplicação de gestão de postura de segurança em nuvem está localizada no link do **Laboratório de inovação** do ServiceNow Store. As outras aplicações podem ser encontradas em **Aplicações e soluções**.

2. Instale as aplicações na ordem a seguir.

Aplicação	Versão do app e plug-ins de dependência
Versão da plataforma	San Diego vx.xx
Vulnerability Response (dependências)	v x.xx
Configuration Compliance (dependências)	v x.xx
CMDB CI Class Models	Instalar CMDB CI Class Models , ramificação principal
Security Support Common	Instale o Security Support Common (ID do plug-in: com.snc.security_support.common) do repositório , recurso de ramificação/EPIC1037528_native_cspm
Security Integration Framework	Instale o Security Integration Framework (ID do plug-in: com.snc.sec.int.framework) do repositório , recurso de ramificação/EPIC1037528_native_cspm
Orquestração de suporte de segurança	Instalar o Security Support Orchestration (ID do plug-in: com.snc.secops.orchestration) do repositório , ramificação secops-dev

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação	Versão do app e plug-ins de dependência
Vulnerability Response (aplicação principal)	Instale o Vulnerability Response (ID do plug-in: com.snc.vulnerability) do repositório , recurso de ramificação/EPIC1037528_native_cspm
Configuration Compliance (aplicação principal)	Instale o Configuration Compliance (ID do plug-in: com.snc.vulc) do repositório , recurso de ramificação/EPIC1037528_native_cspm
Vulnerability Response e Configuration Compliance para nuvem	Instale o Vulnerability Response e o Configuration Compliance for Cloud (ID do plug-in: com.snc.vul_cloud) do repositório , ramificação zero/STRY53500471_overview
Performance Analytics for Vulnerability Response	Instale o Performance Analytics para Vulnerability Response (ID do plug-in: com.snc.vulnerability.analytics) do repositório , recurso de ramificação/EPIC1037528_native_cspm
ServiceNow IntegrationHub Enterprise Pack Installer	Instalar o ServiceNow IntegrationHub Enterprise Pack Installer (ID do plug-in: com.glide.hub.integrations.enterprise)
Cloud Provisioning and Governance Core	Instalar Cloud Provisioning and Governance Core (ID do plug-in: com.snc.cloud.core)
Biblioteca de ações na nuvem	Instalar a Biblioteca de ação de nuvem (ID do plug-in: com.sn.itom.cal) do repositório , ramificação principal
Cloud Configuration Governance	Instalar Cloud Configuration Governance (ID do plug-in: com.sn.itom.ccg) , ramificação principal
Gestão de posturas de segurança para nuvem	Instale o Cloud Security Posture Management (ID do plug-in: com.snc.secops.cspm) do repositório , ramificação de rascunho/desenvolvimento

3. Depois de baixar as aplicações do ServiceNow Store, em sua instância Now Platform, navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
4. Localize as aplicações listadas na tabela anterior e clique em **Instalar** para ativá-las.
   Todas as aplicações de dependência que também são instaladas automaticamente junto com uma aplicação são exibidas na caixa de diálogo de instalação da aplicação. No entanto, se você for solicitado a instalar plug-ins de dependência durante a instalação, siga os prompts fornecidos. Verifique se você tem todas as aplicações e dependências listadas na tabela anterior instaladas e ativadas.

   Uma caixa de diálogo é exibida depois que uma aplicação é ativada com sucesso.
5. Depois de instalar e ativar as aplicações, se ainda não estiverem atribuídas, atribua as funções a seguir.

   Essas funções são necessárias para várias atividades de fluxo de trabalho na integração:

   - discovery_admin ou sn_cmmp.cloud_admin: configura as contas de serviço em nuvem no Now Platform para as contas de serviço correspondentes do AWS.
   - cspm_security_admin. Esta função também herda as seguintes funções:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_itom_ccg.governor: cria novas políticas, conjuntos de políticas e coletores. A função de administrador executa a "política de teste" e cria novas entidades usadas pelo administrador de programação.
- sn_itom_ccg.operator — o operador Cloud Configuration Governance testa as políticas e verifica os resultados. O operador também corrige resultados de testes e grupos de resultados de testes.
- sn_itom_ccg.scheduling_admin - configura Cloud Configuration Governance para as contas de serviço da AWS. Cria configurações de verificação e programação de verificação. Tem acesso aos resultados da verificação para ver entidades e políticas importadas.

◦ cspm_cloud_account_admin. Esta função também herda a função sn_itom_ccg.scheduling_admin.

◦ mid_server - configura um MID Server.

◦ sn_vulc.admin - configura a aplicação Configuration Compliance, tem visibilidade de todos os registros e pode modificar propriedades. Atribui funções na aplicação Configuration Compliance. Para obter mais informações sobre funções na aplicação Configuration Compliance, consulte Componentes instalados com Configuration Compliance.

◦ sn_vuln.admin — configura a aplicação Performance Analytics para Vulnerability Response.

Execute as etapas a seguir para criar um registro de verificação para verificar os ativos em seu ambiente da AWS.

6. Se ainda não tiver concluído, configure as contas de serviço e as credenciais da AWS e o alias de credencial. Um usuário com discovery_admin ou sn_cmmp.cloud_admin configura as contas de serviço Amazon Web Services (AWS). Para obter mais informações, consulte . Essas credenciais são exibidas na coluna Credenciais do Discovery nos registros de Contas de serviço em nuvem que você cria.

7. Configure políticas com o nível necessário de permissões para fornecer acesso aos recursos da AWS para Cloud Discovery e Cloud Provisioning and Governance.
Coloque o seguinte JSON no seu apêndice para criar suas permissões. Copie o texto e faça as edições necessárias. Use este arquivo para criar suas permissões de política. No mínimo, essas são as permissões necessárias para esta aplicação. Para obter mais informações, consulte .

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "iam:GenerateCredentialReport",
    "access-analyzer:ListAnalyzers",
    "iam:GetPolicyVersion",
    "iam:GetAccountPasswordPolicy",
    "iam:ListServerCertificates",
    "s3:GetBucketLogging",
    "cloudtrail:GetTrailStatus",
    "ec2:DescribeFlowLogs",
    "ec2:DescribeRegions",
    "logs:DescribeMetricFilters",
    "cloudtrail:GetEventSelectors",
    "iam:ListVirtualMFADevices",
    "s3:GetEncryptionConfiguration",
    "kms:GetKeyRotationStatus",
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
        "iam:ListAttachedUserPolicies",
        "rds:DescribeDBInstances",
        "iam:GetCredentialReport",
        "ec2:DescribeNetworkAcls",
        "iam:ListPolicies",
        "sns:ListSubscriptionsByTopic",
        "iam:ListEntitiesForPolicy",
        "iam:ListUserPolicies",
        "s3:GetBucketVersioning",
        "config:DescribeConfigurationRecorderStatus",
        "cloudtrail:DescribeTrails",
        "ec2:DescribeSecurityGroups",
        "kms:ListKeys",
        "config:DescribeConfigurationRecorders",
        "ec2:DescribeVpcs",
        "cloudwatch:DescribeAlarms",
        "iam:GetLoginProfile",
        "iam:GetAccountSummary"
      ],
      "Resource": "*"
    }
  ]
}
```

8. Um usuário com a função sn_itom_ccg.scheduling_admin configura uma conta de serviço em nuvem com as credenciais da AWS em Cloud Configuration Governance para as contas de serviço Amazon Web Services que você criou na etapa anterior.

   Consulte para obter mais informações sobre as etapas necessárias.

9. Se ainda não estiver concluído, um usuário com a função mid_server configurará um Now Platform MID Server para conectar sua instância com suas contas da AWS.

   Para obter mais informações, consulte .

10. Depois de configurar o MID Server, um usuário com o sn_itom_ccg.scheduling_admin executa a descoberta de DATACENTER para identificar os DATACENTERS com as contas de serviço.

    Para obter mais informações, consulte .

    Nota:
    Se você não preencher a tabela na conta de serviço em nuvem, a integração não será executada corretamente.

11. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Regras de Grupo** e selecione o **Grupo de atribuição, teste a regra** para abrir o registro e defina o campo Ativo como **verdadeiro**.

    No Configuration Compliance, as regras de grupo e de atribuição incluídas com a aplicação são desativadas por padrão. Um usuário com o sn_vulc.admin ativa essas regras.

    Esta regra agrupa os resultados de testes criados durante a auditoria. Todos os resultados de testes de uma determinada política que têm um retorno falso no resultado do teste são agrupados em um grupo de resultados de teste.

    Por padrão, os grupos de resultados de testes são atribuídos ao grupo de usuários de suporte de IC. Esta regra de atribuição está inativa por padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

12. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Regras de atribuição** e selecione o registro Atribuir ao grupo de suporte de IC para abri-lo e clique na caixa de seleção **Ativo** para ativá-lo.

    Esta regra atribui os grupos de resultados de testes a usuários no grupo de suporte de IC. Atribua quaisquer usuários a este grupo que você deseja trabalhar nesses resultados de testes.

    Esta é uma regra de atribuição padrão que pode não ser útil para atribuir problemas de configuração de nuvem em sua organização, dependendo de suas práticas internas. Você pode preferir criar uma regra de atribuição que atenda aos seus requisitos. Você pode usar metadados da conta de nuvem fazendo referência com pontos na tabela Item descoberto da tabela Resultado de testes para definir regras de atribuição.

13. Navegar até **Performance Analytics** > **Coletor de Dados** > **Trabalhos** e localize os trabalhos do coletor diário de PA CC e verifique se esses trabalhos estão ativados.

    Para exibir os resultados da auditoria nos painéis Performance Analytics para Vulnerability Response, um usuário com a função sn_vuln.admin habilita a aplicação e ativa os coletores de dados.

    Você concluiu a configuração da integração. Você está pronto para criar um registro de configuração de verificação na aplicação CSPM.

[End]

[store-future: BEGIN review]

Verificação de contas de nuvem usando a aplicação CSPM [ServiceNow com AWS

Esta seção descreve como configurar varreduras de segurança para suas contas de nuvem para verificar a conformidade de seus recursos em relação às estruturas de parâmetro de comparação. Um exemplo de política é usado para mostrar esse processo.

Antes de Iniciar

Configuração necessária: este exemplo começa com a criação de um registro de verificação. Se você quiser configurar ou verificar as informações em suas contas de serviço da AWS, consulte as etapas de configuração em .

Funções necessárias: sn_vul.cspm_cloud_account_admin

Procedimento

1. Navegar até **Todos** > **Gestão de posturas de segurança para nuvem** > **Administração** > **Verificações de conta de nuvem** para criar um registro de configuração de verificação na aplicação CSPM.
   A página Regras de avaliação de política é exibida.
2. Clique em **Nova**.
3. Preencha os campos.

   a. Insira um nome exclusivo para a configuração de verificação.

   b. Insira uma descrição resumida para ajudá-lo a localizar o registro mais tarde.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Selecione **Contas de serviço em nuvem** e selecione as contas de serviço de destino desejadas. Estes são os registros que você criou e configurou para suas contas da AWS e inseriu em Cloud Configuration Governance.

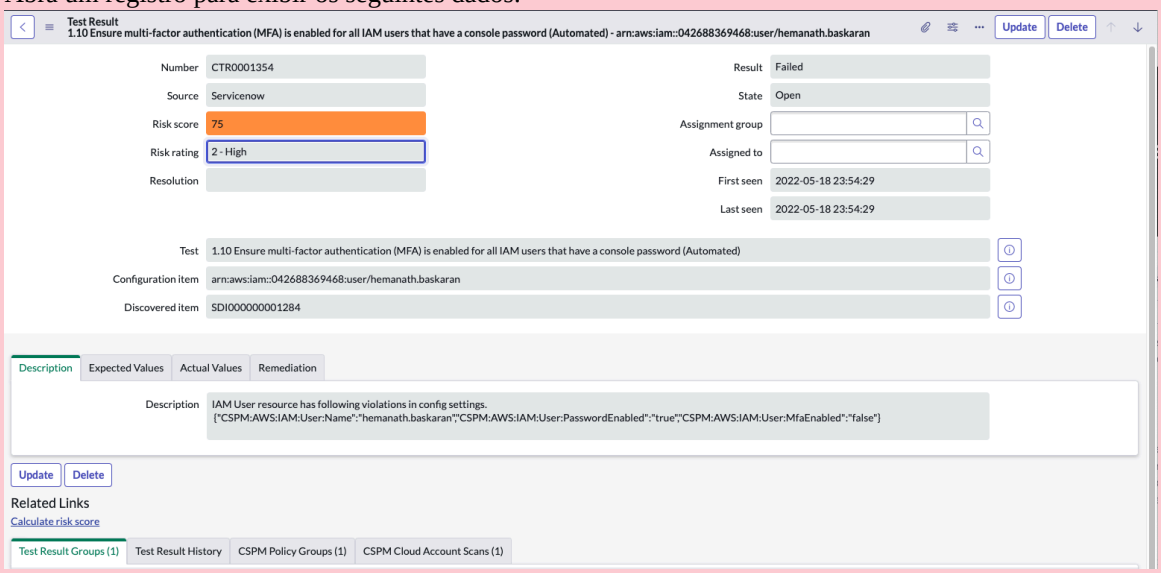
4. Marque a caixa de seleção Verificação em segundo **plano** para ativá-la.
Se você quiser que a verificação seja executada a cada hora, marque a caixa de seleção Verificação em segundo **plano** para ativá-la. Se a caixa de seleção não estiver marcada, você deverá iniciar a verificação sob demanda.

5. Para verificar as contas secundárias vinculadas automaticamente, marque a caixa de seleção Verificar **automaticamente as contas secundárias vinculadas**.

6. Navegar até **Todos** > **Configuration Compliance** > **Resultados de testes** > **Todos**.
A lista de grupos de resultados de testes (CTR#) criada a partir da auditoria de política é exibida.

Registros de Resultado de testes para seus recursos de Nuvem que estão fora de conformidade são criados. Se as violações forem corrigidas, os registros de resultado de testes serão encerrados.

7. Abra um registro para exibir os seguintes dados:



Campo de teste

Este campo exibe o mapeamento um para um entre com a política usada para a auditoria e o registro de teste de auditoria em Configuration Compliance. Clique para visualizar e abrir o registro de teste e exibir as citações, ou seja, a Fonte autorizada. Para este exemplo, a fonte autorizada é o parâmetro de comparação CIS AWS Foundations v1.4.0 e a seção citada, a política, é 1.10. Cada grupo de política ao qual esta política pertence é exibido. Uma política pode estar em mais de um grupo de políticas. Além disso, o número de resultados de testes gerados pela auditoria é exibido.

Campo de Item de configuração

Esses dados se referem a um recurso na AWS.

Campo de item descoberto

Um item descoberto em seu Now Platform está associado ao recurso AWS. Todos os metadados de nuvem importados sobre o recurso da AWS, como região, conta de nuvem e tipo de recurso, por exemplo, são armazenados no registro de item descoberto.

Guia Grupos de resultados de testes

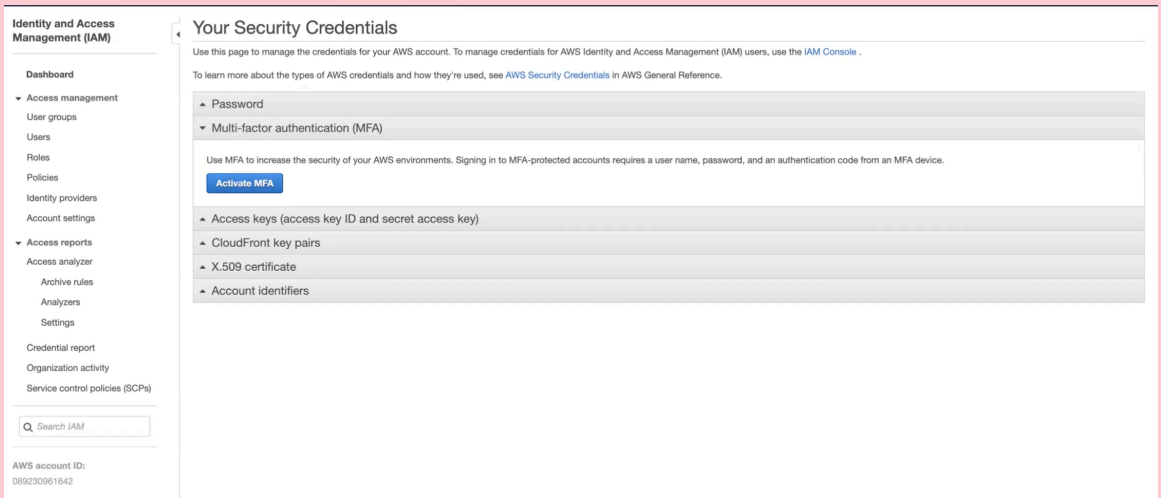
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por padrão, a aplicação Configuration Compliance agrupa os resultados de testes em grupos de resultados de testes com base em um retorno `falso` na auditoria. Somente um registro por resultado de teste é criado para um recurso e é atualizado após as importações de dados. Se a definição de configuração for alterada para um recurso em seu ambiente AWS entre as verificações, o registro será atualizado em sua instância Now Platform.

8. Para verificar os dados importados, você pode voltar para a conta de usuário da AWS.

Neste exemplo, uma verificação nesta conta indica que a Autenticação multifator não está habilitada (**Ativar MFA**). Este status corresponde aos dados de segurança importados sobre os recursos e grupos de recursos da Nuvem. Depois que você mudar a configuração e o recurso estiver em conformidade, suas mudanças serão refletidas na próxima importação de dados. No exemplo a seguir, a MFA deve ser ativada na AWS para este recurso antes que seu registro de resultado de teste seja fechado.



[End]

Exibir dados de auditoria do AWS CSPM nos painéis Performance Analytics para Vulnerability Response

Esta integração inclui painéis na aplicação Performance Analytics para Vulnerability Response.

Antes de Iniciar

Função necessária: pa_viewer

Procedimento

1. Para exibir o painel, navegue até **Configuration Compliance** > **Visão geral**.

Os dados dos painéis são coletados diariamente. Para modificar as configurações, navegue até **Performance Analytics** > **Coletor de Dados** > **Trabalhos**.

Nota:
Se você estiver executando outras integrações de vulnerabilidade de terceiros, todos os seus dados de vulnerabilidade e dados de resultados de auditoria serão exibidos juntos nas visualizações do painel. Você pode definir seus filtros para filtrar os dados de CSPM.

Há três guias incluídas no painel:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Categoria do ativo
- Correção
- Aprovações

2. Clique em uma guia para exibir os dados.
3. As fontes autorizadas incluídas nos dados são listadas abaixo das visualizações de dados.

Criar uma política personalizada para AWS no CSPM

Crie uma política para implementar seus padrões de conformidade personalizados.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Gestão de posturas de segurança para nuvem** > **Políticas de configuração**.
2. Selecione **Novo**.
3. No formulário, preencha os campos.

Formulário de criação de política personalizada de CSPM

Campo	Descrição		
Nome da política	Nome exclusivo da política.		
Descrição	Detalhes da política.		
Tipo de recurso			
Provedor de Nuvem	Plataforma de fornecimento de nuvem para a política.		
Tipo de recurso	Tipo de recurso no ambiente de nuvem. Se o tipo de recurso não estiver lá, crie um tipo de recurso usando as convenções da AWS ou do Azure.		
Condição da política			
Tipo			
Condição	Condição para criar um resultado de teste. Considere os seguintes cenários:		
	Chave de configuração presente?	Tipo de recurso presente?	Próximas etapas
	Sim	Sim, o tipo de recurso e os fluxos para recuperar os metadados estão presentes. Exemplo de um subfluxo: CSPM: Azure Subscription Resource Collector.	Especifique as condições da política.
	Não	Sim	a. Crie uma chave de configuração . b. Crie um coletor de recursos .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição		
			c. Crie um coletor de configuração . **d.** Especifique as condições da política.
Gravidade	Severidade da política.		

4. Selecione **Enviar** para criar a política personalizada.

Cloud Security Posture Management com Microsoft Azure

A aplicação Cloud Security Posture Management (CSPM) desenvolvida por ServiceNow® verifica continuamente seu ambiente de nuvem para identificar qualquer não conformidade ou violação de configuração em relação a estruturas de conformidade, como o CIS.

Principais termos e conceitos

Esta integração de CSPM desenvolvida por ServiceNow oferece suporte a CIS Microsoft Azure. A integração coleta os dados de configuração de ativos de nuvem em seu ambiente Microsoft Azure diretamente da nuvem, os importa para sua instância Now Platform® e audita seus ativos para conformidade.

Os termos a seguir são fornecidos para ajudar você a entender os conceitos desta integração de CSPM. Para obter mais informações sobre os produtos Azure, consulte Azure.com .

Região

As regiões se referem a áreas geográficas compatíveis com seus serviços em nuvem Microsoft Azure. As regiões têm endpoints padrão que permitem acessar os serviços compatíveis com essa região. Exemplos de regiões podem ser Virgínia ou Utah nos Estados Unidos ou outros locais de DATACENTER fora dos EUA.

Recurso

Recurso é um termo usado no ambiente Microsoft Azure que descreve os ativos Microsoft Azure e suas definições de configuração. Recursos são os serviços em seus ambientes Microsoft Azure. Máquinas virtuais, contas de armazenamento, aplicativos Web, bancos de dados e redes virtuais são exemplos de recursos comuns. Em sua instância Now Platform, os recursos são chamados de ativos ou itens de configuração (ICs).

Grupos de recursos

Os recursos em suas contas Microsoft Azure podem ser organizados em grupos de recursos. Os grupos contêm recursos relacionados a uma solução Microsoft Azure ou produto específico. Os recursos em um grupo de recursos podem estar localizados em diferentes regiões e podem estar localizados em uma região fora do próprio grupo. O grupo de recursos armazena metadados sobre seus recursos. Ao especificar um local para o grupo de recursos, você está especificando onde esses metadados são armazenados. Para conformidade, você deve saber que seus dados são armazenados em uma região específica.

Centro de Segurança na Internet (CIS)

O CIS é uma organização sem fins lucrativos orientada pela comunidade que é responsável pelos controles CIS ® e Benchmarks CIS ™, processos reconhecidos globalmente para proteger sistemas e dados de TI. Atualmente,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a aplicação ServiceNow CSPM usa as diretrizes publicadas no Microsoft Azure (CIS Microsoft Azure Foundations Benchmark versão 1.4.0 para auditar a conformidade dos ativos de nuvem.

Automatizado

Este termo se refere às recomendações que resultam de uma auditoria de um ativo ou controle técnico que pode ser totalmente automatizado e validado por um estado de aprovação/reprovação. Esta integração oferece suporte a avaliações automatizadas.

Política (políticas de configuração)

Políticas são diretrizes de governança. No Now Platform, as políticas são chamadas de Políticas de configuração. A aplicação CSPM desenvolvida por ServiceNow fornece políticas de configuração de linha de base para avaliar seu ambiente de nuvem em relação aos padrões de parâmetro de comparação, como CIS. Há um mapeamento um para um entre as políticas de configuração e as diretrizes fornecidas nas estruturas de conformidade.

Conjunto de políticas (configuração de grupos de políticas)

Os conjuntos de políticas são grupos de políticas individuais. No Now Platform, os conjuntos de políticas são chamados de Grupos de políticas de configuração.

Gestão de posturas de segurança para nuvem

As políticas (Políticas de**configuração**) e os conjuntos de políticas (**Grupos de políticas de configuração**) estão localizados no módulo **Cloud Security Posture Management** criado em sua instância para esta integração.

Testar

Testes são registros descritores criados para políticas de configuração. Cada política de configuração no módulo CSPM tem um teste de configuração equivalente criado automaticamente no módulo Configuration Compliance. Os testes de configuração são referenciados pelos resultados do teste, ou seja, descobertas de configuração da verificação, para ajudar a identificar o teste ou a política que foi avaliada em um determinado recurso de nuvem.

Resultados de testes

Os resultados de testes (TR) são criados em sua instância quando uma auditoria descobre que um recurso em seu ambiente de nuvem não está em conformidade. Os resultados do teste são armazenados na aplicação Configuration Compliance em seu Now Platform. Esses registros exibem os resultados (aprovação/reprovação) das auditorias executadas em seus recursos.

Grupos de resultado do teste

Os grupos de resultados de testes ajudam a organizar os resultados de testes em grupos lógicos e a priorizar suas tarefas de correção.

Tradução automática

Funções necessárias de Now Platform

Os administradores de segurança com a função sn_vul.cspm_security_admin podem usar este produto. As verificações de conta em nuvem também podem ser configuradas por usuários com a função sn_vul.cspm_cloud_account_admin.

Para obter uma lista completa das funções necessárias para esta integração, consulte .

Fluxo de trabalho

- Os conjuntos de políticas (**Grupos de políticas de configuração**) incluídos com a aplicação definem quais dados você importa.
- Os dados de configuração de recurso importados são armazenados em tabelas temporárias na sua instância Now Platform. Esses dados armazenados são auditados quanto à conformidade com as políticas listadas na Microsoft Azure. . Existem 56 políticas

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

automatizadas compatíveis com esta integração. As políticas manuais e nove das políticas automatizadas não são compatíveis.

- Os resultados das auditorias são criados como Resultados de testes e Grupos de resultados de testes na aplicação Configuration Compliance na sua instância da plataforma.
- Você pode exibir resultados de testes, grupos de resultados de testes e outros dados Configuration Compliance em painéis e em registros na aplicação Configuration Compliance. Gerentes de segurança, gerentes de vulnerabilidade e analistas de vulnerabilidade podem usar esses dados para identificar, priorizar e responder às vulnerabilidades relacionadas à configuração em seus ativos.

Coleta de dados

Para coletar os dados de configuração de nuvem Microsoft Azure em seu ambiente, a ServiceNow chama a API de nuvem Microsoft Azure por meio de um MID Server da sua instância da plataforma NOW. Os dados de configuração dos recursos do Microsoft Azure são recuperados para avaliar as políticas de configuração. Os serviços ou recursos para os quais os dados de configuração são recuperados incluem o seguinte:

- Gestão de identidade e acesso (IAM)
- Armazenamento
- Serviços de banco de dados
- Registro em log e monitoramento
- Rede
- Máquinas virtuais
- Considerações de segurança, como datas de vencimento da chave
- Serviço de app

Exemplos de não conformidade de segurança e configuração em seus dados importados

A lista a seguir inclui alguns exemplos de políticas de configuração avaliadas em Microsoft Azure recursos de nuvem para identificar os recursos fora de conformidade:

- Verifique se o nível de acesso para Armazenamento de Blob está definido como "Privado".
- Verifique se o armazenamento de blob para dados críticos está criptografado.
- Certifique-se de que as chaves de acesso ao armazenamento sejam geradas periodicamente.
- Verifique se a proteção de endpoint para todas as máquinas virtuais (VM) está instalada.
- Verifique se o acesso padrão para contas de armazenamento está definido como "Negar".
- Verifique se "Impor conexão SSL" está definido como "Habilitado" para o servidor de banco de dados MySQL padrão.

Políticas e padrões de parâmetro de comparação

Existem aproximadamente 123 políticas definidas no Microsoft Azure. . 56 dessas políticas ou recomendações estão incluídas na aplicação CSPM por padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instalar e ativar a aplicação CSPM Innovation Lab para Microsoft Azure

As aplicações necessárias para esta integração estão disponíveis no ServiceNow® Store e listadas no link Exibir dependências e licenciamento na página de listagem da aplicação. Algumas aplicações têm dependências que você deve baixar e instalar separadamente.

Antes de Iniciar

Função necessária: administrador para download, instalação e ativação de todas as aplicações.

O administrador atribui as funções Now Platform listadas na etapa 5. Essas funções Now Platform® são necessárias para a aplicação.

Para obter mais informações sobre como baixar e ativar aplicações, consulte os seguintes tópicos:

Procedimento

1. Clique no link fornecido no e-mail recebido para acessar as aplicações desta integração no ServiceNow Store.

   Para exibir as dependências de uma aplicação, na página da aplicação no ServiceNow Store, clique em **Exibir dependências e requisitos de licenciamento** em Dependências e licenciamento.

   Nota:
   A aplicação de gestão de postura de segurança em nuvem para Microsoft Azure está localizada no link do **Laboratório de inovação** de ServiceNow Store. As outras aplicações podem ser encontradas em **Aplicações e soluções**.

2. Instale as aplicações na ordem listada na tabela a seguir:
3. Depois de baixar as aplicações do ServiceNow Store, em sua instância Now Platform, navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
   Localize as aplicações e ative-as na ordem listada na tabela.
4. Clique em **Instalar** para ativá-los.

   Nota:
   Essas aplicações podem levar de duas a três horas para serem instaladas.

Aplicação	Instalar a versão do app e os plug-ins de dependência
Versão da plataforma	San Diego, Tóquio
Vulnerability Response (dependências)	ID do plug-in: com.snc.vul_dep
Configuration Compliance (dependências)	ID do plug-in: com.snc.vulc_dep
CMDB CI Class Models	Instalar CMDB CI Class Models: com.sn_cmdb_ci_class - 1.39.0
Security Support Common	ID do plug-in: com.snc.security_support.common - 13.3.3
Security Integration Framework	ID do plug-in: com.snc.sec.int.framework - 13.2.2
Orquestração de suporte de segurança	ID do plug-in: com.snc.secops.orchestration - 12.3.0
Vulnerability Response (aplicação principal)	ID do plug-in: sn_vul - 17.0.2

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação	Instalar a versão do app e os plug-ins de dependência
Configuration Compliance (aplicação principal)	ID do plug-in: sn_vulc - 14.4.4
Performance Analytics for Vulnerability Response	ID do plug-in: com.snc.vulnerability.analytics - 12.4.4
ServiceNow IntegrationHub Enterprise Pack Installer	ID do plug-in: com.glide.hub.integrations.enterprise
Cloud Provisioning and Governance Core	ID do plug-in: com.snc.cloud.core
Biblioteca de ações na nuvem	ID do plug-in: com.sn.itom.cal - 1.3.6
Cloud Configuration Governance	ID do plug-in: com.sn.itom.ccg - 1.3.7
Pacote de conteúdo CCG	ID do plug-in: com.sn.itom.ccg_cp - 1.3.7
Gestão de posturas de segurança para nuvem	ID do plug-in: com.snc.secops.condor - 1.1.1

Todas as aplicações de dependência que também são instaladas automaticamente junto com uma aplicação são exibidas na caixa de diálogo de instalação da aplicação. No entanto, se você for solicitado a instalar plug-ins de dependência durante a instalação, siga os prompts fornecidos.

Verifique se você tem todas as aplicações e dependências listadas na tabela anterior instaladas e ativadas antes de prosseguir para as próximas etapas.

Uma caixa de diálogo é exibida depois que uma aplicação é ativada com sucesso.

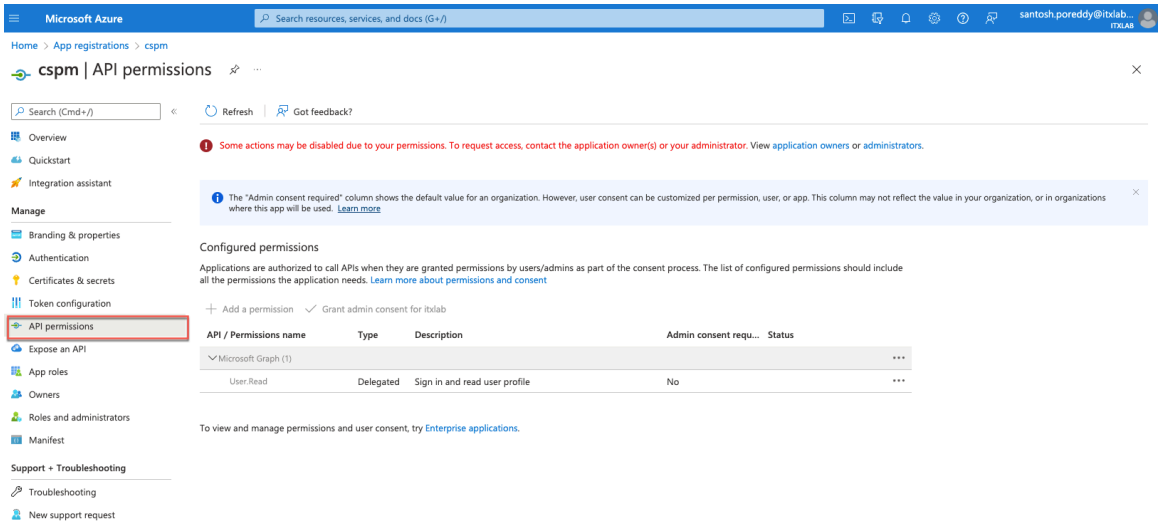
5. Atribua as seguintes funções, se ainda não estiverem atribuídas:
Essas funções são necessárias para várias atividades de fluxo de trabalho na integração.
   - discovery_admin ou sn_cmmp.cloud_admin: configura as contas de serviço em nuvem no Now Platform para as contas de serviço Microsoft Azure correspondentes.
   - cspm_security_admin. Esta função também herda as seguintes funções:
     - sn_itom_ccg.governor: cria políticas, conjuntos de políticas e coletores. A função de administrador executa a "política de teste" e cria entidades usadas pelo administrador de programação.
     - sn_itom_ccg.operator — o operador Cloud Configuration Governance testa as políticas e verifica os resultados. O operador também corrige resultados de testes e grupos de resultados de testes.
     - sn_itom_ccg.scheduling_admin: configura Cloud Configuration Governance para as contas Microsoft Azure. Cria configurações de verificação e programação de verificação. Tem acesso aos resultados da verificação para ver entidades e políticas importadas.
   - cspm_cloud_account_admin. Esta função também herda a função sn_itom_ccg.scheduling_admin.
   - mid_server - configura um MID Server.
   - sn_vulc.admin - configura a aplicação Configuration Compliance, tem visibilidade de todos os registros e pode modificar propriedades. Atribui funções na aplicação Configuration Compliance. Para obter mais informações sobre funções na aplicação Configuration Compliance, consulte Componentes instalados com Configuration Compliance.
   - sn_vuln.admin — configura a aplicação Performance Analytics para Vulnerability Response.

Execute as etapas a seguir para criar um registro de verificação para verificar os ativos em seu ambiente Microsoft Azure.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Em sua conta do Azure, configure políticas com o nível necessário de permissões para fornecer acesso aos recursos Microsoft Azure para Descoberta na nuvem e Provisionamento e governança em nuvem.
   Use a página mostrada na imagem a seguir para criar suas permissões de política. Essas permissões são necessárias para esta aplicação.



   Na aplicação Configuration Compliance, as regras de grupo e de atribuição incluídas na aplicação são desativadas por padrão. Um usuário com o sn_vulc.admin ativa essas regras.

7. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Regras de Grupo**.
8. Clique no **grupo de atribuição, regra de teste** para abrir o registro e defina o campo Ativo como **verdadeiro**.

   Esta regra agrupa os resultados de testes criados durante a auditoria. Todos os resultados de testes de uma determinada política que têm um retorno falso no resultado do teste são agrupados em um grupo de resultados de teste.

   Por padrão, os grupos de resultados de testes são atribuídos ao grupo de usuários de suporte de IC. Esta regra de atribuição está inativa por padrão.

9. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Regras de atribuição**.
10. Clique no registro Atribuir ao grupo de suporte de IC para abri-lo e clique na caixa de seleção **Ativo** para ativá-lo.

    Esta regra atribui os grupos de resultados de testes a usuários no grupo de suporte de IC. Atribua quaisquer usuários a este grupo que você deseja trabalhar nesses resultados de testes.

    Esta regra de atribuição padrão pode não ser útil para atribuir problemas de configuração de nuvem em sua organização, dependendo de suas práticas internas. Você pode preferir criar uma regra de atribuição que atenda aos seus requisitos. Você pode usar metadados da conta de nuvem fazendo referência com pontos na tabela Item descoberto da tabela Resultado de testes para definir regras de atribuição.

Nota:

Para obter mais informações sobre como usar Configuration Compliance, consulte a documentação Configuration Compliance em docs.servicenow.com.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

11. Para exibir os resultados da auditoria nos painéis Performance Analytics para Vulnerability Response, um usuário com a função sn_vuln.admin habilita a aplicação e ativa os coletores de dados.
12. Navegar até **Performance Analytics** > **Coletor de Dados** > **Trabalhos** e localize os trabalhos do coletor diário para verificar se eles estão ativados.
    Você concluiu a configuração da integração. Você está pronto para verificar seu ambiente do Azure usando a aplicação CSPM.

Verificação de contas de nuvem usando a aplicação ServiceNow CSPM

Esta seção descreve como configurar varreduras de segurança para suas contas de nuvem para verificar a conformidade de seus recursos em relação às estruturas de parâmetro de comparação. Um exemplo de política é usado para mostrar esse processo.

Antes de Iniciar

Configuração necessária: este exemplo começa com a criação de um registro de verificação. Se você quiser configurar ou verificar as informações em suas contas de serviço para Microsoft Azure, consulte as etapas de configuração em Instalar e ativar a aplicação CSPM Innovation Lab para Microsoft Azure.

Funções necessárias: sn_vul.cspm_cloud_account_admin

Procedimento

1. Navegar até **Todos** > **Gestão de posturas de segurança para nuvem** > **Administração** > **Verificações de conta de nuvem** para criar um registro de configuração de verificação na aplicação CSPM.
   A página Verificação de conta de nuvem é exibida.
2. Clique em **Nova**.
3. Preencha os campos.
   a. Insira um nome exclusivo para a configuração de verificação.
   b. Insira uma descrição resumida para ajudá-lo a localizar o registro mais tarde.
   c. Selecione **Contas de serviço em nuvem** e selecione as contas de serviço de destino desejadas.
   Você criou esses registros para suas contas Microsoft Azure e os inseriu em Cloud Configuration Governance.
4. Clique na caixa de seleção Verificação em **segundo plano**.
   Isso executará a verificação a cada hora. Se a caixa de seleção não estiver marcada, você deverá iniciar a verificação sob demanda.
5. Navegar até **Todos** > **Configuration Compliance** > **Resultados de testes** > **Todos**.
   A lista de grupos de resultados de testes (CTR#) criada a partir da auditoria de política é exibida.

   Registros de Resultado de testes para seus recursos de Nuvem que estão fora de conformidade são criados. Se as violações forem corrigidas, os registros de resultado de testes serão encerrados.

6. Abra um registro para exibir os seguintes dados:

   Campo de teste

   Este campo exibe o mapeamento um para um entre com a política usada para a auditoria e o registro de teste de auditoria em Configuration Compliance. Clique para visualizar e abrir o registro de teste e exibir as citações, ou seja, a Fonte autorizada. Para este exemplo, a Fonte autorizada é o Microsoft Azure (CIS Microsoft Azure Foundations Benchmark versão 1.4.0 e a seção citada, ou seja, a política, é 3.1.2 Certifique-se de que a "Versão mínima do TLS" esteja definida como "Versão 1.2" (Automatizado).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Cada grupo de política ao qual esta política pertence é exibido. Uma política pode estar em mais de um grupo de políticas. Além disso, o número de resultados de testes gerados pela auditoria é exibido.

Campo de Item de configuração

Esses dados se referem a um recurso em Microsoft Azure.

Campo de item descoberto

Um item descoberto em seu Now Platform está associado ao recurso Microsoft Azure. Todos os metadados de nuvem importados sobre o recurso Microsoft Azure, como região, conta de nuvem e tipo de recurso, por exemplo, são armazenados no registro de item descoberto.

Guia Grupos de resultados de testes

Por padrão, a aplicação Configuration Compliance agrupa os resultados de testes em grupos de resultados de testes com base em um retorno `false` na auditoria. Somente um registro por resultado de teste é criado para um recurso e é atualizado após as importações de dados. Se a definição de configuração for alterada para um recurso em seu ambiente Microsoft Azure entre as verificações, o registro será atualizado em sua instância Now Platform.

7. Para verificar os dados importados, você pode voltar para a conta de usuário Microsoft Azure.

Neste exemplo, uma verificação nesta conta indica que a versão mínima do TLS é 1.0. Este status corresponde aos dados de segurança importados sobre os recursos e grupos de recursos da Nuvem. Depois que você mudar a configuração e o recurso estiver em conformidade, suas mudanças serão refletidas na próxima importação de dados. No exemplo a seguir, a versão mínima do TLS deve ser atualizada para este recurso antes que seu registro de resultado de teste seja fechado.

Exibir dados de auditoria do Azure CSPM no Performance Analytics para painéis do Vulnerability Response

Esta integração inclui painéis na aplicação Performance Analytics para Vulnerability Response.

Antes de Iniciar

Função necessária: pa_viewer

Procedimento

1. Para exibir o painel, navegue até **Configuration Compliance** > **Visão geral**.

Os dados dos painéis são coletados diariamente. Para modificar as configurações, navegue até **Performance Analytics** > **Coletor de Dados** > **Trabalhos**.

Nota:
Se você estiver executando outras integrações de vulnerabilidade de terceiros, todos os seus dados de vulnerabilidade e dados de resultados de auditoria serão exibidos juntos nas visualizações do painel. Você pode definir seus filtros para filtrar os dados de CSPM.

Há três guias incluídas no painel:

- Categoria do ativo
- Correção
- Aprovações

2. Clique em uma guia para exibir os dados.
3. As fontes autorizadas incluídas nos dados são listadas abaixo das visualizações de dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar uma política personalizada para o Azure no CSPM

Crie uma política para implementar seus padrões de conformidade personalizados.

Antes de Iniciar

Função necessária: sn_sec_cspm.cspm_security_admin

Procedimento

1. Navegar até **Todos** > **Gestão de posturas de segurança para nuvem** > **Políticas de configuração**.
2. Selecione **Novo**.
3. No formulário, preencha os campos.

Formulário de criação de política personalizada de CSPM

Campo	Descrição		
Nome da política	Nome exclusivo da política.		
Descrição	Detalhes da política.		
Tipo de recurso			
Provedor de Nuvem	Plataforma de fornecimento de nuvem para a política.		
Tipo de recurso	Tipo de recurso no ambiente de nuvem. Se o tipo de recurso não estiver lá, crie um tipo de recurso usando as convenções da AWS ou do Azure.		
Condição da política			
Tipo			
Condição	Condição para criar um resultado de teste. Considere os seguintes cenários:		
	Chave de configuração presente?	Tipo de recurso presente?	Próximas etapas
	Sim	Sim, o tipo de recurso e os fluxos para recuperar os metadados estão presentes. Exemplo de um subfluxo: CSPM: Azure Subscription Resource Collector.	Especifique as condições da política.
	Não	Sim	**a.** Crie uma chave de configuração . **b.** Crie um coletor de recursos . **c.** Crie um coletor de configuração . **d.** Especifique as condições da política.
Gravidade	Severidade da política.		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

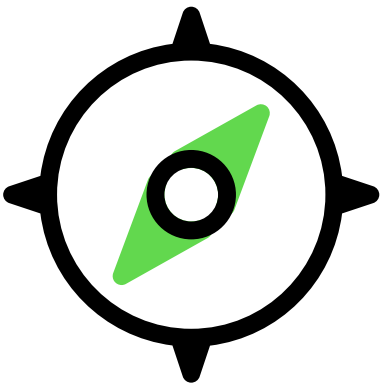
4. Selecione **Enviar** para criar a política personalizada.

Vulnerability Response

O banco de dados nacional de vulnerabilidades (NVD) e outras fontes coletam informações sobre vulnerabilidades conhecidas. Essas vulnerabilidades podem incluir pontos fracos no software, sistemas operacionais que o malware pode explorar e outros ataques. A aplicação ServiceNow® Vulnerability Response ajuda a rastrear, priorizar e resolver essas vulnerabilidades.

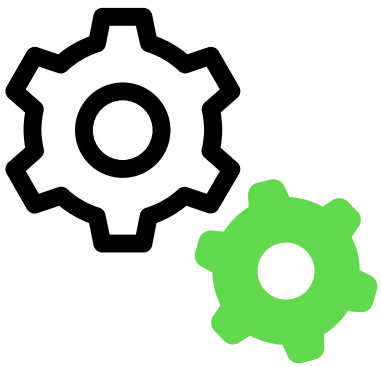
Vulnerability Response

Explorar



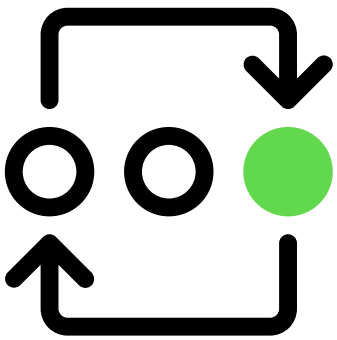
Saiba mais sobre os recursos do Vulnerability Response

Instalar e configurar



Instalar e configurar sua aplicação Vulnerability Response

Integrar

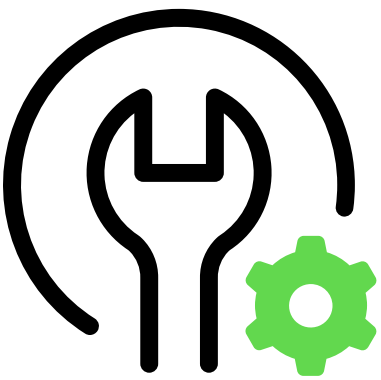


Estenda o Vulnerability Response integrando-o a outras aplicações

Explorar e usar os Espaços do Vulnerability Response

Saiba como usar o Vulnerability Manager e o IT Remediation Workspaces

Corrigir



Use os recursos do Vulnerability Response para corrigir suas vulnerabilidades e proteger seus ativos

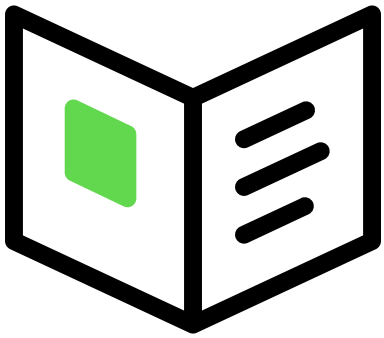
Análise e relatório

Monitorar o andamento da correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Referência



Obtenha mais detalhes sobre notas de versão do Vulnerability Response, componentes e informações de referência sobre campos, tabelas e propriedades

Tradução automática

Explorando a aplicação Vulnerability Response

A aplicação ServiceNow® Vulnerability Response importa e agrupa automaticamente itens vulneráveis de acordo com regras que permitem corrigir vulnerabilidades rapidamente. Os dados de vulnerabilidade são extraídos de fontes externas, como o National Vulnerability Database (NVD) e integrações de terceiros, e processados com aplicações desenvolvidas por ServiceNow®.

Assista a uma visão geral sobre a resposta de vulnerabilidade que define itens vulneráveis, tarefas de correção e seus ciclos de vida.

Visão geral da resposta de vulnerabilidade típica em uma empresa versus a resposta de vulnerabilidade com a ServiceNow e define itens vulneráveis, grupos de vulnerabilidades e seus ciclos de vida.

Vulnerability Response e seu ambiente empresarial

Normalmente, em um ambiente empresarial, as organizações usam scanners de vulnerabilidade e ferramentas de avaliação para identificar e gerenciar os riscos que as vulnerabilidades representam para seus ativos. As vulnerabilidades identificadas por essas ferramentas se traduzem em riscos para as equipes de segurança e de TI responsáveis por manter e proteger os ativos de uma organização. Alguns riscos podem incluir, entre outros, os seguintes tipos de vulnerabilidades identificadas:

- Dependência de software desatualizado ou sistemas configurados incorretamente
- Protocolos de rede não seguros
- Dependência de bibliotecas de software de terceiros com falhas

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Higienização de administração do sistema ruim ou inconsistente
- Imagens do sistema de linha de base que não são protegidas

Conforme esses riscos potenciais são expostos, as equipes de segurança e de TI geralmente enfrentam desafios no processamento e manipulação do volume de informações de vulnerabilidade geradas por suas ferramentas de verificação e avaliação. Especificamente, essas equipes se veem sobrecarregadas ao gerenciar um alto volume de vulnerabilidades identificadas e criar esforços de resposta acionáveis para mitigar os possíveis riscos que suas organizações enfrentam.

Você pode identificar esses desafios para sua própria postura de segurança, fazendo as seguintes perguntas:

- Quais vulnerabilidades identificadas devem ser revisadas primeiro?
- O que essas vulnerabilidades identificadas significam para nossa organização?
- Quem deve ser responsável e assumir os riscos identificados?
- Quem deve trabalhar para resolver/mitigar esses riscos?
- Como reduzimos de forma eficaz as vulnerabilidades identificadas com os recursos que temos?
- Quais são os possíveis resultados não intencionais da redução das vulnerabilidades identificadas?
- Qual processo devemos seguir para corrigir vulnerabilidades, rastrear as etapas que realizamos e acompanhar para ter certeza de que nossas ações funcionaram?
- Como saber se estamos progredindo na redução de nossa postura de risco geral?

Vulnerability Response e o Now Platform®

Vulnerability Response é um membro do pacote de aplicações Security Operations. Juntas, essas aplicações conectam a segurança ao seu departamento de TI, aumentam a velocidade e a eficiência de sua resposta e fornecem uma exibição definitiva de sua postura de segurança.

Visão geral do Security Operations

A aplicação ServiceNow Vulnerability Response tem dois objetivos principais:

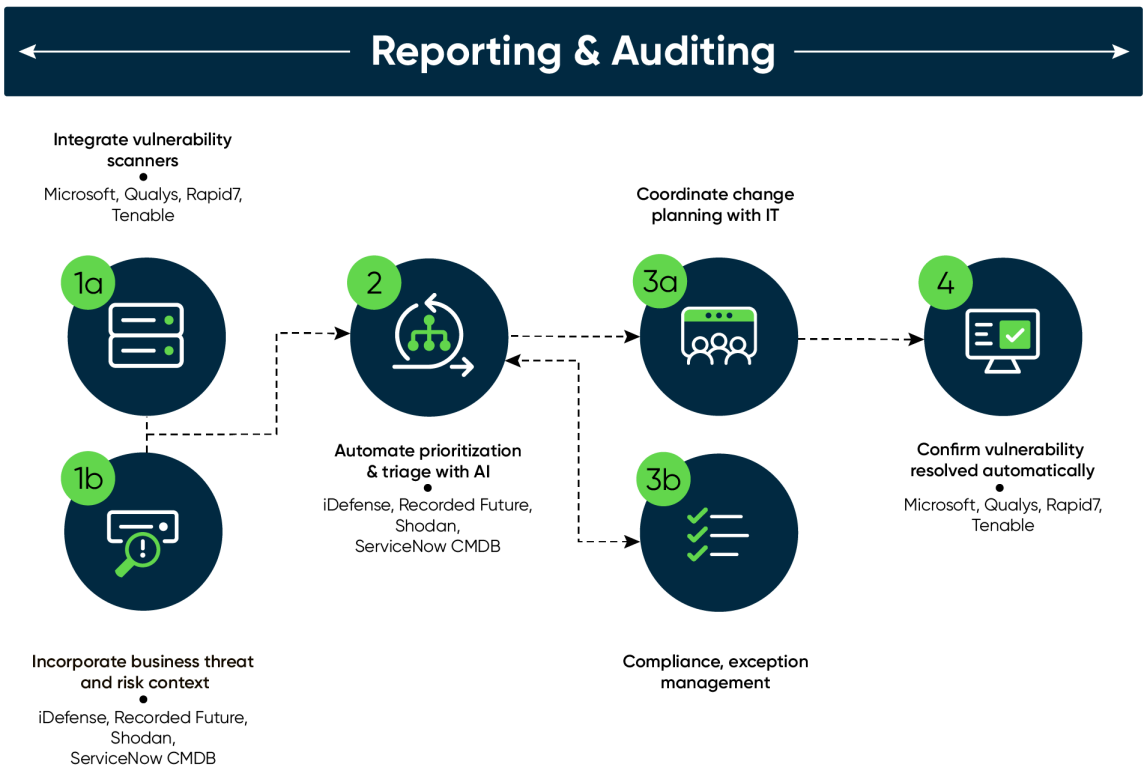
- Ajude as equipes de segurança que precisam lidar com grandes quantidades de dados de vulnerabilidade.
- Ajude as equipes de operações encarregadas de resolver vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Dessa forma, você pode usar a aplicação Vulnerability Response para automatizar o fluxo de informações, desde a integração até a investigação e, em seguida, até a resolução.

O processo de gestão de vulnerabilidades no Now Platform® pode envolver processos, dados, relatórios e automação com o CMDB.



- Integre scanners de terceiros e aplicações ServiceNow® com a aplicação Vulnerability Response para ingerir dados de vulnerabilidade conhecidos.
- Aprimore seus dados de vulnerabilidade ingeridos com exploração, inteligência contra ameaças, risco e contexto de negócios. Use esses dados para ajudá-lo com estratégias de patch e correção.
- As vulnerabilidades importadas do NVD e os dados de detecção de produtos de terceiros são reconciliados com os ativos no seu CMDB. A triagem pode incluir: criar tarefas de correção compostas por vários itens vulneráveis, ou seja, seus ativos que estão determinados a ter vulnerabilidades, agrupar essas tarefas por categoria, priorizá-las e atribuí-las a equipes.
- Empregue mudanças coordenadas e gestão de exceções para ajudá-lo a resolver vulnerabilidades que podem exigir intervenção manual adicional, mais tempo para resolver ou pesquisa extensa.
- Confirme se as vulnerabilidades são resolvidas e atualizadas automaticamente por detecções de seus produtos de verificação.

Quem pode usar Vulnerability Response em sua organização

Vulnerability Response os usuários geralmente se enquadram em duas personas.

- Analista de vulnerabilidade
- Proprietário da correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A persona do analista de vulnerabilidade geralmente é Segurança, Risco e conformidadeou Gestão. Esses usuários monitoram vulnerabilidades e determinam quando iniciar os processos de correção. O analista de vulnerabilidade usa principalmente o Espaço para gerentes de vulnerabilidades e para monitorar e criar tarefas de correção.

A persona do proprietário de correção geralmente faz parte das Operações de TI, DevOps/ Engenharia ou de um responsável pelo serviço. Esses usuários concluem as tarefas de correção necessárias para corrigir vulnerabilidades. Eles podem enviar solicitações de exceção ou mudança se os processos controlados forem necessários para manutenção ou remoção de ativos. O proprietário de correção trabalha principalmente em tarefas de correção de dentro do Espaço de trabalho do proprietário de correção de TI.

Application Vulnerability Response

O recurso Application Vulnerability Response (AVR) da aplicação ServiceNow® Vulnerability Response importa itens vulneráveis da aplicação (AVITs) e, de acordo com as regras, permite corrigir vulnerabilidades da aplicação. Ele está disponível com assinatura separada. Para obter a documentação de Application Vulnerability Response, consulte Explorar o Application Vulnerability Response.

Versões disponíveis

Para obter um glossário de termos e mais referências que incluem links, solução de problemas, artigos de conhecimento, além de dados de campo nos formulários e registros encontrados em Vulnerability Response, consulte Vulnerability Response informações de referência.

Versão de lançamento	Notas de versão
Vulnerability Response v21.0 Vulnerability Response v20.0 Vulnerability Response v19.0 Vulnerability Response v18.2 Vulnerability Response v18.0	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Instalação de Vulnerability Response e aplicações compatíveis

A aplicação Vulnerability Response está disponível no ServiceNow Store. A aplicação oferece suporte a outras aplicações ServiceNow e integrações de terceiros que você também baixa do ServiceNow Store. Mais opções também estão disponíveis para estender a configuração básica.

Tarefas para configuração básica

A aplicação Vulnerability Response é necessária como uma primeira etapa. Para obter mais informações sobre como instalá-lo, consulte Check-list de implementação da aplicação Vulnerability Response e Instalar a aplicação Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Após a conclusão da instalação, você pode Configurar o Vulnerability Response usando o Assistente de configuração.

  Com o Assistente de configuração, atribua usuários e grupos para acesso à aplicação, crie ou edite regras de atribuição, regras de tarefa de correção e datas de destino, configure calculadoras de risco.

- Você também pode selecionar, instalar e configurar uma ou mais integrações de terceiros compatíveis no Assistente de configuração. Essas integrações recuperam dados de vulnerabilidade de sistemas e fornecedores externos. Para obter mais informações sobre como as integrações funcionam e as integrações compatíveis com Vulnerability Response, consulte Integrações do Vulnerability Response.
- Antes de implementar integrações de terceiros, execute a integração do NVD e o trabalho programado do CWE como parte da configuração inicial de Vulnerability Response.

  Consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros e Configurar e executar o trabalho programado para atualizar registros CWE para obter mais informações sobre como instalar, configurar e exibir as bibliotecas NVD e CWE.

- Selecione uma aplicação de análise, quando aplicável. O Pacote de conteúdo do Performance Analytics para a aplicação Vulnerability Response contém relatórios que cobrem todas as fases do ciclo de vida do gerenciamento de vulnerabilidades.

  [Opcional] Instalar e configurar a aplicação Performance Analytics para Vulnerability Response [PA] aplicação.

- Selecione uma aplicação de soluções, quando aplicável. O gerenciamento de soluções ajuda a correlacionar as vulnerabilidades em seu ambiente com as soluções que podem corrigi-las. [Opcional] Instalar a aplicação Solução de gerenciamento do Vulnerability Response.

  Nota:

  - Quando a aplicação Solução de gerenciamento de vulnerabilidade está habilitada, o Integração com a solução Microsoft Security Response Center e o Red Hat Solution Integration ficam disponíveis para edição no Assistente de configuração.

  - Solução de gerenciamento de vulnerabilidade requer uma assinatura separada. Para obter mais informações, consulte Solução de gerenciamento de vulnerabilidade.

- [Opcional] Instale o aplicativo ServiceNow Agent e o Vulnerability Response aplicativo para celular para Experiência de dispositivos móveis Vulnerability Response.

Outras tarefas de configuração que você pode executar

Essas tarefas de configuração adicionais adicionam à sua configuração básica e correção de suporte com opções para relatórios, notificações por e-mail, configuração de integração nativa e trabalho com itens vulneráveis. A maioria dessas tarefas é realizada fora do Assistente de configuração. Consulte Tarefas adicionais Vulnerability Response de instalação e configuração.

Tarefas avançadas fora da configuração básica

Essas tarefas de configuração opcionais são realizadas fora do Assistente de configuração e exigem codificação ou conhecimento avançado ServiceNow e não são consideradas parte da configuração básica. Consulte Tarefas de configuração avançadas Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerability Response personas e funções granulares

Antes de corrigir vulnerabilidades com sucesso com a aplicação Vulnerability Response, você deve atribuir personas e funções aos usuários e grupos no Assistente de configuração.

Uma das primeiras etapas de configuração necessárias para a aplicação Vulnerability Response é atribuir funções a usuários e grupos. As funções definem o que os usuários e grupos podem ver e fazer em Vulnerability Response, Performance Analytics para Vulnerability Responsee todas as integrações de terceiros com Vulnerability Response.

Você atribui funções de persona a usuários e grupos existentes no Assistente de configuração. Consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração.

Nota:

Se você for um cliente de atualização, poderá continuar usando suas funções existentes para a aplicação Vulnerability Response. O acesso para usuários e grupos atribuídos com as permissões sn_vul.vulnerability_read e sn_vul.vulnerability_write e o proprietário de correção antes da v10.3 não foi alterado.

No entanto, para obter mais controle sobre o que usuários e grupos podem fazer e ver na aplicação Vulnerability Response no nível da tarefa, talvez você prefira usar funções granulares. Para obter mais informações, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Se você já atribuiu funções usando o Assistente de configuração e deseja gerenciar atribuições de função granulares para todos os usuários e grupos do módulo Administração de usuários, consulte Gerenciar persona e funções granulares para Vulnerability Response para obter mais informações.

Funções de persona e funções granulares iniciando

Termos-chave.

Função

As funções definem o que os usuários e grupos podem ver e fazer na aplicação Vulnerability Response.

Grupo

Um conjunto de usuários que compartilham determinadas funções e uma finalidade comum.

Função de persona

Uma função pré-configurada na aplicação que é composta por várias funções granulares. As funções de persona em Assistente de configuração, Administrador de vulnerabilidades, Analista de vulnerabilidades, Proprietário de correção, Gerenciador de itens de configuração e Gerenciador de exceções foram projetadas para corresponder a cargos comuns para gerentes, analistas e responsáveis pelo serviço em uma organização de TI ou grupo de correção de vulnerabilidades.

Funções herdadas

Um termo que descreve as funções que os usuários adquirem automaticamente quando outras funções são atribuídas a eles. Por exemplo, todos os usuários ou grupos atribuídos com a função de persona sn_vul.remediation_owner também herdam as funções granulares sn_vul.read_assigned, sn_vul.write_assigned.

Lista de controle de acesso (ACL)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As listas de controle de acesso restringem o acesso aos dados, exigindo que os usuários passem por um conjunto de requisitos antes que possam interagir com eles.

A partir de Vulnerability Response v16.5, para proteger os relatórios contra exposição, defina as **ACLs All report_view** como *active=true*. Essa ACL garante que os dados protegidos estejam disponíveis somente para usuários autorizados.

Você atribui grupos e usuários a funções de persona no Assistente de configuração.

Nota:
No Assistente de configuração, a função de administrador do sistema (admin) é necessária para as tarefas na primeira seção, atribuindo funções e instalando integrações. Depois de atribuir funções de persona no Assistente de configuração e instalar integrações, talvez você prefira atribuir um usuário ou grupo com a função sn_vul.vulnerability_admin para concluir todas as tarefas restantes no Assistente de configuração e gerenciar a aplicação Vulnerability Response.

A tabela a seguir lista Vulnerability Response funções de persona instaladas com a aplicação.

Funções de persona para Vulnerability Response	Descrição
Atribua sn_vul.vulnerability_admin - Vulnerability Admin a usuários ou grupos.	Usuários com esta função têm acesso completo à aplicação Vulnerability Response (VR) e seus registros. Usuários com esta função configuram todas as aplicações e regras de VR e instalam integrações de terceiros.
Atribua sn_vul.vulnerability_analyst - Analista de vulnerabilidade a usuários e grupos.	Usuários e grupos com esta função exibem e atualizam todos os registros para correção de IV.
Atribua sn_vul.remediation_owner - Proprietário da correção a usuários e grupos.	Usuários e grupos com esta função corrigem vulnerabilidades atribuídas a eles ou a um grupo ao qual pertencem. Grupos ou usuários com esta função exibem e atualizam os registros atribuídos a eles ou a um grupo ao qual pertencem.
Atribua sn_vul.ci_manager a usuários e grupos.	Usuários e grupos com esta função gerenciam a reclassificação de itens de configuração (ICs) incompatíveis que não são encontrados no Configuration Management Database (CMDB).
Atribua acesso de leitura a áreas específicas na aplicação por tarefa.	Por exemplo, atribua sn_vul.read_all para que um usuário possa exibir todos os registros de VR. Para obter acesso de leitura para exibir regras de tarefa de correção, atribua sn_vul.read_group_rules. Usuários e grupos com esta função não atualizam registros.

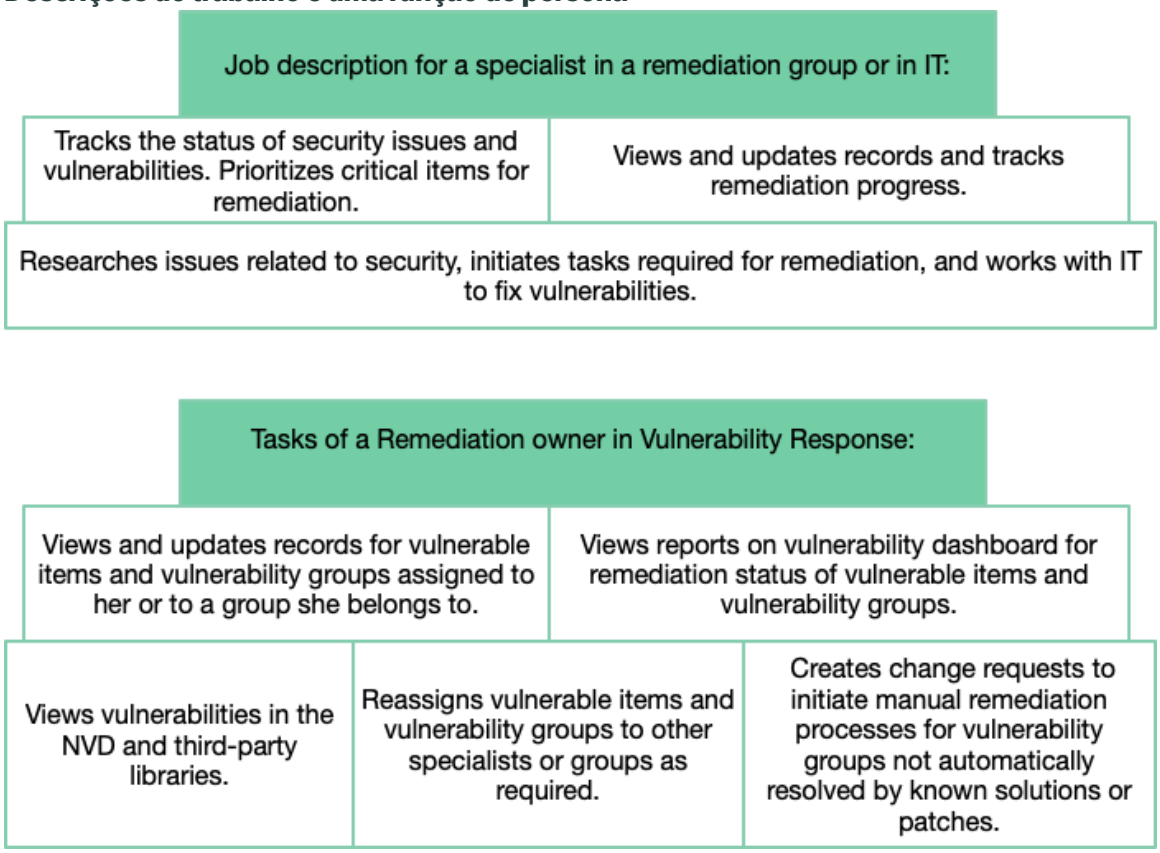
Funções granulares e funções de persona

Uma maneira de pensar sobre as funções de persona é considerar como suas descrições podem se relacionar às descrições de trabalho de várias posições de TI ou de correção de vulnerabilidades em sua organização. A figura a seguir ilustra uma possível descrição de trabalho para um especialista de correção em TI e como as tarefas associadas a este trabalho se relacionam com as tarefas de uma função de persona de proprietário de correção na aplicação Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Descrições do trabalho e uma função de persona



A descrição do trabalho e a função de persona do proprietário de correção podem ser definidas como uma série de tarefas de correção. Na imagem anterior, uma descrição do trabalho e uma função de persona em blocos verdes estão sobre as tarefas que os descrevem. Neste exemplo, alguns dos requisitos de trabalho típicos de um especialista em um grupo de correção correspondem diretamente às tarefas que compõem a persona do proprietário de correção em Vulnerability Response: revisar e atualizar registros, rastrear o status de correção de vulnerabilidades, priorizar itens para correção, e aplique correções e patches com a TI.

Às vezes, no entanto, os trabalhos em sua organização podem não corresponder diretamente às tarefas que compõem uma das cinco funções de persona na aplicação Vulnerability Response. Por vários motivos, como a proteção de dados confidenciais ou a conformidade com as regulamentações, você deve limitar o acesso amplo que algumas das funções de persona fornecem aos usuários e grupos. Ou, inversamente, você deve fornecer aos usuários e grupos mais acesso para que eles possam realizar seus trabalhos. Usando funções granulares, você pode personalizar facilmente as funções e controlar o acesso de usuários e grupos a Vulnerability Response, Performance Analytics para Vulnerability Responsee integrações de terceiros.

As funções granulares definem as tarefas

Os nomes das funções granulares em Vulnerability Response geralmente descrevem o que os usuários podem fazer e ver na aplicação Vulnerability Response. Por exemplo, na imagem anterior, os usuários e grupos com a persona do proprietário de correção atribuída têm as funções granulares sn_vul.read_assigned e sn_vul.write_assigned. Essas funções granulares permitem que usuários ou grupos exibam e atualizem itens vulneráveis e registros de tarefa de correção que são atribuídos a eles. Para exibir descrições de funções granulares específicas, como um usuário com a função de administrador do sistema, navegue até **Administração de usuários** > **Funções** e localize a função desejada. As funções que são

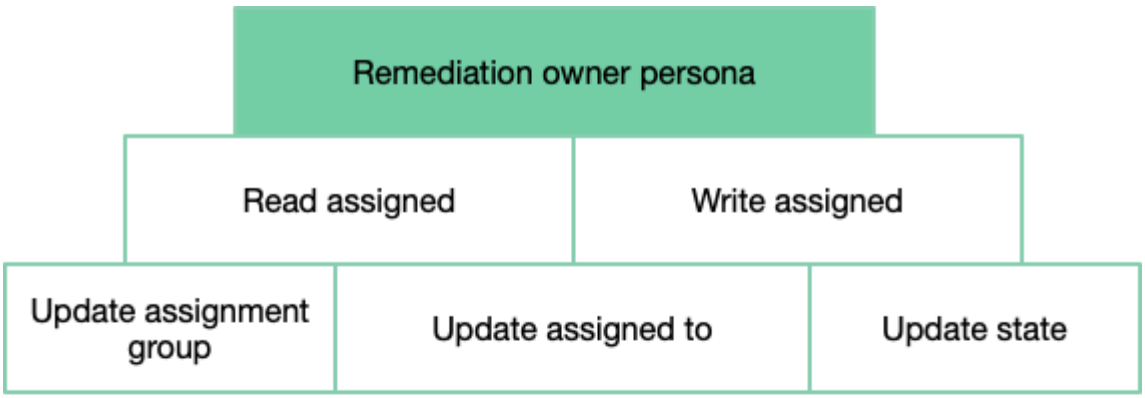
Tradução automática

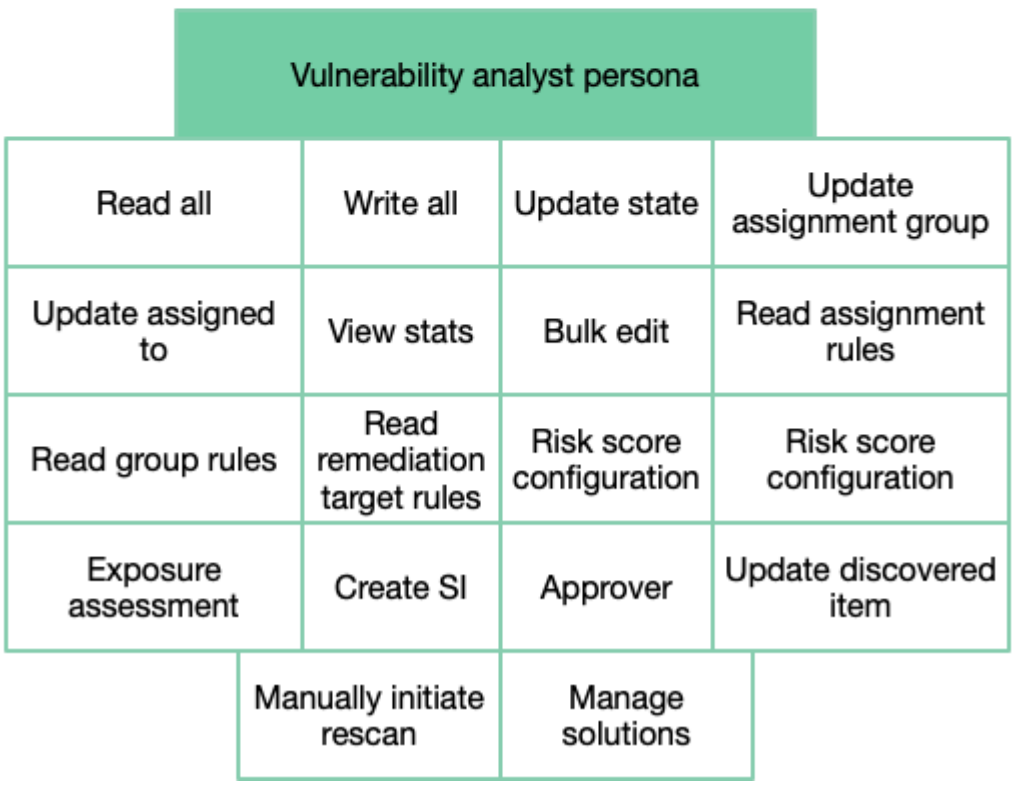
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

herdadas automaticamente quando uma função é atribuída são listadas. Além disso, quando uma função depende de outras atribuições de função, todas as funções necessárias também são listadas.

Na imagem a seguir, as funções granulares da função de persona do proprietário de correção e da persona de analista de vulnerabilidade são ilustradas. Observe que a persona do proprietário de correção não inclui as permissões read_all e write_all da persona do analista de vulnerabilidade. As funções granulares, read_all e write_all, são necessárias para que os usuários e grupos possam ler e editar todos os registros de tarefa de correção e item vulnerável. Para personalizar essas funções, basta adicionar ou remover funções granulares para expandir ou limitar o acesso.

Funções granulares e as personas do responsável pela correção e do analista de vulnerabilidade





Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você quiser que seus usuários e grupos tenham mais acesso do que as funções de persona permitem, você pode adicionar funções mais granulares a usuários e grupos. Por outro lado, se você quiser limitar o acesso de usuários e grupos específicos no nível da tarefa, poderá remover funções granulares.

Nota:
Para atribuir e editar funções granulares no módulo Administração de usuários, a função de administrador do sistema é necessária.

Funções granulares no módulo Administração de usuários

Para obter um exemplo de como gerenciar funções granulares para um usuário ou grupo, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Para atribuir funções de persona, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração.

Vulnerability Response visão geral de regras de atribuição

Defina os critérios pelos quais os itens vulneráveis (IVs) são atribuídos automaticamente a um grupo de atribuição para correção.

Uma regra de atribuição padrão, **Atribuir ao grupo de suporte de IC**, está incluída no sistema de base que atribui itens vulneráveis **ao Grupo de suporte de IC**. A regra Atribuir ao grupo de suporte de IC atribui um IV a qualquer grupo de suporte definido para o item de configuração (IC) associado ao IV.

Nota:
As regras de atribuição não reavaliam as atribuições criadas manualmente.

O tipo de atribuição, seja **Manual** ou **Regra**, está disponível no formulário IV e na exibição de lista. Qualquer IV que foi originalmente atribuído por uma regra, mas posteriormente reatribuído manualmente, contém uma referência à regra original.

Use as informações de Regra de atribuição e Tipo de atribuição para identificar casos em que as regras de atribuição não encontraram uma correspondência correta para o destinatário pretendido. Você também pode usar as informações para identificar quais regras tiveram mais reatribuições.

Os grupos de atribuição definidos pelas Regras de atribuição são usados pelas **Regras de tarefa** de correção para atribuir proprietários a tarefas de correção (VULs).

Nota:
Para disponibilizar Rapid7 InsightVM etiquetas do ativo para uso no filtro de condição para regras de atribuição, você deve executar a integração Rapid7 InsightVM Lista de ativos antes das outras integrações Rapid7 InsightVM.

A diferenciação de maiúsculas e minúsculas para o texto de pesquisa inserido no construtor de condição não é compatível com este registro ou formulário.

Atribuir itens vulneráveis automaticamente

Existem três maneiras diferentes de atribuir itens vulneráveis usando **Atribuir usando**:

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Grupode usuários : esta opção permite selecionar qualquer um dos grupos de usuários Now Platform® existentes.
- Campo de grupo deusuários : esta opção permite escolher qualquer campo de grupo de atribuição disponível usando a tabela cmdb_ci. Por padrão, você vê os três campos de grupo a seguir:
  - Nenhum: indica que não há valor padrão para este campo obrigatório
  - Item de configuração: grupo de aprovação
  - Item de configuração: grupo de atribuição
  - Item de configuração: grupo de suporte
- Script: esta opção permite definir as condições usando um script. Esta opção requer codificação ou conhecimento avançado ServiceNow.

Execute regras de alta prioridade (itens que precisam de tratamento especial, onde o risco é crítico ou um IV deve ser tratado pela conformidade regulatória) primeiro. Em seguida, execute suas regras gerais, onde nenhum tratamento especial é necessário, e você saberá quem deve ser responsável por elas. Por fim, crie uma regra padrão para atribuir IVs ao grupo que descobrirá a qual grupo de atribuição ele deve pertencer. Este grupo pode adicionar outra regra para cobrir suas decisões. Esta regra padrão seria executada por último.

Processo de avaliação da regra de atribuição

As regras de atribuição são usadas para avaliar e atribuir um IV quando um novo IV é aberto, ou seja, importado, criado manualmente ou reaberto. A menos que você reaplicar manualmente as regras de atribuição após o IV ou seu estado mudar, um IV será avaliado uma vez.

O processo a seguir é usado para cada IV novo, atualizado ou reaberto:

- Para cada regra de atribuição de vulnerabilidade, o IV é comparado ao filtro de atribuição, a regra de ordem mais baixa primeiro.
- Quando a condição corresponde, o IV é atribuído a um grupo de atribuição. A pesquisa é interrompida.
- Quando as condições não encontrarem uma correspondência entre todas as outras regras, o IV será atribuído ao grupo de atribuição padrão, se houver uma regra padrão.

  Depois que o item vulnerável tiver sido atribuído, a regra de tarefa de correção apropriada usará a atribuição como um dos critérios para colocar os itens vulneráveis em uma tarefa de correção. Para obter mais informações, consulte Vulnerability Response tarefas de correção e regras de tarefa visão geral e Filtragem em Vulnerability Response.

Nota:
A regra padrão é a regra com o maior valor de ordem de execução. Uma regra final a ser usada que é um bom contato alternativo é active=true. Se não houver regra padrão, o IV permanecerá não atribuído quando a regra de tarefa de correção fizer a atribuição.

Reaplicar regras de atribuição

Ao alterar uma regra de atribuição, use o botão **Aplicar mudanças** na página da lista Regras de atribuição para executar novamente todas as regras alteradas em todos os IVs abertos ativos, exceto aqueles que foram atribuídos manualmente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Se o trabalho programado *Reapply all vulnerability assignment rules* não tiver sido executado antes da primeira vez em que você usa **Aplicar mudanças**, ele executará todas as regras de atribuição em todos os IVs abertos, exceto os IVs que foram atribuídos manualmente. Depois disso, todos os usos subsequentes de **Aplicar mudanças** executam novamente somente as regras alteradas e todas as regras dependentes. Mudanças em uma regra podem resultar em um IV correspondendo a uma regra não modificada diferente. A reaplicação das regras de atribuição não reagrupa os itens vulneráveis.

O trabalho programado [*Reapply all vulnerability assignment rules*] está inativo por padrão. Quando ativado, ele aplica todas as regras a todos os IVs abertos, exceto aqueles atribuídos manualmente. Ele pode ser executado **diariamente**, **semanalmente**, **mensalmente**, **periodicamente**, **uma vez**ou **sob demanda**. Dependendo de quantos IVs ativos você tem em seu ambiente, lembre-se de definir o campo **Executar** corretamente após a execução inicial para evitar impactos no desempenho.

Os clientes de atualização devem consultar as Notas de versão de VR para obter informações sobre o impacto deste recurso nos IVs existentes.

Quando um grupo de atribuição em uma regra de atribuição muda, os itens vulneráveis podem ser reavaliados e reagrupados automaticamente, habilitando a propriedade do sistema sn_vul.rerun_task_rules e o link da regra de negócio para tarefas de correção.

Para habilitar a propriedade do sistema:

1. Navegar até **Todos** > **Propriedades do sistema** > **Todas as Propriedades**.
2. Abra a propriedade do sistema sn_vul.rerun_task_rules.
3. No campo **Valor**, defina o valor como verdadeiro.

Quando a propriedade do sistema é definida como verdadeira e as regras de atribuição são reaplicadas, os itens vulneráveis são desvinculados das tarefas de correção, onde a condição não corresponde mais.

Nota:
Por padrão, a propriedade do sistema sn_vul.rerun_task_rules é definida como falsa.

Para automatizar o reagrupamento de itens vulneráveis, você deve ativar a regra de negócio Vincular tarefas de correção.

Para habilitar a regra de negócio:

1. Navegar até **Todos** > **Definição do Sistema** > **Regras de negócios**.
2. Abra a regra de negócio Link para Tarefas de correção.
3. Marque a caixa de seleção **Ativa** para ativar a regra de negócios.

A regra de negócios ao ser habilitada reagrupa os itens vulneráveis, movendo-os para o grupo relevante ou criando um grupo se eles não puderem ser agrupados em qualquer grupo existente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Os itens vulneráveis são removidos dos grupos sem excluir os grupos.
- Somente os itens criados usando regras de tarefa de correção ou esforço de correção são removidos.
- O reagrupamento é feito automaticamente somente quando o grupo de atribuição muda como parte de uma regra de atribuição e não quando é alterado manualmente.

O reagrupamento em espaços é realizado para tarefas de correção, que são criadas a partir de um esforço de correção.

Vulnerability Response tarefas de correção e regras de tarefa visão geral

Configure tarefas de correção (VULs) para ajudar analistas e especialistas em correção a organizar itens vulneráveis (IV) e analisá-los em massa. Os critérios pelos quais os grupos são formados são configurados para que você não precise atribuir manualmente itens vulneráveis em grupos. Usando tarefas de correção, você pode monitorar o andamento e conduzir o processo de correção com mais eficiência.

Contagens de adiamento de rastreamento para itens vulneráveis e tarefas de correção

Rastreie o número de vezes que um item vulnerável, um item vulnerável da aplicação, um item vulnerável de contêiner ou uma tarefa de correção é adiado. Um trabalho programado, **definir contagens de adiamento**, é executado diariamente para publicar contagens dos registros que são adiados mais de uma vez na coluna Contagem de adiamento. Os registros são exibidos nos módulos Vários adiamentos para VR, AVR e CVR.

Atualizando itens vulneráveis automaticamente

Nota:
A automação de atualização de item vulnerável se aplica somente a grupos criados usando o filtro de condição ou o grupo de filtros. A automação não se aplica a IVs que foram adicionados manualmente ou agrupados usando Regras de tarefa de correção.

Quando a caixa de seleção **Atualizar itens vulneráveis** automaticamente está marcada, novos IVs que correspondem aos critérios de filtro da tarefa de correção são adicionados automaticamente à tarefa. Itens vulneráveis na tarefa de correção que não correspondem mais aos critérios de filtro são removidos automaticamente da tarefa.

Por padrão, quando a tarefa de correção sai do estado **Aberto**, a caixa de seleção é desmarcada. Se você quiser que os itens vulneráveis continuem sendo adicionados à tarefa de correção, independentemente do estado, desabilite a regra de negócios *`Set auto refresh vulnerable items`*.

Você pode marcar a caixa de seleção novamente manualmente no estado Sob investigação. **A opção Atualizar itens vulneráveis automaticamente** não é desabilitada quando a tarefa de correção passa para o estado **Aguardando implementação**. Uma vez no estado Aguardando implementação, nenhum novo item vulnerável pode ser adicionado à tarefa existente, nem itens vulneráveis existentes podem ser removidos dela.

Nota:
Quando uma tarefa de correção é criada manualmente e os IVs são adicionados usando o filtro **Condição** ou o **Grupo**de filtros, a caixa de seleção é desmarcada. Você tem a opção de marcar a caixa ou não.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atualizando itens vulneráveis manualmente

Para tarefas de correção criadas manualmente com um **grupo de filtros** ou filtro de **condição**, quando você clica no link relacionado **Atualizar** itens vulneráveis associados na página **Tarefa** de correção, todos os itens vulneráveis que correspondem aos critérios de filtro são adicionados. Os itens que não correspondem mais aos critérios são removidos. Esta ação permite uma atualização imediata da lista de itens vulneráveis e é usada com a caixa de seleção **Atualizar item vulnerável automaticamente marcada** ou não.

As tarefas de correção criadas manualmente usando os tipos de filtro **Condição** ou **Grupo** de filtros são atualizadas uma vez por hora.

Noções básicas sobre regras de tarefa de correção

As regras de tarefa de correção permitem definir como os itens vulneráveis são automaticamente agrupados e atribuídos. Uma regra padrão, **Vulnerabilidade**, está incluída no sistema de base que reúne itens vulneráveis com base em suas vulnerabilidades. No entanto, você pode agrupar por qualquer outro conjunto de valores em colunas acessíveis pelo IV. Esses valores podem incluir grupo de suporte de item de configuração (IC), severidade da vulnerabilidade e assim por diante.

Você pode criar qualquer número de condições. Depois de definir um Agrupar por seleção, outra linha será exibida. Você pode ter até seis seleções **de Agrupar por**. Você também pode automatizar a atribuição de grupo. Para obter mais informações, consulte Criar ou editar Vulnerability Response regras de tarefa de correção e Filtragem em Vulnerability Response.

Nota:
Para disponibilizar Rapid7 InsightVM tags de ativo para uso no filtro de condição para Regras de tarefa de correção, você deve executar a integração Rapid7 InsightVM Lista de ativos antes das outras integrações Rapid7 InsightVM.

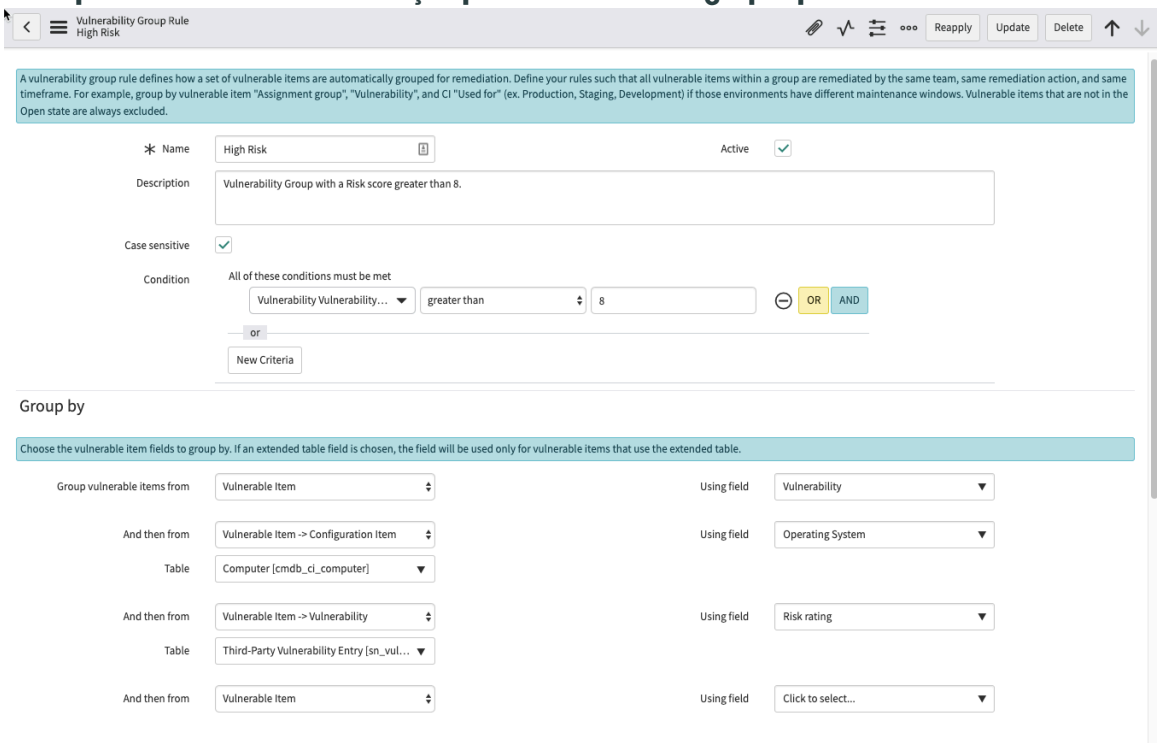
Por exemplo, você pode agrupar seus itens vulneráveis pelo centro de custos do IC vulnerável ou pelo vetor de ataque da vulnerabilidade. Você pode ter uma regra de tarefa para vulnerabilidades de baixa severidade ou ICs de baixo risco. Você pode ter outra regra de tarefa para servidores críticos e vulnerabilidades com explorações - itens vulneráveis que expõem a empresa a mais riscos.

Um conjunto diferente de regras pode ser usado para itens vulneráveis que expõem a empresa a mais riscos. O nome da tarefa de correção é anexado à regra de tarefa de correção **Agrupar por** valores para fazer a descrição resumida do novo registro. Consulte Criar um grupo do Vulnerability Response para obter mais informações sobre os campos disponíveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de construtor de condição para entradas de Agrupar por



Quando um novo item vulnerável é criado, importado ou reaberto após ser fechado, as regras de vulnerabilidade são avaliadas em relação a ele. Um IV é avaliado apenas uma vez, automaticamente, a menos que seja reaberto após ser fechado ou as regras sejam reaplicadas manualmente.

O processo a seguir é usado para cada IV novo ou reaberto:

- Para cada regra de tarefa de correção, o IV é comparado ao filtro de regra de tarefa de correção.
- Para cada regra em que a condição da regra da tarefa de correção corresponde, a regra extrai os dados do **Agrupar por** seleções no IV. Ele cria um nome de grupo e um campo. Nesse caso, **Alto risco: QID-32342:***`resumo de QID-3242`* (Nome: ID da vulnerabilidade: resumo da vulnerabilidade).

  Nota:
  O campo de descrição resumida é limitado a 160 caracteres. Resumos de vulnerabilidade mais longos são truncados.

  A regra verifica se há uma tarefa de correção em **aberto** correspondente que seja atribuída ao mesmo grupo de atribuição que o IV.
  - Se a tarefa for encontrada, o IV será adicionado à tarefa existente no estado **Aberto**.
  - Se nenhuma tarefa no estado **Aberto** for encontrada, a regra criará uma tarefa **de alto risco: QID-32342**, a atribuirá ao mesmo grupo de atribuição que o IV e colocará o IV na tarefa de correção.

Mais de uma regra de tarefa de correção pode ser definida para agrupar diferentes tipos de vulnerabilidades. Como cada vulnerabilidade é comparada com as condições de regra da tarefa de correção antes de colocá-la em um grupo, muitas regras podem afetar o desempenho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por padrão, as regras de tarefa de correção usam o grupo de atribuição definido pelas **Regras de atribuição** no item vulnerável ao agrupar os itens e atribui a tarefa de correção para corresponder aos itens vulneráveis.

Como parte da regra de tarefa padrão, a atribuição dessas tarefas de correção é controlada pelas regras no módulo **Regras de atribuição**. Para obter mais informações sobre regras de atribuição, consulte Vulnerability Response visão geral de regras de atribuição.

Quando uma regra de tarefa é excluída, no formulário ou na exibição de lista, você tem a opção de excluir todas as tarefas **abertas** criadas por essa regra. As tarefas que não estão em **Aberto** são excluídas.

Reaplicar regras de tarefa de correção

Quando você quiser mudar uma regra de tarefa de correção, use o botão **Reaplicar** na página de regra de tarefa de correção para executar novamente a regra alterada em todas as tarefas de correção em **aberto** ativas criadas por essa regra. Ele exclui e recria tarefas de correção com base na regra alterada automaticamente.

Vulnerability Response regras de destino de correção

As regras de destino de correção definem o intervalo de tempo esperado para corrigir itens vulneráveis (IV), assim como os SLAs fornecem um intervalo de tempo para corrigir a própria vulnerabilidade. Por exemplo, se um ativo contiver dados de PCI (dados de cartão de crédito), a vulnerabilidade nesse item precisará ser corrigida em 30 dias de acordo com o PCI DSS.

Os gerentes de vulnerabilidade podem criar regras de destino de correção definindo:

- A meta de correção
- O destino do lembrete
- Os destinatários do lembrete e da notificação - que devem ser notificados quando os itens vulneráveis (IVs) passarem da data de destino do lembrete ou da correção e não forem corrigidos.

Os analistas e gerentes de vulnerabilidade podem ver a data de destino da correção no formulário do item de vulnerabilidade e nas exibições de lista, desde que os itens vulneráveis não estejam no estado **Adiado**, **Resolvido**ou **Encerrado**. As regras de destino de correção serão executadas na importação e serão executadas novamente se um IV for reaberto.

A **data de destino** da correção é codificada por cores na exibição da lista de IVs como pontos, da seguinte forma:

- Itens vulneráveis que não atingiram a data de notificação são mostrados em verde.
- Itens vulneráveis que se aproximam da data de meta de correção são mostrados em laranja.
- Itens vulneráveis após a data de meta de correção são mostrados em vermelho.

Um e-mail de resumo, por regra de destino de correção, é enviado quando um ou mais IVs estão se aproximando da data de destino de correção ou a data de destino de correção passou.

As regras de destino de correção podem ser desativadas ou excluídas

Quando uma regra é desativada, as datas de destino de correção atuais dos IVs aos quais ela foi aplicada são apagadas. Se um IV atender a qualquer regra ativa, essa regra será

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

aplicada, caso contrário, o IV não terá regra ou data de destino e seu status será **Sem meta**.

Quando as regras são excluídas, a data de **destino** da correção e os campos relacionados em IVs encerrados, adiados ou resolvidos são preservados. A data de **destino** da correção e os campos relacionados em IVs não encerrados são limpos e todas as regras dependentes são reaplicadas.

Cenário de regra de destino de correção

Quando várias regras de destino de correção são aplicadas ao mesmo item vulnerável, a regra mais restritiva é aplicada.

Nota:
As metas de correção são calculadas a partir da data da **última abertura** mais o número de dias (medidos como incrementos de 24 horas).

A partir da V17.1, as metas de correção são calculadas a partir da **meta de (data)**. O valor padrão permanece **Data da última abertura**.

Por exemplo, se um item vulnerável atender à condição para duas regras de destino de correção:

Cenário: item vulnerável aberto pela última vez em 01/03/2018 às 10:00:00.

- Regra de destino de correção 1: aberta pela última vez em 03/07/2018; a meta de correção é de 15 dias desde que foi aberta pela última vez; A data de destino da correção calculada é 16/03/2018 10:00:00.
- Regra de destino de correção 2: aberta pela última vez em 10/03/2018; a meta de correção é de 10 dias desde que foi aberta pela última vez; A data de destino da correção calculada é 11/03/2018 10:00:00.

Neste cenário, a Regra de destino de correção 2 se aplica ao item vulnerável, já que ele tem a data mais restritiva. 10 dias desde que o item vulnerável foi identificado pela primeira vez, versus 15 dias.

Nota:
Depois que a Regra de destino de correção for definida, as datas de destino de correção serão calculadas pelo trabalho programado `Evaluate remediation targets` .

Sobre o trabalho programado Avaliar destinos de correção

`Evaluate remediation targets` é executado uma vez às 4:00:00 diariamente.

Ele itera por meio de todas as regras de vulnerabilidade ativas, começando pelas regras com a data de meta de correção mais antiga. Ele analisa todos os itens vulneráveis que:

- Não estejam em um estado **Encerrado**, **Adiado**ou **Resolvido**.
- Não tem data de meta de correção.
- Tenha uma data de destino de correção posterior à data na regra de destino de correção.

`Evaluate remediation targets` adiciona uma data de destino de correção, se não houver uma, ou se uma regra resultar em uma data anterior à do registro, ele atualizará a data de destino existente. Por fim, ele atualiza os campos Destino de **correção** e **Status** da correção no formulário de item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois que o *Evaluate remediation targets* for executado, as notificações disponíveis serão enviadas.

Evaluate remediation targets limpa os campos de correção no IV e para de enviar notificações.

Começando com Vulnerability Response v19.0, a propriedade *sn_sec_cmn.evaluate_targetmissed_records*, quando habilitada, impede que o trabalho programado *Remediation Target Rules*] avalie IVs ausentes. Esta propriedade está habilitada por padrão.

Reaplicar regras de destino de correção

Ao alterar uma regra de destino de correção, use o botão **Aplicar mudanças** na página da lista Regras de destino de correção para executar novamente todas as regras alteradas em todos os IVs abertos ativos, exceto aqueles no estado **Encerrado**, **Adiado** ou **Resolvido**. Dependendo de quantos IVs você tem, isso pode levar algum tempo.

Nota:

Se o trabalho programado, *Evaluate remediation targets* estiver em execução, você não poderá iniciar um processo de reaplicação. No entanto, se um processo de reaplicação já estiver em execução e o trabalho programado que ele acionou, eles serão executados em paralelo.

Os processos de reaplicação em Vulnerability Response e Application Vulnerability Response são independentes e podem ser executados em paralelo.

Tópicos relacionados

Criar ou editar Vulnerability Response regras de destino de correção

Exibir o status da meta de correção de um item vulnerável Vulnerability Response

Criar ou editar notificações de destino de correção

Regras e grupos de classificação de vulnerabilidade

Os grupos de classificação automatizam a classificação de valores de uma tabela com base nas regras de classificação definidas no grupo. A condição de cada regra é avaliada na ordem e a primeira regra correspondente é usada.

O sistema básico do Vulnerability Response inclui os dois grupos de classificação a seguir, que classificam os itens descobertos e as vulnerabilidades, respectivamente:

- Classificação de itens descobertos
- Classificação de entrada de vulnerabilidade

Sempre que vulnerabilidades e itens descobertos são importados, as regras de classificação de vulnerabilidade nos respectivos grupos são executadas. Com base nas condições definidas na regra, os registros são classificados para o grupo de classificação relevante. Você pode criar, editar, excluir ou reaplicar essas regras a uma vulnerabilidade existente.

Nota:

- Para uma tabela selecionada, só pode haver um grupo de classificação ativo.
- Depois de criar um grupo, você não pode excluí-lo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações, consulte Criar e editar uma regra de classificação, Aplicar uma regra a uma vulnerabilidade existente e Desativar ou excluir uma regra de classificação.

Soluções de aprendizado de máquina para Vulnerability Response

Recomendações de atribuição de vulnerabilidade usa ServiceNow® Inteligência preditiva e aprendizado de máquina para recomendar grupos de atribuição para itens vulneráveis (IVs) e tarefas de correção (VULs ou RTs). Você pode reduzir o tempo gasto na identificação dos responsáveis pelas descobertas de vulnerabilidade não atribuídas ou atribuídas incorretamente. Além disso, você pode ver uma pontuação de confiança gerada pelo sistema que avalia se o grupo de atribuição recomendado é adequado para resolver a vulnerabilidade.

Os recursos Inteligência preditiva são usados em Vulnerability Response para fornecer melhores experiências de trabalho, criando e treinando um modelo de definição de solução que pode prever o grupo de atribuição com base nos dados existentes.

Para obter mais informações, consulte Inteligência preditiva .

Recomendações de atribuição de vulnerabilidade

Com a aplicação Recomendações de atribuição de vulnerabilidade (com.snc.vulnerability.recom), o sistema pode atribuir recomendações em Vulnerability Response usando ServiceNow Inteligência preditiva. Este plug-in requer:

- Vulnerability Response (com.snc.vulnerability)
- Inteligência preditiva (com.glide.platform_ml)

Para obter mais informações, consulte Inteligência preditiva .

Pontuações de confiança

Use a aplicação Recomendações de atribuição de vulnerabilidade para gerar a pontuação de confiança que relata o nível de confiança dos grupos de atribuição recomendados para os RTs ou VIs selecionados. A pontuação de confiança avalia se o sistema está confiante de que o grupo de atribuição recomendado é adequado para resolver a vulnerabilidade. São exibidas até 10 recomendações. Essas recomendações são baseadas na maior probabilidade de atribuições bem-sucedidas. A primeira recomendação na lista significa que o sistema tem a maior confiança de que é o grupo de atribuição correto.

Por exemplo, em uma escala de 0 a 100, para cada grupo de atribuição, a pontuação de confiança sugere a probabilidade de um IV ou RT pertencer a esse grupo específico.

Tópicos relacionados

- Predictive Intelligence
- Criar e treinar uma solução de classificação
- Criação e treinamento de uma solução de semelhança
- Criação e treinamento de uma solução de clustering
- Como definir configurações avançadas para suas soluções de ML

Regras de pesquisa de IC para identificar itens de configuração de Vulnerability Response integrações de vulnerabilidade de terceiros

Quando os dados são importados de uma integração de terceiros, o Vulnerability Response usa automaticamente os dados do host para pesquisar correspondências no Configuration

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Management Database (CMDB). Ele faz isso usando **Regras de Pesquisa de IC**. Essas regras são usadas para identificar itens de configuração (ICs) e adicioná-los ao registro de item vulnerável para ajudar na correção.

A partir da versão 19.0, navegue até **Security Operations** > **CMDB** > **Regras de pesquisa** para localizar a lista em sua instância.

Conforme os ativos são importados, uma pesquisa é realizada primeiro na lista de **itens descobertos** usando IDs de terceiros para encontrar correspondências com os itens de configuração (ICs) de importações anteriores. Quando uma correspondência de ID de host é encontrada, ela é usada como o campo **Item de configuração** no registro do item vulnerável.

Você pode ver como os ativos importados são mapeados para ICs usando a lista de **Itens descobertos**. Se uma correspondência não for encontrada ou o campo ID do host estiver vazio, as regras usarão as outras informações do host para tentar identificar corretamente o IC. Se uma correspondência ainda não for encontrada, um IC de espaço reservado será criado e designado como **IC incompatível**. Consulte ICs incompatíveis para obter mais informações sobre como esses ICs são tratados.

As regras de pesquisa de IC podem ser separadas por domínio e são específicas da origem. Cada origem pode ter várias implantações.

Nota:
As regras de pesquisa de IC são compartilhadas por todas as implantações da integração de origem da vulnerabilidade. Se uma regra for excluída ou modificada, a exclusão ou as mudanças afetarão todas as implantações da integração de vulnerabilidade.

Ao tentar uma correspondência, a primeira etapa é uma pesquisa de ID de fornecedor para uma correspondência exata entre origem, source_instance e ID de fornecedor. Em seguida, as regras de pesquisa são executadas em ordem, da menor para a maior, e param quando uma regra retorna apenas um único IC como uma correspondência. Se uma regra for criada de forma a retornar mais de um IC, somente a primeira correspondência será usada.

Nota:
Para evitar a correspondência em elementos de network de baixo nível, se um IC correspondente for `dscy_switchport`, `cmdb_ci_network_adapter`, `cmdb_ci_nic` ou `cmdb_ci_ip_address`, o IC primário será retornado.

Uma propriedade do sistema para excluir classes de IC está disponível. Esta propriedade não está disponível com atualização. Consulte Ignorar classes de IC para obter informações de atualização e instruções sobre como definir a propriedade.

Para facilitar a localização de problemas de correspondência, quando uma correspondência for encontrada, a regra de pesquisa de IC usada para localizá-la será adicionada ao registro de item descoberto no campo **Regra de correspondência de IC**. As regras de pesquisa são avaliadas primeiro pelo menor valor de **Pedido**.

Essas regras Qualys de pesquisa de IC são enviadas com o sistema de base.

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

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Essas regras Rapid7 de pesquisa de IC são enviadas com o sistema de base.

- MACAddress
- FQDN
- HostName
- IP

Essas regras de pesquisa de IC da Tenable.io são enviadas com o sistema de base.

- FQDN
- NETBIOS
- HOSTNAME
- MACAddress
- DNS

Essas regras de pesquisa de IC da Tenable.sc são enviadas com o sistema de base.

- MACAddress
- FQDN
- NETBIOS

Nota:
As regras, depois de removidas, não podem ser recuperadas. Em vez de remover as regras existentes, desative-as ao criar novas.

A importação de dados de vulnerabilidade pode sobrecarregar uma instância e podem ocorrer problemas de desempenho com recursos se as regras não forem construídas com cuidado. A lógica usada para iterar e executar a correspondência dentro do CMDB pode resultar em longos tempos de processamento. Para evitar qualquer degradação potencial de recursos ou complicações de desempenho, teste todas as regras de pesquisa de IC personalizadas ou modificações nas **regras de pesquisa de IC** predefinidas. Consulte Etapas para ajudar a evitar registros duplicados ou órfãos após a execução de Vulnerability Response regras de pesquisa de IC para obter mais informações sobre como evitar registros órfãos duplicados, excluir dados e limpar dados.

Nota:
Para obter informações sobre correspondência de IC, consulte KB0998706 .

Aplicar novamente as regras de pesquisa de IC atualizadas

Ao alterar uma regra de pesquisa de IC, clique em **Aplicar mudanças** na página da lista Regras de pesquisa de IC para executar novamente todas as regras nos itens descobertos que:

- Foram correspondidos pelas regras atualizadas
- Não são correspondidos por nenhuma regra

Se o item de configuração (IC) mudar após a reaplicação das regras de pesquisa, os itens descobertos serão atualizados com o novo IC. As detecções afetadas e os itens vulneráveis também são atualizados. Para obter mais informações, consulte Reaplicar regras de pesquisa de IC em itens descobertos selecionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Hardware não classificado

Se um ativo não encontrar uma correspondência no Configuration Management Database (CMDB) pelas regras de pesquisa de IC, o ativo será denominado como um hardware não classificado.

Quando os dados são importados de ServiceNow integrações criadas, Vulnerability Response usa automaticamente os dados do host para pesquisar correspondências no CMDB. As regras de pesquisa de IC são usadas para identificar itens de configuração (ICs) e adicioná-los ao registro de item vulnerável para ajudar na correção. Se os ativos não forem encontrados no CMDB, o mecanismo de Identificação e Reconciliação (IRE) executará suas próprias regras de identificação definidas na classe de hardware e em todos os seus secundários e criará um IC em uma classe de hardware não classificada. Quando Descoberta encontra este ativo, em vez de reclassificar o hardware não classificado existente, ele cria um IC. Isso ocorre porque a regra de identificação depende do nome do IC de hardware.

Se o mecanismo de Identificação e Reconciliação (IRE) estiver ativado, a opção de reclassificação de itens descobertos não será compatível.

As extrações a seguir mostram a carga útil do IRE para criar IC em hardware não classificado via Vulnerability Response e Descoberta respectivamente.

```
"className": "cmdb_ci_unclassed_hardware",

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

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

```
"className": "cmdb_ci_cmdb_ci_win_server"

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

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

Nesse caso, o IC de hardware não classificado existente não é reclassificado para o servidor Windows e, em vez disso, um novo IC no servidor Windows é criado. O motivo é que a regra de identificação depende do nome do IC de hardware. Se você observar as cargas úteis, o nome na carga útil de Vulnerability Response é o mesmo que FQDN/NETBIOS, mas é apenas o nome do host da carga útil de Descoberta.

Tópicos relacionados

Reclassificar hardware não classificado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ICs incompatíveis

Os itens de configuração (ICs) são correspondidos automaticamente aos ICs no Configuration Management Database (CMDB) quando são importados. Por padrão, o **Security Operations** > **CMDB** > **Itens Descobertos** O módulo lista os itens de configuração sem uma correspondência.

Se você acha que um IC incompatível pertence a uma classe existente no CMDB, revise suas regras de pesquisa de IC. Caso contrário, considere reclassificar o item de configuração.

Nota:
O filtro padrão desta lista é definido como **Incompatível**. Você pode exibir todos os itens descobertos de uma importação removendo o filtro.

Se o mecanismo de Identificação e Reconciliação (IRE) estiver ativado, a opção de reclassificação de itens descobertos não será compatível.

Tópicos relacionados

- Exibir e reclassificar itens de configuração incompatíveis
- Reconciliar itens descobertos sem correspondência
- Etapas para ajudar a evitar registros duplicados ou órfãos após a execução de Vulnerability Response regras de pesquisa de IC
- Desduplicando itens de configuração existentes

Criando ICs para Vulnerability Response usando o mecanismo de Identificação e Reconciliação

Você pode criar itens de configuração (ICs) no Configuration Management Database (CMDB) usando a API do mecanismo de identificação e reconciliação (IRE). Ao usar a API do IRE para criar ICs, você pode impedir a criação de ICs duplicados e reconciliar atributos de IC, permitindo que somente fontes de dados autorizadas gravem em CMDB.

Uma classe de IC (tabela) é o nome da tabela original no banco de dados da instância. CMDB contém classes do sistema de base que armazenam dados sobre ICs.

Uso de IRE para criação de IC

Antes de Vulnerability Response v12.2, se um IC correspondente não for encontrado na lista de itens descobertos ou CMDB, um IC será criado na classe de IC incompatível (sn_sec_cmn_unmatched_ci). Para obter mais informações, consulte ICs incompatíveis.

A partir de Vulnerability Response v12.2 a v18.0, se nenhuma correspondência for encontrada quando as regras de pesquisa de IC forem aplicadas, as informações do ativo serão enviadas para o IRE e um IC será criado em uma das *classes de hardware não classificado* e *dispositivo identificado por IP incompleto*. A partir de Vulnerability Response v18.0, uma nova classe, *Recurso de Nuvem*, também está incluída. Para obter mais informações sobre como configurar a categorização de recursos de nuvem incompatíveis em sua classe de IC preferencial, consulte Atualizando classe de IC para ativos de nuvem incompatíveis.

CMDB Classes de IC

Nota:
Para usar as novas classes, ative o plug-in CMDB CI Class Models. Caso contrário, os ICs serão criados na classe de IC incompatível.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se o host que você importou de um scanner de terceiros não puder ser encontrado na lista de Itens Descobertos ou CMDB, ele será criado em uma das seguintes novas CMDB classes de IC.

CMDB Classes de IC

CMDB Classe de IC	Descrição
Dispositivo identificado por IP incompleto (*cmdb_ci_incomplete_ip*)	O IC será criado nesta tabela se somente o endereço IP estiver disponível nas informações de host recebidas do scanner.
Hardware sem classificação (*cmdb_ci_unclassed_hardware*)	O IC será criado nesta tabela se qualquer uma das seguintes informações estiver disponível nas informações do host recebidas do scanner: • Nome do host • Endereço IP • DNS • NETBIOS • Endereço MAC **Nota:** Se o endereço MAC estiver disponível, a entrada do adaptador de rede será criada e relacionada ao IC de hardware não classificado. Se os endereços IP e MAC estiverem disponíveis, o IC de endereço IP também será criado e relacionado ao IC de hardware não classificado.
Recurso de nuvem (*cmdb_ci_cmp_resource*)	O IC será criado nesta tabela se *Cloud Resource ID* estiver disponível nas informações do host recebidas do scanner. **Nota:** Se o tipo de ativo de uma integração de scanner for *híbrido* e a propriedade do sistema *sn_sec_cmn.unmatched_cloud_resource_enabled* for falsa, os ICs serão criados na classe *Hardware* sem classificação, mas não na classe *Recurso de nuvem*.

Se o mecanismo de Identificação e Reconciliação (IRE) estiver ativado, a opção de reclassificação de itens descobertos não será compatível.

O sistema usará automaticamente uma classe de IC incompatível se ocorrer um dos seguintes:

- O plug-in CMDB Classe de IC não está ativado.
- O IRE gera uma exceção ao criar um IC.

  Para obter mais informações, consulte ICs incompatíveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Aplicação da Store do CMDB CI Class Models

Mecanismo de Identificação e Reconciliação (IRE)

Atualizando classe de IC para ativos de nuvem incompatíveis

A partir do Vulnerability Response v20.0, você pode categorizar os ativos de nuvem incompatíveis dos scanners Qualys, Rapid7 e Tenable em *`hardware não classificado`* usando a propriedade do sistema *`sn_sec_cmn.unmatched_cloud_resource_enabled`*.

Esta propriedade do sistema com `falso` como valor padrão é enviada com o sistema de base. Ele classifica os ativos de nuvem incompatíveis em uma *`classe de hardware não classificado`* (*`cmdb_ci_unclassed_hardware`*) ou *`recurso de nuvem`* (*`cmdb_ci_cmp_resource`*) para as integrações que reúnem ativos de infraestrutura e de nuvem.

A partir da Vulnerability Response v20.0, a coluna Tipo de ativo é adicionada à tabela Integrações de terceiros (`sn_sec_int_integration`) para identificar as integrações que oferecem suporte a ativos de infraestrutura e de nuvem. A coluna Tipo de ativo tem o valor *`Híbrido`* para os scanners que geram ativos de infraestrutura e de nuvem. Por exemplo, as integrações Qualys, Rapid7 e Tenable têm o valor como *`Híbrido`* na coluna Tipo de ativo.

- Para a nova instalação de Vulnerability Response v20.0 e superior, todos os ativos de nuvem incompatíveis são categorizados em:
  - *`Classe de hardware não`* classificada por padrão.
  - Classe*`Recursos de nuvem`*, se você alterar a propriedade do sistema *`sn_sec_cmn.unmatched_cloud_resource_enabled`* para `verdadeiro`.
- Para atualizações para Vulnerability Response v20.0:
  - Se houver ativos na classe *`Recurso de nuvem`*, a propriedade do sistema *`sn_sec_cmn.unmatched_cloud_resource_enabled`* será definida como verdadeira para que os ativos de nuvem incompatíveis continuem a ser adicionados à classe *`Recurso de nuvem`* (*`cmdb_ci_cmp_resource`*).
  - Caso contrário, a propriedade do sistema *`sn_sec_cmn.unmatched_cloud_resource_enabled`* será definida como falsa para que os ativos de nuvem incompatíveis sejam categorizados na classe de *`hardware sem`* classificação.

Nota:
Se você modificar o valor da propriedade do sistema *`sn_sec_cmn.unmatched_cloud_resource_enabled`*, certifique-se de excluir itens de configuração incompatíveis na classe de IC de destino anteriormente e reaplicar as regras de pesquisa. Para saber mais sobre como excluir os ICs existentes e reaplicar as regras de pesquisa de IC para que os novos ICs sejam criados na classe correta, consulte KB1533376 .

Itens Descobertos

Os ativos são correspondidos automaticamente aos itens de configuração (ICs) no Configuration Management Database (CMDB) quando são importados usando **Regras de pesquisa de IC**. Os itens descobertos fornecem visibilidade de como a identificação de ativo é mapeada para ICs no CMDB.

Os itens descobertos são considerados **correspondentes**, não **correspondentes**ou **reclassificados**. Os ICs identificados estão no estado **Correspondente**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para facilitar a localização de possíveis problemas de correspondência, a regra de pesquisa de IC que correspondeu ao IC aparece no campo **de regra de correspondência de IC**.

Por padrão, o **Security Operations** > **CMDB** > **Itens Descobertos** O módulo lista itens de configuração incompatíveis. Você pode exibir todos os itens descobertos de uma importação removendo o filtro.

Para obter uma descrição dos campos em Itens descobertos, consulte Campos de formulário de Itens descobertos. Para obter mais informações sobre como reconciliar itens descobertos incompatíveis e reaplicar regras de pesquisa de IC em itens descobertos selecionados, consulte Reconciliar itens descobertos sem correspondência e Reaplicar regras de pesquisa de IC em itens descobertos selecionados respectivamente.

Mudanças de IC para itens descobertos

Quando um item de configuração (IC) em um item descoberto (DI) muda, as detecções afetadas e os itens vulneráveis (IVs) são atualizados. A pontuação de risco, as regras de atribuição, as regras de grupo e a regra de destino de correção são reavaliadas.

Se houver um IV com a mesma vulnerabilidade e IC, as detecções serão atualizadas com o IV existente e o IV atual será encerrado com o subestado como invalidCI. As anotações de trabalho são adicionadas pelos seguintes motivos:

- Quando as detecções são movidas de um IV para outro.
- Quando um IV duplicado é encerrado.

Se você não quiser atualizar o IC para o IV existente, defina a propriedade sn_sec_cmn.update_on_ci_change como false. Em seguida, quando um IC muda, um novo IV é criado e o existente é encerrado como um IC inválido.

O valor padrão da propriedade sn_sec_cmn.update_on_ci_change é verdadeiro.

Reavaliando itens descobertos

Quando novos dados são recebidos em um item descoberto, o item descoberto não é reavaliado imediatamente. Ao receber novos dados, a opção *reevaluate_ci* é definida como *true* por padrão.

O trabalho programado *Re-apply CI Lookup Rules on the Changed Discovered items* avalia todos os itens descobertos cujos dados de origem estão sendo alterados pelo scanner. Ele reprocessa os itens descobertos e atualiza os itens vulneráveis relacionados ao item descoberto cujos dados de origem foram alterados. O valor deste trabalho programado é *On Demand* por padrão.

Nota:
Você também pode optar por executar este trabalho programado diariamente.

Vulnerability Response tarefa de correção e estados de item vulnerável

Com a aplicação Vulnerability Response, você pode usar o modelo de estado para ver o status de uma tarefa de correção a qualquer momento. Saber como cada estado se relaciona e afeta um ao outro ajuda a determinar quando e como corrigir seus itens vulneráveis (IVs).

Estados da tarefa de correção

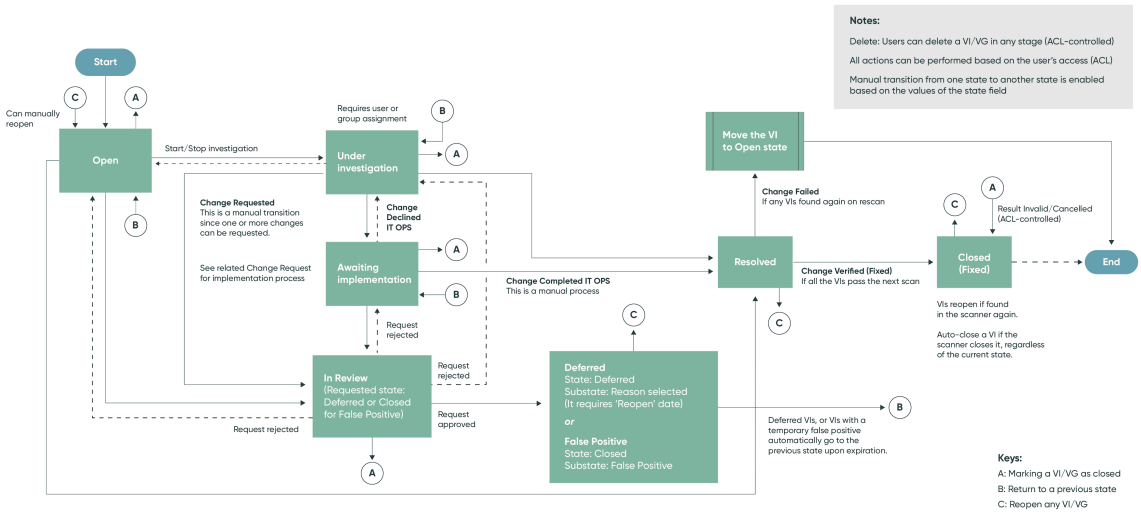
Às vezes, casos de uso complexos podem fazer com que um item vulnerável esteja em um estado diferente de sua tarefa de correção. Entender como os estados funcionam ajuda a explicar esse comportamento e pode ajudar na criação de tarefas de correção e na criação ou edição de regras de tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As tarefas de correção têm muitos estados possíveis, conforme mostrado no diagrama a seguir.

Fluxo de estado do Vulnerability Response



Nota:
Cada formulário de tarefa contém botões **Seguir** e **Atualizar** que são padrão para tarefas ServiceNow.

Para obter mais informações sobre os estados da tarefa de correção e as ações que você pode executar em um respectivo estado, consulte Vulnerability Response estados da tarefa de correção.

Para obter mais informações sobre detecções, tarefa de correção e estados de item vulnerável, consulte Detecções, tarefas de correção e estados de item vulnerável.

Para obter mais informações sobre a tarefa de correção e os estados de IV, consulteTarefas de correção e estados de item vulnerável.

Para obter mais informações sobre o estado da tarefa de correção para IVs em vários grupos, consulte Estado da tarefa de correção para itens vulneráveis (IVs) em vários grupos.

Cálculo e exibição de idade do item vulnerável

A idade dos itens vulneráveis (IVs) é exibida na aplicação Vulnerability Response com mais detalhes.

Visão geral

A idade do item vulnerável (VI) é exibida no formato Dias/Horas/Minutos na coluna Idade na exibição de lista de Itens vulneráveis e nos campos Idade e Idade encerrada nos registros de IV (VIT). A idade exibida em dígitos mais significativos pode ajudar você a executar as seguintes atividades com mais precisão:

- Configure regras no módulo Regras de exclusão automática para direcionar e excluir registros de IV específicos por Dias/Horas/Minutos. Remover registros com mais precisão pode aumentar seu desempenho, especialmente se você tiver um grande número de registros de IV em sua instância.
- Exiba relatórios com detalhes mais específicos no Performance Analytics para a aplicação Vulnerability Response.
- Crie filtros que identificam somente os IVs desejados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Remova as exibições de lista para exibir somente os IVs desejados.
- Referência com pontos com mais facilidade.

Um trabalho programado calculou a idade e atualizou todos os IVs ativos. Em instâncias com um grande número de registros de IV, esse processo pode ser lento e afetar negativamente o desempenho. A idade do IV é calculada com mais eficiência sob demanda e exibida com dígitos mais significativos com uma coluna Idade aprimorada. A coluna Idade aprimorada é adicionada automaticamente quando você instala ou atualiza a aplicação Vulnerability Response.

Nota:
Se você executar um upgrade e a idade do IV não for exibida na exibição de lista de Itens vulneráveis e nos campos Idade e Idade encerrada em registros de IV ativos (VIT) no formato Dias/Horas/Minutos (9 Dias, 18 Horas, 29 Minutos) , a coluna de idade não será a atual em sua instância. Para obter mais informações sobre como resolver esse problema após um upgrade, consulte KB0749231 .

A coluna e os campos de idade não são editáveis. Um gerenciador de vulnerabilidades com a permissão sn_vul.vulnerability_read ou a persona de administrador de vulnerabilidade pode exibir esse valor, e os proprietários de correção de TI com a função sn_vul.remediation_owner podem exibi-lo nos registros atribuídos a eles.

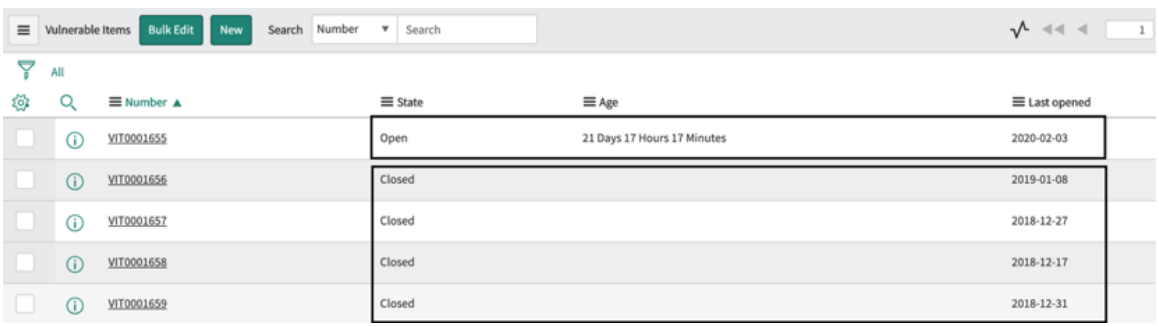
Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

A idade do IV é exibida conforme mostrado nas imagens a seguir.

Lista de itens vulneráveis

Conforme mostrado na figura a seguir, na exibição de lista de Itens vulneráveis, a Idade é exibida na coluna Idade em Dias/Horas/Minutos (21 Dias 17 Horas 17 minutos) somente para IVs ativos. IVs ativos são IVs em qualquer estado diferente de "Encerrado". Este valor de idade representa o número de dias que o IV está ativo.

A idade não é exibida para IVs no estado "Encerrado". Para IVs anteriormente em um estado “Encerrado” e depois reaberto, o valor representa o número de dias que o IV está ativo desde a data em que foi aberto pela última vez.

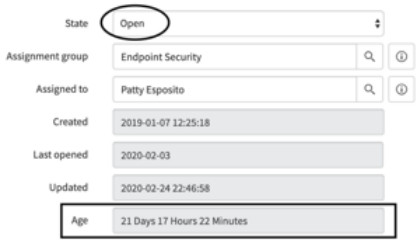


Idade nos registros IV

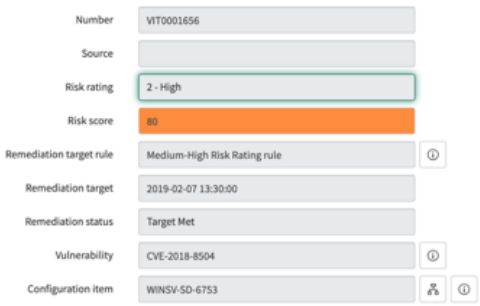
Nos registros de IV, o valor da coluna Idade na exibição de lista está visível para IVs ativos no campo Idade.

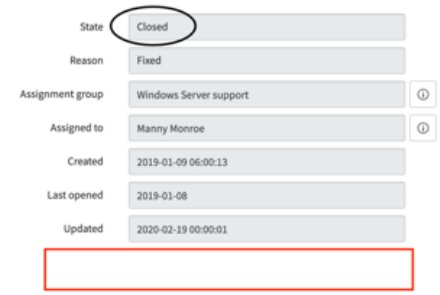
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



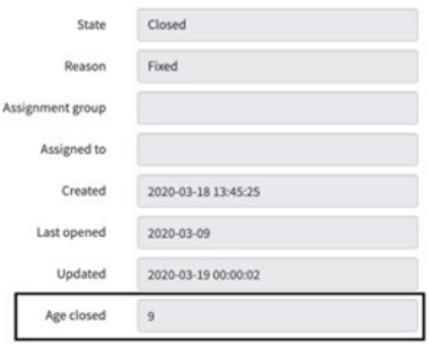
O valor da coluna Idade não é exibido para registros de IV no estado "Encerrado".





Idade na lista de itens vulneráveis e nos registros de IV quando um IV é atualizado

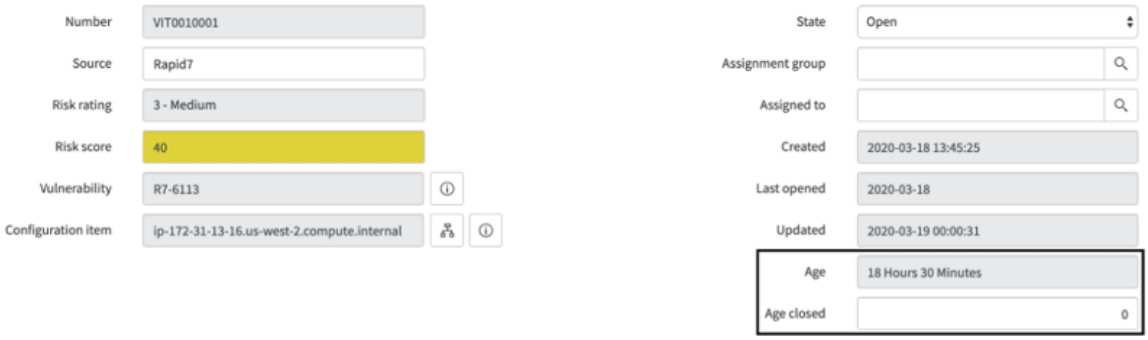
Quando um IV está no estado "Encerrado", o campo Idade não é exibido. Quando o IV muda para "Encerrado", o valor em número de dias da coluna Idade é exibido no campo Encerrado com idade (9), conforme mostrado na figura a seguir. Este valor representa o número de dias que o IV estava ativo antes de mudar para "Encerrado". Por exemplo, na imagem a seguir, este IV está ativo por 9 dias, 18 horas e 29 minutos, mas somente o número de dias (9) é exibido no registro encerrado.



Se este IV for reaberto, quando o estado do IV mudar novamente para "Aberto", o campo Idade encerrada será redefinido como 0. Como o IV está ativo novamente, a idade em Dias/Horas/Minutos é exibida na exibição de lista na Idade coluna e no campo Idade no VIT.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Removendo atribuições de itens vulneráveis e tarefas de correção

Você pode limpar os campos **Atribuído a** e **Grupo de atribuição** em itens vulneráveis diretamente do item vulnerável (VIT) e dos registros de tarefa de correção que você determinar que podem ter sido atribuídos incorretamente a você ou seus grupos.

Visão geral

A partir da **v16.5**, os responsáveis pela correção podem atualizar os registros para reatribuição com o botão Cancelar atribuição nas aplicações Vulnerability Response e Application Vulnerability Response.

Caso de uso

Se você determinar que os IVs não estão dentro do seu escopo de correção ou se achar que os registros foram atribuídos incorretamente a você ou aos seus grupos, convém remover a si mesmo ou aos seus grupos dos campos **Atribuído a** e **Grupo de atribuição** na vulnerabilidade registros de item e tarefa de correção.

Desatribuir módulo

O botão **Cancelar atribuição** é exibido nos seguintes registros em qualquer estado que não seja Encerrado ou Resolvido:

- Tarefas de correção (VULs) no ambiente clássico e nos espaços Vulnerability Response. Se uma tarefa de correção for atualizada com este recurso, os campos **Atribuído a** e **Grupo de atribuição** em todos os seus IVs associados também serão limpos.
- Itens vulneráveis (VITs) no ambiente clássico e nos espaços Vulnerability Response.
- Itens vulneráveis da aplicação (AVITs).

Todos os registros que você atualiza com o botão de IU ou manualmente são exibidos no módulo Não atribuído em seus respectivos módulos.

Para saber como reatribuir registros usando a ação de IU `Unassigned`, consulte Remover atribuições de itens vulneráveis para você ou seus grupos.

Edição em massa

Você pode limpar os campos de atribuição de vários IVs em uma lista. Depois de selecionar os IVs e selecionar **Edição em massa**, na caixa de diálogo exibida, marque a caixa de seleção **Cancelar atribuição**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades e notificações do sistema

Se você for um administrador com a função **sn_vulc.vulnerability_admin**, ao clicar em Cancelar atribuição em um registro, por padrão, a propriedade do sistema *sn_vul.unassign_vr.approval_required* acionará o fluxo de aprovação e criará um registro de aprovação de mudança de estado no estado de revisão e a solicitação de aprovação será gerada para o aprovador que é exibido na lista **Minhas aprovações**.

Nota:
Como administrador de vulnerabilidade, você pode definir a propriedade do sistema *sn_vul.unassign_vr.approval_required* como **falsa** para desabilitar o processo de aprovação.

- Se o aprovador aprovar a solicitação, *sn_vul.default_assignment_group* limpará os campos **Atribuído a** e **Grupo de atribuição** e preencherá o campo **Tipo de atribuição** com **Não atribuído**. Como administrador de vulnerabilidade, você pode alterar o valor na propriedade do sistema *sn_vul.default_assignment_group* para que os campos de atribuição sejam limpos e um grupo específico seja atribuído. Por exemplo, se um usuário clicar em **Cancelar atribuição** em um registro e você quiser redirecioná-lo para um grupo específico para revisão, você poderá adicionar um ID de sistema para o grupo de sua escolha no campo de valor da propriedade do sistema.

  Nota:
  Se você alterar este valor, as notificações de todos os IVs, AVITs e CVITs que não estão atribuídos serão enviadas para o grupo especificado.

- Se o aprovador rejeitar sua solicitação, o motivo da rejeição será exibido na guia **Anotações**.

Como alternativa, se *sn_vul.default_assignment_group* não estiver configurado para um grupo específico, por padrão, os usuários que você adicionar ao grupo de usuários de notificação de cancelamento de atribuição serão alertados quando os registros não forem atribuídos. A propriedade do sistema *sn_vul.default_assignment_group* determina as notificações para este grupo.

O tipo de atribuição, seja **Manual**, **Regra**ou **Não atribuído**, está disponível nos registros de IV e na exibição de lista. O tipo de atribuição **Não atribuído** é exibido nos registros depois que os campos **Atribuído a** e **Grupo de atribuição** são limpos pela propriedade do sistema do recurso.

Monitorar suas regras de atribuição com o trabalho programado para este recurso

Um trabalho programado diário conta os registros quando eles fazem a transição para o tipo de atribuição **não atribuída**. Com essa contagem, os analistas de vulnerabilidade podem monitorar e ajustar quaisquer regras de atribuição que possam não estar funcionando bem com base em quaisquer regras de atribuição que tenham contagens mais altas de IVs não atribuídos.

O trabalho programado *Reassignment count for assignment rules* é executado diariamente e publica o número total de IVs não atribuídos por este recurso para uma regra de atribuição específica.

As contagens coletadas por este trabalho se aplicam aos itens vulneráveis e às regras de atribuição exclusivas para Vulnerability Response e Application Vulnerability Response. As

Tradução automática

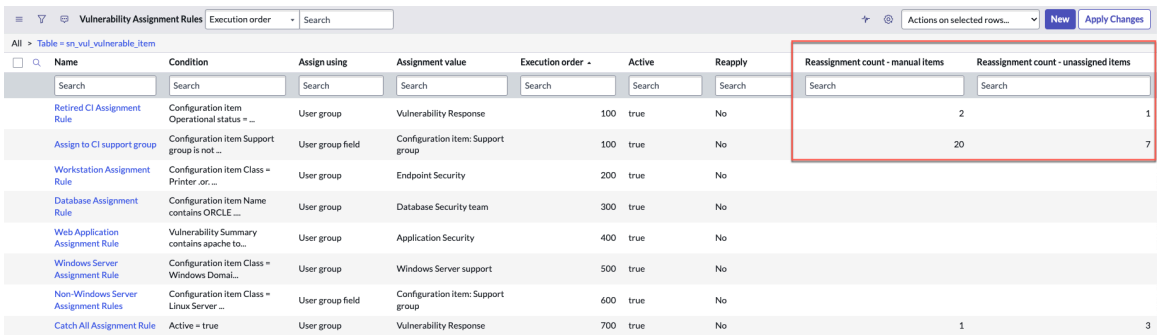
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

contagens são exibidas por regra de atribuição em cada lista de regras de atribuição para cada módulo.

O trabalho também conta todos os registros que são desatribuídos manualmente. As contagens manuais e as contagens coletadas por este recurso são publicadas na lista Regras de atribuição de vulnerabilidade em duas colunas: *`Reassignment count - manual items`* e *`Reassignment count - unassigned items`*.

1. Como administrador de vulnerabilidades, para exibir essas contagens, navegue até **Vulnerability Response** > **Administração** > **Regras de atribuição**.
2. Clique no ícone de engrenagem no canto superior direito da lista e selecione *`Reassignment count - manual itemse Reassignment count - unassigned items`* para exibição.
3. Qualquer IV que foi originalmente atribuído por uma regra, mas posteriormente reatribuído de forma automática ou manual, contém uma referência à regra original na exibição de lista.

O exemplo a seguir mostra as contagens de reatribuição para duas regras de atribuição.



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

Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade

As calculadoras de vulnerabilidade automatizam o cálculo dos valores iniciais dos campos em itens vulneráveis. A condição de cada calculadora é avaliada na ordem e a primeira calculadora correspondente é usada.

Calculadoras de vulnerabilidade

O sistema de base Vulnerability Response inclui duas calculadoras de vulnerabilidade que definem a **pontuação de risco** base no item vulnerável.

- **Calculadora de Risco Padrão**
- **Severidade da Vulnerabilidade**

Calculadoras de vulnerabilidade podem ser criadas para priorizar e classificar o impacto de itens vulneráveis com base em qualquer critério usando filtros de condição. Seja o impacto nos negócios da vulnerabilidade, a classe do item de configuração (IC) ou a idade do item vulnerável, você pode criar calculadoras de vulnerabilidade adicionais para definir outros campos em itens vulneráveis. Ou você pode personalizar as calculadoras de vulnerabilidade existentes. Uma calculadora pode ser escrita para refletir qualquer conjunto de prioridades. Para obter mais informações, consulte Criar uma calculadora Vulnerability Response e Filtragem em Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Além disso, você pode usar atributos no configuration_item [cmdb_ci] no Configuration Management Database (CMDB) para ajudá-lo a criar lógica para suas calculadoras de risco do Vulnerability Response. Se, por exemplo, você determinar que os ICs externos em sua organização são mais vulneráveis e podem exigir correção imediata, você pode atribuir atributos como *Internet Facing* para esses ICs. Este atributo e outros estão listados nas notas de versão do Common Service Data Model para a versão da família Orlando. Para obter informações e orientações atuais sobre o CMDB, consulte os seguintes tópicos:

- Modelo conceitual de modelo de dados de serviço comum
- Modelo de esquema do CMDB

Cada calculadora contém uma lista de regras da calculadora, com uma condição que determina quando aplicá-la. Quando a calculadora é executada, a condição de cada regra da calculadora é avaliada na ordem e a primeira regra da calculadora correspondente é usada.

A calculadora de **severidade da vulnerabilidade** calcula a **pontuação de risco** para itens vulneráveis usando a severidade da vulnerabilidade normalizada.

Nota:
Somente uma calculadora por campo de destino (**pontuação de risco**) pode estar ativa de cada vez. **A severidade da vulnerabilidade** está desabilitada por padrão.

Todas as calculadoras de vulnerabilidade habilitadas definem os campos selecionados sempre que um item vulnerável é criado, quando um IC ou vulnerabilidade associada muda ou quando o link relacionado **Calcular pontuação de risco** em um item vulnerável é usado. Por exemplo, a pontuação de risco é atualizada automaticamente em registros de item vulnerável quando o valor de severidade é atualizado em uma vulnerabilidade importada. Depois que uma importação de vulnerabilidade tiver atualizado uma pontuação de vulnerabilidade, o sinalizador de recalcular será habilitado para essa vulnerabilidade. As pontuações de risco dos itens vulneráveis que têm o sinalizador de recalcular habilitado (verdadeiro) com essa vulnerabilidade são recalculadas.

Em um item vulnerável existente, se você clicar no link relacionado **Calcular pontuação de risco** e uma das calculadoras estiver habilitada, o campo **Pontuação de risco** no item vulnerável será atualizado.

Nota:
O link relacionado **Calcular pontuação de risco** só fica visível quando pelo menos uma calculadora de vulnerabilidade está habilitada.

Regras da Calculadora de Vulnerabilidade

A **Calculadora de risco padrão** do sistema básico contém a regra de regra de **risco padrão**, uma regra de calculadora de vulnerabilidade especializada chamada regra de **risco**. Ele calcula a **pontuação de risco** com base em vários valores:

- Gravidade da vulnerabilidade
- Explorar informações
- Criticidade
- Exposição externa do IC com a vulnerabilidade
- Pontuações de EPSS

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode ajustar os valores a serem usados na **Regra de risco padrão** e quanto peso atribuir a cada um desses valores. Os pesos são usados para ajustar o quanto cada elemento conta ao definir a **Pontuação de risco**base.

Você pode personalizar os critérios para a regra de risco padrão. Para obter mais informações, consulte Definir campos e pesos para a regra de risco das Calculadoras de risco do Vulnerability Response.

Para obter um exemplo de como as pontuações de risco das calculadoras de regra de risco são determinadas, consulte Exemplo de cálculo de pontuação de risco para Vulnerability Response.

Atribuição de uma porcentagem de ponderação

Você também pode atribuir uma porcentagem de ponderação (0-100) no nível de valor do campo, por exemplo, você pode atribuir uma porcentagem de ponderação a cada nível de Severidade (de Nenhum a Crítico).

Se a ponderação de severidade for 50 para a regra de risco, os seguintes valores de ponderação forem atribuídos para o nível de severidade:

Gravidade da vulnerabilidade	Pontuação de risco
Crítico	100
Alto(a)	50
Média	20
Nenhum(a)	0

Se a severidade for crítica, a ponderação equivalente será 50. Se a severidade for alta, a ponderação equivalente será 25 e se a severidade for média, a ponderação equivalente será 10. Se a severidade for Nenhuma, o peso equivalente será 0. Para obter mais informações, consulte Exemplo de cálculo de pontuação de risco para Vulnerability Response.

Configurações de regra da calculadora de vulnerabilidade

Cada regra tem uma configuração de **Ordem**. No entanto, o primeiro a corresponder às condições atualiza o campo **Pontuação de risco** no item vulnerável. Para obter mais informações sobre configurações de regra da calculadora de vulnerabilidade, consulte Criar uma calculadora Vulnerability Response. Regras de calculadora sem script normalmente criam menos impacto no desempenho do que regras de calculadora com script.

A calculadora de **Severidade de Vulnerabilidade** do sistema básico contém regras de calculadora que atribuem a cada nível de severidade (de Nenhum a Crítico) um valor (0-100) para **Pontuação de Risco** com base na severidade. A**Severidade Desconhecida** recebe automaticamente uma pontuação de risco de 100. Esses valores podem ser ajustados e, como **Calculadora de risco padrão**, novas regras de calculadora ou novas regras de risco podem ser criadas.

Ponderações de Pontuação de Risco de Vulnerabilidade

Todas as vulnerabilidades são atribuídas a uma pontuação de risco e classificação com base em fatores como severidade, criticidade, informações de exploração e assim por diante. A regra de negócios `Update Risk Rating from Risk Score` na tabela de item vulnerável é responsável pelo cálculo da classificação de risco. Sempre que a pontuação de risco muda, a classificação de risco é calculada e preenchida nos itens vulneráveis. Antes da versão 17.1 da aplicação Vulnerability Response (VR), as classificações de risco a seguir eram fornecidas como parte da inclusão de script VulnerabilityUtils, que eram codificadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Valor (classificação de risco)	Peso (pontuação de risco)
1	90–100
2	70–89
3	40–69
4	1 a 39
5	0

Começando com a versão 18.0 de Vulnerability Response,

- Os tipos de classificação de risco são enviados na tabela base como vr_risk_rating. Esses tipos são passados como parte da regra de negócios em cada tabela em que a classificação de risco é calculada.
- O script foi modificado para que você possa consultar as entradas nos valores da tabela Ponderações de pontuação de risco para o cálculo de classificação de risco.
- Adicione entradas adicionais para um tipo existente ou crie um novo tipo. Ao criar um novo tipo, certifique-se de adicionar os rótulos para a nova classificação de risco e também de modificar os scripts e as regras de negócios relacionados. Você também deve adicionar um novo estilo para a nova pontuação de risco.
- Modifique o script para consultar os registros na tabela base.

Você pode acessar a tabela Ponderações de pontuação de risco inserindo sn_sec_cmn_risk_score_weight no navegador de filtros.

Além disso, a pontuação de risco é recalculada automaticamente nos seguintes cenários:

- Quando um item de configuração (IC) muda de não voltado para a internet para voltado para a internet.
- Quando as Vulnerabilidades e exposições comuns (CVEs) associadas ou as entradas de terceiros (TPEs) nos itens de vulnerabilidade (IVs) estão vinculadas a uma Vulnerabilidade de exploração conhecida (KEV) de CVE.

Integração de vulnerabilidade da Tenable e regra de risco da Tenable

A regra de risco da Tenable está disponível com o Tenable Vulnerability Integration. A classificação de prioridade de vulnerabilidade (VPR) é um atributo do produto Tenable que é importado e usado com uma nova calculadora de risco padrão em Vulnerability Response. A Regra de risco da Tenable é instalada com a aplicação Integração do Vulnerability Response com Tenable como parte da Calculadora de risco padrão nas Calculadoras de vulnerabilidade da Vulnerability Response.

Esta regra de risco está desabilitada por padrão. Consulte Configurar a integração de vulnerabilidade da Tenable usando o assistente de configuração.

Vulnerability Response detecções de item vulnerável de integrações de terceiros

Exiba todas as informações coletadas por verificações de terceiros na sua instância Now Platform®. Exiba os resultados retornados das verificações na detecção e nos registros de item vulnerável (VI) em sua instância, pois esses resultados são exibidos nos scanners.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

A aplicação Vulnerability Response oferece suporte a integrações de terceiros que recuperam dados de item vulnerável do seu ambiente empresarial. Dados detalhados sobre detecções, ou seja, ocorrências únicas e distintas de vulnerabilidades conforme relatado pelos scanners de suas integrações de terceiros, são importados e exibidos na detecção e nos registros de item vulnerável em sua instância da Now Platform.

As integrações de terceiros recuperam dados de detecção de item vulnerável. As detecções são ocorrências distintas de vulnerabilidades, conforme relatado pelos scanners. Os dados de detecção são emparelhados com itens vulneráveis e o estado do IV é atualizado com base no estado das detecções. Se um IV não for encontrado, um novo será criado. As detecções são abertas ou encerradas somente pelos dados encontrados diretamente por um scanner.

Em versões anteriores do Vulnerability Response, as detecções de item vulnerável, o relacionamento entre um IC (ativo) em seu ambiente e uma vulnerabilidade importada de um scanner de terceiros, criavam um item vulnerável exclusivo em sua instância da Now Platform.

A granularidade dos dados originais fornecidos pelo scanner é preservada. Com as detecções, os dados de detecção são emparelhados com itens vulneráveis. Durante uma ingestão, se um item vulnerável não for encontrado, um novo IV será criado.

A partir da versão 21.0 do Vulnerability Response, uma propriedade do sistema `sn_vul.show_last_open_detection` é fornecida no sistema de base. Por padrão, o valor desta propriedade é definido como falso e o comportamento atual de agregar os valores da detecção inicial ao IV permanece inalterado. No entanto, se for definido como verdadeiro, um IV será atualizado automaticamente com a última detecção aberta após uma ingestão. Os campos como endereço IP, SSL, Porta, Protocolo, NetBIOS e Prova são atualizados para as detecções de IV. Se necessário, você pode personalizar os campos de detecção que devem ser atualizados modificando o script DetectionBase.

Para exibir os valores da última detecção de abertura, navegue até a guia **Última detecção de abertura** na exibição do formulário IV. Para atualizar todos os IVs abertos no ano passado com os últimos valores de detecção de abertura, você pode executar o trabalho programado `Update Last Open Detection Value To VITs` sob demanda. Este trabalho programado também é fornecido no sistema de base.

Nota:
Quando um item de configuração (IC) muda em um item descoberto, as atualizações correspondentes também são refletidas nas detecções. Como resultado, as detecções podem ser movidas de um IV para outro. Com base nessa mudança e no valor da propriedade `sn_vul.show_last_open_detection`, os valores das detecções são acumulados para os IVs de origem e de destino.

Versões compatíveis de Vulnerability Response

Para obter mais informações sobre como instalar ou atualizar a aplicação Vulnerability Response, consulte Como instalar Vulnerability Response.

Integrações de terceiros compatíveis

Uma integração de terceiros compatível com a aplicação Vulnerability Response é necessária para detecções de itens vulneráveis. As seguintes integrações de terceiros são compatíveis com a aplicação Vulnerability Response para detecções de item vulnerável:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Qualys Host Detection Integration
- Depósito de dados da Rapid7:
  - Integração de item vulnerável
  - Integração de resolução de item vulnerável
- Integração de resolução de item vulnerável Rapid7 (InsightVM)
  - Insight VM integration
  - Integração de item vulnerável - API
- Tenable Vulnerability Integration
- Microsoft Defender Threat and Vulnerability Management

Essas integrações de terceiros estão disponíveis com uma assinatura separada da ServiceNow Store. Para obter mais informações sobre essas integrações, consulte Integrações do Vulnerability Response e Security Operations e o ServiceNow Store para obter mais informações sobre como obter o direito.

Para verificar se o scanner de terceiros está configurado para importação, consulte Instalar e configurar a aplicação Rapid7 Integration for Security Operations e Instalar o Qualys Vulnerability Integration.

Termos-chave para detecções de item vulnerável

Vulnerabilidade

Dados sobre pontos fracos em software, sistemas operacionais e ativos importados de fontes internas e externas. Esses dados são importados e comparados aos ativos existentes (itens de configuração, ICs) listados no CMDB.

Item vulnerável

Um item vulnerável é criado ou atualizado quando uma vulnerabilidade importada corresponde a um IC no CMDB.

Detecção

Uma ocorrência única e distinta de uma vulnerabilidade, conforme relatado por um scanner conhecido como Detecção de item vulnerável no ambiente Now Platform. Uma detecção inclui dados aprimorados sobre uma vulnerabilidade e todos os itens vulneráveis correspondentes. Esses dados são exibidos no registro de detecção (nº de VID) e na exibição da lista de itens vulneráveis que inclui os seguintes detalhes:

- Encontrado pela primeira vez (dados)
- Último encontrado (data)
- Nome DNS
- Net BIOSname
- Endereço IP
- Porta
- Protocolo
- Prova
- SSL
- Horas encontradas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Adicionar uma regra de negócios na tabela de detecção afetará o desempenho da ingestão.

Chave de detecção

Uma combinação de hash de campos que fornecia uma maneira de identificar e vincular uma detecção a um item vulnerável. As chaves de detecção são específicas da integração.

Configurações de chave de detecção

Scanner	Vulnerabilid	Porta	Protocolo	ID do ativo	Prova	NIC
Qualys	Sim	Sim	Sim	Sim	Não	N/D
Tenable	Sim	Sim	Sim	Sim	Não	N/D
Rapid7	Sim	Sim	Sim	Sim	Sim (não faz distinção entre maiúsculas e minúsculas)	Sim

Nota:

- Se a chave de detecção não for especificada, ou para versões anteriores a Vulnerability Response 14.0, a chave de detecção será uma combinação de entrada de vulnerabilidade, porta, protocolo, ID de ativo e prova.
- A partir da v19.0 de Vulnerability Response, uma nova chave de detecção NIC é adicionada para Rapid7 InsightVM, que é ativado por padrão. As detecções existentes sem NIC são atualizadas com a primeira NIC de entrada na carga útil de Rapid7. A chave de detecção é recalculada e preenchida novamente na detecção, incluindo o NIC. Novas detecções serão criadas se detecções semelhantes forem vistas com diferentes valores de NIC. Esses dados não são acumulados na tabela Item vulnerável. O valor do NIC é armazenado em uma nova coluna na tabela sn_vul_detection_key_config e sn_vul_detection.

Duplicata

O processo usado pela aplicação Vulnerability Response de recolher detecções individuais em um único IV quando os dados atendem a determinados critérios codificados.

ID externo do IV

O valor armazenado no campo ID externo da tabela IV. Este valor é um hash composto pela combinação de chaves em um IV que representa o que o torna exclusivo na aplicação. Ele é composto por um IC e uma entrada vulnerável.

Reabrir itens vulneráveis resolvidos

Itens vulneráveis definidos como **Resolvidos** na sua instância Now Platform, mas não transicionados para **Encerrado/Corrigido** pelas execuções de integração subsequentes, serão reabertos se forem detectados durante novas verificações.

Os IVs encerrados com um subestado **fixo** ou **obsoleto** serão reabertos se uma nova detecção for criada e os IVs puderem ser correspondidos com a nova vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

De acordo com a inclusão de script, *DetectionBase*, método *_shouldReOpenVI()*, se o VIT foi **encerrado** anteriormente com subestado **Fixo**, **Obsoleto**ou **IC desativado**, ele será reaberto e a detecção será mapeada para o VIT existente.

Por exemplo, digamos que a data de encerramento de um VIT seja posterior à data last_found de uma detecção. Você esperaria que esses registros de VIT permanecessem fechados. No entanto, se você vir um VIT encerrado anteriormente reaberto, isso significa que o VIT foi encerrado por uma detecção anterior e a vulnerabilidade foi encontrada novamente em uma verificação posterior. Quando é encontrada uma nova detecção que corresponde ao VIT encerrado que tem a mesma vulnerabilidade no item de configuração do VIT, o VIT é reaberto.

Para Rapid7 detecções, agora está disponível uma opção na página de configuração do Rapid7 em sua instância para reabrir IVs resolvidos por idade. Se habilitado, os IVs definidos como **Resolvidos**, mas não transicionados para **Encerrado/Corrigido** pelas verificações subsequentes, retornam para **Aberto** após o número de dias inserido.

Para Qualys detecções, se o scanner continuar a encontrar IVs que foram definidos como **Resolvidos**, mas não transicionados para **Encerrado/Corrigido** pelas verificações subsequentes, esses IVs retornam para **Aberto** quando a última data encontrada for posterior à data Resolvido.

Exibir dados de detecção

Você exibe os dados importados das detecções de item vulnerável no registro IV. Para obter mais informações, consulte Exibir Vulnerability Response dados de detecção de item vulnerável e Verificar Vulnerability Response registros de dados de detecção de item vulnerável na execução de integração (VINTRUN).

Solução de gerenciamento de vulnerabilidade

Correlacione automaticamente as vulnerabilidades em seu ambiente com as soluções que podem corrigi-las. Identifique as ações de correção que se aplicam às suas vulnerabilidades e priorize-as pela maior redução no risco de vulnerabilidade.

Solução de gerenciamento de vulnerabilidade

As equipes de segurança e TI geralmente gastam um tempo significativo pesquisando descobertas de vulnerabilidade para identificar os tratamentos mais eficazes para o ambiente. Dado o volume e a complexidade das vulnerabilidades em grandes organizações, traduzir as descobertas de vulnerabilidade em tarefas de correção é um processo manual, entediante e sujeito a erros.

Com Solução de gerenciamento de vulnerabilidade, você pode correlacionar automaticamente suas descobertas de vulnerabilidade com as soluções que as corrigem. Identifique os patches de software, as atualizações de configuração e outros controles que têm o maior impacto para sua organização sem a sobrecarga manual.

Requisitos do Solução de gerenciamento de vulnerabilidade

Solução de gerenciamento de vulnerabilidade é um recurso disponível na aplicação Vulnerability Response. Solução de gerenciamento de vulnerabilidade requer uma assinatura separada.

Para obter mais informações sobre como obter direitos para aplicações do ServiceNow Store, consulte Obter direito para um produto ou aplicação Security Operations. Consulte Instalar a aplicação Solução de gerenciamento do Vulnerability Response para obter mais informações sobre como instalar a aplicação depois de baixá-la em sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de instalado, o Solução de gerenciamento de vulnerabilidade fornece acesso aos dados da solução Microsoft Security Response Center e Red Hat de dentro de Vulnerability Response.

Nota:

Você pode configurar as duas aplicações da solução no Assistente de configuração. Consulte Configurar integrações de soluções instaladas para Solução de gerenciamento de vulnerabilidade usando o Assistente de configuração.

Consulte Noções básicas sobre o Integração com a solução Microsoft Security Response Center e Noções básicas sobre o Red Hat Solution Integration para obter mais informações sobre as soluções importadas.

Versões disponíveis

Para a versão mais atual de Solução de gerenciamento de vulnerabilidade, verifique se você tem a versão mais atual de Vulnerability Response instalada.

Versão de lançamento de Solução de gerenciamento de vulnerabilidade	Versões compatíveis de Vulnerability Response	Notas de versão
Solução de gerenciamento de vulnerabilidade v10.3	Vulnerability Response v18.0	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Noções básicas sobre soluções e substituição

Uma atualização substituída é uma substituição completa de uma versão ou versões anteriores. Por exemplo, uma atualização de hotfix pode ser substituída por um Service Pack. As soluções estão relacionadas a vulnerabilidades. As soluções também podem estar relacionadas a outras soluções em uma cadeia de substituição. As soluções também abordam vulnerabilidades em soluções anteriores, já que são cumulativas. Solução de gerenciamento de vulnerabilidade associa automaticamente vulnerabilidades de soluções anteriores a soluções substitutas. Se uma vulnerabilidade mais antiga for encontrada, qualquer solução de substituição mais alta poderá resolvê-la, mas a solução de substituição mais alta será a preferencial, já que é a mais cumulativa.

Soluções potenciais versus preferenciais

Uma possível solução é aquela que pode solucionar uma vulnerabilidade. As vulnerabilidades geralmente têm muitas soluções possíveis. Uma solução preferencial é a solução única direcionada para corrigir uma vulnerabilidade ou item vulnerável (IV). Ele comunica a intenção e permite métricas de implantação mais detalhadas.

Soluções Preferenciais

Solução de gerenciamento de vulnerabilidade define automaticamente a solução mais eficaz (**Solução preferencial**) para a vulnerabilidade detectada com base na substituição mais alta quando existe apenas uma solução de substituição mais alta. Se houver mais de uma substituição mais alta para a vulnerabilidade, nenhum valor será definido. Em Vulnerability

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Response, uma **Solução preferencial** é a solução Microsoft Security Response Center ou Red Hat com a maior substituição derivada das soluções associadas à vulnerabilidade.

Os valores de solução preferencial podem ser definidos no item vulnerável ou na vulnerabilidade. Quando definido diretamente na vulnerabilidade, todos os itens vulneráveis associados à vulnerabilidade herdam essa solução. Altere os valores de **Solução Preferencial** para vários itens vulneráveis usando o recurso de edição em massa. Quando editado em massa, somente a **Solução preferencial** no item vulnerável é atualizada, já que definir a **solução preferencial** no nível de entrada da vulnerabilidade definiria a **solução preferencial** para todos os novos IVs daqui para frente. A edição em massa se aplica somente aos itens vulneráveis atuais.

Nota:
Se houver várias soluções de substituição mais alta para uma vulnerabilidade, os valores de **Solução Preferencial** no nível de vulnerabilidade serão apagados, já que essa solução depende do ativo afetado. Quando houver várias soluções de substituição mais alta para uma vulnerabilidade, defina uma **Solução preferencial** no item vulnerável. Você pode definir uma solução diferente usando a lista de **pesquisa** no formulário de **item vulnerável**.

Todas as soluções preferenciais para os itens vulneráveis em uma tarefa de correção estão em uma lista relacionada no registro da **Tarefa** de correção.

Nem todas as importações de solução resultam em atualizações de dados completas. O processo de substituição é atualizado quando:

- Um item vulnerável foi criado.
- Os dados foram alterados em um IV ativo.
- Um novo mapeamento é criado para uma entrada de terceiros com o CVE.
- Novos dados de solução foram liberados desde a última importação, uma solução existente foi atualizada ou, com qualquer mudança manual que afeta as métricas da solução..

O que Solução de gerenciamento de vulnerabilidade faz

- Associa automaticamente novos itens vulneráveis e tarefas de correção a soluções durante Integração com a solução Microsoft Security Response Center e Red Hat Solution Integration importação.

  MSRC As soluções estão associadas ao boletim mais recente em que a solução aparece.

- Associa automaticamente itens vulneráveis e tarefas de correção a soluções quando os registros de vulnerabilidade são associados manualmente a soluções.

  Nota:
  Itens vulneráveis reatribuídos manualmente a outra solução não são atualizados automaticamente com as mudanças de solução no nível de vulnerabilidade.

- MSRC: cria cadeias de substituição durante a importação que você pode exibir na lista relacionada da solução.
- Indica se uma solução é uma solução de substituição mais alta ou não.
- Lista a **pontuação de risco** da solução associada a cada solução para fornecer a você as maiores oportunidades de redução de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Mantém o **status** de correção das soluções em **entradas de vulnerabilidade de terceiros**, **tarefas**de correção e registros de **solução de vulnerabilidade** para que você possa acompanhar o andamento da correção.

  Ele contém:

  - Contagens de itens vulneráveis por porcentagem corrigida, para os IVs com Soluções Preferenciais, com e sem esses IVs no estado Adiado.
  - Contagens de itens de configuração (IC) por porcentagem corrigida, para os IVs com Soluções preferenciais, com e sem esses IVs no estado Adiado.
  - Contagens de itens vulneráveis por porcentagem corrigida, para esses IVs com possíveis soluções, com e sem esses IVs no estado Adiado.
  - Contagens de itens de configuração por porcentagem corrigida, para os IVs com Soluções preferenciais, com e sem esses IVs no estado Adiado.

O que você pode fazer com Solução de gerenciamento de vulnerabilidade

- Crie, atualize, exiba ou exclua soluções associadas a vulnerabilidades para que você possa rastrear soluções de vulnerabilidade que não sejam cobertas pelo conteúdo da solução de terceiros. A integração da solução com o data warehouse Rapid7 não é compatível no momento.
- Associe vulnerabilidades de terceiros e entradas de NVD a um registro de solução.
- Remova e reassocie itens vulneráveis e tarefas de correção com uma solução.
- Exiba a **Solução Preferencial** aplicável a uma determinada vulnerabilidade nos formulários de item vulnerável e de vulnerabilidade.
- Exiba uma lista relacionada de **Soluções preferenciais** em formulários de tarefa de correção que listam todas as soluções que foram preferenciais por pelo menos um IV ativo nesse grupo.
- Exiba os detalhes do **status** de correção em uma solução que mostra a redução de risco associada à implantação da **solução preferencial** em vulnerabilidade, item vulnerável, tarefas de correção e formulários de solução.
- Exibir vulnerabilidades aplicáveis a uma determinada solução no formulário de solução.
- MSRC: exibe as soluções de substituição de uma determinada solução em uma vulnerabilidade para encontrar a atualização mais recente a ser implantada ou uma atualização anterior, mais focada e eficiente.
- Exiba listas de soluções classificadas por diferentes características.
  - Todos: soluções classificadas por data de publicação e número.
  - MSRC: substituição mais alta: soluções com itens vulneráveis ativos e não adiados. Classificado por **Maior substituição**, **Data de publicação**e **Número**.
  - Com itens vulneráveis: soluções com itens vulneráveis ativos não adiados. Classificado por **Substituição mais alta** ou **Preferencial**, **Pontuação de risco**e **Número**. Se implantadas, as principais entradas na lista fornecem a maior redução de risco para os ativos em seu ambiente.

Pontuação de risco e classificação de risco do registro da solução

Nota:
A **pontuação de risco** do registro da solução e a **classificação** de risco são distintas dos campos usados para vulnerabilidades, itens vulneráveis e tarefas de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A **pontuação de risco** do registro de solução é um cálculo ponderado com base na **pontuação de risco** do item vulnerável e em uma contagem de itens vulneráveis ativos com esta solução como sua **possível solução**. **A pontuação de risco** da solução fornece uma estimativa da redução no risco que a solução deve realizar.

A pontuação de risco do registro da solução é calculada da seguinte forma:

- Ele começa obtendo 85% da **pontuação de risco** mais alta ou máxima de um item vulnerável ativo com essa possível solução.
- **A pontuação de risco** do registro da solução tabula o número total de itens vulneráveis com essa possível solução. Para cada intervalo do número de itens vulneráveis, ele adiciona alguns pontos e chega a um total.
  - 0 a 09 itens vulneráveis não adicionam pontos
  - De 10 a 99 itens vulneráveis adicionam 5 pontos
  - De 100 a 999 itens vulneráveis adicionam 10 pontos
  - 1000 e além de itens vulneráveis adicionam 15 pontos

  Por exemplo, para uma **pontuação de risco** de item vulnerável de 80, a **pontuação de risco** do registro de solução iniciaria em 68. Se houver um total de 200 itens vulneráveis ativos com essa possível solução, a **pontuação final de risco** da solução será 78.

A **classificação de risco** do registro da solução separa a **pontuação de risco** do registro da solução em intervalos de Crítico a Nenhum. A classificação de **risco da solução classifica** a redução de risco dos itens vulneráveis que esta solução corrige.

Até o VR v16.1, as classificações de risco separavam a **pontuação de risco** da solução resultante nos seguintes intervalos:

- 1 - Crítico (**pontuação de risco de**solução de 90+)
- 2 - Alta (**pontuação de risco**do registro da solução 70-89)
- 3 - Médio (30-69 **Pontuação de risco**do registro da solução)
- 4 - Baixo (1-29 **Pontuação de risco**do registro da solução)
- 5 - Nenhum (0 **pontuação de risco do**registro da solução)

A partir do VR v16.1, as classificações de risco separam a **pontuação de risco** da solução resultante nos seguintes intervalos para a Gestão de soluções:

- 1 - Crítico (**pontuação de risco de**solução de 90+)
- 2 - Alta (**pontuação de risco**do registro da solução 70-89)
- 3 - Médio (40-69 **Pontuação de risco**do registro da solução)
- 4 - Baixo (1-39 **Pontuação de risco**do registro da solução)
- 5 - Nenhum (0 **pontuação de risco do**registro da solução)

Casos de Uso

Exiba o andamento da implantação do status de um ciclo de patch atual usando o módulo de substituição mais alto, classificado por data.

Exiba soluções de maior valor usando o módulo Com itens vulneráveis, classificadas por pontuação de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As listas de soluções comunicam os principais detalhes da solução, pontuações de risco e métricas de implantação. Use a **pontuação de risco** e as contagens de IV ativas para priorização. Veja quais soluções no ciclo de patch atual não estão progredindo, possivelmente uma indicação de um pré-requisito de implantação ausente.

Nota:
Adicione **%VIs corrigidos (percent_nd_pref_vis_remediated)** no menu **Personalizar colunas da lista** para obter o andamento da correção no formulário Soluções de vulnerabilidade.

Noções básicas sobre o Integração com a solução Microsoft Security Response Center

Analise e implemente as soluções de correção propostas fornecidas pelo Integração com a solução Microsoft Security Response Center.

Integração com a solução Microsoft Security Response Center está incluído no recurso [Solução de gerenciamento de vulnerabilidade de Vulnerability Response, disponível por assinatura separada. Consulte Solução de gerenciamento de vulnerabilidade para obter mais informações sobre como Vulnerability Response incorpora soluções.

Microsoft Security Response Center investiga relatórios de vulnerabilidades de segurança que afetam os produtos e serviços da Microsoft e fornece informações da solução para ajudar a gerenciar os riscos de segurança. Soluções são correções conhecidas importadas para o seu Integração com a solução Microsoft Security Response Center do produto Microsoft Security Response Center.

O Integração com a solução Microsoft Security Response Center contém pontos de entrada para o produto Microsoft Security Response Center, invocados como trabalhos programados. Os trabalhos programados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades. Os trabalhos programados são executados automaticamente e na ordem especificada. Você também pode executar trabalhos programados individuais manualmente.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Versões disponíveis

Para a versão mais atual das soluções Solução de gerenciamento de vulnerabilidade e Microsoft Security Response Center, verifique se você tem a versão mais atual do Vulnerability Response instalada.

Para obter mais informações sobre como instalar e configurar Solução de gerenciamento de vulnerabilidade e integrações de solução, consulte Instalar a aplicação Solução de gerenciamento do Vulnerability Response e Configurar integrações de soluções instaladas para Solução de gerenciamento de vulnerabilidade usando o Assistente de configuração.

Versão de lançamento de Vulnerability Response	Versão de Solução de gerenciamento de vulnerabilidade	Notas de versão
Vulnerability Response v15.0	v10.3	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções

Integração com a solução Microsoft Security Response Center As tarefas do envolvem as funções a seguir.

- sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto): pode ler, gravar e excluir registros.
- sn_vul.vulnerability_write: pode ler e gravar registros.
- sn_vul.vulnerability.read: pode ler registros.
- sn_vul.remediation_owner: pode ler e escrever anotações internas em registros atribuídos ao grupo de especialistas de correção ou ao indivíduo. (Contido na função itil.)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Integração com a solução Microsoft Security Response Center

Para exibir o Integração com a solução Microsoft Security Response Center, navegue até **Todos** > **Vulnerability Response** > **Administração** > **Integrações**.

A integração a seguir está incluída no sistema de base.

Integração com a solução Microsoft Security Response Center

Integração	Descrição
Integração da Solução do Microsoft Security Response Center	Recupera soluções e mapeamento do banco de dados nacional de vulnerabilidades (NVD) para associar soluções a vulnerabilidades, itens vulneráveis e tarefas de correção. **Nota:** O Integração com a solução Microsoft Security Response Center não fornece soluções anteriores a 2016.

Soluções

Para exibir soluções importadas em uma lista, consulte Exibir uma solução.

Noções básicas sobre o Red Hat Solution Integration

Você pode revisar e implementar as soluções de correção propostas fornecidas por Red Hat Solution Integration na aplicação Vulnerability Response.

Red Hat Solution Integration está incluído no recurso [Solução de gerenciamento de vulnerabilidade de Vulnerability Response, disponível por assinatura separada. Consulte Solução de gerenciamento de vulnerabilidade para obter mais informações sobre como Vulnerability Response incorpora soluções.

Red Hat Solution Integration investiga relatórios de vulnerabilidades de segurança que afetam Red Hat produtos e serviços e fornece informações de solução para ajudar a gerenciar riscos de segurança. Soluções conhecidas como correções são importadas para seu Red Hat Solution Integration de Red Hat.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A partir da versão 21.0 do Vulnerability Response, o Red Hat transmite cargas úteis no formato CSAF (Common Security Advisory Framework) em vez do formato CVRF (Common Vulnerability Reporting Framework). O CSAF, um padrão baseado em XML, difere do CVRF na estrutura e no formato. Para acomodar essa mudança, um novo analisador de CSAF foi desenvolvido. Este analisador interpreta o formato CSAF, extraindo os campos obrigatórios para preencher as tabelas de acordo.

Nota:
Por padrão, você receberá a carga no formato CSAF.

As extrações a seguir mostram o script de integração para analisar a carga recebida de Red Hat nos formatos CSAF e CVRF, respectivamente.

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

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

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

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

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

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

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

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

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

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

Red Hat Solution Integration contém pontos de entrada para o produto Red Hat, invocado como um trabalho programado. O trabalho programado simplifica o ciclo de vida de correção de vulnerabilidade, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades. Ele é executado automaticamente. Você também pode executar o trabalho programado manualmente.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Versões disponíveis

Para a versão mais atual das soluções Solução de gerenciamento de vulnerabilidade e Red Hat, verifique se você tem a versão mais atual do Vulnerability Response instalada.

Para obter mais informações sobre como instalar e configurar Solução de gerenciamento de vulnerabilidade e integrações de solução, consulte Instalar a aplicação Solução de gerenciamento do Vulnerability Response e Configurar integrações de soluções instaladas para Solução de gerenciamento de vulnerabilidade usando o Assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versão de lançamento de Vulnerability Response	Versão de Solução de gerenciamento de vulnerabilidade	Notas de versão
Vulnerability Response v15.0	v10.3	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Funções

Red Hat Solution Integration tarefas envolvem a seguinte função: sn_vul.configure_rhsa_integration

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Red Hat Solution Integration

Para exibir o Red Hat Solution Integration, navegue até **Vulnerability Response** > **Administração** > **Integrações**.

A integração a seguir está incluída no sistema de base.

Integração do Red Hat

Integração	Descrição
Red Hat Solution Integration	Recupera soluções e mapeamento do banco de dados nacional de vulnerabilidades (NVD) para associar soluções a vulnerabilidades, itens vulneráveis e tarefas de correção.

Soluções

Para exibir soluções importadas em uma lista, consulte Exibir uma solução.

Rapid7 gestão de soluções

Soluções são correções conhecidas que são importadas para o seu Rapid7 Vulnerability IntegrationRapid7 do data warehouse [] ou Rapid7 InsightVM. Rapid7 O data warehouse importa soluções e soluções de substituição. Com Rapid7 InsightVMo, você obtém soluções como parte da Rapid7 Vulnerable Item Integration - API.

A partir da versão 21.0 de Vulnerability Response, há uma mudança na forma como as soluções são criadas por Rapid7 InsightVM. Em vez de contar com os campos **solution_summary**, **solution_fix**ou **solution_type**, Rapid7 InsightVM agora cria soluções usando o solution_id fornecido pelo scanner. Isso significa que, mesmo que esses campos estejam vazios, uma solução será criada desde que um ID de solução esteja disponível.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para exibir soluções importadas como uma lista, navegue até **Rapid7** > **Soluções**.

Se o plug-in Solução de gerenciamento de vulnerabilidade estiver ativado, a versão mais recente do Rapid7 Vulnerability Integration fornecerá os seguintes recursos principais em relação às soluções:

- O gerenciamento de soluções Rapid7 é movido para o gerenciamento de soluções de vulnerabilidade.
- Uma nova integração Rapid7 Prerequisito Solution Management para o data warehouse. A integração busca a solução de pré-requisito do data warehouse Rapid7.
- A lista relacionada de Rapid7 (solução) em entradas de terceiros (TPE) está oculta.
- Os dados importados anteriormente podem ser exibidos no novo modelo de dados. As Soluções Rapid7, a Substituição de solução e o mapa de Solução de vulnerabilidade são reimportados e o campo **Importar desde** é definido como vazio. O campo é preenchido na Gestão de soluções.
- As detecções são atualizadas para preencher o campo de solução. As detecções mostram as soluções, pois elas fazem parte do Vulnerability Solution Management.
- Rapid7 obtém maior preferência sobre outras soluções ao definir a solução preferencial em TPE para Rapid7 data warehouse.
- As soluções acumulam itens vulneráveis (IV) de detecções para Rapid7 InsightVM.

Nota:
Se você não ativou o plug-in Solução de gerenciamento de vulnerabilidade, a aplicação funcionará como está.

Gerenciamento de soluções de vulnerabilidade

Se você ativou o plug-in Solução de gerenciamento de vulnerabilidade, as soluções Rapid7Rapid7 para o data warehouse [] e Rapid7 InsightVM] serão preenchidas na tabela Soluções de vulnerabilidade [sn_vul_solution]. No entanto, se você não ativou o plug-in Solução de gerenciamento de vulnerabilidade, o Rapid7 Vulnerability Integration funcionará como está e importará as soluções na tabela [sn_vul_r7_solution] personalizada.

Para exibir a tabela de soluções de vulnerabilidade, navegue até **Todos** > **Vulnerability Response** > **Soluções de vulnerabilidade** onde você pode exibir e comparar as soluções de diferentes fornecedores. Para exibir soluções importadas na tabela personalizada, navegue **Todos** > **Rapid7 Vulnerability Integration** > **Soluções**.

Nota:
Agrupe por origem para exibir soluções com base em fornecedores.

Integração da Gestão de soluções de pré-requisitos da Rapid7

Se você ativou o plug-in Solução de gerenciamento de vulnerabilidade, um script de correção será executado e mudará a ordem das integrações. A nova integração de solução de pré-requisito Rapid7 para data warehouse Rapid7 mapeia as soluções com as soluções de pré-requisito. As integrações são executadas na seguinte sequência:

1. Rapid7 Integração da Solução
2. Rapid7 Solução de pré-requisito
3. Rapid7 Integração da solução substituta

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Rapid7 Integração do mapa de solução de vulnerabilidade
5. Rapid7 VI Solution Integration (de v19.0 de Vulnerability Response)

Nota:
Se você executar as integrações manualmente, comece com a integração da solução Rapid7. Não altere a cadeia de Próxima integração na integração Rapid7. A sequência é definida na coluna Próxima integração.

Lista relacionada Rapid7 (Soluções) em TPE

Se você ativou o plug-in Solução de gerenciamento de vulnerabilidade, poderá fazer o seguinte:

- Você pode exibir os TPEs navegando até **Todos** > **Vulnerability Response** > **Terceiros**.
- Você não pode ver a lista relacionada de Soluções (Rapid7), que estava disponível nas versões mais antigas.
- Você pode ver as soluções relacionadas ao Rapid7 na lista relacionada Soluções junto com as soluções de outras fontes, como RedHat, Microsoft (MSRC) e assim por diante.

Se você não ativou o plug-in Solução de gerenciamento de vulnerabilidade, ocorre o seguinte:

- A funcionalidade de listas relacionadas permanece a mesma.
- Você pode ver a lista relacionada de Soluções (Rapid7).
- A lista relacionada Soluções está oculta.

Solução preferencial em TPE e IVs

Rapid7 obtém a solução do data warehouse no nível de entrada de terceiros (TPE) e para Rapid7 InsightVM no nível de detecção.

Para um data warehouse Rapid7, a solução é gerenciada da seguinte maneira:

- A solução preferencial é definida no TPE com base no mapeamento de vulnerabilidade e solução.
- Se a vulnerabilidade de Rapid7 tiver uma única solução de substituição mais alta de Rapid7, ela será definida como a solução preferencial, independentemente de outras soluções de fornecedores anexados a essa vulnerabilidade.
- Em todos os outros casos, o fluxo da solução preferencial permanece o mesmo. Para obter mais informações sobre o comportamento padrão das soluções preferenciais, consulte Solução de gerenciamento de vulnerabilidade.

Para Rapid7 InsightVM, a solução é gerenciada da seguinte maneira:

- A solução preferencial é acumulada de detecções para IVs.
- Se houver uma única detecção e solução de Rapid7, a solução será acumulada para IV.
- Se houver várias detecções e todas tiverem a mesma solução de Rapid7, a solução será acumulada para IV.
- Se várias detecções tiverem várias soluções de Rapid7, a solução mais recente será acumulada para o IV.

A partir da v19.0 de Vulnerability Response, a solução preferencial, gerada pelo Rapid7 Data Warehouse, é preenchida diretamente em itens vulneráveis por Rapid7 ignorando a

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

necessidade de Solução de gerenciamento de vulnerabilidade. Essa mudança garante que qualquer incerteza sobre possíveis soluções para esses itens vulneráveis seja eliminada.

Para alcançar esse preenchimento direto por meio de Rapid7, as seguintes etapas são realizadas:

- Uma nova integração, Rapid7 VI Solution Integration, é estabelecida e integrada ao fluxo de trabalho de integração de vulnerabilidade Rapid7 existente.
- Uma nova tabela [sn_vul_r7_rapid7_vi_solution_import] é criada.
- Um novo mapa de transformação Rapid7 VI Solution Transform é criado.
- A inclusão de script Rapid7AssetsImportProcessor foi modificada para excluir o processamento de soluções geradas pelo Rapid7 em Solução de gerenciamento de vulnerabilidade.

Após a execução da Rapid7 VI Solution Integration, os dados não processados obtidos de Rapid7 são armazenados na tabela recém-criada. Posteriormente, a transformação da solução Rapid7 VI é acionada, processando esses dados e preenchendo a solução preferencial diretamente na tabela de itens vulneráveis.

Nota:
A integração da solução Rapid7 VI preenche a solução preferencial exclusivamente quando o plug-in Solução de gerenciamento de vulnerabilidade é instalado.

Cadeia de substituição de solução importada do data warehouse Rapid7 para uma vulnerabilidade

Você pode exibir as soluções de substituição de uma solução clicando em uma solução de vulnerabilidade e clicando na lista relacionada de Soluções de substituição. Você pode exibir as soluções anteriores clicando na lista relacionada Soluções anteriores. Quando você anexa qualquer solução ao TPE, a solução substituta dessa solução é anexada a esse TPE.

Alterar a profundidade máxima da cadeia de substituição da solução no gráfico por propriedade do sistema

A cadeia de substituição de solução recebida no modelo de dados Rapid7 é muito longa para criar o gráfico durante o preenchimento da solução preferencial. Portanto, para restringir a profundidade da cadeia, uma propriedade do sistema chamada *sn_vul.max_recursion_depth* com um valor 500 é criada. Se a profundidade da cadeia for maior que 500, o restante da cadeia será ignorado. Para alterar a profundidade máxima da cadeia, navegue até a tabela [sys_properties] e altere o valor da propriedade.

Atualização da aplicação Rapid7

Se você atualizar o plug-in Rapid7 Vulnerability Integration e ainda não tiver ativado o plug-in Solução de gerenciamento de vulnerabilidade, a aplicação funcionará como está.

Se você ativar o plug-in Solução de gerenciamento de vulnerabilidade antes ou depois de atualizar a aplicação Rapid7, o campo **Importar desde** permanecerá vazio para as seguintes integrações:

- Integração da solução substituta Rapid7
- Rapid7 Vulnerability Solution Map Integration

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Integração da Solução Rapid7

Nota:
Na próxima execução de integração, os dados são preenchidos na tabela de solução de vulnerabilidade.

Para Rapid7 InsightVM, os dados são recebidos no nível de detecção. Quando a integração Rapid7 InsightVM é executada, as soluções são importadas na tabela de soluções de vulnerabilidade.

Estrutura genérica para ingerir dados de qualquer fornecedor de solução

O Common Vulnerability Reporting Framework (CVRF) é uma linguagem baseada em XML que permite o compartilhamento de informações críticas relacionadas à segurança em um formato de relatório padrão. Como o CVRF acelera a troca e o processamento de informações, uma estrutura genérica para integração de inteligência de solução é fornecida para habilitar o suporte para fornecedores que oferecem suporte ao formato CVRF. Esses fornecedores principais incluem Oracle, Red Hat, Ciscoe Microsoft.

A gestão de soluções compatível com CVRF inclui os seguintes recursos principais:

- Configuração por meio do Assistente de configuração
- Suporte para importação de dados CVRF por meio de importação de arquivo
- Suporte para importação de dados CVRF por meio de URL CVRF
- Suporte para importação de dados CVRF por meio de consultorias
- Mapeamento de soluções com vulnerabilidades relacionadas

O plug-in Vulnerability Response se encarrega de atualizar os status das métricas da solução criada.

Para obter mais informações, consulte:

- Configurar provedores de soluções de vulnerabilidade
- Importar dados do Common Vulnerability Reporting Framework por meio da importação de arquivo
- Configurar aliases de conexão e credencial
- Configurar um fornecedor do Common Vulnerability Reporting Framework que não seja a Cisco
- Importar dados do Common Vulnerability Reporting Framework de consultorias
- Importar dados do Common Vulnerability Reporting Framework (CVRF) por meio do URL do CVRF
- Importar dados do Common Vulnerability Reporting Framework de consultorias
- Importação de dados do Common Vulnerability Reporting Framework para solução de problemas

Preparando a integração da solução Common Vulnerability Reporting Framework (CVRF)

Use o Assistente de configuração para se preparar para implementar uma integração de inteligência de solução para todos os fornecedores que oferecem suporte ao formato de dados do Common Vulnerability Reporting Framework (CVRF).

Antes de começar

Para integrar com os fornecedores que fornecem as soluções, certifique-se de executar as tarefas na check-list a seguir. Você pode imprimir a check-list e verificar se os itens listados foram concluídos antes de instalar a aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
Aplicações dependentes ☐	Verifique se as seguintes aplicações estão instaladas a partir de ServiceNow Store: • Vulnerability Solution Management: para obter mais informações sobre como instalar Solução de gerenciamento de vulnerabilidade, consulte Instalar Vulnerability Response aplicações de terceiros usando o Assistente de configuração e Instalar a aplicação Solução de gerenciamento do Vulnerability Response. • Vulnerability Response: para obter mais informações sobre como instalar e ativar a aplicação Vulnerability Response, consulte Como instalar Vulnerability Response. Esta integração requer a versão 16.1 de Vulnerability Response ou posterior.
Credenciais de conta de terceiros ☐	Verifique se você tem credenciais de conta de terceiros disponíveis. Eles são necessários para editar algumas integrações de solução.
Autenticação do fornecedor ☐	Verifique se você autenticou os fornecedores para importação de soluções usando as APIs. Para obter mais informações sobre como autenticar fornecedores, consulte Configurar aliases de conexão e credencial. Se você não quiser configurar um fornecedor baseado em API, poderá ignorar esta etapa.
Personalização de fluxo e ação de fluxo ☐	Se você quiser configurar um fornecedor baseado em API que não seja a Cisco, deverá personalizar o fluxo e a ação de fluxo para extrair uma chave exclusiva e um URL CVRF da resposta de um comunicado. **Nota:** A publicação de URL CVRF não é padrão entre os fornecedores. Para personalizar o fluxo para fornecedores que não sejam a Cisco, consulte Configurar um fornecedor do Common Vulnerability Reporting Framework que não seja a Cisco. Você pode ignorar esta etapa se eles não quiserem configurar fornecedores que não sejam a Cisco. Por padrão, o fluxo para Cisco foi enviado com a aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

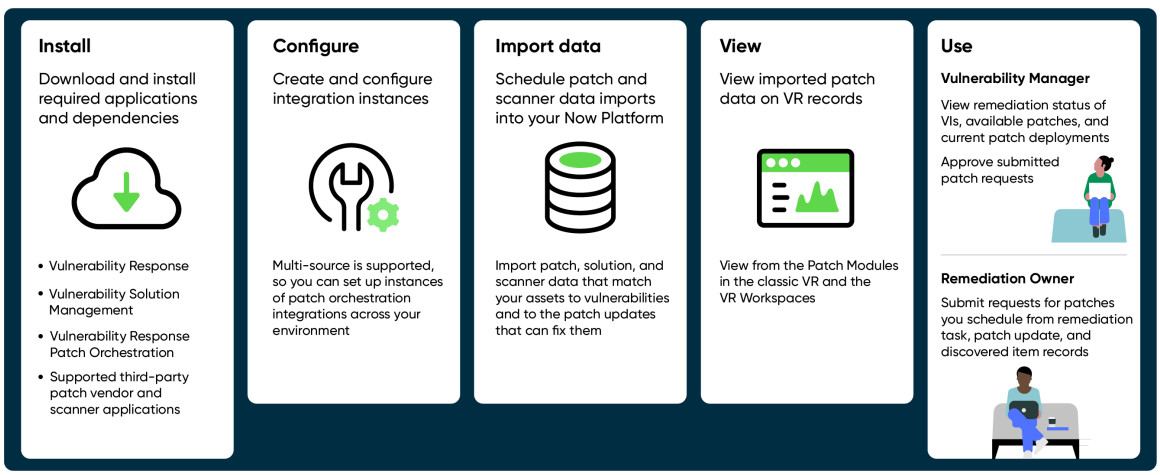
Tarefa	Descrição
Funções ☐	Verifique se você tem um grupo de administradores ou usuário que pode gerenciar a integração. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidade (sn_vul.vulnerability_admin) e outras funções.

Orquestração de patches com Vulnerability Response

Você pode gerenciar patches e implantações de patch para vulnerabilidades críticas para grandes grupos de ativos com a Orquestração de patches com Vulnerability Response. Vulnerability Response Patch Orchestration e as integrações de orquestração de patches estão disponíveis no ServiceNow® Store.

Noções básicas sobre orquestração de patches com Vulnerability Response

A orquestração de patches com Vulnerability Response usa dados de importações programadas de integrações de soluções de terceiros, fornecedores de patches e scanners de vulnerabilidade. Esses dados são correlacionados na aplicação Vulnerability Response. Essa organização de dados permite que você conclua as etapas do ciclo de correção de vulnerabilidade. Comece identificando vulnerabilidades, aplique patches e atualizações e, por fim, feche itens vulneráveis usando dados de scanner de terceiros, tudo isso de dentro da sua instância Now Platform®.



A orquestração de patches com Vulnerability Response é compatível com o ambiente clássico e os espaços Vulnerability Response.

Para obter informações sobre orquestração de patches nos espaços, consulte Orquestração de patches com os espaços Vulnerability Response.

Com a orquestração de patches em Vulnerability Response, os gerentes e analistas de vulnerabilidade e os especialistas em correção de TI podem executar as seguintes tarefas de correção:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Veja mais contexto e informações sobre os tipos de patches e fornecedores que compõem suas soluções (patches).
- Exiba e monitore os dados de vulnerabilidade e solução, bem como o andamento da correção de vulnerabilidades de registros nos espaços Vulnerability Response ou no ambiente clássico.
- Implante patches compatíveis com fornecedores de soluções de terceiros para seus ativos Windows, CentOS, macOS, Oracle e outros em intervalos regulares e programados. Você pode programar patches fora do horário de expediente para evitar conflitos com os que estão no trabalho.
- Usando dados de detecção importados fornecidos por scanners de terceiros, identifique os ativos que têm vulnerabilidades e não foram corrigidos ou não foram atualizados com sucesso por patches programados.
- Inicie e programe os patches disponíveis para ativos que exigem atualizações de Atualização de patch, tarefa de correção e registros de item descoberto na aplicação Vulnerability Response.
- Monitore as implantações de patch com um processo de aprovação opcional para solicitações de patch enviadas por seus especialistas em correção.

Termos-chave

IC (Configuration Item, item de configuração)

ICs são os ativos existentes listados no seu Configuration Management Database (CMDB).

Item vulnerável (IV)

Uma vulnerabilidade importada que corresponde a um ativo existente no seu CMDB. Itens vulneráveis (VITs) são agrupados em tarefas de correção, ou listas, de acordo com determinados critérios que especificam ações de correção para IVs.

Instância

Refere-se a uma conta distinta de uma aplicação do fornecedor da solução. Por exemplo, cada conta de usuário pode ser uma instância na aplicação HCL BigFix. Este termo também se refere a um endereço da Web exclusivo e seguro para uma instância Now Platform®.

Solução

Existem dois tipos de soluções no contexto desta integração, potenciais e preferenciais. Uma possível solução é aquela que pode solucionar uma vulnerabilidade. As vulnerabilidades geralmente têm muitas soluções possíveis. Uma solução preferencial corresponde à solução mais eficaz para uma vulnerabilidade específica detectada.

Patch

Atualizações de software que corrigem vulnerabilidades. Os fornecedores de patch usam seus próprios nomes para patches, por exemplo, Na aplicação HCL BigFix, os patches são chamados de Fixlets.

Patch preferencial

Patches preferenciais são atualizações de software que têm como objetivo corrigir vulnerabilidades específicas. Os patches, uma vez implantados, são mapeados para os itens vulneráveis que estão relacionados a vulnerabilidades específicas e os corrigem.

Implantação

Para fins desta integração, a implantação se refere a quando você aplica, inicia ou programa um patch para uma máquina.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A implantação no Now Platform também pode se referir a uma integração que oferece suporte a várias origens. Uma única existência de integração é chamada de implantação da sua integração. Uma implantação se refere às integrações e produtos em seu ambiente. Por exemplo, você pode ter várias implantações de um scanner de terceiros ou uma integração de fornecedor de solução em seu ambiente.

Versões disponíveis de aplicações e dependências necessárias para a integração de orquestração de patches

- A aplicação Vulnerability Response e os plug-ins de dependência, Security Support Common e Security Support Orchestration.
- Solução de gerenciamento de vulnerabilidade.
- Vulnerability Response Aplicação Patch Orchestration disponível na ServiceNow® Store.
- Uma aplicação de fornecedor de patch de terceiros compatível, como a integração de orquestração de patches do Vulnerability Response com o HCL BigFix ou a integração de orquestração de patches do Vulnerability Response com o Microsoft SCCM.
- Integrações de scanner de terceiros compatíveis com o Vulnerability Response.

Funções necessárias

Os usuários precisam de funções específicas para a integração de orquestração de patches que você está usando para exibir dados e programar patches da aplicação Vulnerability Response. Consulte as informações de configuração das integrações compatíveis que você está usando listadas abaixo para obter mais informações.

- Noções básicas sobre a integração de orquestração de patches do BigFix HCL com Vulnerability Response e a integração de orquestração de patches do Vulnerability Response com o Microsoft SCCM.
- Nos espaços Vulnerability Response e no ambiente clássico, a função sn_vul_patch_orch.read_patch, que permite aos usuários exibir, mas não editar dados, é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst.

  As funções que você precisa atribuir que são necessárias para configurar as conexões com os fornecedores de patch e programar patches são específicas da integração. Consulte Configurar a integração de orquestração de patches Vulnerability Response com HCL BigFix e Configurar a Vulnerability Response Patch Orchestration com MS SCCM para obter mais informações.

Há um processo de envio e aprovação para solicitações de patch incluídas com as aplicações. Por padrão, uma propriedade do sistema é ativada [**sn_vul_patch_orch.patch_approval_required**] na aplicação Vulnerability Response Patch Orchestration em sua instância Now Platform.

Esta propriedade do sistema é ativada para que, quando as implantações de patch forem programadas, elas sejam enviadas para revisão e aprovação dos usuários atribuídos ao Nível 1 - Grupo de aprovação de atualizações de patch. Se você quiser que os usuários com a função sn_vul_patch_orch.configure_patch programem patches sem aprovação, desative a propriedade [**sn_vul_patch_orch.patch_approval_required**]. Você pode preferir deixar as aprovações ativadas para que os patches programados não entrem em conflito com o horário normal de trabalho. Se você desativar a propriedade do sistema de aprovação, qualquer usuário com a função sn_vul_patch_orch.configure_patch poderá programar e implantar patches sem revisão e aprovação.

Para obter mais informações e como desativar esta propriedade do sistema, consulte o tópico de configuração da sua integração compatível.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Configurar a integração de orquestração de patches Vulnerability Response com HCL BigFix.
- Configurar a Orquestração de patches do Vulnerability Response com a integração do SCCM Microsoft.

Programar patches de Vulnerability Response registros

Os especialistas em correção podem programar atualizações de patch para resolver itens vulneráveis e monitorar o andamento da correção, tudo a partir de registros na aplicação Vulnerability Response.

Você pode programar patches dos seguintes registros:

- Atualização de patch
- Tarefa de correção
- Item descoberto

Registros que acumulam contagens de IV ativas no Vulnerability Response

Para evitar possíveis problemas de desempenho com o acúmulo de todos os patches para todas as vulnerabilidades, o trabalho programado que seleciona as mudanças modifica somente a contagem de IV ativa. Essas mudanças de contagem e dados relacionados são acumulados para os seguintes registros na aplicação Vulnerability Response :

- VIT (item vulnerável)
- RT (tarefa de correção)
- Solução de vulnerabilidade
- Atualização de patch

Para obter mais informações sobre como exibir dados de patch e acúmulo de dados de patch para registros e exibir patches sem soluções, consulte os tópicos a seguir.

- Dados de patch e acúmulo de estado para orquestração de patches no Vulnerability Response.
- Exibição de dados de patch e programação de patches no Vulnerability Response.
- Exibir patches sem soluções em Vulnerability Response.

Edição em massa de itens vulneráveis com patches

Você pode editar em massa itens vulneráveis no ambiente clássico que tenham patches do ambiente clássico. Para obter mais informações sobre como a edição em massa funciona, consulte Editar itens vulneráveis em massa no Vulnerability Response. Os patches preferenciais para todos os IVs selecionados para edição em massa. Esta opção de edição funciona somente se houver patches preferenciais mapeados para todos os IVs selecionados.

Visão geral da Gestão de exceções

Quando sua organização não pode estar em conformidade com uma gestão de vulnerabilidades ou política de segurança, padrão ou diretriz publicada, você pode solicitar uma exceção. A gestão de exceções envolve solicitar, revisar, aprovar ou rejeitar exceções a um item vulnerável (IV) ou tarefa de correção (RT) que não pode ser corrigida de acordo com a política.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Algumas vulnerabilidades podem não ter um patch, correção ou solução existente. Quando uma exceção é aprovada, isso também significa que você está aceitando um risco porque está reconhecendo e concordando com as consequências de não corrigir a vulnerabilidade.

Ciclo de vida de uma exceção

Definição de uma exceção

Uma exceção é uma solicitação para adiar a correção de um IV ou RT por um período especificado. Por exemplo, como proprietário de correção, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Solicitar uma exceção

Como proprietário da correção, você pode solicitar uma isenção para um IV ou RT usando o processo de gestão de exceções. Depois que o aprovador de exceção aprova esta solicitação, o IV ou RT é movido para um estado **Adiado**.

Aprovação de uma solicitação de exceção

IVs ou RTs que não podem ser corrigidos imediatamente são revisados por analistas de vulnerabilidade, avaliados quanto ao risco e aprovados para adiamento até que possam ser corrigidos. A aprovação de uma solicitação de exceção pode ser um fluxo de trabalho de dois níveis. Se somente o aprovador de primeiro nível estiver presente, a exceção poderá ser solicitada e aprovada. No entanto, se não houver nenhum aprovador de primeiro nível, uma exceção não poderá ser solicitada. Para obter mais informações, consulte Adicionar um aprovador de exceção.

Nota:

A partir de Vulnerability Response v15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

Depois que uma solicitação de exceção para um IV ou RT for aprovada, você poderá executar as seguintes ações:

- Reabrir
- Excluir
- Atualizar os campos **Atribuição a** ou **Grupos** de atribuição

Como rastrear uma solicitação de exceção

Depois de gerar a exceção, você pode rastrear seu status usando a guia **Aprovações de mudança de estado** do IV ou RT. Se uma ação for realizada em um RT, você não poderá rastrear o status dos IVs individuais nesse RT.

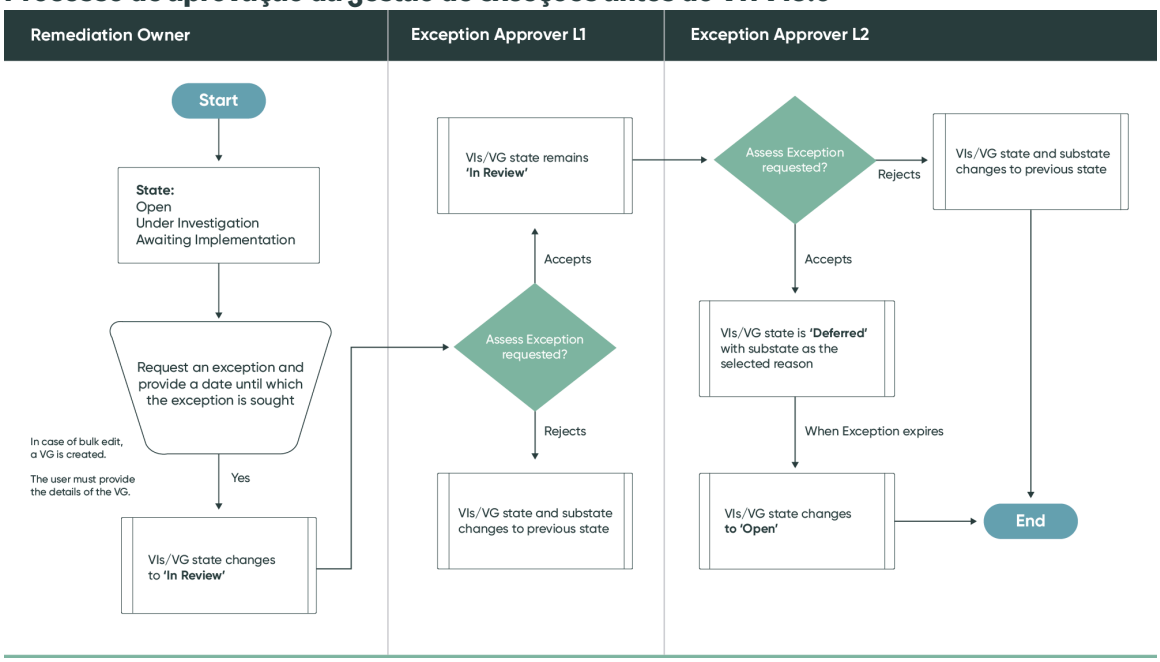
Vencimento de uma solicitação de exceção

Quando uma solicitação de exceção para um IV ou RT específico expira, o IV ou RT afetado é revertido para o estado **Aberto**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Processo de aprovação da gestão de exceções antes do VR v15.0



Se um único IV ou todos os IVs em um RT forem aprovados na próxima verificação, os IVs e, quando aplicável, o campo **Estado** do RT mudarão para **Encerrado** com o subestado **Fixo**.

Visão geral das regras de exceção

As regras de exceção para Vulnerability Response permitem automatizar o processo de adiamento para itens vulneráveis (IVs). Solicite uma exceção para os itens vulneráveis (IVs) que não podem ser corrigidos ou adiados imediatamente, identificando as vulnerabilidades afetadas, itens de configuração (ICs) ou IVs. Adie os IVs correspondentes com base na regra quando o sistema os identificar, automatizando o processo de adiamento de IV.

Usando regras de exceção em sua organização

Use regras de exceção para adiar automaticamente IVs novos e existentes por um período específico se eles corresponderem à condição de regra aprovada. A automação minimiza o risco de perder acordos de nível de serviço e facilita o gerenciamento de vários itens, pois você está eliminando a intervenção manual.

As regras de adiamento oferecem suporte à ordenação, ou seja, a regra com a prioridade mais alta é executada primeiro. Quando uma regra de alta prioridade é aplicada em um IV, nenhuma regra subsequente é aplicada novamente, mesmo que a condição corresponda ao IV.

Nota:

- Você só poderá criar regras se selecionar Vulnerability Response na configuração de Gestão de exceções. Para obter detalhes, consulte Configurar Gestão de exceções para Vulnerability Response.
- Quando os IVs são adiados por uma regra de exceção, eles são copiados para o grupo de vulnerabilidade de adiamento (VG) que é criado. Os IVs continuam a fazer parte dos VGs dos quais faziam parte anteriormente.

O ciclo de vida de uma regra de exceção é o seguinte:

- Criando uma regra de exceção
- Aprovação de uma solicitação de regra de exceção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Ativação de uma regra de exceção
- Adiando uma regra de exceção
- Vencimento de uma regra de exceção

Criando uma regra de exceção

Você pode criar uma regra de exceção para adiar automaticamente os IVs que correspondem às condições definidas para o período especificado. Depois de criar uma regra de exceção, envie-a para aprovação.

Aprovação de uma solicitação de regra de exceção

A aprovação de uma solicitação de regra de exceção é um processo de dois níveis. Se apenas o aprovador de primeiro nível estiver presente, a regra de exceção poderá ser avaliada e aprovada por uma única aprovação. No entanto, se não houver nenhum aprovador de primeiro nível, uma aprovação de regra de exceção não poderá ser aprovada. Depois que a regra é aprovada, uma tarefa de correção (RT) é criada. Para obter mais informações, consulte Aprovar uma solicitação de regra de exceção.

Nota:

A partir de Vulnerability Response v15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

Depois que uma solicitação de regra de exceção for aprovada, você poderá executar as seguintes ações:

- Cancelar
- Excluir

Ativação de uma regra de exceção

Depois que uma regra de exceção é aprovada, uma tarefa de correção é criada em um estado Adiado por padrão. A partir da data "Válido a partir de", a regra de exceção é executada em todos os IVs criados e também nos que são movidos do estado Fechado para Aberto.

Nota:

Se você habilitar a opção Executar em dados existentes, um trabalho programado será executado uma vez nos dados existentes na data "Válido a partir de".

Adiando uma regra de exceção

Você pode adiar IVs que correspondam às condições definidas nesta regra de exceção, até a data "Adiado até" definida para a regra. Nesta data, a tarefa de correção que você criou para a regra de exceção é encerrada e todos os IVs neste grupo são movidos de volta para o estado Aberto. As regras de grupo são aplicadas a eles novamente para alocá-los aos RTs necessários.

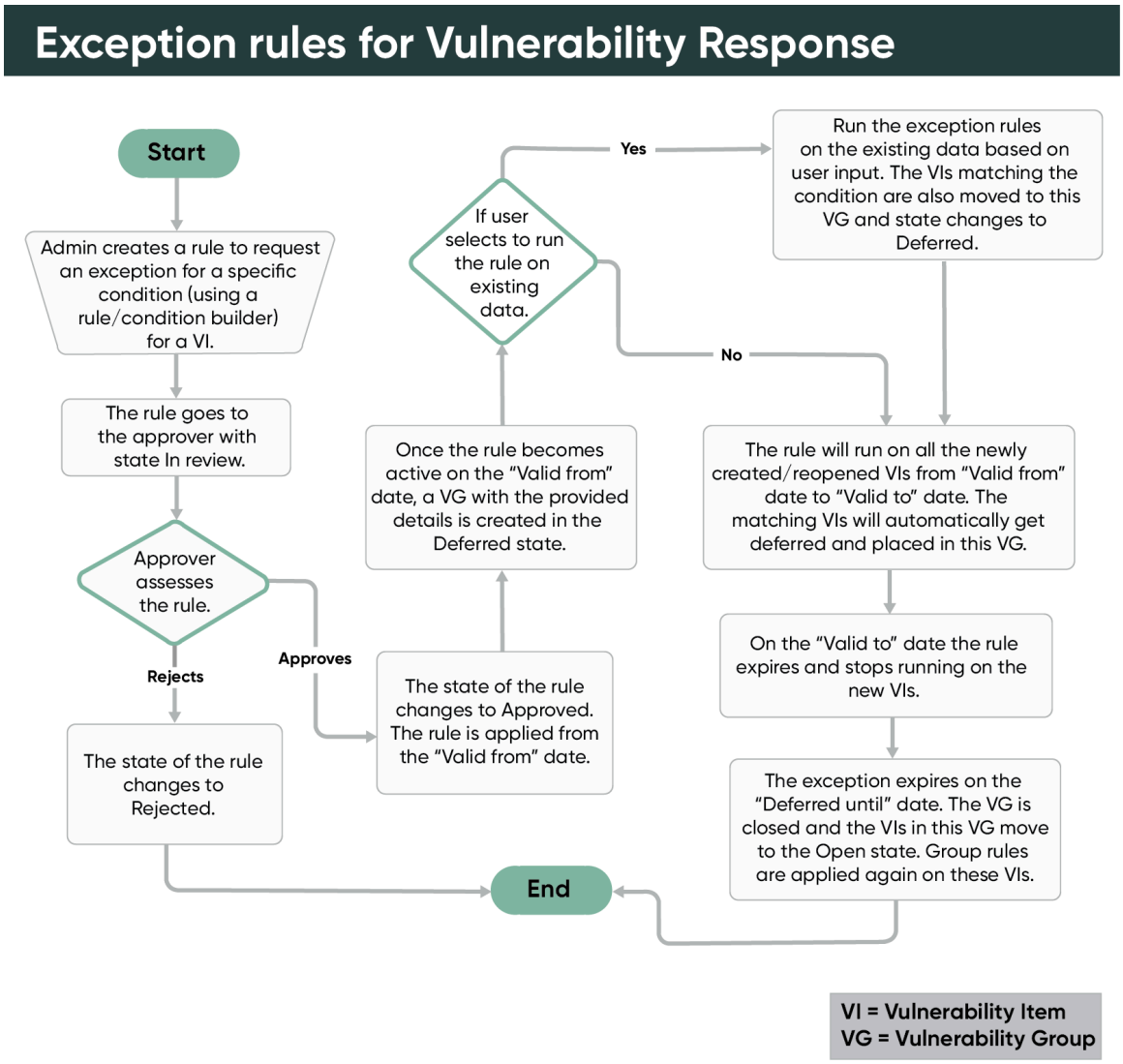
Vencimento de uma regra de exceção

Depois que a regra de exceção expira, ela não é mais executada em IVs novos ou reabertos. O RT associado permanece no estado Adiado até a data "Adiado até".

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de regras de exceção antes de v15.0



Falso-positivo visão geral

Um falso positivo é uma condição em que o scanner relata que existe uma vulnerabilidade no sistema, mas na realidade não há nenhuma vulnerabilidade. Pode haver vários motivos, como classificação incorreta, lógica imprópria ou algoritmo no scanner. O proprietário de correção pode marcar itens vulneráveis (IVs) ou tarefas de correção (RTs) como falsos positivos.

Ciclo de vida de um falso-positivo

Significado de falso-positivo

O scanner às vezes emite um aviso quando, na verdade, não há nenhuma vulnerabilidade. Por exemplo, se um item de configuração foi desativado, mas o scanner ainda está levantando um problema relacionado a ele, marque-o como um falso positivo.

Marcar como falso-positivo

Para obter detalhes sobre como marcar um IV ou RT como falso positivo, consulte Marcar como falso-positivo.

Trabalhando com o falso-positivo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois que um IV ou RT é marcado como falso positivo, o estado é atualizado para Encerrado e o subestado é alterado para Falso positivo. As seguintes ações podem ser realizadas:

- Reabrir
- Excluir
- Atualize a data no campo **Até**. Esta data é usada como data de vencimento para o falso-positivo.

Nota:
Se não for aprovado, o IV ou RT será revertido para o estado anterior.

Aprovação de um falso-positivo

O aprovador pode aprovar o falso positivo de seu fluxo de trabalho de aprovação.

Nota:

A partir do Vulnerability Response v15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

Reabrir um falso-positivo

Um IV ou RT em um subestado falso-positivo pode ser reaberto a qualquer momento.

Acompanhamento de um falso-positivo

Use a seção **Aprovações de mudança de estado** para rastrear o status do falso-positivo. Depois de aprovado, o estado do IV ou RT é atualizado para Encerrado e o motivo é Falso-positivo.

Vencimento de um falso-positivo

Somente o aprovador de falso-positivo pode definir uma data Até para o falso-positivo, para que o IV ou o RT expire. Além disso, somente falsos positivos para os quais o aprovador forneceu uma data Até podem expirar. Essa data pode ser fornecida após a aprovação do falso-positivo.

Um falso positivo sem uma data Até é um falso positivo permanente. Depois que o falso-positivo expirar, o estado do IV ou VR voltará para Aberto.

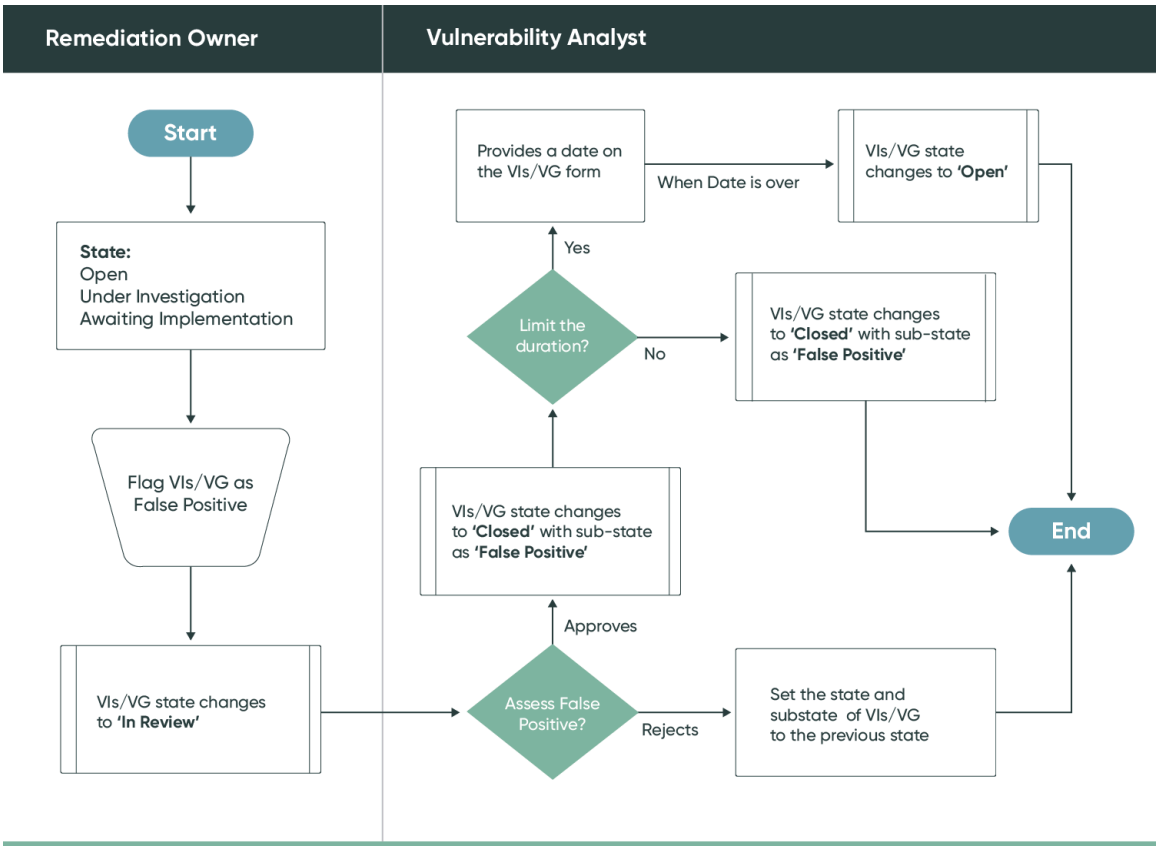
Nota:

A partir da v21.0 de Vulnerability Response, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Processo de aprovação de falso positivo antes da v15.0



O processo de aprovação será automático se todos os IVs forem aprovados na próxima verificação. Os IVs fecham automaticamente, independentemente do estado atual. Os IVs ou, quando aplicável, os campos de **Estado** de RT mudam para **Encerrado** com o subestado **Fixo.**

Para obter mais informações, consulte Marcar e aprovar um falso-positivo.

Watchdog para Vulnerability Response

O watchdog é usado para rastrear tabelas com base nas condições que você especificar. Por exemplo, ele pode ser usado para registrar detalhes de falhas de execução de integração em Vulnerability Response.

Você pode optar por ser notificado sobre essas falhas. Com base nessa notificação, você pode planejar a correção. Os watchdogs padrão são:

- Falha na execução da integração: se o Estado da execução da integração estiver definido como Concluído e o Subestado estiver definido como Falha, os usuários e grupos de usuários serão notificados se a condição retornar uma contagem maior que 0, ou seja, a execução da integração falhará.
- Integrações de longa execução: script para verificar se a execução da integração está excedendo o tempo definido. Este watchdog alerta proativamente sempre que houver um atraso na conclusão da execução da integração.

Log de observação

O watchdog vem com um log de observação, que fornece uma contagem do número de vezes que a condição foi atendida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painel Visão geral

Use o painel Visão geral para monitorar o watchdog nos últimos 30 dias. Você pode criar vários widgets para rastrear outros tópicos de watchdog que está monitorando.

A partir da versão 19.0 do Vulnerability Response, este painel está disponível na IU da nova experiência.

Nota:
Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Relatório

Nome	Descrição
Falha no WatchDog nos últimos 30 dias	Todas as condições atendidas nos últimos 30 dias.

Para obter mais informações, consulte Configurar watchdog e Tratamento de erros para detecções.

Change Management para Vulnerability Response

Como proprietário de correção de TI, você pode criar e gerenciar solicitações de mudança (CHG) diretamente das tarefas de correção (RT) na aplicação Vulnerability Response. As solicitações de mudança ajudam a iniciar e rastrear atividades de mudança em seus ativos para que você possa corrigir suas tarefas de correção e os itens vulneráveis correspondentes.

Solicitações de mudança e fluxo de trabalho de vulnerabilidade

Se você não estiver familiarizado com a aplicação Vulnerability Response, consulte Explorando a aplicação Vulnerability Responsepara obter mais informações.

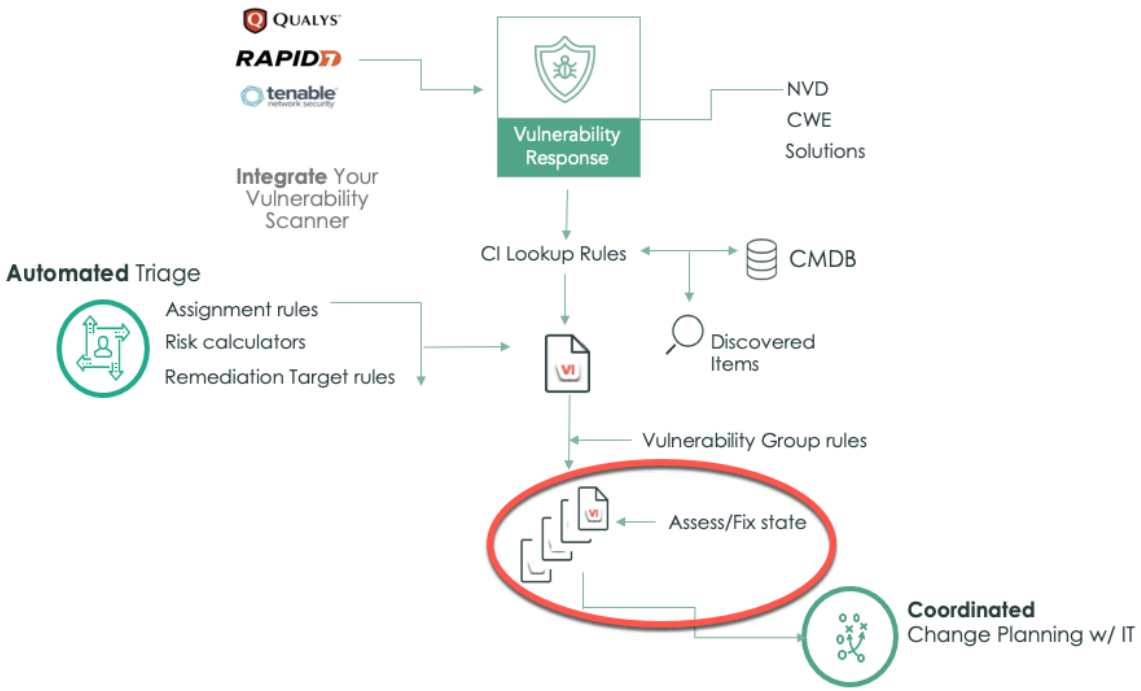
A imagem a seguir ilustra o fluxo de informações para Vulnerability Response, desde a configuração da integração (scanner) até a triagem automatizada e a investigação.

As solicitações de mudança e o gerenciamento de mudanças fazem parte do processo de correção (estado Avaliar/Corrigir) no fluxo de trabalho Vulnerability Response mostrado na figura a seguir. Durante esta fase, você pode usar solicitações de mudança para iniciar e rastrear a correção de vulnerabilidades. Você pode criar e gerenciar solicitações de mudança diretamente da tarefa de correção e tarefas de investigação e correção de lista que incluem soluções para ativos afetados para os itens de configuração (IC) no seu CMDB.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitações de mudança no Vulnerability Response



Quando usar solicitações de mudança na resposta de vulnerabilidade

Como proprietário de correção de TI, você pode criar solicitações de mudança a partir de uma tarefa de correção se um processo manual e controlado de qualquer tipo for necessário para modificação ou remoção de itens de configuração (ICs) compatíveis no seu CMDB. Criar e gerenciar solicitações de mudança diretamente de um registro de tarefa de correção ajuda a investigar e resolver vulnerabilidades rapidamente. Os IVs de tarefas de correção resolvidas podem ser verificados durante a próxima verificação programada na sua Now Platform e retornados para a triagem automatizada do fluxo de trabalho Vulnerability Response. Intervenções manuais que podem exigir solicitações de mudança incluem os seguintes exemplos:

- Um patch de software, correção ou outra tarefa de TI que é necessária em itens vulneráveis antes da resolução de RT.
- Você determina que um subconjunto dos itens vulneráveis em uma tarefa de correção requer investigação adicional ou reatribuição a outro departamento.
- Você determina que um subconjunto de itens vulneráveis em um RT com um grande conjunto de itens vulneráveis pode ser movido para uma nova tarefa de correção.
- Você pode associar uma tarefa de correção a uma solicitação de mudança existente para evitar a duplicação de tarefas de correção.

Tipos de solicitações de mudança para um RT

A aplicação Vulnerability Response utiliza os três tipos de mudanças de serviço compatíveis com o produto ITSM Gestão de mudanças em sua instância Now Platform® — padrão, emergencial e normal. O tipo de mudança selecionado determina qual modelo de estado é invocado e o processo de mudança que deve ser seguido. As solicitações de mudança registram as informações detalhadas sobre a mudança, como o motivo da mudança, a prioridade, o risco, o tipo de mudança e a categoria da mudança. Consulte Tipos de mudança .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como proprietário de correção de TI Vulnerability Response, você tem as seguintes opções para criar solicitações de mudança normais, padrão e de emergência diretamente de uma tarefa de correção:

- Você pode criar solicitações de mudança que contenham informações preenchidas previamente da tarefa de correção para simplificar o processo e economizar tempo.
- Você pode associar uma tarefa de correção a uma solicitação de mudança existente para evitar a criação de solicitações de mudança duplicadas que compartilham informações semelhantes e itens vulneráveis.
- Usando um conjunto de condições, você pode filtrar um subconjunto de itens vulneráveis e dividir uma tarefa de correção. Os itens selecionados são movidos automaticamente para um novo RT.

Você pode filtrar itens vulneráveis usando valores de qualquer campo de uma tarefa de correção e aplicar a solicitação de mudança somente aos itens que correspondem aos seus critérios de filtro.

Tópicos relacionados

Criar uma solicitação de mudança a partir de uma tarefa de correção

Associar uma tarefa de correção a uma solicitação de mudança existente

Dividir uma tarefa de correção

Sincronização de estado entre solicitações de mudança e tarefas de correção

Avaliação de exposição de software usando Software Asset Management (SAM)

Use a aplicação de avaliação de exposição ServiceNow® para determinar a contagem total de software instalado para um pacote de software específico em seus ativos. Quando usado com a aplicação ServiceNow® Gestão de ativos de software ITSM, avalie sua exposição, crie itens vulneráveis e gerencie a correção do software vulnerável que você descobrir.

Determine sua exposição a software vulnerável fornecendo as informações de software vulnerável (fornecedor, produto, edição e versão) sem usar o banco de dados de vulnerabilidades e exposições comuns (CVE). Avalie os casos de vulnerabilidades de software de dia zero (dia atual) para os seguintes casos:

- Quando os produtos ainda não têm dados de CVE.
- Quando há um atraso entre o momento em que uma vulnerabilidade se torna publicamente conhecida e os dados de CVE com a vulnerabilidade são atualizados no NVD.
- Quando você aprende sobre a vulnerabilidade entre as verificações programadas do scanner de vulnerabilidades.

Com a aplicação de avaliação de exposição, se você souber o fornecedor e o produto do software vulnerável, usando os registros que listam o software instalado em sua rede criada pela aplicação SAM, você poderá avaliar sua exposição a pacotes de software potencialmente mal-intencionados sob demanda.

Conhecer a escala de sua exposição a este tipo de vulnerabilidade permite que você responda proativamente implementando um alerta vermelho e desinstalando o software ou informando ao seu centro de operações de segurança (SOC) para procurar um patch específico. Você pode criar itens vulneráveis e atribuir tarefas ao especialista de correção para correção de investigação adicional. Exiba uma lista de tarefas de correção (VUL) para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

verificar se os itens vulneráveis desejados foram criados e associados corretamente ao VUL.

Tópicos relacionados

Configurar avaliação de exposição

Avalie sua exposição a software vulnerável

Vulnerability Cris Management

Crie e rastreie eventos de vulnerabilidade crítica por meio do fluxo de trabalho do Vulnerability Crisis Management. Crie registros de avaliação de vulnerabilidade, registre os principais atributos da vulnerabilidade para calcular o risco, execute a avaliação para identificar o nível de exposição e envolva as partes interessadas para uma resposta coordenada e rápida às vulnerabilidades.

Gerenciamento de eventos de crise de vulnerabilidade

O Vulnerability Crisis Management é um fluxo de trabalho completo para lidar com eventos de crise de vulnerabilidade com os seguintes recursos.

- Identifique com eficiência os itens de configuração vulneráveis, correlacionando vulnerabilidades críticas com o inventário de instalação de software do inventário Gestão de ativos de software e Lista de materiais de software (SBOM), vulnerabilidades relatadas pelo scanner e Configuration Management Database (CMDB).
- Converta os resultados da avaliação em itens vulneráveis para correção.
- Inicie um incidente de segurança grave para garantir uma resposta rápida e coordenada à ameaça.
- Envolva-se e colabore com equipes em toda a organização, facilitando uma resposta unificada às vulnerabilidades.
- Forneça relatórios de status regulares para partes interessadas multifuncionais e equipes envolvidas para manter a transparência e a comunicação durante a crise.

Vulnerability Crisis Management usando o Vulnerability Assessment Workspace

Ao identificar uma vulnerabilidade de interesse, o gerenciador de eventos de vulnerabilidade cria um registro de avaliação de vulnerabilidade com informações sobre a origem da inteligência contra ameaças, características da vulnerabilidade e produtos afetados. Essas informações são usadas para análises adicionais de impacto e exposição.

Depois que o registro de uma vulnerabilidade de interesse foi criado, uma avaliação de risco é realizada. Esta avaliação compreende pontuação de risco estruturada, revisão do registro e as observações do analista que executa a tarefa. A pontuação de risco inicial para uma vulnerabilidade de interesse é calculada usando os atributos disponíveis no momento da criação do evento. A pontuação de risco da avaliação pode mudar conforme a inteligência adicional se torna disponível. Use a pontuação de risco para determinar o possível impacto da exploração e estabelecer prioridades de resposta.

Depois que a avaliação de uma vulnerabilidade de interesse tiver sido criada e determinada como apresentando risco à infraestrutura da organização, você poderá analisar a ameaça ainda mais, atualizando a avaliação de risco com uma avaliação de exposição detalhada com o inventário de instalação de software de Gestão de ativos de software, Lista de materiais de software (SBOM) inventário, vulnerabilidades relatadas pelo scanner e Configuration Management Database (CMDB). Os itens de configuração e as aplicações afetados são identificados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

automaticamente por meio da avaliação. Outros itens afetados podem ser adicionados manualmente.

Depois que a avaliação for concluída, os itens vulneráveis ou os itens vulneráveis da aplicação poderão ser criados para os resultados de exposição que ainda não tenham um item vulnerável associado. A calculadora de pontuação de risco de itens vulneráveis pode ser aproveitada/configurada para ajustar a pontuação de risco de itens vulneráveis vinculados a registros de avaliação de vulnerabilidade. O registro de avaliação de vulnerabilidade pode ser atribuído a nível de exposição e prioridade de evento. Com base na prioridade do evento, o gerenciador de eventos de vulnerabilidade pode optar por propor, promover ou vincular a avaliação de vulnerabilidade a um incidente de segurança grave.

Use Gestão de incidentes graves de segurança para rastrear e gerenciar a atividade de correção, vincular incidentes de segurança em andamento, criar tarefas ad-hoc, envolver as equipes afetadas, enviar relatórios de status e colaborar usando integrações de colaboração disponíveis em Gestão de incidentes graves de segurança.

ServiceNow® Gestão de ativos de software e Lista de materiais de software (SBOM) lógica de processamento de avaliação

Usando os dados Gestão de ativos de software, os CPEs provenientes do NVD para o CVE e os modelos de descoberta são obtidos usando a lógica de correspondência de cadeia de caracteres. Depois de buscar os modelos de descoberta, uma verificação de instalações relacionadas é executada, os itens de configuração relacionados são buscados e a tabela Item de configuração afetado é preenchida. Você pode fornecer mais detalhes como Fornecedor, Produto, Versão e Edição. Com base neles, todos os modelos de descoberta correspondentes e as instalações de software para o registro são buscados. Posteriormente, os itens de configuração relacionados são obtidos e a tabela Item de configuração afetado é preenchida novamente.

Para SBOM, o software associado ao CVE da tabela relacionada (m2m) (entre CVE e Software) é buscado. Depois de extrair os detalhes do software, os componentes do SBOM relacionados são identificados correspondendo o produto e a versão do componente do SBOM ao produto e à versão do software identificado.

Depois que os componentes associados são encontrados, as entidades relacionadas aos componentes são buscadas. O modelo de produto das entidades e o IC relacionado (se encontrado) são obtidos e o item de configuração é salvo na tabela Item de configuração afetado. Se o item de configuração não tiver itens vulneráveis, você poderá usá-lo para criar o item vulnerável. Se um item de configuração não for encontrado, o modelo do produto será salvo na tabela Modelo de software afetado e poderá ser usado para criar itens vulneráveis da aplicação.

Para obter mais informações sobre como usar o fluxo de trabalho Vulnerability Crisis Management, consulte Como usar o espaço de avaliação de vulnerabilidade.

Tópicos relacionados

- Explorando a avaliação de vulnerabilidade
- Explore o Espaço de avaliação de vulnerabilidade
- Guia Avaliação

Separação de domínios e Vulnerability Response

Separação de domínios é compatível com Vulnerability Response. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nível de suporte: Padrão

- Inclui nível de suporte **Básico**.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como o Domain Separation funciona no Vulnerability Response

Com o Domain Separation, você pode padronizar procedimentos de VR (Vulnerability Response) em toda a base de clientes que atende, com custos operacionais reduzidos e uma qualidade de serviço superior.

Espaços separados de trabalho do cliente para fluxos de trabalho, painéis, relatórios e assim por diante garantem que os dados do cliente sejam separados e nunca expostos a outros clientes.

Suporte à separação de domínio no Vulnerability Response por versões

Liberação	Nível de suporte	Anotações
Orlando	Padrão	
Paris	Padrão	
Quebec	Padrão	
Rome	Padrão	
San Diego	Padrão	
Tóquio	Padrão	
Utah	Padrão	
Vancouver	Padrão	
Washingtondc	Padrão	

A separação de domínio para a aplicação Vulnerability Response abrange a seguinte funcionalidade do produto:

- Ingere os itens vulneráveis de scanners de terceiros (por exemplo, Qualys, Rapid 7 ou Tenable) no domínio correto. Os dados ingerem no mesmo domínio do usuário de integração, cujas credenciais são usadas para integração.
- Verifica novamente ativos específicos de Vulnerability Response no domínio do qual foi solicitado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Usa o processo de pesquisa de IC do CMDB para garantir que as informações de IC dos scanners correspondam aos ICs no CMDB do domínio do usuário de integração.
- Calcula as pontuações de risco no nível do item vulnerável de acordo com a calculadora de pontuação de risco definida no mesmo domínio do usuário de integração.
- As regras de destino de correção são executadas em itens vulneráveis de acordo com as regras de destino de correção definidas no mesmo domínio do usuário de integração.
- Regra(s) de tarefa de correção pode(m) ser definida(s) e permanecer(em) no mesmo domínio que o domínio do usuário de integração.
- As tarefas de correção criadas usando as regras de tarefa de correção permanecem no mesmo domínio em que as regras de grupo são criadas.
- O fluxo de trabalho de adiamento passa pelo processo de aprovação no mesmo domínio para o qual o adiamento é solicitado.
- Relatórios e painéis exibem os estados do item vulnerável, como idade do item vulnerável, itens vulneráveis em aberto por IC, vulnerabilidades por impacto e status da data de destino da correção no domínio ao qual pertence.
- O conhecimento de scanners de terceiros ou do banco de dados nacional de vulnerabilidades (NVD) pode ser ingerido no domínio global e os dados podem ser compartilhados entre vários clientes.

Nota:
Em todos os casos acima, os princípios abrangentes de visibilidade na separação de domínios separados na NOW Platform se aplicam.

Para obter mais informações sobre como criar e oferecer suporte a importações separadas por domínio, consulte Criar importações separadas por domínio para uma integração e Criar e oferecer suporte a vários domínios na estrutura de trabalhos em segundo plano.

Casos de uso

A aplicação Vulnerability Response gerencia o ciclo de vida de um item de vulnerabilidade de ponta a ponta. Os casos de uso a seguir reconhecem a separação de domínio:

- **Ingerir** itens vulneráveis (vulnerabilidades no ativo) da integração de terceiros.
  - Ingerir dados de várias instâncias
  - Desduplicar o item vulnerável
  - Corresponda ao IC do CMDB
- **Aprimoramento** de item vulnerável com pontuações de risco e datas de destino de correção
  - Aprimoramento de ativos (CMDB)
  - Pontuação de risco e aprimoramento da data de destino de correção
- **Agrupar** itens vulneráveis e atribuir a tarefa de correção
  - Agrupar automaticamente os itens vulneráveis
  - Atribuir automaticamente a tarefa de correção
- **Corrigir**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

  - Tarefas de correção
  - Ciclo de vida de correção abrangente
  - Fluxo de trabalho de adiamento
- **Medir** a postura de segurança da organização e do programa de gestão de vulnerabilidades
  - Tendência de vulnerabilidade, ativo mais vulnerável, vulnerabilidade por idade
  - Status da correção pela data de destino da correção

Configuração

Configurar o Domain Separation para Vulnerability Response não requer etapas adicionais. Todas as tabelas Vulnerability Response adquirem a coluna Domínio depois que a instância é separada por domínio. Você pode direcionar os dados de importação de integração de vulnerabilidade para domínios específicos. Para obter mais informações, consulte Criar importações separadas por domínio para uma integração.

Dados separados por domínio

Os dados podem ser separados por domínio, o que significa:

- O item vulnerável ingerido de scanners de terceiros permanece no mesmo domínio que o domínio do usuário de integração e não pode ser acessado de nenhum outro domínio.
- Vulnerabilidades, itens vulneráveis (instâncias) ou ativos em um domínio não podem ser exibidos em outros domínios.
- O algoritmo de pontuação de risco, as regras de tarefa de correção e as regras de destino de correção não podem ser exibidas por qualquer pessoa fora do domínio.
- As informações de vulnerabilidade do NVD podem existir no domínio global e ser compartilhadas com todos os clientes.
- Tarefas de correção em um domínio não podem ser exibidas em outro domínio.
- Fluxos de trabalho de adiamento criados em um domínio não são visíveis em outro domínio.
- Todas as notificações por e-mail estão contidas no domínio ao qual pertencem.

Como os analistas de vulnerabilidade gerenciam seus próprios dados de aplicação

- Os analistas criam suas próprias regras de instalação de aplicações, gerenciamento de aplicações de várias origens e pesquisa de IC.
- Os analistas podem configurar integrações específicas exclusivamente para uso no domínio.
- Os analistas podem criar seus próprios fluxos de trabalho de adiamento e gerenciamento de mudanças.
- Os analistas podem criar suas próprias regras de tarefa de correção, lógica de pontuação de risco para priorizar vulnerabilidades com precisão, atribuir automaticamente tarefas de correção e atribuir ao grupo de atribuição correto.
- Os usuários do domínio criam um item de vulnerabilidade manual e fecham o item.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lógica de negócios e processos que podem ser separados por domínio pelo proprietário da instância

- Vulnerability Response usuários e grupos
- Integrações do Vulnerability Response
- Configuração de configuração completa (gestão de usuários e grupos, instalação de aplicações, gestão de aplicações de várias origens, regras de pesquisa de IC, regras de tarefa de correção, calculadoras de risco, regras de destino de correção etc.)
- Concluir o ciclo de vida da correção, incluindo o adiamento
- Programar trabalhos

Tópicos relacionados

Domain Separation para provedores de serviço

Implementação de Vulnerability Response

Use as etapas ilustradas nas imagens a seguir para baixar a aplicação Vulnerability Response do ServiceNow Store, instalá-lo em sua instância Now Platform® e configurá-lo usando o Assistente de configuração.

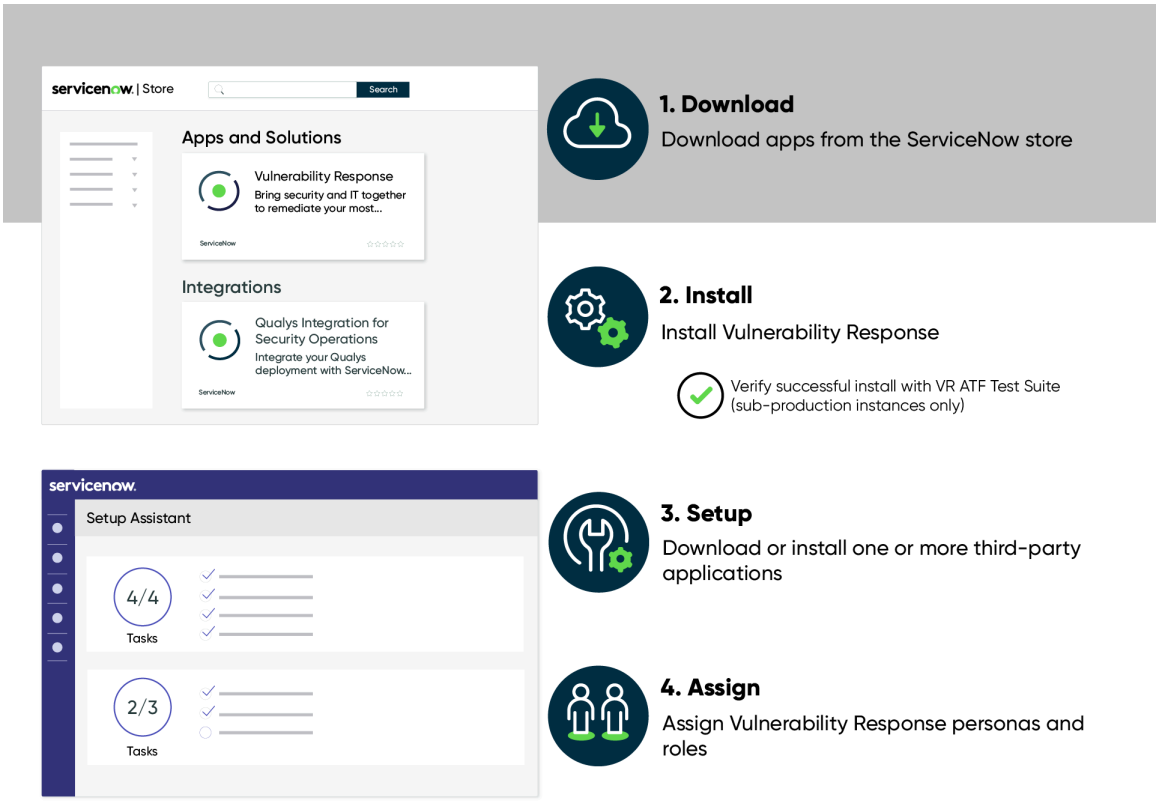
Um exemplo de instalação e configuração para instalar o sistema de base, a aplicação Vulnerability Response e um aplicativo de scanner de terceiros, a aplicação Qualys, é ilustrado nas imagens a seguir. Funções necessárias e tarefas obrigatórias, bem como etapas opcionais, também são listadas.

- Para obter mais informações sobre cada etapa ilustrada nas imagens a seguir e uma check-list com links para a documentação de suporte, consulte Check-list de implementação da aplicação Vulnerability Response.
- Você pode estender os conceitos e a sequência de etapas apresentados neste exemplo para instalar e configurar outros aplicativos compatíveis para Vulnerability Response. Para obter uma lista de aplicações de suporte, consulte Instalação de Vulnerability Response e aplicações compatíveis.
- A função de administrador é necessária para baixar e instalar a aplicação Vulnerability Response e a aplicação de vulnerabilidade Qualys usada para este exemplo.
- A função de administrador também atribui a persona de administrador de vulnerabilidade [sn_vul.vulnerability_admin] e outras funções de persona Vulnerability Response a usuários e grupos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de administrador

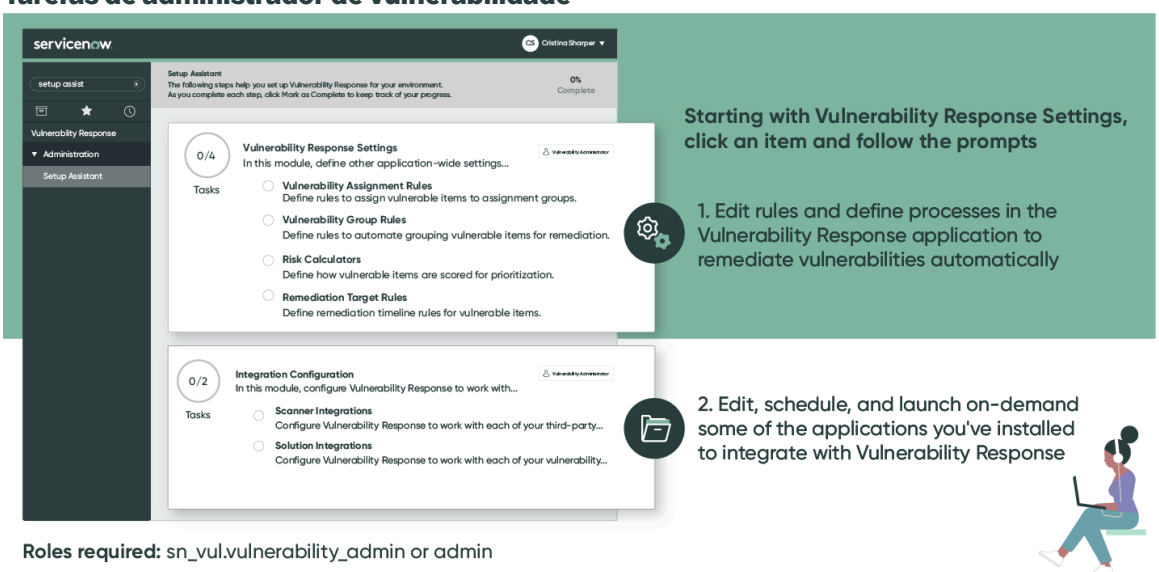


A função sn_vul.vulnerability_admin configura as aplicações Vulnerability Response e Qualys no Assistente de configuração e verifica os resultados esperados.

Siga as etapas e os prompts no Assistente de configuração, começando com a seção Configurações do Vulnerability Response para continuar com a instalação e a configuração. Revisar essas configurações ajuda a entender e verificar os processos de Vulnerability Response conforme você continua a configurar seu ambiente.

Função necessária: sn_vul.vulnerability_admin ou, alternativamente, admin.

Tarefas de administrador de vulnerabilidade



Roles required: sn_vul.vulnerability_admin or admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Revise as descrições, as configurações padrão e os dados de demonstração que você instalou com as aplicações nas seguintes seções:

- Regras de atribuição de vulnerabilidade: atribua automaticamente itens vulneráveis (IVs) ao grupo de atribuição apropriado.
- Regras de tarefa de correção - agrupa automaticamente itens vulneráveis (IVs) conforme eles são importados com base em determinadas condições.
- Calculadoras de risco — A calculadora de risco padrão está habilitada.
- Regras de destino de correção: definem linhas do tempo de correção para IVs e tarefas de correção (RTs).
- Revise e edite as configurações dos aplicativos de terceiros e das soluções instaladas que você instalou e defina as condições para suas importações de dados. Insira as informações da conta de terceiros e defina as configurações de importação e programações, regras de pesquisa de item de configuração (IC), bem como outras configurações.

Para obter mais informações, consulte Check-list de implementação da aplicação Vulnerability Response.

Para obter informações adicionais ao personalizar ou implementar a aplicação Vulnerability Response, consulte KB1000704 .

Como instalar Vulnerability Response

Antes de executar a aplicação Vulnerability Response na sua instância Now Platform, você deve obter o direito e baixar a aplicação da ServiceNow Store, instalá-la na sua instância Now Platform e concluir algumas etapas de instalação no Assistente de configuração.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Tarefas de configuração	Descrição
Verifique se você tem as funções ServiceNow necessárias atribuídas à sua instância.	A função de administrador é necessária para a instalação. Se ainda não estiver atribuído, o administrador do sistema [admin] também atribuirá a função de administrador de vulnerabilidade, sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)].

Função necessária: administrador

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações

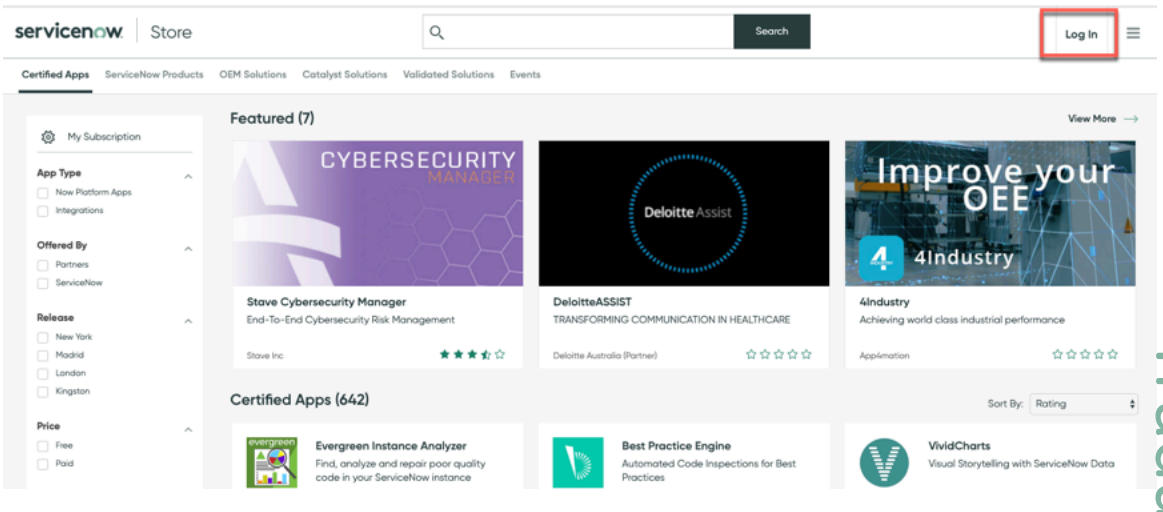
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

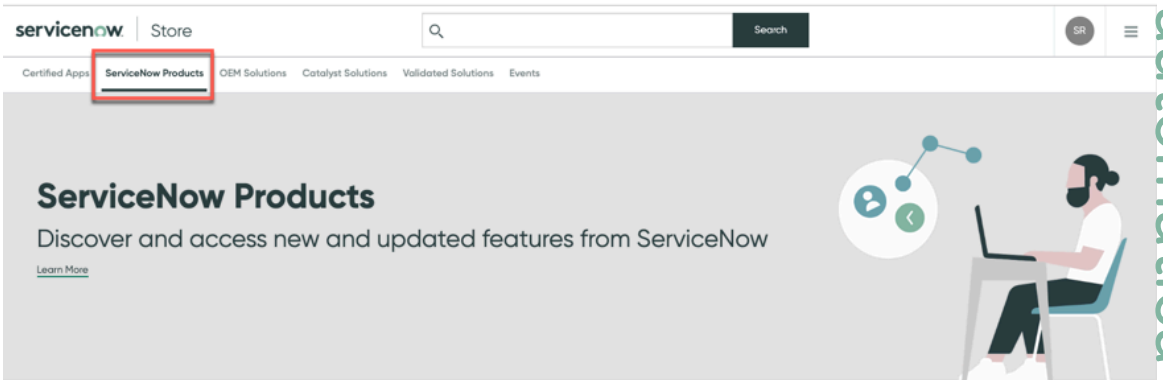
sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Procedimento

1. Para obter o direito e baixar a aplicação principal Vulnerability Response, navegue até ServiceNow Store.
2. No canto superior direito da página, clique em **Fazer login**.



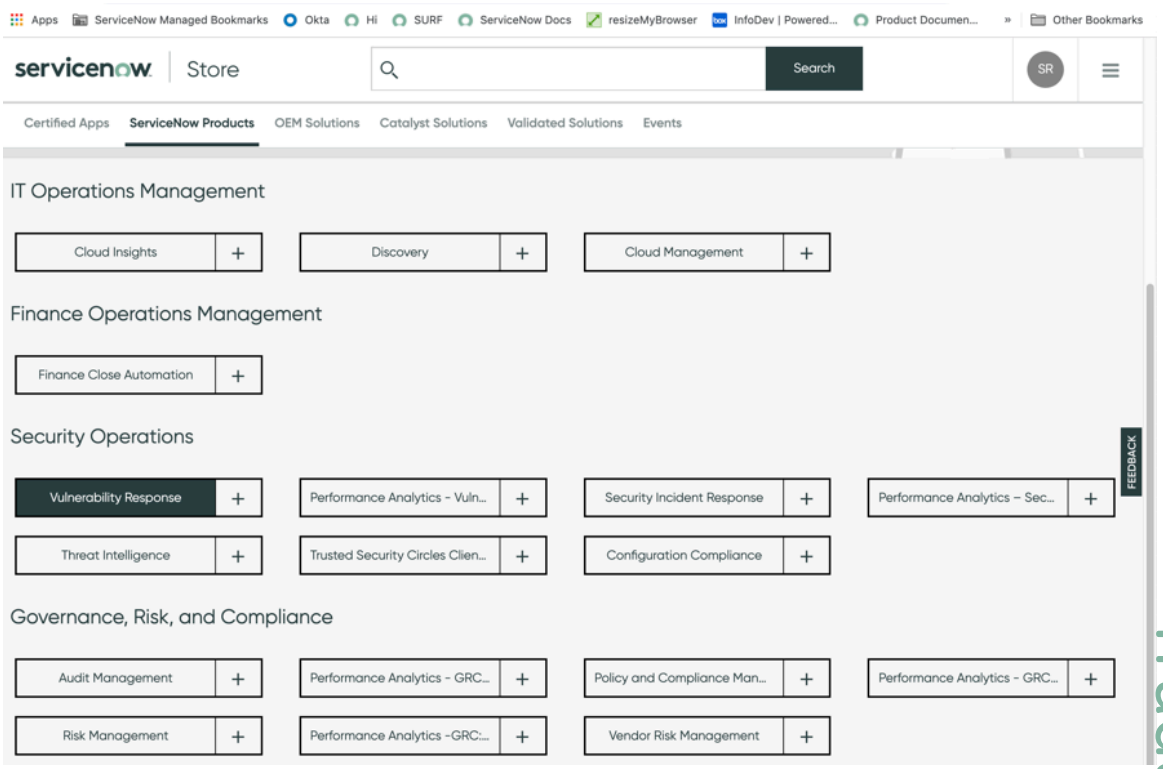
3. Na caixa de diálogo exibida, insira suas credenciais HI e clique em **Login**.
4. Na página exibida, se não estiver selecionada, clique na guia **Produtos da ServiceNow**.



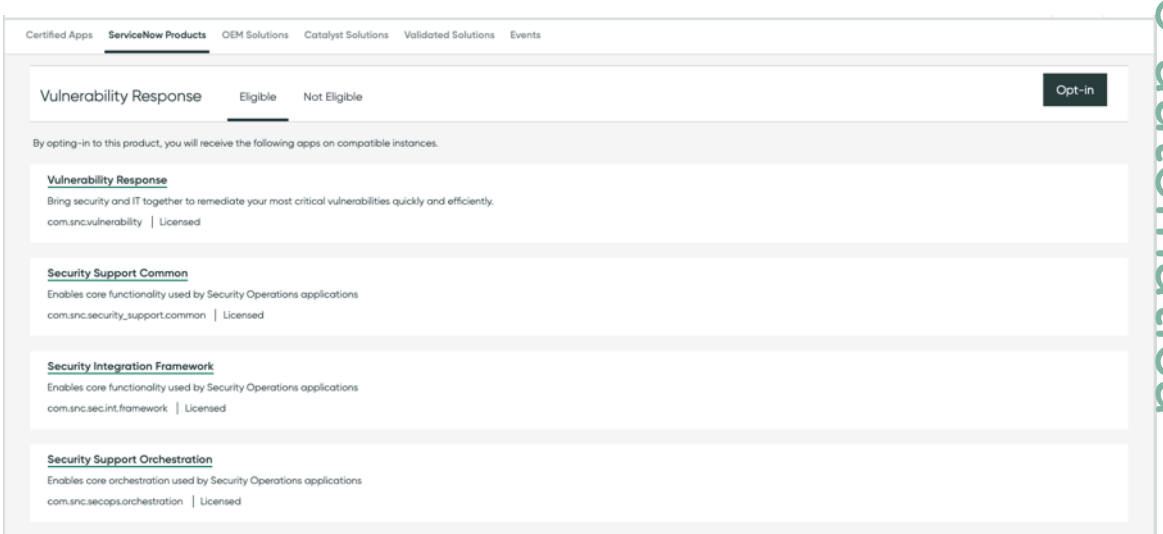
5. Para exibir as aplicações associadas para as quais você está qualificado com a aplicação Vulnerability Response, na página da lista de produtos, clique no produto **Vulnerability Response**.

Tradução automática

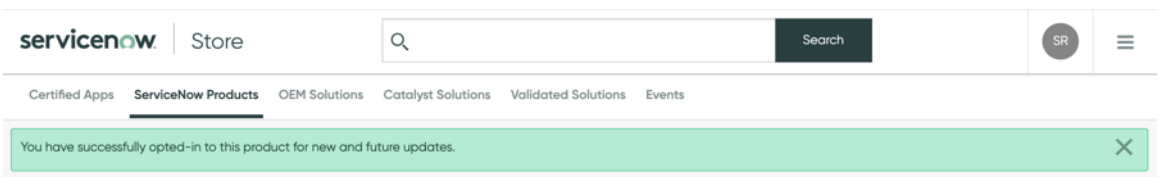
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A guia Qualificado lista todas as aplicações para as quais você está qualificado se aceitar. Para obter mais informações sobre uma aplicação, clique em um link.



6. Para obter a aplicação principal Vulnerability Response, clique em **Aceitar**.
7. Para concordar com os termos e condições, no prompt, marque a caixa de seleção e clique em **Aceitar**.
   Uma mensagem é exibida indicando que você aceitou a aplicação com sucesso.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

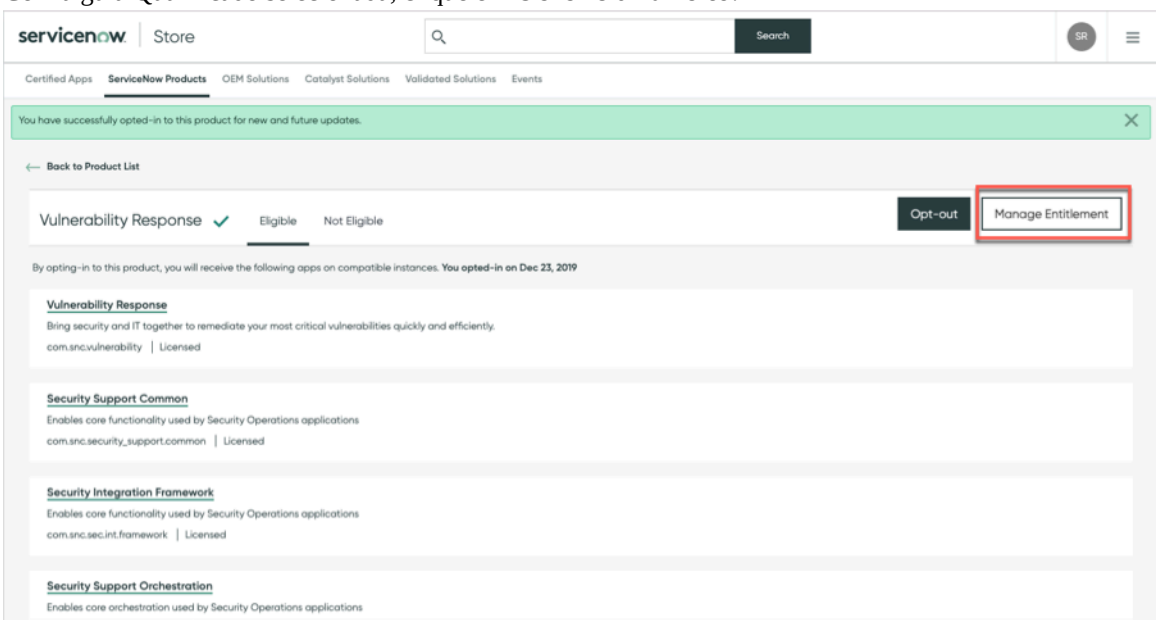
Com a guia Produtos ServiceNow selecionada e exibida, uma marca de seleção verde substitui o sinal de mais à direita da aplicação Vulnerability Response, conforme mostrado na figura a seguir.

Depois de aceitar os termos e condições e os direitos gerenciados de qualquer uma das aplicações na guia **Produtos da ServiceNow**, na página Lista de produtos, você pode clicar no sinal de mais (+) para obter o direito e aceitar as outras aplicações nesta página com um único clique.

8. Pule para a etapa 10 para instalar a aplicação na sua instância Now Platform.
9. **Opcional:** Como alternativa, para gerenciar seu direito da aplicação Vulnerability Response em outras instâncias Now Platform, siga estas etapas.

a. Se o botão Gerenciar direito não for exibido, clique na aplicação Vulnerability Response na lista de produtos para exibi-lo.

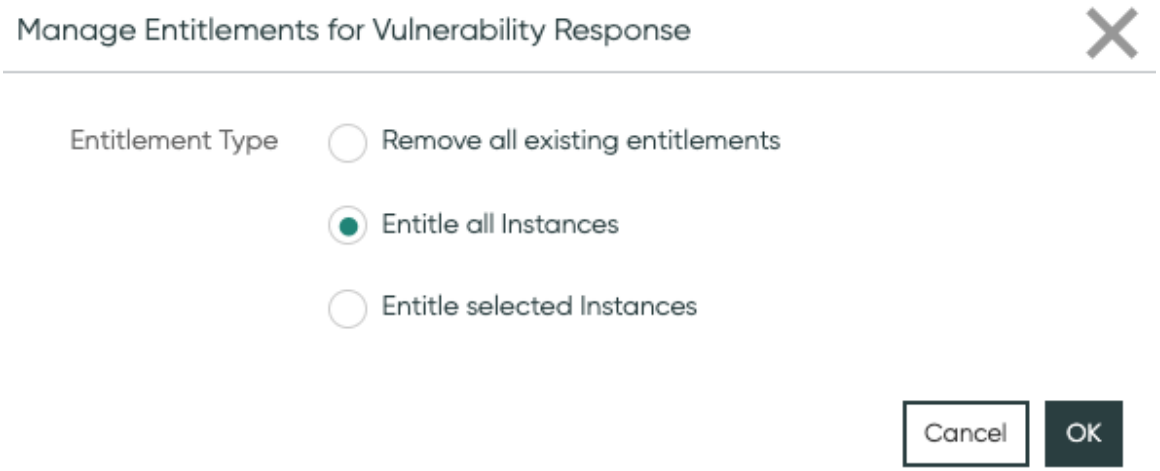
b. Com a guia Qualificado selecionada, clique em **Gerenciar direito**.



c. Na caixa de diálogo Gerenciar direitos para Vulnerability Response exibida, escolha uma:

Tradução automática

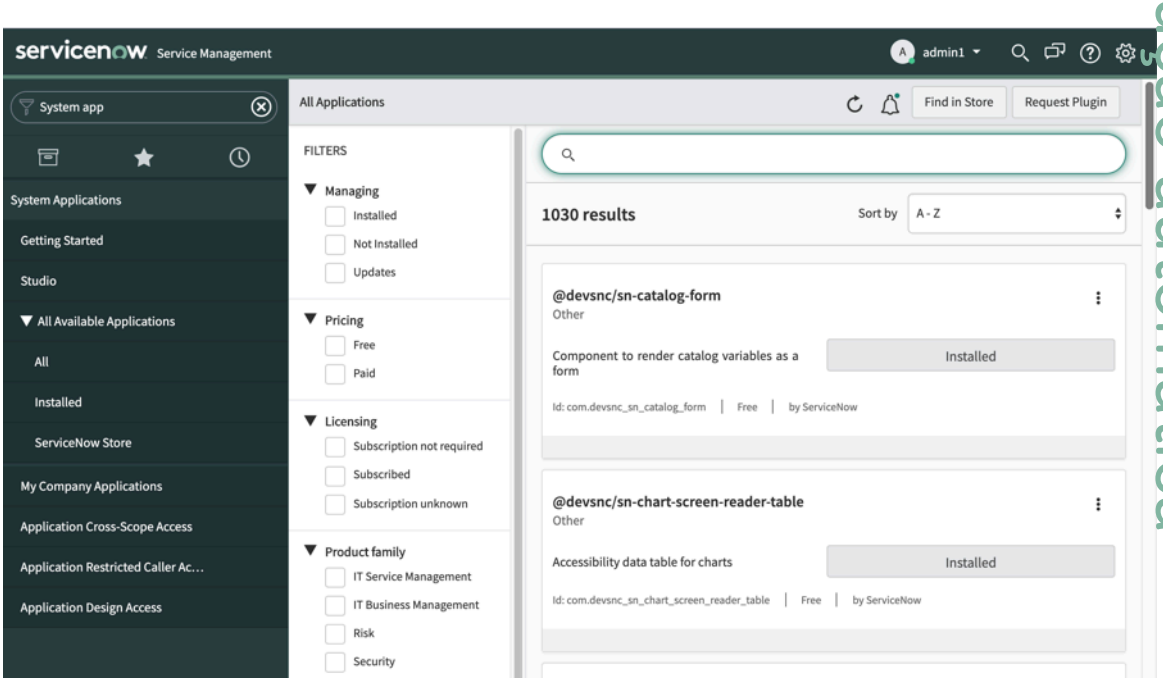
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. Clique em **OK** ou em **Cancelar** para continuar.
Você está pronto para ativar plug-ins e instalar a aplicação em suas Now Platform instância(s).

10. Faça login na instância Now Platform na qual você deseja instalar a aplicação Vulnerability Response.

11. Navegar até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.



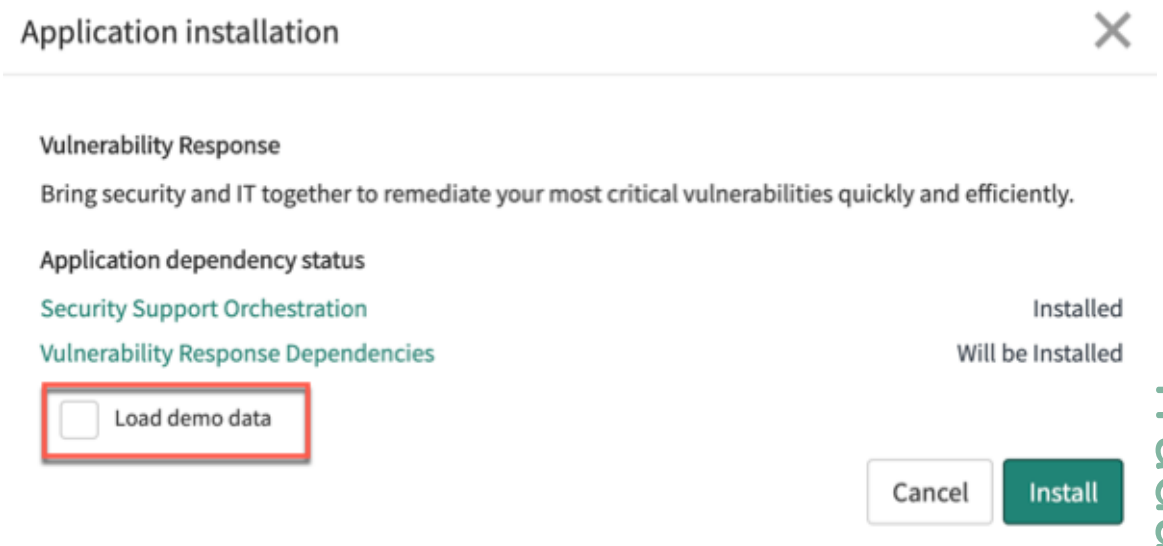
12. Entre as aplicações listadas, localize a aplicação Vulnerability Response (sn_vul), selecione uma versão na lista de seleção e clique em **Instalar**.
A caixa de diálogo de instalação da aplicação é exibida. Todas as dependências que serão instaladas serão exibidas.

13. **Opcional:** Se você quiser dados de demonstração, marque a caixa de seleção Carregar dados de demonstração e clique em **Instalar**.

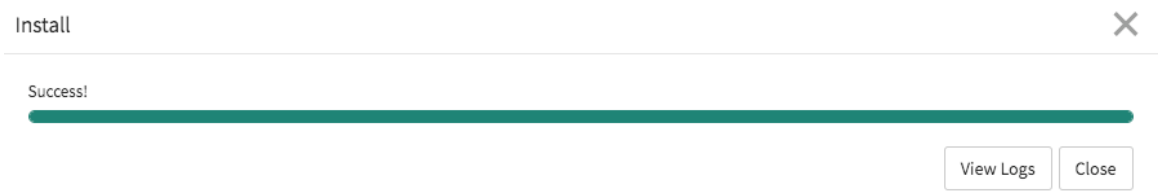
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Se você não marcar a caixa de seleção **Carregar dados** de demonstração, os dados de demonstração não ficarão disponíveis para instalação no **Gerenciador de aplicações** posteriormente. Para obter informações sobre como instalar ou reinstalar os dados de demonstração após a instalação inicial, consulte o artigo Solução alternativa para instalar dados de demonstração se a aplicação já estiver instalada [KB0722909] na Base de conhecimento Now Support.



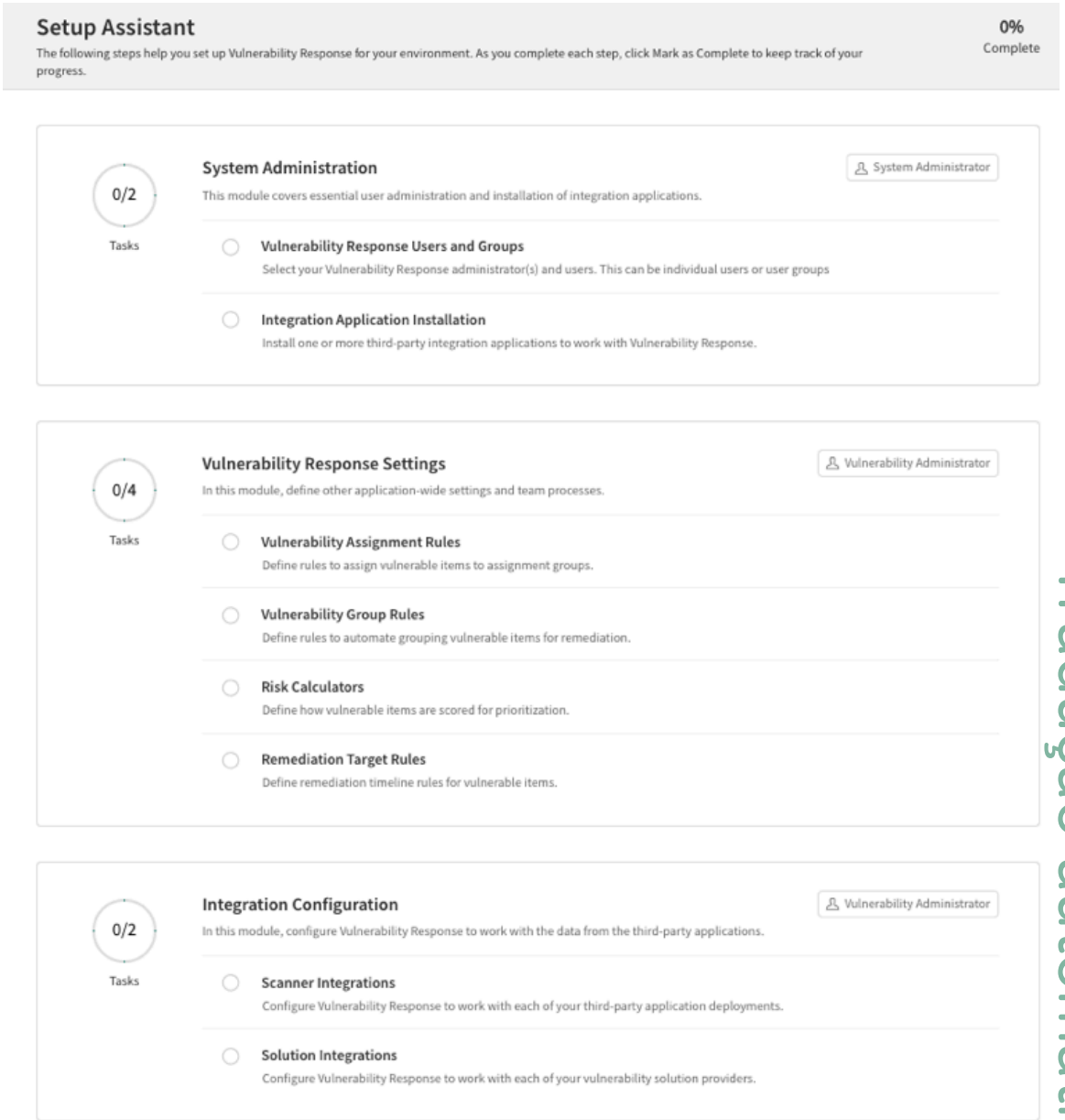
Esta instalação pode levar algum tempo. Uma mensagem é exibida na caixa de diálogo Instalar depois que a aplicação é instalada com sucesso.



14. Clique em **Fechar**.
15. Depois que a instalação for concluída com êxito, navegue até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

16. Siga as instruções nos formulários de cada seção.

O que Fazer Depois

Para obter mais informações sobre Vulnerability Response configurações, instalação de aplicações, configuração, integrações, regras de grupo, calculadoras de risco e regras de destino de correção, consulte Configuração de Vulnerability Response usando o Assistente de configuração.

Componentes instalados com Vulnerability Response

Vários tipos de componentes são instalados com a ativação da aplicação Vulnerability Response, incluindo tabelas, funções de usuário e trabalhos programados.

Exibir listas filtradas de componentes instalados com uma aplicação

Filtre a tabela Arquivos de aplicações para que somente as funções, os trabalhos programados e as tabelas que são instaladas com uma aplicação sejam exibidos. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.
2. Selecione o construtor de condição (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação. Por exemplo, **Aplicação** > **é** > **Vulnerability Response**.
3. No construtor de condição, para adicionar um segundo filtro, selecione **E e**, em seguida, selecione, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função**, **Trabalho programado**ou **Tabela**.
4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

Funções instaladas

Nota:
Funções, Trabalhos programados e Tabelas para Application Vulnerability Response podem ser encontrados em Componentes instalados com Application Vulnerability Response.

Título da função [nome]	Descrição	Contém as funções
sn_vul_cisa.configure_intelligence_integration	Configura integrações do Intelligence.	
Gerentes de vulnerabilidade e analistas sênior [sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)]	Atualizar propriedades e integrações de vulnerabilidade. A função sn_vul.vulnerability_admin ou sn_vul.admin (obsoleta) é necessária para a administração Vulnerability Response, incluindo integrações de vulnerabilidade, regras de tarefa de correção, calculadoras e regras e tarefas de destino de correção, relatórios e configuração de integração de terceiros.	• sn_vul.vulnerability_write • sn_vul.ciso_write • sn_sec_cmn.admin • sn_vul_qualys.admin (quando o Qualys Vulnerability Integration es instalado.) • sn_vul_r7.admin (quando o Rapid7 Vulnerability Integration está instalado.) • sn_vul_shodan.admin (quando o Shodan Exploit Integration está instalado.) • sn_vul.configure_nvd_integration (quando as integrações do NVD estão instaladas). • treemap_admin (quando a aplicaçã Performance Analytics está instalada.)
Orquestração de patches	Configura integrações de fornecedor de patch de terceiros compatíveis. Exiba e aplique dados de patch e registros de patch.	• sn_vul_patch_orch.configure_patc Configure e aplique patches. • sn_vul_patch_orch.read_patch

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
		Pode exibir registros e dados de patch. • sn_vul_bigfix.configure_integration Configura a aplicação BigFix Patch Orchestration Integration. Esta função contém as funções granulares sn_vul_bigfix.read_integration e connection_admin que permitem q o usuário se conecte ao console d BigFix. • sn_vul_sccm.configure_integration Esta função contém as funções granulares sn_vul_sccm.read_integration e connection_admin que permitem q o usuário se conecte ao console d SCCM. • sn_vul_bigfix.read_integration Usuários com esta função podem exibir (somente leitura) os registro da aplicação Vulnerability Respons e do BigFix Patch Orchestration Integration e os dados de orquestração de patches. • sn_vul_sccm.read_integration Usuários com esta função podem exibir (somente leitura) os registro do Vulnerability Response e da aplicação Microsoft SCCM Patch Orchestration Integration e os dad de orquestração de patches.
Analistas de vulnerabilidade [sn_vul.vulnerability_write]	A função sn_vul.vulnerability_write é necessária para gerenciar grupos de vulnerabilidades e itens vulneráveis e monitorar o andamento da correção.	• sn_vul.vulnerability_read • sn_sc_cmn.write • sn_vul_qualys.user (quando o Qualys Vulnerability Integration es instalado.) • sn_vul_shodan.write (quando o Shodan Exploit Integration está instalado.)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
V19.0: gerenciador de eventos de vulnerabilidade [sn_vul_analyst.vul_event_manager]	A função sn_vul_analyst.vul_event_manager é usada para avaliar o impacto de uma nova vulnerabilidade ou software, ou adicionar uma vulnerabilidade de dia zero para identificar os ativos afetados e criar itens vulneráveis (IVs).	• sn_sec_cmn.read • canvas_user • sn_vul_analyst.emergency_respon • sn_vul.manage_exposure_assessm
Outros [sn_vul.read_all] A função sn_vul.vulnerability_read está obsoleta.	A função sn_vul.read_all é necessária para qualquer pessoa que precise de visibilidade sobre a gestão de vulnerabilidades. Por exemplo, executivos de TI e segurança ou alguém que queira fazer uma busca detalhada dos painéis de alto nível até os itens que compõem os recursos visuais do painel.	• sn_sec_cmn.read • sn_vul_qualys.read (quando o Qualys Vulnerability Integration es instalado. • sn_vul_shodan.read (quando o Shodan Exploit Integration está instalado.) • pa_viewer (quando a aplicação Performance Analytics está instalada.) • sn_vul_tenable.read_integration (quando o Tenable Vulnerability Integration está instalado.)
Administrador de importação do sistema de VR [sn_vul.vr_import_admin]	Sistema executado como usuário. Executa trabalhos programados. **Nota:** Este usuário é o padrão para executar como usuário para cada registro de integração. Não mude.	• import_admin • sn_vul.vulnerability_write
Proprietário da correção [sn_vul.remediation_owner]	Exiba e atualize a permissão para itens vulneráveis, tarefas de correção atribuídas a você ou seu grupo. Pode exibir todas as vulnerabilidades e soluções. Tem acesso de gravação ao**campo Anotações internas** no registro da solução.	Contido na função itil.
CISOs e executivos de vulnerabilidade [sn_vul.vulnerability_ciso]	Exiba o painel do CISO no Performance Analytics para Vulnerability Response.	• sn_vul.ciso_read • sn_vul.read_all

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalhos programados instalados

Trabalho programado	Descrição
Preencher filtros salvos OOTB para o módulo Host e App	Migra módulos relacionados ao módulo Host e App.
Preencher filtros salvos OOTB para o módulo CC	Migra módulos relacionados ao módulo CC.
Preencher filtros salvos OOTB para o módulo Contêiner	Migra módulos relacionados ao módulo de contêiner.
Atualizar filtros salvos relacionados ao host	Atualiza todos os dados de agregação relacionados aos filtros salvos do módulo Host.
Atualizar filtros salvos relacionados a CC	Atualiza todos os dados de agregação relacionados aos filtros salvos do módulo CC.
Atualizar filtros salvos relacionados ao contêiner	Atualiza todos os dados de agregação relacionados aos filtros salvos do módulo Contêiner.
Atualizar filtros salvos relacionados à aplicação	Atualiza todos os dados de agregação relacionados aos filtros salvos do módulo da aplicação.
Acionar criação e execução de agregação para filtro salvo	Cria, atualiza, executa e atualiza as agregações relacionadas ao filtro salvo.
Versão 19.0 do Vulnerability Response e v4.0 do Veracode Vulnerability Integration	A integração Veracode CWE recupera Veracode - dados de enumeração de fraqueza comum (CWE) para informações de ameaça e recomendações de correção. O Veracode SBOM Integration ingere informações de lançamento, versão e vulnerabilidade que se originam em Veracode sobre os componentes em seus projetos de software. A integração gera SBOMs no formato CycloneDx JSON e os carrega em sua instância A integração de categorias do Veracode recupera dados de categorias aprimoradas de Veracode. A integração Veracode de DevOps permite que os usuários de DevOps exibam detalhes de resumo para verificações de vulnerabilidade de terceiros sem uma licença de SecOps. APIs baseadas em JSON para as seguintes integrações Veracode: item vulnerável da aplicação, resumo de verificação, lista de aplicações. As versões de API baseadas em XML dessas integrações estão obsoletas.
Associar IVs existentes à regra de exceção automática	Associa automaticamente a regra de exceção automática aos IVs existentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho programado	Descrição
Encerrar automaticamente detecções vulneráveis	Encerra automaticamente as detecções vulneráveis obsoletas com base na configuração definida na tabela "sn_vul_auto_close_config".
Versão 16.1: Coleção HCL BigFix, Fixlet e Integrações de ações.	Gerencie patches e implantações de patch para vulnerabilidades com patches do produto HCL BigFix.
Calcular contagens relacionadas para todas as soluções	Desabilitado por padrão. Processa dados de soluções uma vez por noite em vez de continuamente.
Calcular contagens de IV relacionadas para tarefa de vulnerabilidade e correção	Captura mudanças de importação manuais e de IV para o dia. Reconcilia a vulnerabilidade e os relacionamentos da solução e recalcula os totais. Os dados das soluções são enfileirados e processados separadamente pelo trabalho programado **Processar fila de métricas de solução de vulnerabilidade**.
Verificar tempo limite do MID Server	Faz ping no MID Server e elimina os erros após 30 segundos.
V19.0: verificar possível exposição de vulnerabilidade	Processa os CVEs delta, o software e as instalações para obter a exposição.
Verificar estado de execução Aguardando concluído	Marca uma execução de integração como concluída depois que ela é verificada como totalmente concluída.
Verificar expiração do adiamento de itens vulneráveis e grupos	Envia notificações se itens vulneráveis ou vulnerabilidades expirarem (e se elas expirarem em uma semana). Verifica se alguma regra de exceção é aplicável em um IV adiado e atualiza os campos **Motivo** e **Até** de acordo com a regra de exceção. O estado do IV permanece Adiado até a data de vencimento mais recente.
VITs de cancelamento de encerramento que não têm um IC associado	Fecha automaticamente itens vulneráveis que não têm um item de configuração (IC) associado e não foram atualizados há três dias. O estado é definido como Encerrado/Cancelado.
Fechar IV na exclusão do registro de exp	Fecha um IV quando ele é excluído.
Integração de resultados de conformidade	Importa resultados de testes junto com políticas, testes de configuração (controles) e citações com fontes autorizadas para processamento na aplicação Configuration Compliance.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho programado	Descrição
Compliance Results Backfill Integration	Parte de uma integração encadeada executada com a Tenable.io Integração de ativos, importa dados de avaliação de configuração para ativos ignorados que são descobertos (importados por meio da integração de ativos).
Sincronização de estado de CR	O script adapta todas as tarefas de correção existentes aos relacionamentos CHG para que sejam sincronizados. Habilita a sincronização daqui para frente.
Versão 15.0 Scan Credential Integration	Importa e armazena com segurança temporariamente Tenable.io credenciais usadas para acessar o verificador para novas verificações sob demanda.
Integração abrangente do CWE 2000	Integração de vulnerabilidade que extrai informações de vulnerabilidade do conjunto de dados Common Weakness Enumeration (CWE), selecionado pela MITRE Corporation.
V18.0: excluir registros de ação de divisão obsoletos	Trabalho diário para limpar registros obsoletos em tabelas intermediárias de tarefa de divisão.
Desabilitar soluções de VR quando a aplicação de soluções não estiver ativa	Desabilita e oculta o recurso Solução de gerenciamento de vulnerabilidade quando a aplicação Solução de gerenciamento do Vulnerability Response não está instalada.
Avaliar metas de correção	Define ou atualiza datas de destino de correção em todos os itens vulneráveis. Determina o status das datas de destino da correção em relação às regras.
• Corrigindo as detecções da chave atualizada do Rapid7 • Corrigindo as detecções da chave atualizada para Qualys • Corrigindo as detecções da chave atualizada da Tenable	Limpa os dados de detecção automaticamente por um trabalho programado específico da integração que é acionado após a atualização para Vulnerability Response.
Versão 16.1: Gerar resumo de correção	Este trabalho gera automaticamente um resumo de e-mail para todos os usuários no grupo de usuários do responsável pela correção. O trabalho é ativado por padrão.
V19.0: inserir CVE explorado CISA na configuração de exposição	Insere CVEs CISA na tabela Configuração de exposição para calcular a exposição.
V18.0: inserir tarefas de correção clássicas na tarefa de correção unificada	Trabalho programado único para inserir todas as tarefas de correção criadas na IU clássica na tarefa de correção unificada (sn_vul_remediation_task).
Integração da solução Microsoft Security Response Center	Solução de gerenciamento de vulnerabilidade integração que recupera soluções do Microsoft Security Response Center.
Versão 16.1: Coleção do Microsoft SCCM, Atualização de Patch	Gerencie patches e implantações de patch para vulnerabilidades com Microsoft patches do SCCM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho programado	Descrição
e Integrações de Implantações	
Escolher processo de integração limitado	Cria o processo de integração para o Shodan Exploit Integration.
Preencher texto de produtos afetados	Após o upgrade, o lida com as soluções existentes para preencher o texto dos produtos afetados. Este trabalho é executado uma vez.
Preencher nova coluna de contagem de CR	Preenche automaticamente a nova coluna de contagem de CR para clientes com dados existentes na tabela de tarefa de correção [sn_vul_vulnerability].
Processar fila de métricas de solução de vulnerabilidade	Enfileira e processa continuamente os dados de soluções quando eles são importados ou atualizados manualmente.
Preencher registros na tabela de mapeamento de fornecedor de vulnerabilidade Preencher registros na tabela de mapeamento de fornecedor de vulnerabilidades para vulnerabilidades do Rapid7	Insere registros na tabela de mapeamento do fornecedor de vulnerabilidades para vulnerabilidades existentes.
Reabrir grupos de vulnerabilidade adiados	Reabre adiadas tarefas de correção quando a data de adiamento tiver passado.
Reaplicar todas as regras de atribuição de vulnerabilidade	Reavalia as regras de atribuição em relação a todos os IVs em **aberto**.
Versão 16.5: contagem de reatribuições para regras de atribuição	É executado diariamente e publica o número total de IVs e tarefas de correção que não estão atribuídos por este recurso para uma regra de atribuição específica.
Red Hat Solution Integration	Solução de gerenciamento de vulnerabilidade integração que recupera soluções do Red Hat Security Advisory.
V17.1: atualizar e resolver VITs duplicados na tarefa de correção	Encontra itens vulneráveis duplicados para os itens na tarefa de correção com "Atualizar IVs duplicados automaticamente" como ativos.
Atualizar itens vulneráveis associados para tarefa de correção baseada em regra de tarefa de não correção	Atualiza a tarefa de correção com itens vulneráveis que correspondem aos critérios de Grupo de filtros e Grupos de condições.
Reparar itens vulneráveis com erro abertos e encerrados pela última vez	Repara dados de IU existentes corrompidos por defeitos corrigidos anteriormente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho programado	Descrição
Reexecutar calculadoras	Reaplica as calculadoras a todos os itens vulneráveis afetados pela mudança. Isso aciona um recálculo das pontuações de risco cumulativas de suas tarefas de correções. **Nota:** A reexecução de calculadoras pode levar muito tempo, dependendo do seu ambiente.
Repetir conjuntos de importação de integração cancelados	Recupera conjuntos de importação de integração cancelados. Tenta cinco vezes antes de retornar um erro.
Repetir processos de integração	Recupera processos de integração. Tenta cinco vezes antes de retornar um erro.
Acumular valores de item vulnerável para vulnerabilidade e grupo	Calcula a pontuação de risco, o número de itens vulneráveis e o status do destino de correção para tarefas de correção, usando a calculadora de acúmulo.
Executar calculadora de severidade após a promoção de entrada de vulnerabilidade	Executa a calculadora de severidade depois que uma vulnerabilidade ausente anteriormente é atualizada com sua pontuação e outros dados de um provedor de terceiros, como Qualys Cloud Platform, Rapid7 Nexpose.
V19.0: executar avaliação de exposição para CVEs configurados	Calcula a exposição de todos os registros de CVE na tabela Configuração de exposição.
V19.0: executar exposição de software	Calcula a exposição de todos os registros de software na tabela Configuração de exposição.
Processador de fonte de dados de vulnerabilidade programado	Verifica a fila de importação em busca de entradas a serem processadas e atribui um trabalho de importação programada com base nos recursos disponíveis.
Limpeza de anexo do processo de integração de vulnerabilidade programada	Remove anexos XML de integração quando eles completam 14 dias. Este tempo de retenção não é configurável.
Verificador de tempo limite de integração de vulnerabilidade programado	Cancela execuções de integração que levam mais de 60 minutos para serem concluídas.
Definir serviços de IC relacionados para IV	Depois que a importação de integração estiver concluída, vinculará os serviços de negócios afetados aos ICs conectados a itens vulneráveis, no tempo especificado.
Definir contagens de adiamento	Coleta o número de vezes que um item vulnerável, um item vulnerável da aplicação, um item vulnerável de contêiner ou uma tarefa de correção é adiado.
Acionar a próxima integração	Aciona a próxima integração em uma execução de integração encadeada.
Integração de modelo	Um único registro de modelo é enviado para Tenable.io durante a nova verificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho programado	Descrição
Atualizar itens vulneráveis não agrupados	Determina se um item vulnerável está emtarefa de correção e o adiciona ou remove da lista de **Itens vulneráveis** não agrupados. **Nota:** Este trabalho é executado após o upgrade e, dependendo do conjunto de dados, pode levar muito tempo para ser concluído.
Atualizar vulnerabilidade no VG	Atualiza o campo **Vulnerabilidade** na tabela Grupo de vulnerabilidades (sn_vul_vulnerabilty) após o upgrade. Este trabalho é acionado uma vez e desabilitado em seguida.
Modelo de importação de vulnerabilidade	Mecanismo que processa a fila de importação. Um de 10.
Atualização encerrada da idade do Vulnerability Response	Atualiza a coluna de idade encerrada na tabela IV.
Contagem de IC do Vulnerability Response	Calcula o número de ICs verificados por scanners de terceiros nos últimos 30 dias.
Upgrade do status de risco e correção do Vulnerability Response	Atualiza a classificação de risco nos dados ao atualizar.
v20.0: verificar expiração da redução de risco	Verifica se os controles compensatórios expiraram para um item vulnerável e uma tarefa de correção. Se expirarem, ele reverterá a pontuação de risco para a pontuação de risco original e enviará uma notificação por e-mail indicando que os controles compensatórios expiraram. Também envia uma notificação por e-mail se os controles compensatórios forem definidos para expirar em 7 dias.

Tabelas instaladas

Tabela	Descrição
sn_vul_cmn_ws_saved_filter	Armazena os dados do filtro salvo.
sn_vul_licensing_usage	Contém o ativo duplicado, o ativo IP incompleto, as contagens totais de ativos do scanner e o uso final.
sn_vul_m2m_entry_compensating_control	Representa a associação entre entradas de vulnerabilidade e controles de compensação.
v21.0 Mecanismo de verificação Rapid7 [sn_vul_r7_scan_engine]	Armazene os registros importados dos dados do mecanismo de verificação responsáveis por descobrir ativos durante uma verificação e verificar se há vulnerabilidades neles.
v21.0 Importação do mecanismo de verificação Rapid7 [sn_vul_r7_scan_engine_import]	Usado pela integração do Rapid7 Scan Engine para preparar os dados de importação antes do processamento.
Versão 19.0: [sn_vul_veracode_cwe_import]	Estende a tabela Categoria Veracode para recomendações de correção do CWE.
Versão 19.0:	Armazena dados de categoria importados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_vul_veracode_category_import]	
Versão 19.0: [sn_vul_veracode_sbom_import]	Armazena dados SBOM importados originados do Veracode.
V17.1: adicionar prova à chave IV [sn_vul_prova_key_vulnerability]	Vulnerabilidades do Rapid7 para as quais a prova deve ser incluída na chave IV.
Itens vulneráveis avaliados [sn_vul_m2m_exp_sw_vi]	Atribui um grupo de tarefas de correção a um grupo de atribuição durante a criação da tarefa de correção.
Regra de atribuição [sn_vul_vgr_assignment_rule]	Atribui um grupo de tarefas de correção a um grupo de atribuição durante a criação da tarefa de correção. Antes da v15.0: atribui uma tarefa de correção a um grupo de atribuição durante a criação da [tarefa de correção .
Associar Solicitação de Mudança [sn_vul_action_associate_cr]	Tabela de preparação usada para processar novas associações de tarefa de correção-CHG. Antes da v15.0: tabela de preparação usada para processar novas associações VG-CHG.
Trabalho de Item Vulnerável Assíncrono [sn_vul_async_vi_job]	Contém trabalhos em segundo plano que processam itens vulneráveis. Somente um tipo de trabalho é compatível; usado para editar vulnerabilidades em massa.
Tipo de trabalho de item vulnerável assíncrono [sn_vul_async_vi_job_type]	Contém os tipos de trabalhos em segundo plano e faz referência ao script relevante. Tem apenas um processador, o **VulnerabilityBulkEditProcessor**
Encerrar automaticamente detecções obsoletas [sn_vul_auto_close_config]	Armazena a configuração de como as detecções obsoletas são encerradas automaticamente.
Configurar granularidade de item vulnerável [sn_vul_action_vi_granularity_config]	Armazena o formulário de IU usado para habilitar ou desabilitar Incluir porta na página de configuração do módulo Configurar granularidade de IV.
Criar solicitação de mudança [sn_vul_action_create_cr]	Usado para criar solicitações de mudança a partir da tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Criar Itens vulneráveis [sn_vul_action_create_vi]	Uma tabela de preparação que é usada como um espaço reservado para informações. Esta tabela não armazena nenhum registro.
Coleção [sn_vul_patch_orch_collection]	Armazena dados de coleta de instâncias distintas.
CWE [sn_vul_cwe]	Catálogo de vulnerabilidades de software de Enumeração e Pontos Fracos Comuns (CWE).
Plataforma aplicável do CWE [sn_vul_cwe_m2m_cwe_platform]	Contém os dados de plataforma aplicáveis do CWE importados.
Categoria CWE [sn_vul_cwe_category]	Contém os dados de categoria CWE importados.
Consequência CWE comum [sn_vul_cwe_conquence]	Contém os dados de consequência comuns do CWE importados.
Referência externa do CWE [sn_vul_cwe_reference]	Contém os dados de referência externa do CWE importados.
Exemplo observado do CWE [sn_vul_m2m_cwe_cve]	Contém os dados CWE CVE importados.
Plataforma do CWE [sn_vul_cwe_platform]	Contém os dados importados da plataforma CWE.
Referência externa do CWE [sn_vul_cwe_reference]	Contém os dados de referência externos relacionados ao CWE importados.
Relacionamento do CWE [sn_vul_m2m_cwe_relation]	Contém os dados de relacionamento do CWE importados.
Exibição do CWE [sn_vul_cwe_view]	Contém os dados de exibição do CWE importados.
Ponto fraco do CWE	Contém os dados de fraqueza do CWE importados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_vul_cwe_weakness]	
Versão 16.1: coleção de dispositivos [sn_vul_patch_orch_m2m_src_ci_collection]	Armazena dados de coleções sobre itens descobertos.
Versão 16.1: atualização de dispositivo [sn_vul_patch_orch_m2m_src_ci_update]	Armazena dados sobre os patches implantados, junto com o status da implantação, que são exibidos em registros de item descoberto.
Correspondência de software vulnerável do modelo de descoberta [sn_vul_discovery_model_software_match]	Complementa a correspondência de software vulnerável a um modelo de descoberta.
Configuração de gestão de exceções [sn_vul_exception_config]	Armazena as definições de configuração do recurso de gestão de exceções.
Regra de exceção [sn_vul_auto_exception_rule]	Contém o conjunto de regras avaliadas para a Gestão de exceções.
Explorar [sn_vul_exploit]	Contém as definições de explorações: código disponível publicamente que aproveita uma vulnerabilidade.
Estrutura da Exploração sn_vul_exploit_framework	Contém os nomes das estruturas de exploração: pacotes de software completos que são capazes de executar muitas explorações.
Modelos de descoberta expostos [sn_vul_m2m_exp_sw_model]	Armazena o mapeamento entre o modelo do Discovery e a avaliação de exposição.
Avaliação de Exposição [sn_vul_exp_by_sw]	Armazena os registros para avaliação de exposição.
V19.0: manifesto de exposição sn_vul_analyst_exposure_manifest	Tabela de manifesto para processamento delta.
Entradas de Vulnerabilidade de Exposição [sn_vul_m2m_entry_exp]	Armazena o mapeamento entre Vulnerabilidade (sn_vul_entry) e Avaliação de exposição.
Kit de malware [sn_vul_malware_Kit]	Contém os detalhes dos kits de malware: ferramentas pré-escritas que facilitam a execução de uma exploração ou de um conjunto de explorações relacionadas sem precisar codificar ou configurar trabalhos adicionais

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Tabela de ativo ausente [sn_vul_tenable_missing_asset]	Contém IDs de ativo temporário para dados de avaliação de conformidade de configuração ignorados com ativos incompatíveis.
Atualização da Solução do Microsoft Response Center [sn_vul_msrc_update]	Contém a última vez em que os dados da solução foram atualizados pela Microsoft. Usado para comparar com a importação noturna para determinar os dados delta para download.
Microsoft Security Response Center Importação de solução [sn_vul_msrc_solution_import]	Usado pela integração da solução Microsoft Security Response Center para preparar dados de importação antes do processamento.
Integração com a solução Microsoft Security Response Center [sn_vul_msrc_integration]	Estende a tabela Integração de vulnerabilidade [sn_vul_integration] para Integração com a solução Microsoft Security Response Center.
Entrada do Banco de Dados de Vulnerabilidades Nacionais [sn_vul_nvd_entry]	Vulnerabilidade documentada do banco de dados nacional de vulnerabilidades do NIST.
Importação de CVSS do NVD [sn_vul_nvd_cvss_import]	Contém dados de preparação que ainda não foram transformados para o esquema Vulnerability Response durante a importação do NVD.
Versão 16.1 [sn_vul_patch_orch.patch_approval_required]	Quando as implantações de patch são programadas a partir de uma integração de patch, as solicitações são enviadas para revisão e aprovação aos usuários atribuídos ao Nível 1 - Grupo de aprovação de atualizações de patch. Esta propriedade é ativada por padrão.
Versão 16.1: Implantação de patch [sn_vul_patch_orch_deployment]	Armazena informações sobre patches implantados sobre Coleções e ICs.
Versão 16.1: Atualização de patch [sn_vul_patch_orch_update]	Armazena informações sobre os patches que estão disponíveis em instâncias distintas.
Versão 16.1: possível patch [sn_vul_patch_orch_m2m_vuln_patch]	Armazena dados sobre patches e vulnerabilidades que identificam os patches que podem ser usados para resolver uma vulnerabilidade.
V19.0: possível exposição de vulnerabilidade sn_vul_analyst_m2m_pot_exp_sw_model	Tabela de avaliação de exposição para CVE.
Categoria do produto [sn_vul_product_category]	Contém os dados da categoria de produto importada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Red Hat Security Advisory [sn_vul_rhsa_update]	Compara as soluções Red Hat com o trabalho noturno para determinar os dados delta para importação.
Red Hat Importações de solução [sn_vul_rh_solution_import]	Usado pelo Red Hat Solution Integration para preparar dados de importação antes do processamento.
Red Hat Solution Integration [sn_vul_rh_integration]	Estende a tabela Integração de vulnerabilidade [sn_vul_integration] para Red Hat Solution Integration.
Serviços de negócios relacionados [sn_vul_m2m_ci_services]	Vincula ICs a serviços de negócios para pesquisa de serviços afetados. Contém um sinalizador que indica se foi adicionado pelo Service Mapping.
V18.0: Contagens de esforço de correção [sn_vul_daily_count_re]	Contagem diária de esforços de correção. Esta tabela é atualizada diariamente.
V18.0: registro do esforço de correção [sn_vul_remediation_effort_record]	Rastreia o andamento da correção dos esforços de correção (RE). Contém referências aos REs.
Regra de destino de correção [sn_vul_ttr_rule]	Define o intervalo de tempo esperado para corrigir um item vulnerável. Estende o arquivo da aplicação.
V18.0: tarefa de correção [sn_vul_remediation_task]	Armazena todas as tarefas de correção para VR, AVR, CVR e grupos de resultados de testes.
Integração REST [sn_vul_rest_integration]	Estende a tabela Integração de vulnerabilidade [sn_vul_integration] para as integrações baseadas em REST.
Detecção de vulnerabilidade do NVD do SAM [sn_vul_sam_config]	Contém quais ICs e vulnerabilidades são monitorados com o SAM NVD e se a detecção de vulnerabilidade do SAM NVD está habilitada ou não.
Pool de Importação Programada [sn_vul_sched_import_pool]	Coleção de registros de conjunto de importação programada usada para facilitar importações simultâneas de fonte de dados.
Selecionar item vulnerável [sn_vul_action_select_vi]	Tabela de preparação base usada para lidar com dividir VG, criar CHGs e associar CHGs
Status de configuração [sn_vul_setup_status]	Somente interno: usado pelo Assistente de configuração. Sempre que o Assistente de configuração é aberto, ele mostra o status das etapas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
	Concluídas e a porcentagem no canto superior direito vem desta tabela.
Mapa de Gravidade [sn_vul_severity_map]	Contém os mapeamentos da severidade de origem para a severidade normalizada.
Mapeamento do Scanner de Solução [sn_vul_solution_scanner_mapping]	Mapeia fornecedor, scanner e palavras-chave para exclusão ou inclusão.
Dividir grupo de vulnerabilidades [sn_vul_action_split_vg]	Tabela de preparação usada para dividir tarefas de correção.
Entrada de Vulnerabilidade de Terceiros [sn_vul_ third_party_entry]	Vulnerabilidade documentada de uma fonte de terceiros.
[sn_vul_tenable_io_template	Um registro de modelo é enviado para Tenable.io e importado durante a nova verificação para itens que têm Tenable.io como origem.
Atualizar manifesto [sn_vul_update_manifest]	Lista de tarefas de correção que foram atualizadas e exigem recálculo pela calculadora de acúmulo.
V17.1: uso por classes de IC [sn_vul_licensing_usage_by_ci_classes]	Contém a contagem de uso agregada pela classe de IC.
Contagem de Itens de Configuração de VR [sn_vul_vr_configuration_item_count]	Contém a média cumulativa de 90 dias consecutivos de itens de configuração importados de integrações de terceiros.
Regras de Atribuição da Vulnerabilidade [sn_vul_assignment_rule]	Contém o conjunto de regras avaliadas para definir o grupo de atribuição em IVs.
Calculadora de Vulnerabilidade [sn_vul_calculator_group]	Contém as regras da calculadora de vulnerabilidade. A ordem da calculadora determina qual calculadora é avaliada primeiro e, em cada calculadora, uma regra de calculadora, no máximo, é usada.
Regra da Calculadora de Vulnerabilidade [sn_vul_calculator]	Contém as regras para todas as calculadoras. Para cada calculadora, as regras da calculadora são revisadas em ordem. A primeira calculadora que corresponde à condição usa os valores dessa regra.
CVEs de vulnerabilidade [sn_vul_m2m_entry_cve]	Vincula os dados de CVE (Common Vulnerability Exposures, exposições de vulnerabilidade comum) do NVD a entradas vulneráveis.
Entrada da Fila de Importação da Fonte de dados de Vulnerabilidade [sn_vul_ds_import_q_entry]	Fila para anexos antes de serem processados por uma fonte de dados. Usado por integrações de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Entrada de Vulnerabilidade [sn_vul_entry]	Vulnerabilidade documentada.
Verificação de entrada de vulnerabilidade [sn_vul_entry_scan]	Armazena o relacionamento entre uma verificação e a entrada de vulnerabilidade.
Estrutura de Exploração de Vulnerabilidade [sn_vul_m2m_framework_vul]	Contém o relacionamento entre estruturas de exploração e vulnerabilidades.
V19.0: avaliação de exposição de vulnerabilidade sn_vul_analyst_sam_config	Tabela de configuração de avaliação de exposição para CVE.
Configuração de granularidade de vulnerabilidade [sn_vul_granularity_config]	Armazena e mantém o estado da Porta de inclusão ou exclusão do módulo Configurar granularidade de IV.
Grupo de Vulnerabilidades [sn_vul_vulnerability]	Coleção de itens vulneráveis organizados para correção.
Solicitações de mudança de grupo de vulnerabilidade [sn_vul_m2m_vg_change_request]	Armazena a associação de tarefas de correção e solicitações CHG.
Item do Grupo de Vulnerabilidades [sn_vul_m2m_vul_group_item]	Associação de tarefas de correção e itens vulneráveis.
Regra do Grupo de Vulnerabilidades [sn_vul_grouping_rule]	Contém as regras que definem os critérios com os quais os grupos são criados automaticamente para um conjunto de itens vulneráveis.
Integração de Vulnerabilidade [sn_vul_integration]	Registro programável para importar dados de vulnerabilidade de uma fonte externa. Estende a execução programada de script.
Fonte de dados de integração de vulnerabilidade [sn_vul_int_data_src]	Fonte de dados a ser usada com uma integração de vulnerabilidade.
Log de Integração de Vulnerabilidades [sn_vul_integration_log]	Registra a saída de informações de log por execuções de integração de vulnerabilidade.
Processo de Integração de Vulnerabilidades [sn_vul_integration_process]	Ocorrência de processo único para uma integração de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Fila de Integração de Vulnerabilidade [sn_vul_integration_queue]	Coloca na fila as solicitações de importação para uma integração executada quando todas as fontes de dados estão em uso.
Execução de Integração de Vulnerabilidades [sn_vul_integration_run]	Invocações de integração de vulnerabilidade. **Nota:** Se uma execução de integração estiver em andamento, somente uma integração poderá estar no estado pronto no backlog.
Estatísticas de execução de integração de vulnerabilidade [sn_vul_integration_stats]	Armazena o detalhamento de cada etapa: por exemplo, tempo de REST API, tempo de criação de IV etc. para uma execução de integração
Tarefa de Item de Vulnerabilidade [sn_vul_m2m_item_task]	Itens vulneráveis associados a problemas, mudanças e incidentes de segurança.
Kit de Malware de Vulnerabilidade [sn_vul_m2m_malware_ kit_vul]	Contém os relacionamentos entre vulnerabilidades e kits de malware.
Solução de pré-requisitos de vulnerabilidade [sn_vul_m2m_solution_prerequisito]	Contém os pré-requisitos específicos da origem para aplicar uma solução, quando disponível.
Limite de taxa de vulnerabilidade [sn_vul_rate_limit]	Define um limite de taxa a ser usado em um scanner.
Referência de Vulnerabilidade [sn_vul_reference]	Referências externas para vulnerabilidades conhecidas.
Status de Correção de Vulnerabilidade [sn_vul_m2m_ttr_status]	Status do item vulnerável em relação à regra de destino de correção aplicada mais próxima.
Regra do Risco de Vulnerabilidade [sn_vul_calcul_risk]	Regra de calculadora especializada usada com as calculadoras de pontuação de risco. Usa pesos indicando quais valores, relacionados a um IV, usar para calcular a pontuação de risco.
Calculadora de Rollup de Vulnerabilidade [sn_vul_rollup]	Lista de calculadoras de acúmulo de vulnerabilidades.
Verificação de Vulnerabilidades [sn_vul_scan]	Verificação de vulnerabilidade. Contém o que verificar, com qual scanner e um resumo dos resultados da verificação.
Item de Configuração da Verificação de Vulnerabilidades	Associa ICs do CMDB que estão na fila para serem verificados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_vul_m2m_scan_configuration_item]	
Entrada da Fila de Verificação de Vulnerabilidades [sn_vul_scan_q_entry]	Registro de verificação enfileirado para verificação ou processamento. Facilita as solicitações dentro dos limites de taxa declarados.
Origem da Verificação de Vulnerabilidades [sn_vul_m2m_scan_source]	Associa origens a um registro de verificação e significa que todos os registros estão na fila para serem verificados.
Tarefa da Verificação de Vulnerabilidades [sn_vul_m2m_scan_vulnerability]	Associa tarefas de vulnerabilidade às origens de um registro de verificação.
Scanner de vulnerabilidade [sn_vul_scanner]	Define scanners de terceiros a serem usados em verificações.
Limite de taxa do scanner de vulnerabilidade [sn_cmn_scanner_rate_limit]	Associa um scanner a um limite de taxa.
Software de Vulnerabilidade [sn_vul_m2m_entry_software]	Contém associações entre vulnerabilidades e software vulnerável.
Solução de Vulnerabilidade [sn_vul_solution]	Contém os dados de relacionamento entre a vulnerabilidade e as possíveis soluções para ela.
Solução de Vulnerabilidade [sn_vul_m2m_vulnerability_solution]	Vincula a tabela de entrada de vulnerabilidade (sn_vul_entry) à tabela de solução de vulnerabilidade (sn_vul_solution).
Aprovação de Mudança do Estado de Vulnerabilidade [sn_vul_change_approval]	Rastreia o processo de aprovação de vulnerabilidades.
Solução de Substituição de Vulnerabilidade [sn_vul_m2m_solution_supersedence]	Contém o relacionamento específico de origem entre soluções.
Manifesto de Atualização de Vulnerabilidade [sn_vul_vuln_update]	Contém uma lista de vulnerabilidades que precisam de seus dados de acúmulo atualizados depois que seus itens vulneráveis são atualizados, encerrados ou têm mudanças de pontuação de risco.
Mapeamento de Fornecedor de Vulnerabilidade [sun_vul_vulnerability_vendor_mapping]	Contém uma lista de vulnerabilidades e seus fornecedores.
Item Vulnerável [sn_vul_vulnerable_item]	Contém a ocorrência de uma vulnerabilidade em um item de configuração.

Tradução automática

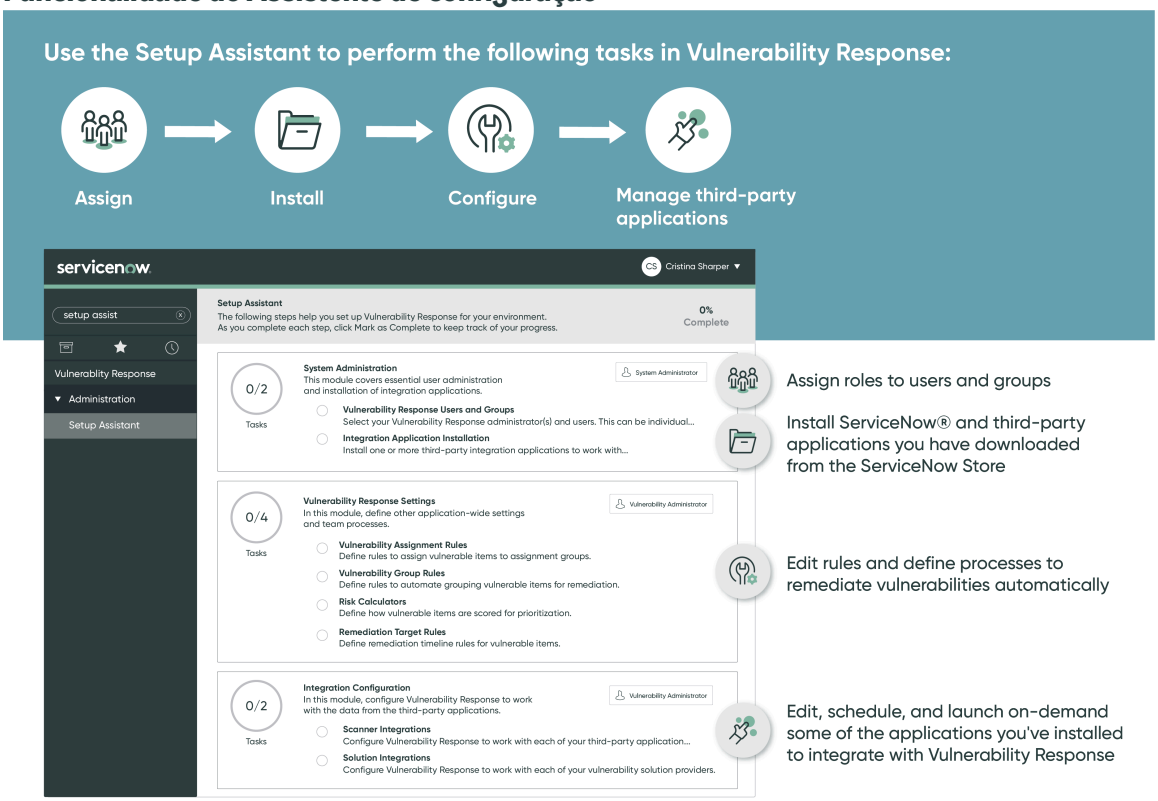
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Detecção de Item Vulnerável [sn_vul_detection]	Contém as detecções de item vulnerável de integrações de terceiros.
Software Vulnerável [sn_vul_software]	Software que é conhecido por ter determinadas vulnerabilidades.

Configuração de Vulnerability Response usando o Assistente de configuração

O Assistente de configuração orienta você na configuração do Vulnerability Response e de determinadas integrações de terceiros para o seu ambiente. O Assistente de configuração fornece quase tudo o que você precisa para instalar e configurar seu ambiente para que você possa usar Vulnerability Response.

Funcionalidade do Assistente de configuração



Now Platform® roles: admin and vulnerability admin

O uso do Assistente de configuração requer duas funções Now Platform® diferentes: administrador e administrador de vulnerabilidade.

Consulte as seções a seguir para complementar as instruções e os avisos fornecidos no Assistente de configuração.

Administração do sistema - atribuir usuários e grupos e instalar aplicações de integração

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma lista de usuários e integrações deve ser obtida do gerenciador de vulnerabilidades antes de iniciar essas tarefas.

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração**.
2. Na primeira seção, Administração do sistema, o administrador atribui funções a usuários e grupos e instala integrações compatíveis.

   Atribua Vulnerability Response personas e funções a usuários e grupos no Assistente de configuração.

   Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.
3. Atribua funções no Assistente de configuração.
   - Atribua a função de sn_vul.admin a usuários ou grupos.
   - Atribua a função sn_vul.admin para administração e configuração do Vulnerability Response, incluindo integrações de vulnerabilidade, regras de tarefa de correção, calculadoras e regras de tempo de correção.
   - Atribua a função sn_vul_vulnerability_write para a criação e atualização de tarefas de correção e itens vulneráveis.

     Nota:
     Todos os outros usuários recebem automaticamente o acesso de gravação somente para tarefas de correção que são atribuídas a eles.

   - Atribua a função sn_vul_vulnerability_read para exibir tarefas de correção, itens vulneráveis e outras informações de vulnerabilidade.

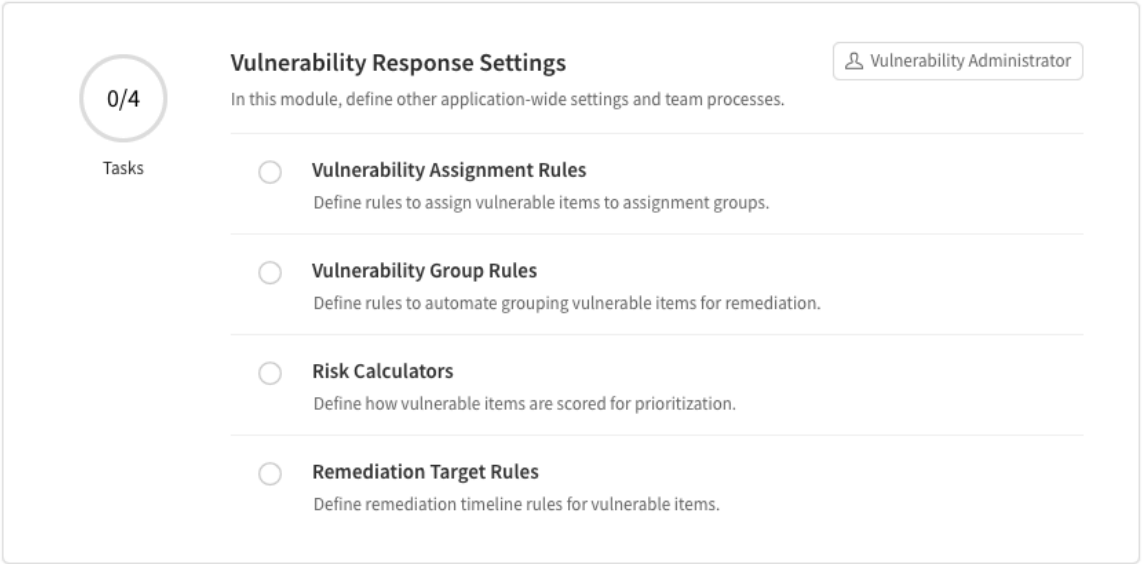
     Nota:
     Usuários com a função itil recebem automaticamente a função sn_vul.remediation_owner, permitindo que eles vejam tarefas de correção e itens vulneráveis atribuídos a eles, entradas de vulnerabilidade e soluções na aplicação Vulnerability Response em sua instância e na aplicação Mobile Agent. Nenhuma atribuição adicional é necessária.
4. Instale aplicações de integração de terceiros.
   - Consulte Instalação de Vulnerability Response e aplicações compatíveis e Integrações do Vulnerability Response para obter mais informações sobre aplicações compatíveis com Vulnerability Response.
   - Para obter mais informações sobre como usar o assistente de configuração para instalar aplicativos compatíveis, consulte Instalar Vulnerability Response aplicações de terceiros usando o Assistente de configuração.

Vulnerability Response Configurações

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) ou admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Em Configurações do Vulnerability Response, o administrador de vulnerabilidade define as configurações de toda a aplicação e define regras para Vulnerability Response. Como alternativa, o administrador pode executar essas tarefas.

1. Crie regras de atribuição de vulnerabilidade.

Crie regras que definam a atribuição automática de tarefas de correção para resolução. Pelo menos uma regra é enviada com o sistema de base. Para obter mais informações, consulte Vulnerability Response visão geral de regras de atribuição.

Nota:

O recurso de reaplicação requer uma aplicação de linha de base das regras. Depois que suas regras forem criadas, ative o trabalho programado *`Reapply all vulnerability assignment rules`* para executar, conforme sua conveniência. Caso contrário, será necessário reaplicar todas as regras a todos os IVs abertos antes de alterá-los.

Quando o trabalho estiver concluído, defina o campo **Executar** no trabalho programado para se ajustar ao seu ambiente. Dependendo do número de IVs ativos que você tem, avaliá-los e atualizá-los diariamente pode ter um impacto não comum no desempenho. Para ambientes maiores, considere atualizar uma vez por semana ou até mesmo uma vez por mês.

A reaplicação das regras de atribuição não reagrupa os itens vulneráveis.

2. Crie regras de tarefa de correção.

Crie regras que definem a criação automática de tarefas de correção para resolução. Pelo menos uma regra, **Vulnerabilidade,** é enviada com o sistema de base. Você pode reaplicar as regras do formulário ou da exibição de lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Quando uma regra de grupo é excluída, no formulário ou na exibição de lista, você tem a opção de excluir todos os grupos **Abertos** criados por essa regra. Os grupos que não estão no estado **Aberto** são excluídos.
- Consulte Regras de pesquisa de IC para identificar itens de configuração de Vulnerability Response integrações de vulnerabilidade de terceiros para obter mais informações sobre como criar regras para seu ambiente.
- Consulte Explorando a aplicação Vulnerability Response para obter mais informações sobre como usar Vulnerability Response para corrigir vulnerabilidades.

3. Crie e habilite Calculadoras de risco.

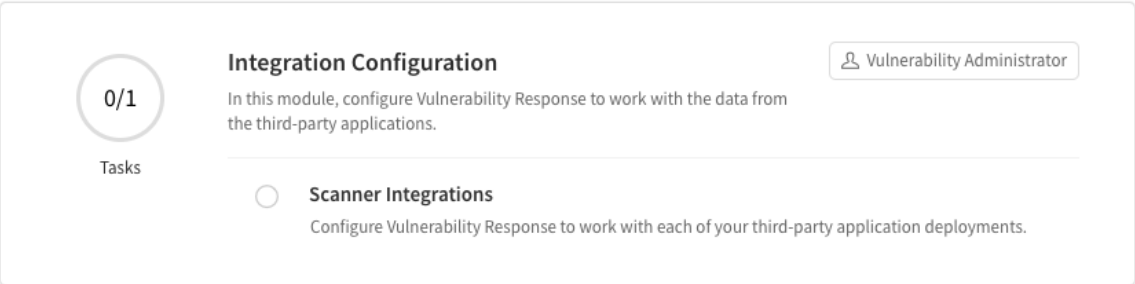
   Habilite calculadoras de risco que definem como os itens vulneráveis são pontuados para priorização. Várias calculadoras de risco são enviadas com o sistema básico. Consulte Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade informações sobre como criar ou editar calculadoras de risco para seu ambiente.

4. Crie Regras de destino de correção.

   Crie regras de destino de correção para categorias de correção. Pelo menos uma regra é enviada com o sistema de base. Consulte Vulnerability Response regras de destino de correção para obter mais informações sobre como criar regras para seu ambiente.

Configuração de Integração

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) ou admin.



Na seção Configuração de integração, configure, programe, edite e inicie sob demanda as seguintes integrações de scanner de vulnerabilidade de terceiros e, se a aplicação Solução de gerenciamento do Vulnerability Response estiver instalada, provedores de soluções.

- Consulte Configurar o Qualys Vulnerability Integration usando o Assistente de configuração para obter mais informações sobre como configurar o Qualys Vulnerability Integration.
- A configuração da aplicação Integração do Vulnerability Response com Tenable é compatível. Consulte Configurar a integração de vulnerabilidade da Tenable usando o assistente de configuração.
- Depois de instalar a aplicação Solução de gerenciamento de vulnerabilidade, a opção **Integrações da solução** é exibida abaixo **de Integrações do scanner**. Clique em **Integrações de solução** para configurar os provedores de solução de vulnerabilidade instalados nesta seção do Assistente de configuração. Red Hat Solution Integration e Integração com a solução Microsoft Security Response Center são compatíveis.

  Consulte Solução de gerenciamento de vulnerabilidade para obter mais informações sobre as soluções instaladas. Consulte Instalar a aplicação Solução de gerenciamento do Vulnerability Response para obter mais informações sobre a instalação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Consulte Configurar integrações de soluções instaladas para Solução de gerenciamento de vulnerabilidade usando o Assistente de configuração para obter mais informações sobre como configurar as soluções instaladas.

- Se uma integração for de várias origens, você poderá ter várias implantações da mesma integração de terceiros.
- As configurações da integração original de terceiros são usadas como modelo para as configurações de cada nova integração.

Nota:
Se você excluir a integração de vulnerabilidade original, precisará selecionar outra integração para usar como modelo. Considere desabilitar a integração em vez de excluí-la. As integrações criadas a partir de modelos desabilitados são desabilitadas por padrão.

Os dados de cada integração de terceiros são identificados exclusivamente e estão disponíveis em uma única instância de Vulnerability Response.

Nota:
Várias integrações de vulnerabilidade para Rapid7 InsightVM não estão disponíveis no Assistente de configuração. Consulte Criar importações separadas por domínio para uma integração para obter informações sobre como configurar e criar várias integrações Rapid7 InsightVM.

Tarefas adicionais

Consulte Tarefas adicionais Vulnerability Response de instalação e configuração para obter mais informações sobre tarefas de configuração não incluídas no Assistente de configuração.

Atribua as funções de persona Vulnerability Response usando o Assistente de configuração

Atribua as funções de persona Vulnerability Response a grupos ou usuários com o Assistente de configuração.

Antes de Iniciar

Se você já atribuiu funções de persona em Vulnerability Response usando o Assistente de configuração e deseja obter mais informações sobre como editar e gerenciar suas funções granulares e atribuições de função no módulo Administração de usuário, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Se você for um cliente de atualização, poderá continuar usando suas funções existentes para a aplicação Vulnerability Response. O acesso de usuários e grupos atribuídos com as permissões sn_vul.vulnerability_read e sn_vul.vulnerability_write e as funções de proprietário de correção disponíveis nas versões anteriores de Vulnerability Response não foi alterado.

No entanto, para obter mais controle sobre o que usuários e grupos podem fazer e ver na aplicação Vulnerability Response no nível da tarefa, talvez você prefira usar funções granulares e de persona.

Se você ainda não atribuiu a função de persona sn_vul.vulnerability_admin usando o Assistente de configuração, siga as etapas abaixo para atribuí-la. Depois de atribuído, o administrador de vulnerabilidade com esta função de persona tem permissão para concluir as tarefas do Assistente de configuração após a primeira seção e gerenciar regras e integrações de terceiros na aplicação Vulnerability Response.

Para obter uma visão geral sobre funções de persona e granulares, consulte Vulnerability Response personas e funções granulares.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você for um cliente de atualização, use a tabela a seguir como referência.

Antes da v10.3	Iniciando com v10.3
Se você atribuiu sn_vul.admin	Você pode preferir atribuir sn_vul.vulnerability_admin - Vulnerability Admin a usuários ou grupos. Usuários com esta função têm acesso completo à aplicação Vulnerability Response (VR) e seus registros. Usuários com esta função configuram todas as aplicações e regras de VR e instalam integrações de terceiros.
Se você atribuiu sn_vulnerability_write para usuários e grupos.	Você pode preferir atribuir sn_vul.vulnerability_analyst - Vulnerability Analyst a usuários e grupos. Usuários e grupos com esta função exibem e atualizam todos os registros para correção de IV.
Se você atribuiu sn_vul.remediation_owner	Você pode preferir atribuir sn_vul.remediation_owner - Proprietário da correção a usuários e grupos. Usuários e grupos com esta função corrigem vulnerabilidades atribuídas a eles ou a um grupo ao qual pertencem. Grupos ou usuários com esta função exibem e atualizam os registros atribuídos a eles ou a um grupo ao qual pertencem.
Se você atribuiu sn_vul.admin para gestão de itens de configuração (IC) incompatíveis	Você pode preferir atribuir sn_vul.ci- Gerente de IC a usuários e grupos. Usuários e grupos com esta função gerenciam itens de configuração (ICs) incompatíveis não encontrados no Configuration Management Database (CMDB). Grupos ou usuários com esta função atualizam itens descobertos.
Se você atribuiu sn_vul.admin para adiamentos e aprovações de exceção.	Você pode preferir atribuir sn_vul.exception_approver - Exception Approver a usuários e grupos. Usuários e grupos com esta função aprovam exceções, adiamentos e fechamentos de tarefas de correção e itens vulneráveis. A partir da v20.0, a função granular, sn_vul.read_all, foi removida desta função para que você possa acessar os itens vulneráveis e as tarefas de correção atribuídos a você e seu grupo em vez de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes da v10.3	Iniciando com v10.3
	todos os itens vulneráveis e tarefas de correção.
Se você atribuiu sn_vul.vulnerability_read para fornecer visibilidade sobre a gestão de vulnerabilidades.	Você pode preferir atribuir acesso de leitura a áreas específicas na aplicação por tarefa. Por exemplo, atribua sn_vul.read_all para que um usuário possa exibir todos os registros de VR. Para obter acesso de leitura para exibir regras de tarefa de correção, atribua sn_vul.read_group_rules. Usuários e grupos com esta função não atualizam registros.

Para exibir as funções granulares que um usuário ou grupos com uma função de persona herda por padrão, navegue até **Todos** > **Administração de usuários** > **Funções**. Localize a função desejada e clique nela para abrir o registro. A guia Contém funções lista todas as funções granulares da função de persona, bem como todas as funções herdadas.

Você pode preferir verificar se todos os usuários e grupos necessários foram criados antes de atribuir funções no Assistente de configuração. Como alternativa, para adicionar novos usuários e grupos de dentro do Assistente de configuração, clique no link do **módulo Administração de usuários** no formulário mostrado na figura a seguir.

Para o exemplo a seguir, para limitar o acesso à aplicação Vulnerability Response, este exemplo mostra como atribuir um usuário com a persona de administrador de vulnerabilidade. Normalmente, você pode preferir atribuir funções de persona diferentes de sn_vul.vulnerability_admin aos grupos.

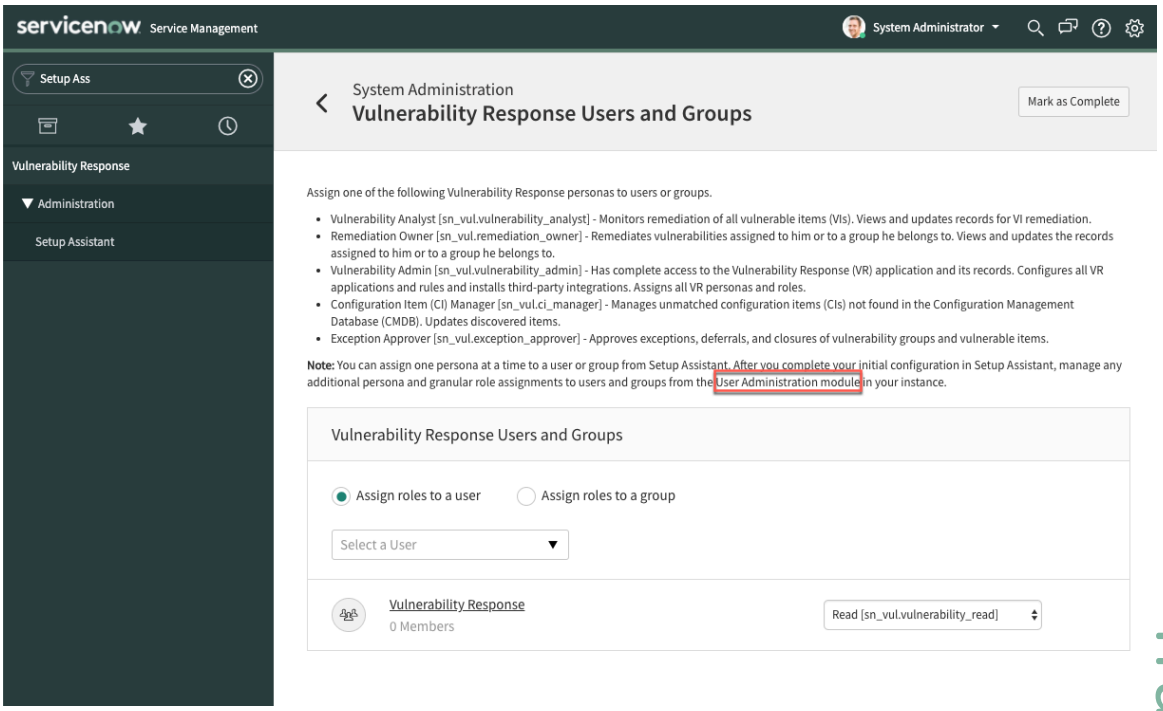
Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração Assistente de configuração**.
   A página do Assistente de configuração é exibida.
2. Clique em Usuários e grupos do Vulnerability Response.
   A página Usuários e grupos do Vulnerability Response da Administração do sistema será exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Com Atribuir funções a um usuário selecionado, escolha um usuário existente na lista.

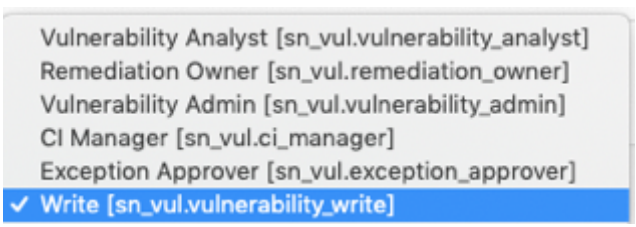
Você só pode atribuir um usuário ou grupo com uma função de persona.

À direita do formulário, depois de selecionar um usuário ou grupo, a persona padrão, Proprietário de correção [sn_vul.remediation_owner] é atribuída por padrão e permanece exibida na lista até que você a altere.

Nota:
Se você estiver atualizando para uma versão mais recente do Vulnerability Response e tiver atribuído anteriormente a função sn_vul.vulnerability_read ou sn_vul.vulnerability_write a um usuário ou grupo antes da atualização, ela será exibida junto com as novas funções de persona, conforme mostrado na figura a seguir .

Se você for um cliente de atualização, poderá continuar usando suas funções existentes para a aplicação Vulnerability Response. O acesso para usuários e grupos atribuídos com as permissões sn_vul.vulnerability_read e sn_vul.vulnerability_write e o proprietário de correção antes da v10.3 não foi alterado.

Observe que, para usuários existentes ou grupos atualmente atribuídos com as funções sn_vul.vulnerability_read ou sn_vul.vulnerability_write, essas funções são exibidas junto com as funções de persona na lista. Depois de atribuir uma função de persona, a função antiga não estará mais disponível no futuro. Por exemplo, conforme mostrado na figura a seguir, a função Gravar [sn_vul.vulnerability_write] não é mais exibida como uma opção para este usuário ou grupo depois que uma das funções de persona é atribuída a ele.

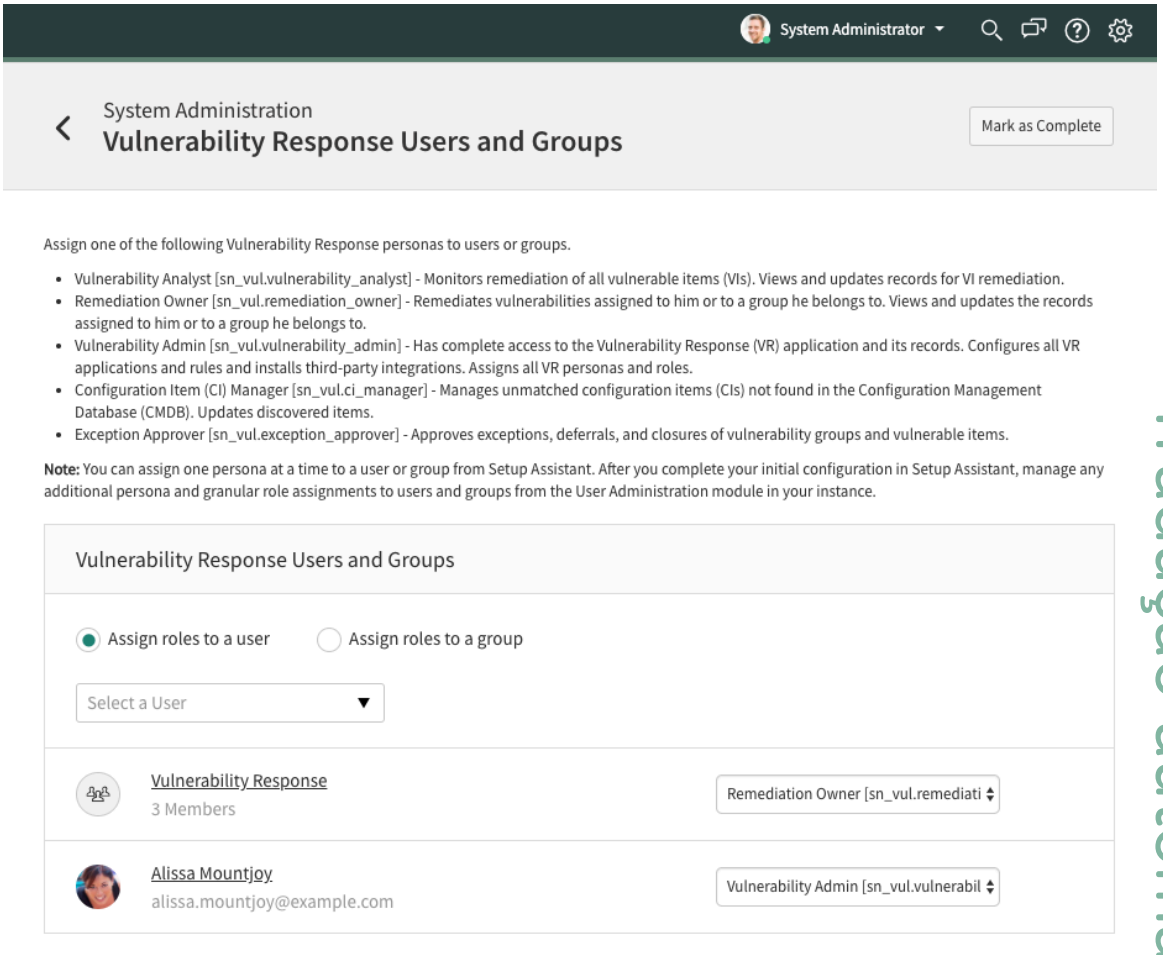


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Na lista à direita do formulário, selecione **Administrador de vulnerabilidade [sn_vul.vulnerability_admin]**.
   Uma mensagem é exibida indicando que o usuário ou grupo foi atribuído com sucesso à persona.

Persona do proprietário de correção atribuída a um grupo e persona do administrador de vulnerabilidade atribuída a um usuário



5. Usando as descrições das funções de persona listadas acima, continue a atribuir usuários e grupos às funções de persona restantes: Proprietário de correção, Analista de vulnerabilidade, Gerente de IC e Aprovador de exceção.
   Você concluiu com sucesso a atribuição de funções de persona a usuários e grupos usando o Assistente de configuração.
6. **Opcional:** Para editar os usuários em um grupo no Assistente de configuração, siga estas etapas.

   a. Com o grupo exibido no formulário, clique no nome do grupo que você deseja editar.
      O registro do grupo é exibido.

   b. Com a guia Membros do grupo selecionada, clique em **Editar**.
      O formulário Editar membros é exibido

   c. Use a interface de caixa de listagem dupla para selecionar ou remover usuários.

   d. Clique em **Salvar** para salvar suas mudanças e retornar ao registro do Grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e. Clique em **Atualizar** para retornar ao Assistente de configuração.

f. Na página do Assistente de configuração, clique em **Usuários e grupos do Vulnerability Response** para continuar com a configuração no Assistente de configuração.

O que Fazer Depois

Como administrador do sistema, continue com a configuração de Vulnerability Response no Assistente de configuração. Observe que, após a conclusão da primeira seção, você pode fazer com que um usuário atribuído com a função de persona de administrador de vulnerabilidades conclua as tarefas no Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares e exemplos, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Gerenciar persona e funções granulares para Vulnerability Response

Depois de concluir sua atribuição inicial de funções de persona usando o Assistente de configuração, gerencie atribuições de função granulares adicionais a usuários ou grupos do módulo Administração de usuário em sua instância.

Antes de Iniciar

Se você ainda não concluiu a instalação e a configuração iniciais de Vulnerability Response usando o Assistente de configuração ou atribuiu funções de persona a usuários e grupos, navegue até **Vulnerability Response** > **Administração** > **Assistente de configuração**. Consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração.

Para obter os principais termos e uma visão geral das funções de persona, consulte Vulnerability Response personas e funções granulares.

Uma função de persona é uma função pré-configurada na aplicação que é composta por várias funções granulares. As funções de persona em Assistente de configuração, Administrador de vulnerabilidades, Analista de vulnerabilidades, Proprietário de correção, Gerenciador de itens de configuração e Gerenciador de exceções foram projetadas para corresponder a cargos comuns para gerentes, analistas e responsáveis pelo serviço em uma organização de TI ou grupo de correção de vulnerabilidades.

Se você quiser que seus usuários e grupos tenham mais acesso do que uma das funções permite, você pode adicionar funções mais granulares a usuários e grupos. Por outro lado, se você quiser limitar o acesso de usuários e grupos específicos no nível da tarefa, poderá remover funções granulares. Além disso, você pode criar funções personalizadas para atender às suas necessidades.

Função necessária: administrador

Procedimento

1. Para gerenciar funções granulares para usuários e grupos, escolha uma para continuar.

   Os nomes das funções granulares em Vulnerability Response geralmente descrevem o que os usuários podem fazer e ver. Para exibir descrições de funções granulares específicas, navegue até **Todos** > **Administração de usuários** > **Funções** e localize a função desejada. A descrição da função, as funções que são herdadas automaticamente quando uma função é atribuída e todas as funções que dependem de outras funções também são listadas.

2. Para atribuir ou remover uma função granular de um usuário ou grupo, siga estas etapas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como exemplo, suponha que você queira atribuir a um gerente de TI uma função que permita a esse gerente exibir registros, mas não atualizá-los ou editá-los. Para exibir registros em Vulnerability Response, Performance Analytics para Vulnerability Responsee para todas as integrações de terceiros, atribua a este usuário a função granular sn_vul.read_all.

a. Navegar até **Todos** > **Administração de usuários** > **Usuários**.

b. Localize o usuário e, na coluna Nome, clique no registro para abri-lo.
O registro do usuário é exibido.

c. Se não for selecionado, selecione a guia Funções.
As funções atualmente atribuídas ao usuário são exibidas.

d. Clique em **Editar**.
O formulário Editar membros é exibido.

e. No campo Coleção da caixa de listagem dupla, insira o nome da função, se você souber, ou insira `* sn_vul` para exibir somente as funções granulares disponíveis para o Vulnerability Response.

f. Localize e mova sn_vul.read_all para a lista de funções.

> **Nota:**
> Use o mesmo processo para remover funções granulares específicas de usuários na interface de caixa de listagem dupla movendo a função da lista Funções para a lista Coleção.

g. Clique em **Salvar**.
O registro do usuário é exibido com a nova função granular.

h. Clique em **Atualizar** para salvar suas mudanças e retornar à lista Usuários.
Você forneceu a um usuário permissão para ler, mas não atualizar registros em Vulnerability Response, Performance Analytics para Vulnerability Responsee para integrações de terceiros.

3. Para editar um grupo para que somente membros específicos tenham acesso expandido com funções mais granulares, siga estas etapas.
Por exemplo, suponha que você queira permitir que determinados usuários no grupo Proprietário de correção (sn_vul.remediation_owner) criem itens vulneráveis manualmente, mas não queira expandir essa permissão para todos os usuários do grupo. A permissão para criar itens vulneráveis manualmente é concedida pela função granular sn_vul.create_vulnerable_items. Para conceder essa permissão somente para selecionar usuários deste grupo, siga estas etapas.

a. Navegar até **Todos** > **Administração de usuários** > **Grupos**.

b. Localize o grupo de responsáveis pela correção e, na coluna Nome, clique no grupo para abrir o registro.
O registro do grupo é exibido.

c. Se não for selecionado, selecione a guia Membros do grupo.
Os membros atuais do grupo são exibidos.

d. Clique em um nome da lista ao qual você deseja atribuir a função granular e abra o registro.

e. No registro, role até a guia Funções e selecione-a.
As funções atribuídas ao usuário são exibidas.

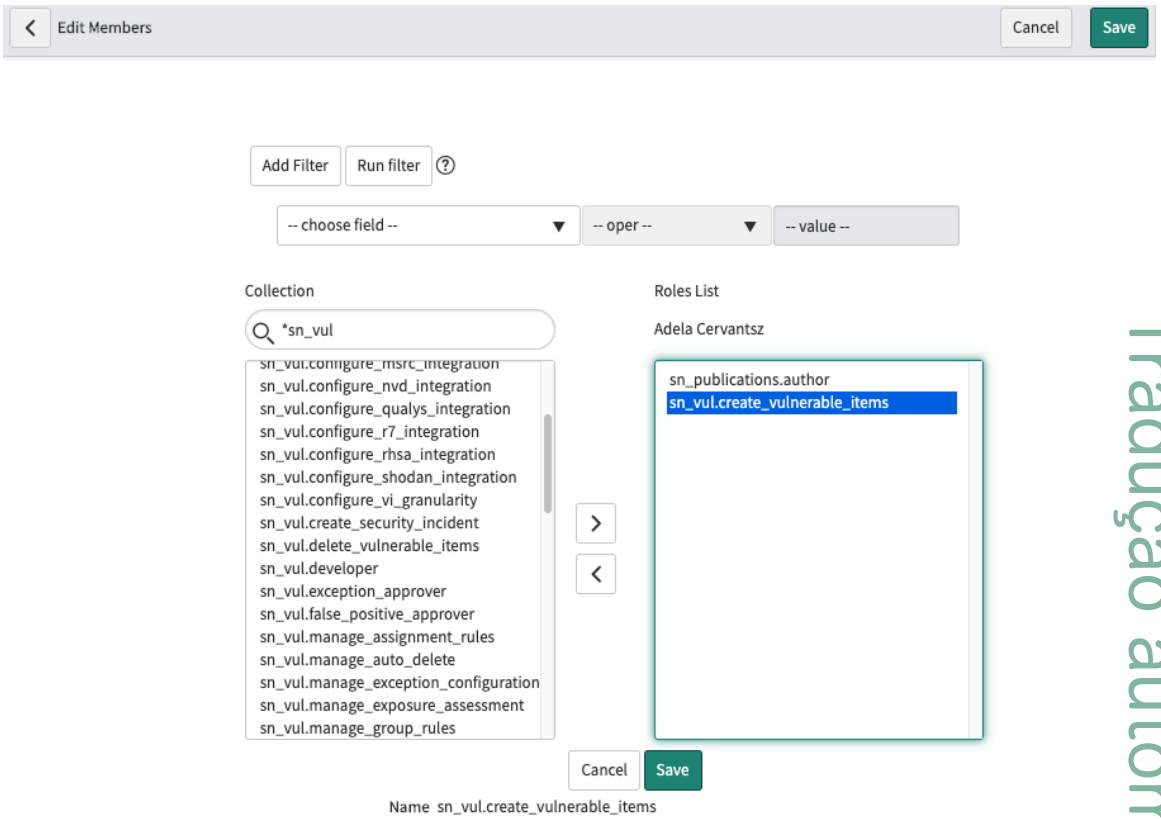
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

f. Clique em **Editar**.
O formulário Editar membros é exibido.

g. No campo Coleção, insira o nome da função, se você souber, ou insira `*sn_vul` para exibir todas as funções granulares disponíveis para o Vulnerability Response.

h. Localize e mova sn_vul.create_vulnerable_items para a lista de funções.



i. Clique em **Salvar**.
O registro do usuário é exibido com a nova função granular.

j. Clique na seta de voltar para exibir os usuários no registro do grupo de responsáveis pela correção

k. Clique nos nomes da lista aos quais você deseja atribuir esta função granular, abra seus registros e use a interface de caixa de listagem dupla para atribuir a função.

l. Depois de concluir as edições, clique em **Atualizar** para salvar as mudanças e retornar à lista de grupos.
Você forneceu a alguns usuários do grupo Proprietário de correção (sn_vul.remediation_owner) permissão para criar itens vulneráveis manualmente.

4. Para criar uma nova função usando somente funções granulares selecionadas, siga estas etapas.
Para este exemplo, suponha que você queira criar a função para um auditor de conformidade. Esta função funciona em estreita colaboração com Governance, Risk, and Compliance (GRC), e o trabalho requer as seguintes permissões e tarefas em Vulnerability Response:

- Gerencia prazos de correção para itens vulneráveis e grupos de vulnerabilidades
- Aprova solicitações de exceção para estender prazos ou adiar a correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Gerencia a limpeza de itens vulneráveis mais antigos com exclusão automática
- Definir pontuações de risco
- Lê todos os registros em Vulnerability Response, mas não tem permissão para editá-los.

a. Navegar até **Todos** > **Administração de usuários** > **Funções**.

b. Na lista Funções, clique em **Novo**.

c. No registro Função, preencha os campos.

Crie um nome, selecione a aplicação que contém este registro e insira uma descrição resumida da sua nova função. Para obter mais informações sobre os outros campos do formulário, consulte Criar uma função .

Nota:
Ao criar um nome para sua nova função, você pode preferir usar um nome que seja facilmente reconhecido na lista de funções e que descreva a funcionalidade da função. Para este exemplo, talvez você prefira um título como Auditor de conformidade - GRC-VR.

d. Clique em **Enviar**.
A lista Funções é exibida.

e. Localize sua nova função e clique nela para abrir o registro.

f. Clique em **Editar**.
O formulário Editar membros é exibido.

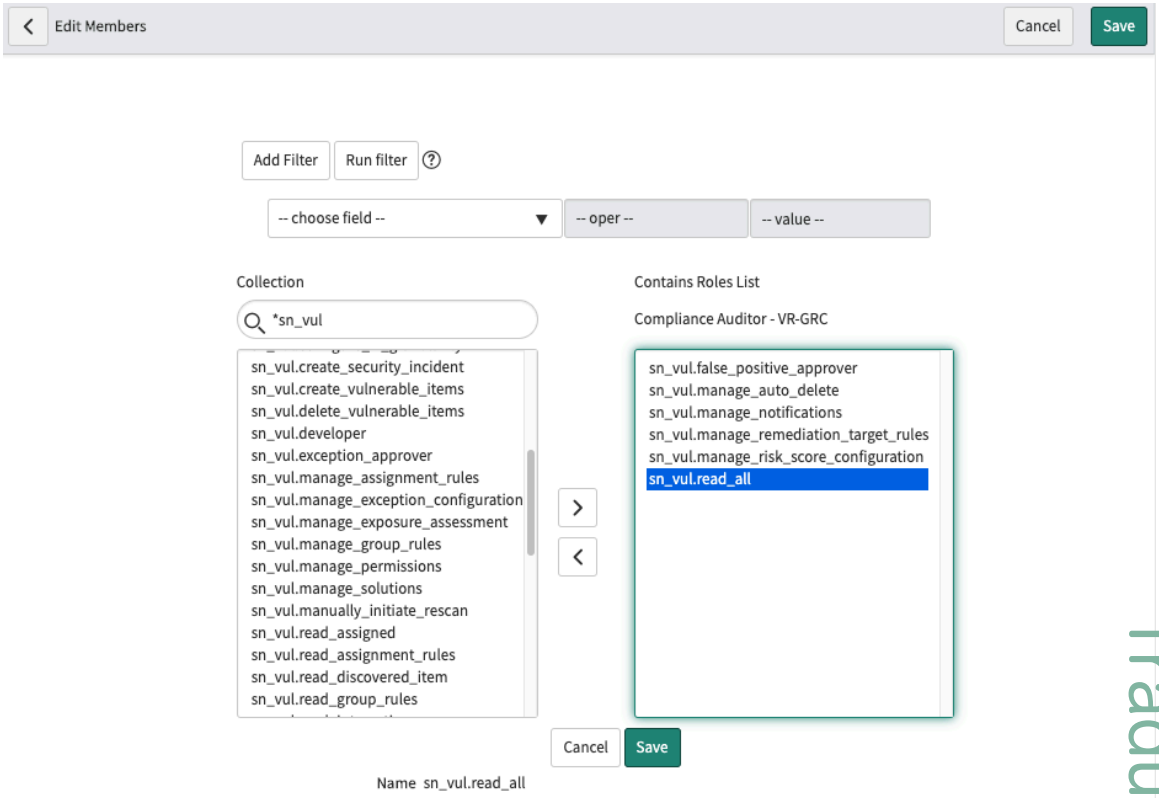
g. Use a interface de caixa de listagem dupla para adicionar funções granulares à sua nova função.

Para este exemplo, as funções necessárias para esta nova função são exibidas na coluna à direita na figura a seguir.

Para exibir somente as funções granulares do Vulnerability Response, no campo Coleção, insira `*sn_vul`.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



h. Clique em **Salvar**.
O registro da sua nova função é exibido. Começando com a guia Contém funções, continue editando a função conforme necessário.

i. Clique em **Atualizar** para salvar suas mudanças.
Sua nova função será exibida na lista Funções.

Instalar Vulnerability Response aplicações de terceiros usando o Assistente de configuração

Instale as aplicações de integração de terceiros para as quais você tem direito em Vulnerability Response usando o Assistente de configuração.

Antes de Iniciar

O Assistente de configuração oferece suporte à instalação da maioria das aplicações de integração de terceiros com Vulnerability Response, mas você continua com a configuração de algumas aplicações instaladas a partir de módulos de configuração em sua instância. Consulte Integrações do Vulnerability Response para obter uma lista de aplicações compatíveis com Vulnerability Response.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

- Depois de instalado, o recurso [Solução de gerenciamento de vulnerabilidade de Vulnerability Response fornece acesso a Integração com a solução Microsoft Security Response Center e Red Hat Solution Integration no Assistente de configuração.
- Solução de gerenciamento de vulnerabilidade está disponível por assinatura separada. Consulte Solução de gerenciamento de vulnerabilidade para obter mais informações sobre como Vulnerability Response incorpora soluções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de instalar e ativar aplicações de terceiros no Assistente de configuração, execute as seguintes tarefas para garantir uma instalação sem problemas:

Tarefas de configuração	Descrição
Verifique se você tem direitos ServiceNow válidos para as aplicações de integração que deseja instalar.	Navegar até **Gestão de assinaturas** > **Assinaturas** em sua instância para verificar os direitos. A lista exibe as assinaturas que sua organização comprou. Para obter mais informações sobre como obter direitos para uma aplicação Security Operations do ServiceNow Store, consulte Obter direito para um produto ou aplicação Security Operations.
(Opcional) Se ainda não estiver instalado e ativado, talvez você prefira instalar a aplicação Vulnerability Response antes de instalar a aplicação de terceiros.	Para obter mais informações sobre como instalar e ativar a aplicação Vulnerability Response, consulte Instalar e configurar Vulnerability Response.
Se ainda não estiver instalado e ativado, você deverá ativar e importar dados de vulnerabilidade com o trabalho programado de integração do NVD e CWE antes de executar uma aplicação de scanner de terceiros para importar dados.	Execute as integrações de NVD e CWE como parte de sua configuração inicial de Vulnerability Response e antes de importar dados de vulnerabilidade para sua instância com um produto de scanner de terceiros. Para obter mais informações, consulte Noções básicas sobre as integrações do NVD.
Verifique se você concluiu todas as tarefas de configuração necessárias para as integrações de terceiros para Vulnerability Response.	Revise todas as tarefas de configuração necessárias para cada integração que você deseja instalar em Integrações do Vulnerability Response.

Função necessária: administrador

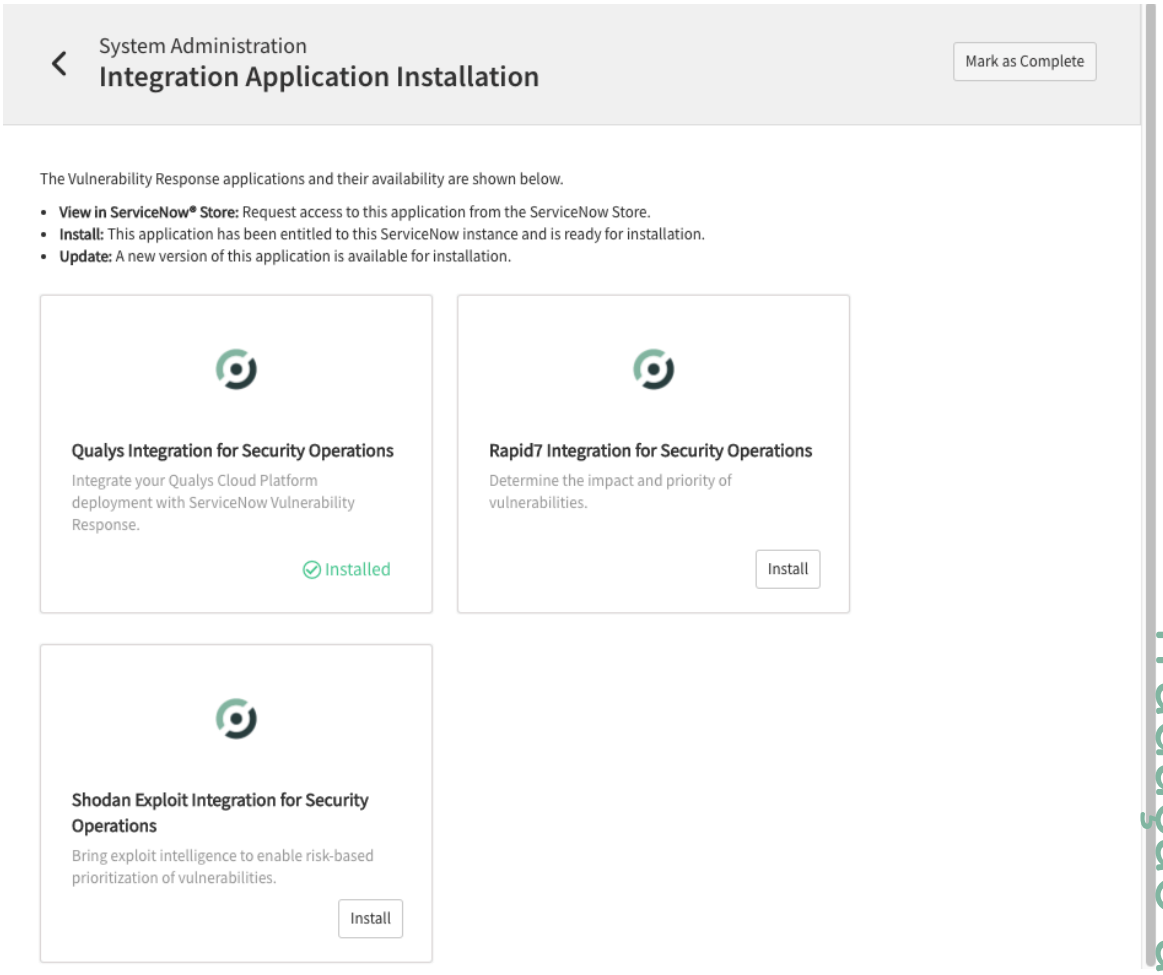
Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Administração do Sistema** > **Instalação de aplicação de integração**.

   Após alguns momentos, as aplicações para as quais você tem direito e que estão disponíveis para instalação em sua instância serão exibidas.

Tradução automática

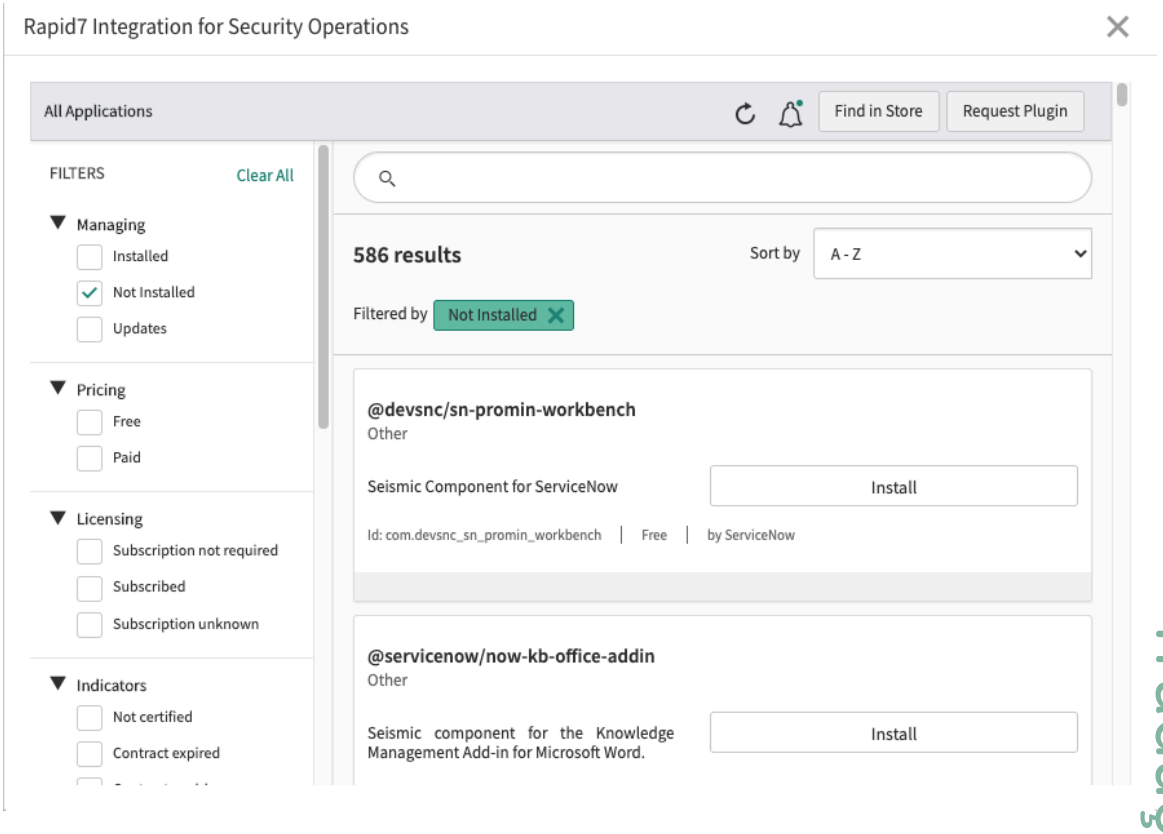
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Localize a aplicação que deseja instalar e clique em **Instalar** no bloco da aplicação.
A caixa de diálogo Todas as aplicações é exibida com o nome do bloco da aplicação em que você clicou, por exemplo, Rapid7 Integration for Security Operations, conforme mostrado na figura a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

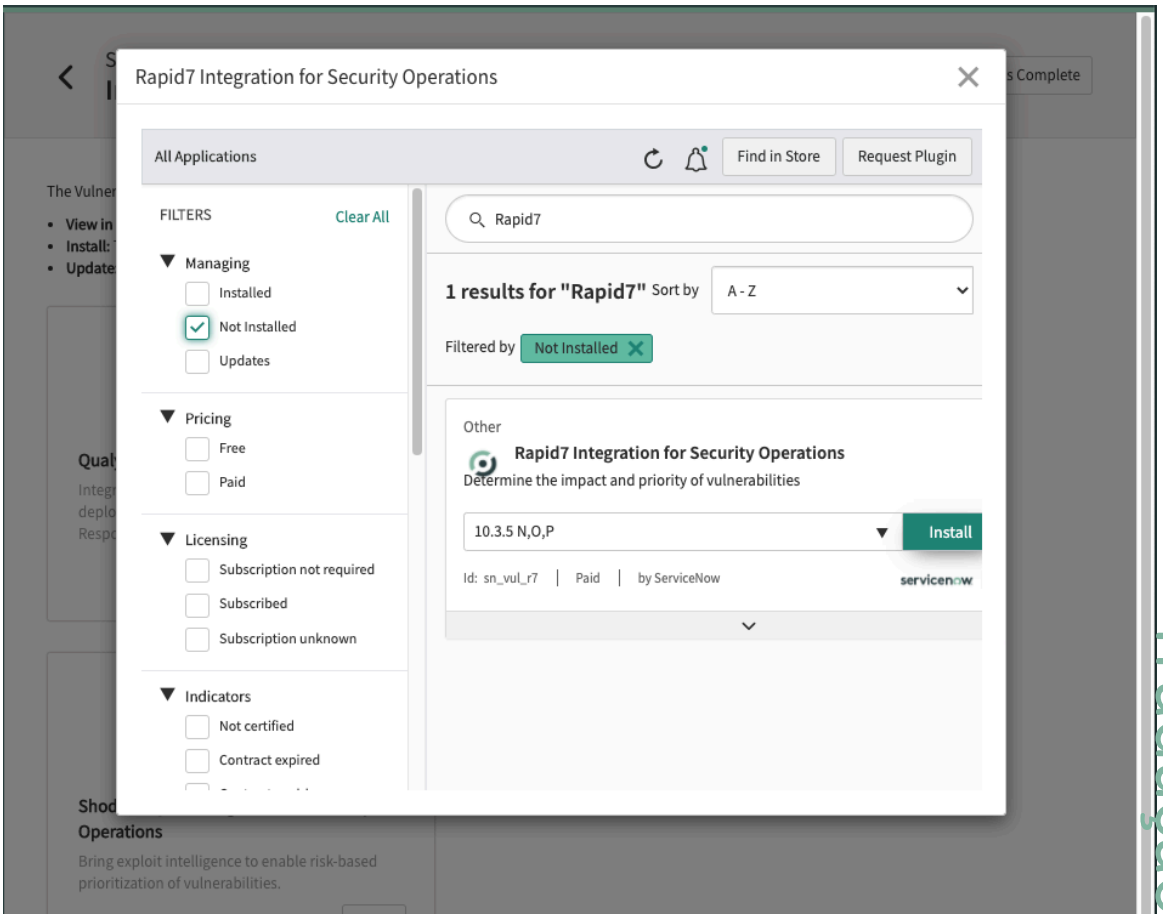


3. Localize a aplicação, selecione uma versão na lista de seleção e clique em **Instalar**.

Se uma atualização estiver disponível para a aplicação, o botão **Atualizar** será exibido.

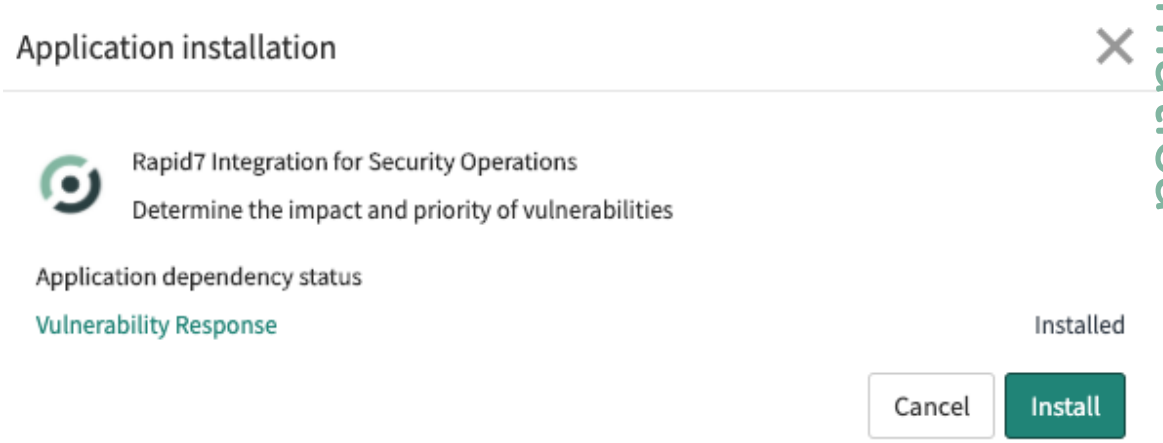
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A caixa de diálogo de instalação da aplicação exibe o status de dependência da aplicação. Todas as dependências necessárias ainda não instaladas são instaladas automaticamente junto com a aplicação.

4. Na caixa de diálogo de instalação da aplicação, clique em **Instalar**.



A caixa de diálogo Instalar indica quando a instalação foi concluída com sucesso.

5. Feche a caixa de diálogo.
A página Todas as aplicações é exibida e mostra que a aplicação foi instalada com sucesso.

Após a instalação e a ativação, você pode configurar, programar e iniciar as seguintes aplicações e soluções instaladas diretamente da seção Configuração de integração do Assistente de configuração:

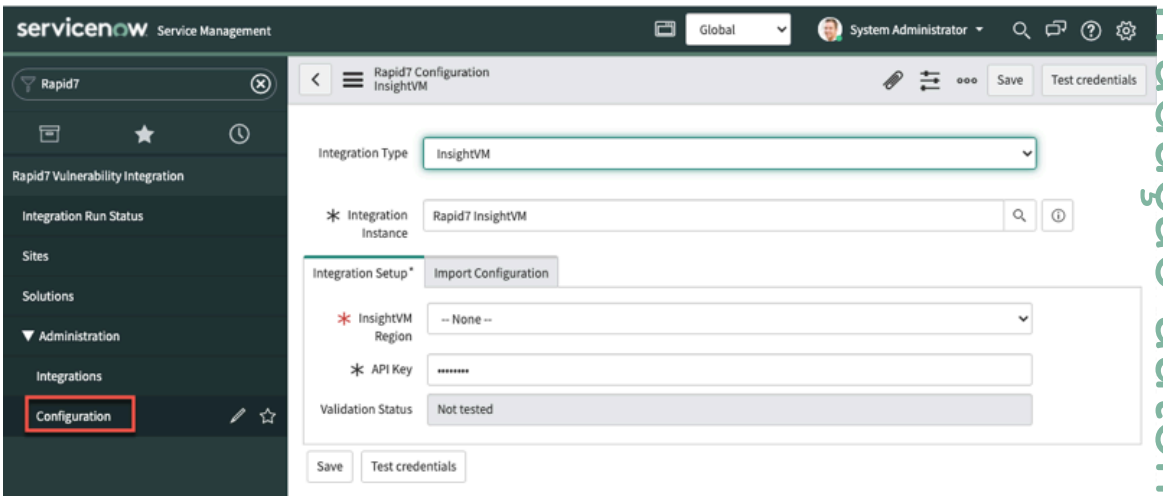
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O Qualys Vulnerability Integration
- O Integração do Vulnerability Response com Tenable.
- O Integração com a solução Microsoft Security Response Center
- O Red Hat Solution Integration
- Integração com a solução Microsoft Security Response Center
- A integração Microsoft Defender Threat and Vulnerability Management

Para outras aplicações não listadas acima, navegue diretamente para o módulo de configuração da aplicação para continuar com a configuração e para inserir as credenciais de terceiros necessárias. Por exemplo, a imagem a seguir mostra o local do módulo Configuração e para a aplicação Rapid7.

Para obter mais informações sobre como configurar aplicações específicas, consulte a documentação do produto de instalação e configuração pelo nome do produto fornecido para cada aplicação.



O que Fazer Depois

Continue com a configuração da aplicação no Assistente de configuração se a sua aplicação for compatível.

Se a sua aplicação não for compatível com a configuração no Assistente de configuração, navegue diretamente para o módulo de configuração da aplicação para continuar com a configuração. Para exibir as aplicações compatíveis no Assistente de configuração, consulte Instalação de Vulnerability Response e aplicações compatíveis.

Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros

Se ainda não estiver instalado, baixe e execute a integração do NVD e execute o trabalho programado do CWE como parte da configuração inicial do Vulnerability Response e antes de importar dados de vulnerabilidade para sua instância com um scanner de terceiros. O Vulnerability Response Integration with NVD está disponível na ServiceNow Store.

Ingestão de dados do CWE e do NVD

Os dados importados das integrações do NVD e do CWE são usados para aprimorar os dados de vulnerabilidade em sua instância e ajudar você a decidir se deve escalar a correção de uma vulnerabilidade, item vulnerável ou tarefa de correção. Após uma importação inicial, você pode atualizar os registros da biblioteca sob demanda ou configurar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

um trabalho programado para atualizar os registros regularmente. Vulnerability Response os armazena em **Bibliotecas**.

O Common Vulnerability Scoring System (CVSS), incluído no NVD e nas entradas de terceiros, captura as principais características de uma vulnerabilidade. Vulnerability Response usa dados CVSS para produzir um valor normalizado que reflete a severidade da vulnerabilidade. Quando a severidade é calculada, a vulnerabilidade fornece uma melhor compreensão do risco representado por esta vulnerabilidade para sua organização. A severidade ajuda a avaliar e priorizar a correção de vulnerabilidades.

Se esta for sua primeira instalação de Vulnerability Responseou antes de ingerir dados pela primeira vez com um scanner de terceiros:

1. Execute uma importação inicial de dados do CWE com a Integração abrangente do CWE 2000.

   Para obter mais informações, consulte Configurar e executar o trabalho programado para atualizar registros CWE. Você executa atualizações do CWE **sob demanda** a partir do registro de integração por padrão e deve configurá-lo se quiser que ele seja executado como um trabalho programado.

   Nota:
   Programe a atualização do CWE para ser executada antes da atualização do banco de dados do NVD. O dia padrão para a atualização do NVD é **Semanalmente** na segunda- **feira**.

2. Verifique se a aplicação Vulnerability Response Integration with NVD está instalada e se os dados da integração do banco de dados de vulnerabilidades do NIST - API (somente CVE) ou da integração do banco de dados de vulnerabilidades do NIST - API (CVE e CPE) foram importados com sucesso.

   A ativação desse plug-in em instâncias de produção pode exigir uma licença separada. Depois de instalada, a integração do NIST National Vulnerability Database Integration - API (somente CVE) é ativada por padrão. Ele é executado diariamente. Consulte Noções básicas sobre as integrações do NVD e Instalar a integração Vulnerability Response com o banco de dados nacional de vulnerabilidades do NIST para obter mais informações.

3. Bibliotecas de terceiros são atualizadas como trabalhos programados. Consulte a documentação de integração em Integrações do Vulnerability Response para obter mais informações sobre integrações de terceiros.

Exibição de dados de vulnerabilidade importados e itens vulneráveis

As seguintes bibliotecas estão disponíveis:

Bibliotecas	Descrição
NVD	Lista de vulnerabilidades encontradas pelo NVD e inclui check-lists de segurança, falhas de software relacionadas à segurança, configurações incorretas, nomes de produtos e métricas de impacto, incluindo explorações.
CWE	Lista de tipos de pontos fracos de software desenvolvidos pela comunidade. Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco. Você não pode escalar uma vulnerabilidade na tela Enumerações de Pontos Fracos Comuns, é apenas para referência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Bibliotecas	Descrição
Terceiros	Lista de vulnerabilidades de terceiros importadas em sua instância. Contém uma lista de referências relacionadas, itens vulneráveis, explorações e CVEs.

Tópicos relacionados

Exibir Vulnerability Response bibliotecas de vulnerabilidade

Instalar a aplicação Solução de gerenciamento do Vulnerability Response

Antes de usar o recurso [Solução de gerenciamento do Vulnerability Response de Vulnerability Response em sua instância, você deve concluir a instalação da aplicação Solução de gerenciamento de vulnerabilidade. Esta aplicação está disponível como uma assinatura separada no ServiceNow Store.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Execute estas tarefas de configuração para uma instalação sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

O Integração com a solução Microsoft Security Response Center e Red Hat Solution Integration são os aplicativos de solução disponíveis em Solução de gerenciamento do Vulnerability Response depois de instalar Solução de gerenciamento de vulnerabilidade.

Tarefas de configuração	Descrição
Verifique se a aplicação Vulnerability Response está instalada e ativada.	Solução de gerenciamento do Vulnerability Response requer a aplicação Vulnerability Response. Para a versão mais atual de Solução de gerenciamento de vulnerabilidade, verifique se você tem a versão mais atual de Vulnerability Response instalada. Consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e mudanças de esquema de versão . Se a aplicação não estiver instalada e ativada, consulte Como instalar Vulnerability Response.
Verifique se você tem direito à aplicação.	Para verificar se você tem direito à aplicação Solução de gerenciamento de vulnerabilidade, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Para obter o direito da aplicação Solução de gerenciamento de vulnerabilidade do ServiceNow Store e baixá-lo para sua instância Now Platform,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	consulte Obter direito para um produto ou aplicação Security Operations.
Certifique-se de que seus registros de NVD estejam atualizados para os últimos 10 anos.	Consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.
Certifique-se de que suas vulnerabilidades de terceiros estejam atualizadas.	Consulte Integrações do Vulnerability Response para obter informações sobre integrações de vulnerabilidade de terceiros.
Verifique se você tem as funções Now Platform necessárias atribuídas à sua instância.	As funções a seguir são necessárias para a instalação e a verificação dos resultados esperados: Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response. • O administrador do sistema [admin] instala a aplicação. Se ainda não estiver atribuído, o administrador atribuirá a função de administrador de vulnerabilidade [sn_vul.vulnerability_admin ou sn_vul.admin (preterido)]. • O administrador de vulnerabilidades supervisiona a configuração e verifica os resultados esperados.

Funções necessárias: administrador para instalar a aplicação Solução de gerenciamento de vulnerabilidade e administrador de vulnerabilidade para configurá-la.

Procedimento

1. Navegue até o ServiceNow Store.
2. Clique **em Fazer login** e insira suas credenciais HI.
3. Clique na guia **Produtos da ServiceNow** para exibir os produtos ServiceNow disponíveis.
4. Clique no sinal de mais (**+**) ao lado de **Vulnerability Solution Management** para exibir todas as aplicações associadas para as quais você está qualificado.
5. Clique **em Aceitar** para verificar se você tem direito a Solução de gerenciamento de vulnerabilidade na aplicação.
6. Se você já tem direito, pule para a etapa 10 para instalar a aplicação na sua instância Now Platform.
7. Marque a caixa de seleção e clique em **Aceitar** para concordar com os termos e condições no prompt. Uma mensagem é exibida indicando que você aceitou a aplicação com sucesso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. **Opcional:** Clique em Gerenciar direito se quiser gerenciar seu direito para Solução de gerenciamento de vulnerabilidade em outras instâncias Now Platform.

   Nota:
   Se o botão **Gerenciar direito** não for exibido, clique na aplicação **Vulnerability Solution Management** na Lista de produtos para exibi-lo.

   a. Escolha uma opção

   b. Clique em **OK** ou em **Cancelar** para continuar.
   Você está pronto para ativar plug-ins e instalar a aplicação em suas instâncias.

9. Faça login na instância Now Platform na qual você deseja instalar a aplicação Solução de gerenciamento de vulnerabilidade.
10. Navegar até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
11. Localize a aplicação Solução de gerenciamento de vulnerabilidade (sn_vul_solution) e clique em **Instalar**.
    A caixa de diálogo de instalação da aplicação exibe o status do plug-in de dependência da aplicação. Todas as dependências necessárias ainda não instaladas são instaladas automaticamente junto com a aplicação.
12. Clique em **Instalar**.
    Esta instalação pode levar algum tempo. Uma mensagem é exibida na caixa de diálogo Instalar depois que a aplicação e suas dependências são instaladas com sucesso.

    O administrador de vulnerabilidades agora pode configurar a aplicação de dentro do Assistente de configuração.

13. Clique em **Fechar**.

    O Integração com a solução Microsoft Security Response Center e Red Hat Solution Integration são os aplicativos de solução disponíveis em Solução de gerenciamento do Vulnerability Response depois de instalar Solução de gerenciamento de vulnerabilidade.

    Exiba as Soluções de vulnerabilidade navegando até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções**. Para obter mais informações, consulte Configurar integrações de soluções instaladas para Solução de gerenciamento de vulnerabilidade usando o Assistente de configuração.

O que Fazer Depois

Depois de configurar a aplicação e as soluções disponíveis, verifique se os CVEs e as Soluções estão de acordo usando a tabela Solução de vulnerabilidade [sn_vul_m2m_vulnerability_solution].

Instalar e configurar a aplicação Performance Analytics para Vulnerability Response [PA]

Antes de usar a aplicação Performance Analytics para Vulnerability Response, você deve obter o direito e baixar a aplicação de ServiceNow Store, instalá-lo em sua instância Now Platform® e concluir algumas etapas de instalação e configuração. A aplicação PA não é instalada como parte da aplicação Vulnerability Response. Ele está disponível com uma assinatura separada.

Antes de Iniciar

Se você já tiver a aplicação em sua instância e estiver atualizando para uma versão mais recente da aplicação, prossiga para a etapa 8 nas etapas a seguir para continuar com a atualização e a configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para uma nova instalação, conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Para verificar se os plug-ins e aplicações estão instalados e ativados, navegue até **Todos** > **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Tarefas de configuração	Descrição
Verifique se o plug-in de dependências do Vulnerability Response (com.snc.vul_dep) está instalado e ativado.	**Dependências do Vulnerability Response** Este plug-in contém todos os plug-ins de dependência necessários para oferecer suporte à aplicação. Para verificar se o plug-in está instalado e ativado, na sua instância, você deseja que a aplicação navegue até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**. Se você for solicitado a atualizar outros plug-ins de dependência, clique nos links nas caixas de diálogo e siga as instruções para continuar.
Verifique se a aplicação ServiceNow Vulnerability Response (sn_vul) está instalada e ativada.	**Vulnerability Response** Para verificar se o plug-in está instalado e ativado, na sua instância, você deseja que a aplicação navegue até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**. Se você for solicitado a atualizar outros plug-ins de dependência, clique nos links nas caixas de diálogo e siga as instruções para continuar. A ativação desse plug-in em instâncias de produção pode exigir uma licença separada. Entre em contato com a ServiceNow para obter mais detalhes.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados:

Tradução automática

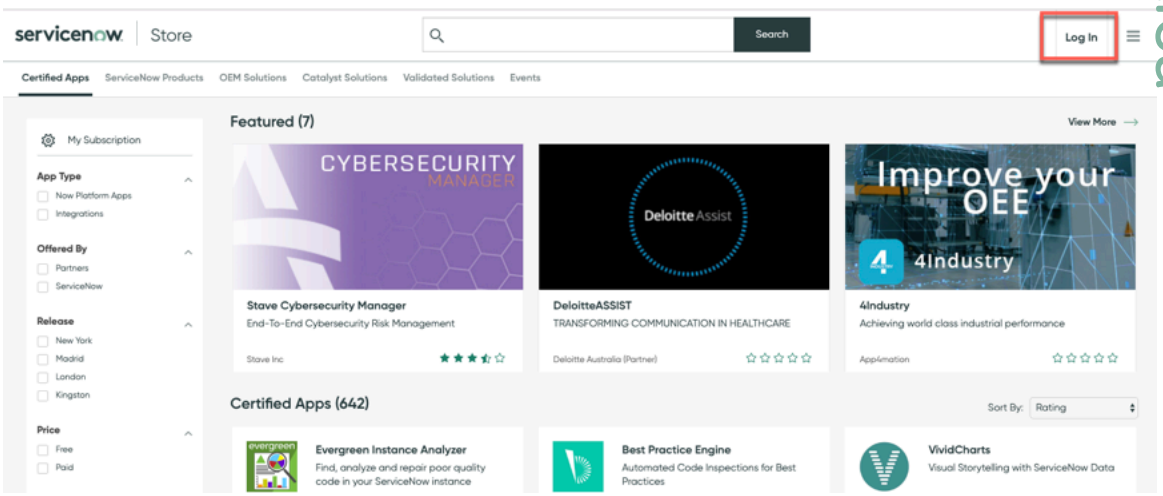
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.	• O administrador do Performance Analytics [pa_admin] ou o sistema [admin] instala a aplicação e verifica os resultados esperados. • O Administrador de vulnerabilidade [sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado)] supervisiona a configuração e verifica os resultados esperados com os painéis de PA. • O proprietário de correção [sn_vul.remediation_owner] supervisiona as tarefas de gerenciamento de mudanças e lê e atualiza os registros atribuídos. A função sn_vul.remediation_owner também é atribuída automaticamente quando qualquer usuário é atribuído à função itil.
Verifique se as aplicações Performance Analytics e Vulnerability Response são compatíveis.	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Função necessária: admin ou pa_admin

Procedimento

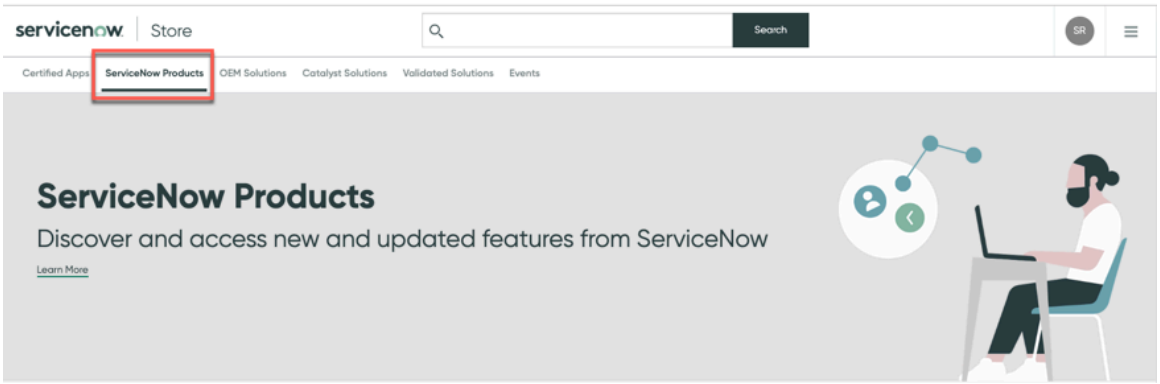
1. Para obter o direito e baixar a aplicação na sua instância Now Platform, navegue até ServiceNow Store.
2. No canto superior direito da página, clique **em Fazer login**.



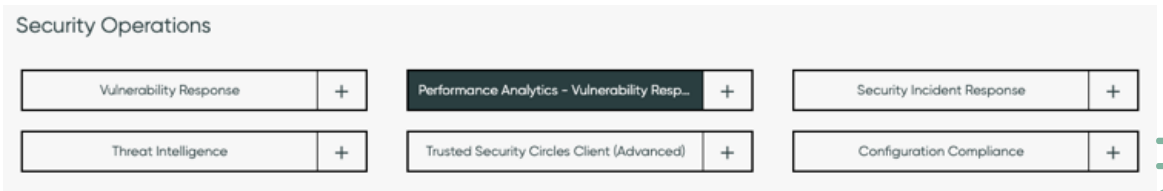
3. Na caixa de diálogo exibida, insira suas credenciais HI e clique em **Login**.
4. Na página exibida, se não estiver selecionada, clique na guia **Produtos da ServiceNow**.

Tradução automática

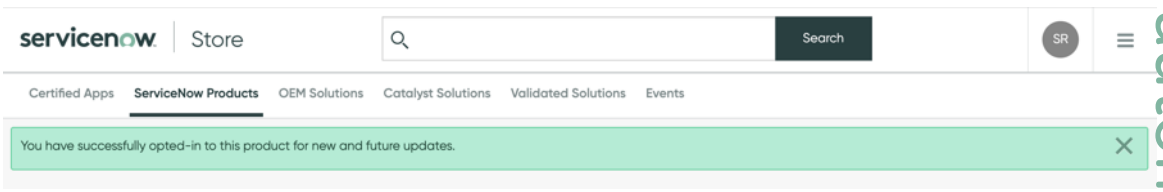
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Na página da lista de produtos, clique em **Performance Analytics - Vulnerability Response**.



6. Insira o **Nome da instância** e **o Motivo da instância**e clique em **Validar instância**.
   Uma página com o botão Aceitar será exibida.
7. Para obter a aplicação Performance Analytics para Vulnerability Response, clique em **Aceitar**.
8. Para concordar com os termos e condições, no prompt, marque a caixa de seleção e clique em **Aceitar**.



9. **Opcional:** Como alternativa, para gerenciar seu direito da aplicação em outras instâncias Now Platform, siga estas etapas.

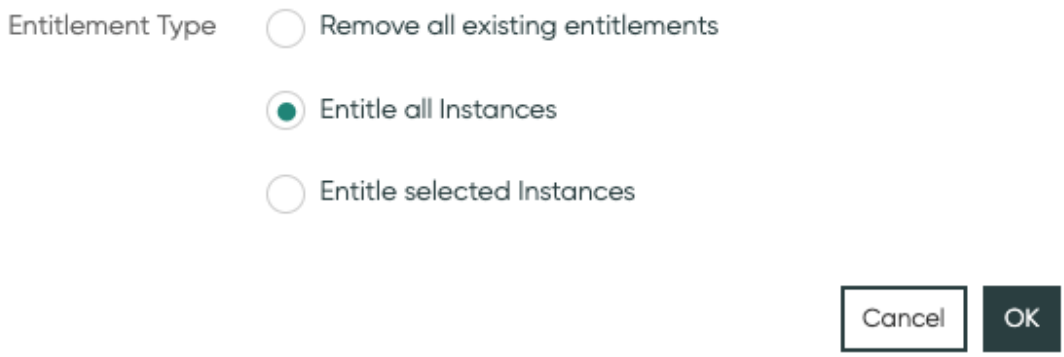
   a. Se o botão Gerenciar direito não for exibido, clique na aplicação Performance Analytics para Vulnerability Response na lista de produtos para exibi-lo.

   b. Com a guia Qualificado selecionada, clique em **Gerenciar direito**.

   c. Na caixa de diálogo Gerenciar direitos para Vulnerability Response exibida, escolha uma:

Tradução automática

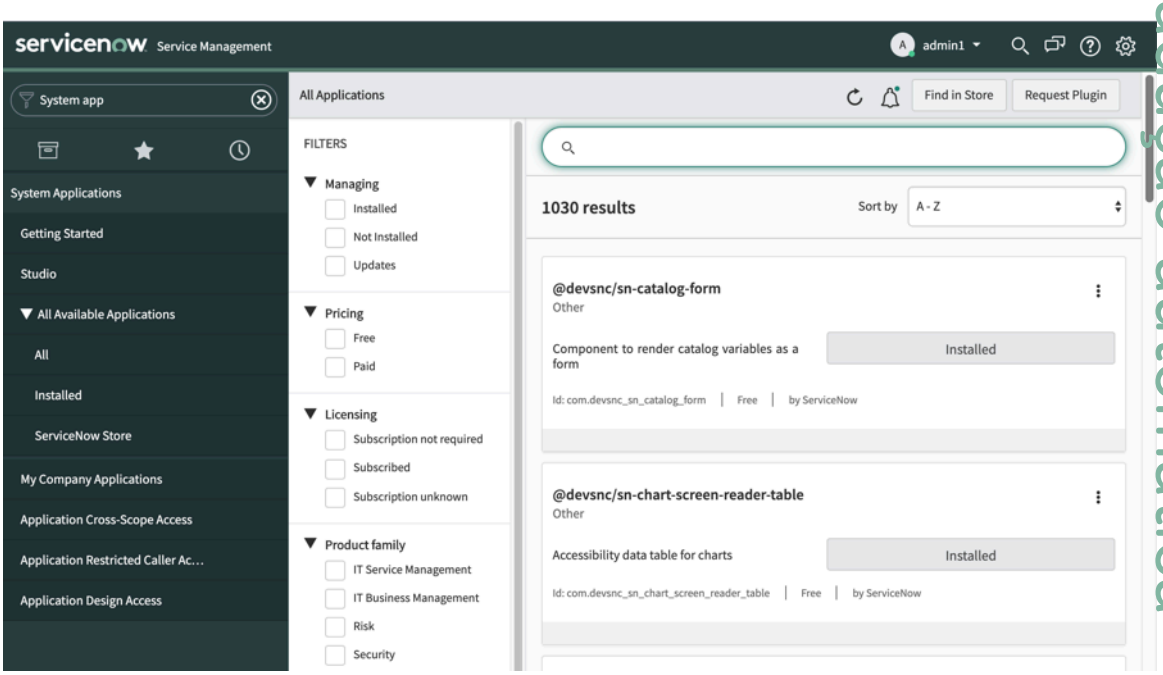
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. Clique em **OK** ou em **Cancelar** para continuar.
Você está pronto para ativar plug-ins e instalar a aplicação em suas Now Platform instância(s).

10. Faça login na instância Now Platform na qual você deseja instalar a aplicação Vulnerability Response.

11. Navegar até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.



12. Nas aplicações listadas, localize a aplicação Performance Analytics - Content Pack - Vulnerability Response (sn_vul_analytics) e clique em **Instalar**.

Nota:
Se você estiver atualizando para uma nova versão, selecione a versão desejada na lista de seleção.

e clique em **Atualizar**.
A caixa de diálogo de instalação da aplicação é exibida. Todas as dependências que serão instaladas automaticamente com a aplicação também serão exibidas.

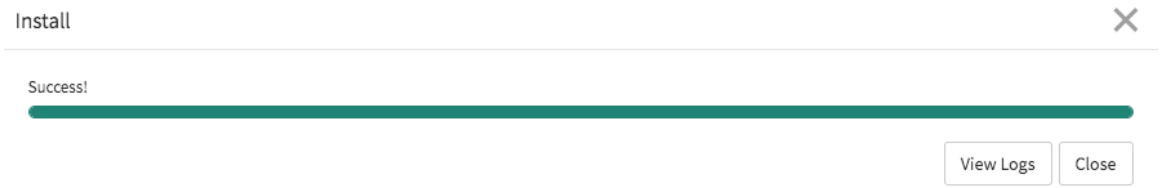
13. **Opcional:** Se você quiser dados de demonstração, marque a caixa de seleção Carregar dados de demonstração e clique em **Instalar**.

Tradução automática

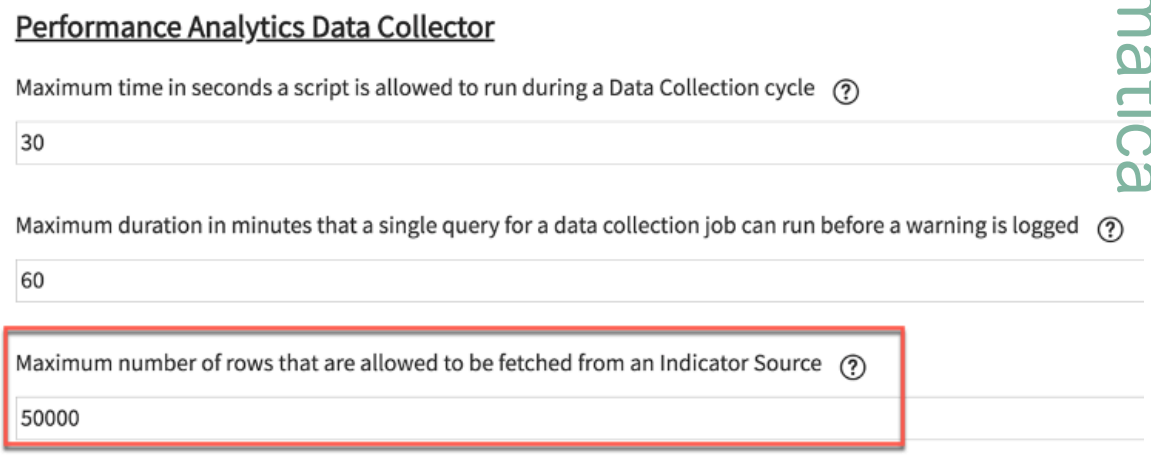
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Se você não marcar a caixa de seleção **Carregar dados** de demonstração, os dados de demonstração não ficarão disponíveis para instalação no **Gerenciador de aplicações** posteriormente. Para obter informações sobre como instalar ou reinstalar os dados de demonstração após a instalação inicial, consulte o artigo Solução alternativa para instalar dados de demonstração se a aplicação já estiver instalada [KB0722909] na Base de conhecimento Now Support.

Esta instalação pode levar algum tempo. Uma mensagem é exibida na caixa de diálogo Instalar depois que a aplicação é instalada com sucesso.



14. Clique em **Fechar**.
15. **Opcional:** Se você antecipar um grande número de itens vulneráveis ativos em seu ambiente, talvez prefira mudar a configuração padrão do número máximo de registros coletados, habilitar trabalhos programados e definir horários de coleta fora do horário de expediente.
Para alterar essas e outras configurações da aplicação depois de instalada, siga estas etapas.
    a. Navegar até **Todos** > **Performance Analytics** > **Console do administrador**.
    b. No bloco Configuração avançada, clique no link **Propriedades do Performance Analytics**.
    c. Na página do Console de administração [Performance Analytics], role até a seção Performance Analytics Coletor de dados.
    A configuração padrão (50.000 registros) é exibida para o Número máximo de linhas que podem ser buscadas de uma origem de indicador.



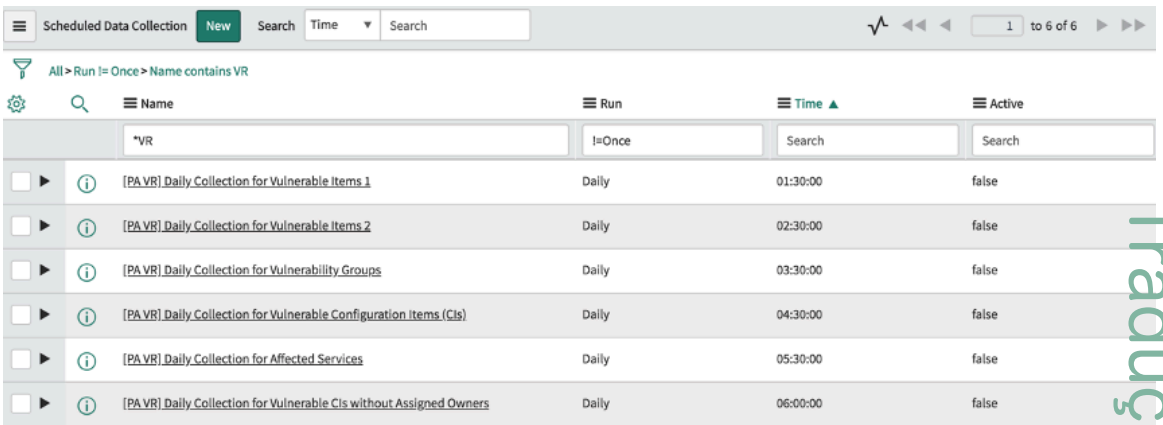
    d. Você pode preferir aumentar esse número para um valor que é aproximadamente 20% a mais do que o número total de itens vulneráveis (IVs) ativos que você antecipa em seu ambiente.
    e. Clique em **Salvar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

f. Para ativar trabalhos programados, navegue até **Performance Analytics** > **Coletor de Dados** > **Trabalhos**.
A lista Coleta de dados programada é exibida. Na coluna Ativo, os trabalhos programados listados na coluna Aplicação para Performance Analytics - Pacote de conteúdo - Vulnerability Response por padrão são desabilitados (falso).

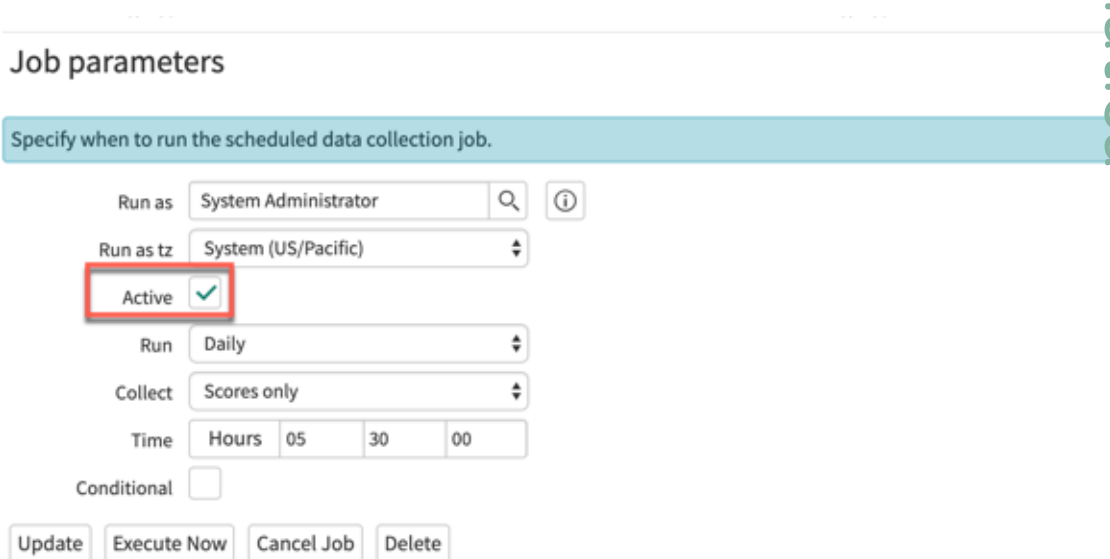
Nota:
um trabalho programado para coleta de dados históricos não é exibido na lista de trabalhos. Para grandes conjuntos de dados, talvez você prefira começar a coletar dados e tendências ao longo do tempo, habilitando seus trabalhos diários ao configurar a aplicação Performance Analytics para Vulnerability Response.



g. Na coluna Nome, clique em um link para abrir um registro de trabalho do PA_VR.

h. Se os campos não forem editáveis, clique no link **aqui** para editá-los.

i. Na seção Parâmetros do trabalho, clique na caixa de seleção Ativo para programar um trabalho.
Os campos Hora são exibidos.



j. Insira a hora de início do trabalho.
Se você antecipar um grande volume, talvez prefira definir horários de coleta fora do horário de expediente. Se você antecipar 10 milhões de IVs ativos ou mais em seu ambiente, entre em contato com

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

seu parceiro de implementação ServiceNow® para obter mais informações sobre como configurar seu ambiente de coleta de dados.

Para obter mais informações sobre os indicadores usados para coleta de dados, consulte Exibir os Performance Analytics indicadores para Vulnerability Response [PA].

k. Depois de habilitar todos os trabalhos desejados, clique em **Atualizar**.
A lista Coleta de dados programada é exibida. Para obter mais informações, consulte Propriedades do Performance Analytics .

O que Fazer Depois

Navegar até **Vulnerability Response** > **Visão geral** para exibir o painel.

Criar ou editar Vulnerability Response regras de atribuição

Depois de concluir sua avaliação inicial das regras de atribuição usando o Assistente de configuração, você pode criar regras para atribuir automaticamente itens vulneráveis com base nas condições do filtro. Essas regras atribuem itens vulneráveis conforme eles são importados ou criados manualmente.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)
Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa

O sistema básico é fornecido com uma regra de atribuição de vulnerabilidade, **Atribuir ao grupo de suporte de IC**, que atribui itens vulneráveis ao mesmo grupo de atribuição que o grupo de suporte de IC. Esta regra pode ser modificada usando condições de filtro ou você pode criar uma nova regra. Com as regras de atribuição, você define as condições de atribuição e a ordem de execução. Quando um IV corresponde a uma condição de regra, a pesquisa de atribuição é interrompida.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de atribuição**.
2. Abra a regra **Atribuir ao grupo de suporte de IC** ou clique em **Novo**.
3. Se **Novo**, preencha os campos no formulário, conforme apropriado.

Regras de Atribuição da Vulnerabilidade

Campo	Descrição
Nome	Nome da regra de grupo.
Ativo	Indica se a regra de atribuição está ativa.
Ordem de execução	Ordem na qual as regras são avaliadas. Regras de alta prioridade, itens que precisam de tratamento especial, onde o risco é crítico, ou um IV deve ser tratado pela conformidade regulatória, para ser executado primeiro. Em seguida, execute suas regras gerais, onde nenhum tratamento especial seja rnecessário, e você saberá quem deve ser

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	responsável por elas. Por fim, crie uma regra padrão para atribuir IVs ao grupo que descobrirá a qual grupo de atribuição ele deve pertencer. Este grupo pode adicionar outra regra para cobrir suas decisões. Esta regra padrão seria executada por último.
Descrição	Descrição da regra de atribuição.
Condição	
Visualização	Mostra quantos resultados esta consulta retornará.
Campos de condição	Condições que devem ser atendidas. **Nota:** Para disponibilizar Rapid7 InsightVM etiquetas do ativo para uso no filtro de condição para regras de atribuição, você deve executar a integração Rapid7 InsightVM Lista de ativos antes das outras integrações Rapid7 InsightVM. A diferenciação de maiúsculas e minúsculas para o texto de pesquisa inserido no construtor de condição não é compatível com este registro ou formulário.
Novos critérios	Adiciona mais campos de filtro de condição para você escolher.
Atribuir usando	Para automatizar a atribuição de grupos criados com base nesta regra, escolha uma das opções disponíveis. ◦ Grupo de usuários: selecione um grupo de usuários na tabela de pesquisa. ◦ Campo de grupo de usuários: selecione um campo de grupo de usuários no menu suspenso. ◦ Script: crie ou edite um script. **Nota:** Criar ou editar um script requer experiência em ServiceNow.

4. Clique em **Enviar**.
Regras novas ou atualizadas são avaliadas na próxima importação.

Nota:

O recurso de reaplicação requer uma aplicação de linha de base das regras. Depois que as regras forem criadas, se você ainda não tiver feito isso, ative o trabalho programado `Reapply all vulnerability assignment rules` para executar, quando quiser. Aplica todas as regras a todos os IVs abertos, exceto aqueles atribuídos manualmente. Dependendo de quantos IVs ativos você tem em seu ambiente, lembre-se de definir o campo **Executar** corretamente após a execução inicial para evitar impactos no desempenho.

Se você não executou este trabalho programado, ao tentar usar o botão **Aplicar mudanças** no formulário Regras de atribuição, será necessário fazê-lo. A reaplicação das regras de atribuição não reagrupa os itens vulneráveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar uma regra de atribuição Vulnerability Response usando ML

Use o script a seguir para criar uma regra de atribuição de contato alternativo para itens vulneráveis que usa recomendações de ML da Inteligência preditiva para atribuí-los automaticamente para correção.

Antes de Iniciar

A aplicação Recomendações de atribuição de vulnerabilidade para Vulnerability Response deve ser instalada e ativada. Esta aplicação está disponível no ServiceNow Store.

Uma solução de classificação deve ser definida, ativa e treinada. Você usa este modelo para ajudar a prever o grupo de atribuição apropriado para itens vulneráveis (IV)s nos casos em que suas regras de atribuição não encontrarem uma correspondência correta para os destinatários pretendidos.

Esta regra pode ajudar a reduzir o número de IVs não atribuídos depois que outras regras de atribuição já foram concluídas.

Para obter mais informações, consulte Instalar Recomendações de atribuição de vulnerabilidade para Vulnerability Response e Criar e treinar uma definição de solução para Vulnerability Response.

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Talvez você prefira executar esta tarefa somente se tiver experiência avançada em codificação ou conhecimento profundo sobre o Now Platform, seus recursos de Inteligência preditiva e como as regras de atribuição funcionam.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de atribuição**.
2. Selecione **Novo**.
3. Preencha os campos no formulário, conforme apropriado.
   Consulte Criar ou editar Vulnerability Response regras de atribuição para obter mais informações sobre esses campos.
4. Na lista de seleção Atribuir usando, selecione **Script**.
5. No editor, copie e cole o script a seguir.

```
  /*
  * Catch-all assignment rule using ML recommendation
  * NOTE: Requires Vulnerability Assignment Recommendations for Vulnerability Response
  * Classification Solution must be active and trained
  */
var vitID = current.sys_id;
getMLAssignmentRecommendation(vitID);

function getMLAssignmentRecommendation(vulnerableItemSysId) {
  var ARU = new sn_vul.AssignmentRecommendationUtils();
  ARU.initialize();

  var viPredictionObj = ARU.getPredictionsForVI(vulnerableItemSysId);
  /*
  *returns object containing array of predictions
  *payload structure:
  *
  {
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
    "predictions": [
      {
        "sys_id": "b6ed54f3db7b23005daef4eabf9619f3",
        "name": "Windows Server support ",
        "confidence_score": "57.54"
      },
      ...
    ],
    "exception": ""
  }
  */
  var viPredictionArray = viPredictionObj['predictions'];
  var topPredictionObj = viPredictionArray.shift();

  return topPredictionObj['sys_id'];
}
```

6. Selecione **Enviar**.

O que Fazer Depois

Revise Vulnerability Response visão geral de regras de atribuição para obter informações mais gerais sobre regras de atribuição e o trabalho programado *`Reapply all vulnerability assignment rules`*.

Criar uma regra de atribuição Vulnerability Response para suporte de serviço

Use o script a seguir para criar uma regra que atribua itens vulneráveis para correção com base nos serviços de negócios que eles afetam.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Talvez você prefira executar esta tarefa somente se tiver experiência avançada em codificação ou conhecimento profundo sobre o Now Platform e como as regras de atribuição funcionam.

Com esta regra, os IVs são atribuídos de acordo com a correspondência com os serviços de negócios listados no seu CMDB. Se nenhum serviço, departamento ou grupo de suporte relacionado for correspondido, os IVs serão atribuídos ao grupo de analistas de vulnerabilidade.

Esta regra pode ajudar a reduzir o número de IVs que são atribuídos incorretamente ou permanecem não atribuídos após a conclusão de outras regras de atribuição.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de atribuição**.
2. Selecione **Novo**.
3. Preencha os campos no formulário, conforme apropriado.
   Consulte Criar ou editar Vulnerability Response regras de atribuição para obter mais informações sobre esses campos.
4. Na lista de seleção Atribuir usando, selecione **Script**.
5. No editor, copie e cole o script a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
/*
Assigns Vulnerable Item based on related Business Service
Assigns to default Vulnerability Analyst group if no related Business Service
*/
assignToServiceSupport(current);

function assignToServiceSupport(vitGR) {
   var ci = vitGR.getValue('cmdb_ci');
   var defaultAssignmentGroup = 'Vulnerability Analyst';
   var defaultGR = new GlideRecord('sys_user_group');
   defaultGR.get('name', defaultAssignmentGroup);
   var defaultAssignmentGroupID = defaultGR.sys_id;

   var maxSizeValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_size", 1000);
   var maxDepthValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_depth", 10);
   var customValues = {
      "maxDepth": maxDepthValue,
      "maxSize": maxSizeValue
   };
   var ciu = new global.CIUtils();
   var services = ciu.servicesAffectedByCI(ci, customValues);
   var svc = new GlideRecord("cmdb_ci_service");
   var hasSvc = false;
   if (services && services.length > 0) {
      svc.addQuery("sys_id", "IN", services.join(",")); // returns the service with highest
business criticality. Implement alternate logic here.
      svc.addNotNullQuery("busines_criticality"); // typo intended
      svc.orderBy("busines_criticality");
      svc.setLimit(1);
      svc.query();
      hasSvc = svc.next();
   }
   if (!hasSvc) {
      // If there are no services it should be assigned to a default assignent group
      return defaultAssignmentGroupID;
   } else {
      var serviceAssignmentGroup = hasSvc.getValue('support_group'); //Also consider
managed_by_group, assignment_group, change_control
      return !gs.nil(serviceAssignmentGroup) ? serviceAssignmentGroup :
defaultAssignmentGroupID; //Return the Service assignment group if it is not empty, return
the default assignment group otherwise.
   }
}
```

6. Selecione **Enviar**.

O que Fazer Depois

Revise Vulnerability Response visão geral de regras de atribuição para obter informações mais gerais sobre regras de atribuição e o trabalho programado *`Reapply all vulnerability assignment rules`*.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar ou editar Vulnerability Response regras de tarefa de correção

Depois de concluir sua avaliação inicial das regras de tarefa de correção usando o Assistente de configuração, você pode criar regras para agrupar automaticamente itens vulneráveis com base nas condições do filtro. Essas regras agrupam automaticamente itens vulneráveis conforme eles são importados ou criados manualmente. Use o filtro para limitar os itens vulneráveis agrupados por esta regra, como a seleção de todos os itens vulneráveis com explorações.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Por Que e Quando Desempenhar Esta Tarefa
O sistema básico é fornecido com uma regra de tarefa de correção, **Vulnerabilidade**, que agrupa itens vulneráveis por vulnerabilidade e grupo de atribuição (de **Regras**de atribuição). Você pode reaplicar as regras do formulário ou da exibição de lista. Para algumas entradas de amostra, Vulnerability Response exemplos de regra de tarefa de correção.

Esta regra pode ser modificada da seguinte forma:

Usando condições de filtro e Agrupar por opções.

Por padrão, as tarefas de correção usam **Regras de atribuição**, quando disponíveis, como parte dos critérios de filtro.

Nota:
Se não houver regras de atribuição, você poderá selecionar um grupo usando o campo Grupo de **usuários**.

A partir da versão 18.0 de Vulnerability Response, a regra da tarefa de correção de **vulnerabilidade** é desativada em Vulnerability Response para novas implementações.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de tarefa de correção**.
2. Abra a regra ou clique em **Novo**.
3. Se **Novo**, preencha os campos no formulário, conforme apropriado.

Regra de tarefa de correção

Campo	Descrição
Nome	Nome da regra de tarefa.
Ativo	Indica se a tarefa está ativa.
Descrição	Descrição da regra.
Diferenciação entre maiúsculas e minúsculas	Determina se uma condição faz distinção entre maiúsculas e minúsculas ou não. **Nota:** O valor padrão não faz distinção entre maiúsculas e minúsculas.
Condição	Condições de filtro opcionais para a regra.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Para disponibilizar Rapid7 InsightVM tags de ativo para uso no filtro de condição para Regras de tarefa de correção, você deve executar a integração Rapid7 InsightVM Lista de ativos antes das outras integrações Rapid7 InsightVM. Por padrão, (caixa de seleção**Diferenciar maiúsculas de minúsculas** desabilitada), o texto de pesquisa inserido no construtor de condição em registros e formulários de regras de tarefa não faz distinção entre maiúsculas e minúsculas. Você tem a opção de habilitar pesquisas que diferenciam maiúsculas de minúsculas em registros e formulários de tarefa.
Agrupar por (até seis conjuntos de condições estão disponíveis)	
Agrupar itens vulneráveis de	A tabela que a regra usa para agrupar IVs. Você pode ter até seis filtros. As opções são: ◦ Item vulnerável [sn_vul_vulnerable_item] ◦ Item vulnerável → Item de configuração [cmdb_ci] ◦ Item vulnerável → Vulnerabilidade [sn_vul_ third_party_entry] **Nota:** Se você escolher uma tabela estendida, o **campo Usando** será aplicado somente para itens vulneráveis que usam essa tabela estendida.
Usando o campo	Campo na tabela que a regra usa para agrupar IVs.
Atribuição	
Atribuir tarefas de correção por	Ao atribuir automaticamente tarefas de correção, a opção Atribuição é usada além das opções **Agrupar por** para agrupar os itens vulneráveis. Novas tarefas são criadas, conforme necessário, para garantir que cada item vulnerável seja colocado em uma tarefa com um conjunto de grupo de atribuição correspondente. Para automatizar a atribuição de tarefas criadas com base nesta regra, escolha uma das opções disponíveis. ◦ Agrupar por campo: se você selecionou qualquer campo de grupo de usuários na seção **Usar valores de campo** na seção **Agrupar por**, eles serão exibidos no menu suspenso. ◦ Grupo de usuários: use a lista de pesquisa para selecionar um grupo de usuários estático.

Nota: Se você mudar de ideia sobre qualquer uma das configurações **de Agrupar por**, o link relacionado **Limpar grupo por campos** redefinirá o **Agrupar por** campos no formulário.

Quando uma regra de grupo é excluída, no formulário ou na exibição de lista, você tem a opção de excluir todos os grupos **Abertos** criados por essa regra. Os grupos que não estão no estado **Aberto** são excluídos.

Para obter alguns exemplos de entradas, consulte Vulnerability Response exemplos de regra de tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir campos e pesos para a regra de risco das Calculadoras de risco do Vulnerability Response

Personalize os parâmetros e pesos da regra de risco para que você possa gerar pontuações de risco que usam os dados de vulnerabilidade e ativo exclusivos da sua organização. Ao selecionar os campos incluídos na regra de risco, você pode definir uma estrutura de pontuação de risco eficaz.

Antes de Iniciar

Além disso, você pode usar atributos no configuration_item [cmdb_ci] no Configuration Management Database (CMDB) para ajudá-lo a criar lógica para suas calculadoras de risco do Vulnerability Response. Se, por exemplo, você determinar que os ICs externos em sua organização são mais vulneráveis e podem exigir correção imediata, você pode atribuir atributos como `Internet Facing` para esses ICs. Este atributo e outros estão listados nas notas de versão do Common Service Data Model para a versão da família Orlando. Para obter informações e orientações atuais sobre o CMDB, consulte os seguintes tópicos:

- Modelo conceitual de modelo de dados de serviço comum
- Modelo de esquema do CMDB

Função necessária: sn_vul.manage_risk_score_configuration

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Calculadoras de vulnerabilidade**.
2. Na página Calculadoras de vulnerabilidade, clique em **Calculadora de risco padrão**.
3. Navegar até **Página da calculadora de vulnerabilidade** > **Guia Regras da Calculadora de Vulnerabilidade** > **Regra de Risco Padrão**.
4. **Opcional:** Na seção Critérios da calculadora de risco da página Regra de risco de vulnerabilidade, defina o peso de cada critério de acordo com sua importância no cálculo de pontuação de risco geral.
5. Para desativar a regra, você deve desmarcar a caixa de seleção **Ativo**.
6. Para adicionar campos de regra de risco aos Critérios da calculadora de risco, clique em **Adicionar critérios**.
7. No formulário, preencha os campos.

Formulário de campo de regra de risco

Campo	Descrição
Escolher tabela de referência	Tabela que você usa para definir a ponderação da pontuação de risco. Você pode selecionar uma destas opções: ○ **Item vulnerável**: adicione campos que podem ser percorridos com pontos diretamente do item vulnerável (IV). ○ **Item vulnerável - Item de configuração**: adicione campos de referência com pontos que fazem parte das extensões da tabela base, como a tabela Hardware. Esses campos não fazem parte da tabela base (cmdb_ci).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **Item vulnerável - Vulnerabilidade**: adicione campos de referência com pontos que fazem parte das tabelas que estendem a tabela base, por exemplo, Entrada de terceiros. Esses campos não fazem parte da tabela base de entrada de vulnerabilidade. ○ **Tabela de referência de item vulnerável**: adicione campos que fazem parte das tabelas relacionadas (m2m) ou tabelas que têm uma referência ao item vulnerável. Esses campos não podem ser usados como referência com pontos diretamente do IV. ○ **Tabela de referência do item de configuração**: adicione campos que fazem parte das tabelas relacionadas (m2m) de cmdb_ci ou tabelas que têm uma referência a cmdb_ci. Esses campos não podem ser usados como referência com pontos diretamente do IV. ○ **Tabela de referência de vulnerabilidade**: adicione campos que fazem parte das tabelas relacionadas (m2m) de sn_vul_entry ou tabelas que têm uma referência a sn_vul_entry. Esses campos não podem ser usados como referência com pontos diretamente do IV. ○ **Condições personalizadas**: use esta opção para atribuir pesos à regra avaliando a condição. Por exemplo, o filtro voltado para a Internet determina se um item de configuração (IC) é externo ou interno.
Tabela	Campo que aparece somente quando uma das seguintes opções é selecionada na tabela Escolher referência: ○ **Item vulnerável -> Item de configuração** ○ **Item vulnerável -> Vulnerabilidade** ○ **Tabela de referência do item vulnerável** ○ **Tabela de referência do item de configuração** ○ **Tabela de referência de vulnerabilidade**
Campo	Campo a ser usado para cálculo de pontuação de risco para esta regra.
Agregação	Campo que aparece somente quando uma tabela de referência é selecionada na tabela Escolher referência. Selecione o valor mínimo ou máximo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	a ser considerado para cálculos quando Campo for selecionado nas Tabelas relacionadas (m2m).
Ponderação	Ponderação deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
Definir ponderação do valor	Componente para atribuir pesos a cada valor de campo. Para campos numéricos, os valores de campo podem ser definidos como um intervalo (por exemplo, 1 a 5). Os pesos devem ser um número inteiro entre 0 e 100. **Nota:** Este campo não será exibido se a opção Condições personalizadas for selecionada na tabela Escolher referência.
Tabela de condição	Campo que aparece somente quando Condições personalizadas são selecionadas na tabela Escolher referência. Selecione uma condição na lista.
Nome do campo	Campo que aparece somente quando Condições personalizadas são selecionadas na tabela Escolher referência. Insira um nome para os critérios de risco.
Condição	Campo que aparece somente quando Condições personalizadas são selecionadas na tabela Escolher referência. Visualize os itens nesta tabela que correspondem às condições definidas.

8. Clique em **Enviar**.
9. Na página Regra, ative e reaplique a regra para reavaliar a pontuação de risco nos itens vulneráveis ativos.

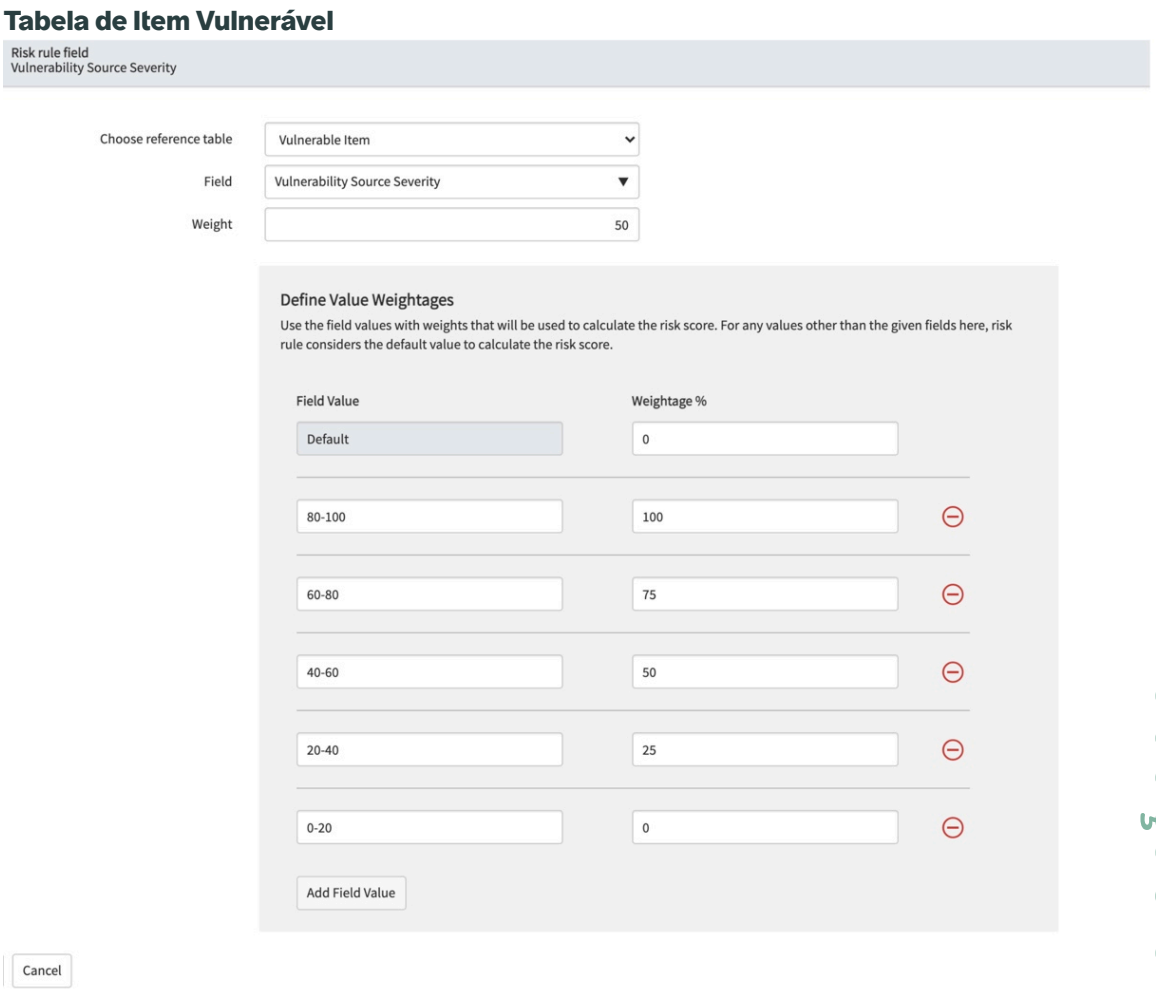
Example:
Exemplo 1: adicione uma severidade de origem como critério para uma regra de risco.

Caso de uso: fornecedores terceirizados, como Qualys e Tenable, fornecem suas próprias pontuações. Essas pontuações são preenchidas no campo **Severidade de origem** na tabela sn_vul_entry. Use este campo para cálculos de pontuação de risco. Para usar essa pontuação para calcular a pontuação de risco, faça o seguinte:

1. Navegue até a página Regra de risco.
2. Para desativar a regra, desmarque a caixa de seleção **Ativo**.
3. Para adicionar campos de regra de risco aos Critérios da calculadora de risco, clique em **Adicionar critérios**.
4. Na lista Escolher tabela de referência, selecione **Item vulnerável**.
5. Na lista Campo, selecione **Vulnerability.Source Severity**.
6. No campo **Peso**, insira a importância relativa deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
7. Na seção Definir ponderação do valor, adicione valores de campo e atribua um peso a eles.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. Clique em **Enviar**.

Exemplo 2: adicione uma criticidade aos negócios como critério para uma regra de risco.

Caso de uso: vamos supor que sua organização tenha muitos serviços de negócios. O item de configuração (IC) LINUX-SF-6381 está sendo usado pelos seguintes serviços:

Criticalidade dos serviços de negócio

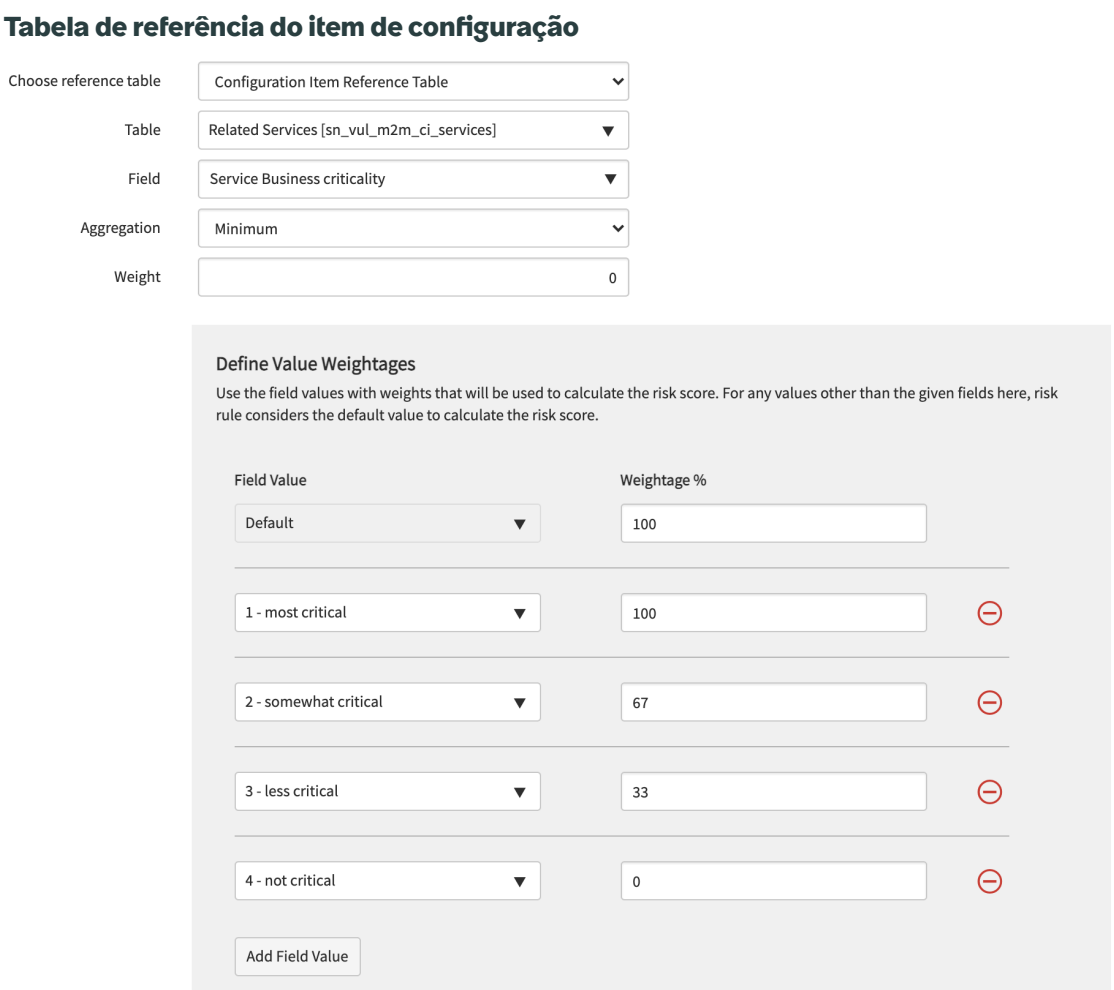
Serviço de negócio	Criticidade
Gestão de nuvem	1 - Mais crítico
Comércio eletrônico	2 - Um pouco crítico
Serviços ao cliente	3 - Menos crítico
Viagem e despesa	4 - Não crítico

O mapeamento entre o IC e os serviços é armazenado na tabela Serviços relacionados [sn_vul_m2m_ci_services]. Quando uma vulnerabilidade é encontrada no ativo LINUX-SF-6381, um item vulnerável (IV) é criado. Você pode usar o valor da criticidade dos negócios dos serviços afetados para calcular a pontuação de risco para este IV. Para usar o valor de criticalidade desses serviços para calcular a pontuação de risco, faça o seguinte:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegue até a página Regra de risco.
2. Para desativar a regra, desmarque a caixa de seleção **Ativo**.
3. Para adicionar campos de regra de risco aos Critérios da calculadora de risco, clique em **Adicionar critérios**.
4. Na lista Escolher tabela de referência, selecione **Tabela de referência do item de configuração**.
5. Na lista Tabela, selecione **Serviços relacionados [sn_vul_m2m_ci_services]**.
6. Na lista Campo, selecione Serviço. **Criticalidade**dos negócios .
7. No campo **Agregação**, selecione **Mínimo** para recuperar o serviço mais crítico para este caso de uso (**1- Valor mais crítico**) ou Máximo para recuperar o serviço menos crítico para este caso de uso (**4 – Valor não crítico**) para este caso de uso.
8. No campo **Peso**, insira a importância relativa deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
9. Na seção Definir Ponderações de Valor, adicione valores de campo e atribua um peso a eles.



10. Clique em **Enviar**.

Exemplo 3: adicione um critério condicional à calculadora de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

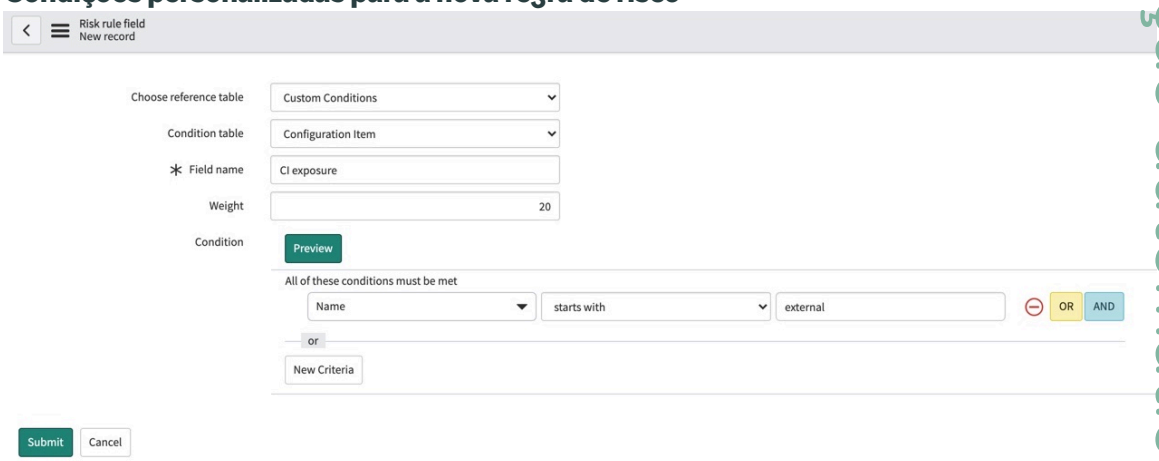
Vamos supor que uma organização tenha vários itens de configuração (ICs), dos quais apenas alguns podem ser acessados por um usuário externo. Os usuários podem adicionar ponderações de pontuação de risco para esses ICs externos.

Nota:
Você pode identificar esses ICs pelo nome. Os nomes começam com "externo".

Para adicionar um critério condicional à regra de risco, faça o seguinte:

1. Navegue até a página Regra de risco.
2. Para desativar a regra, desmarque a caixa de seleção **Ativo**.
3. Para adicionar campos de regra de risco aos Critérios da calculadora de risco, clique em **Adicionar critérios**.
4. Na lista Escolher tabela de referência, selecione **Condições personalizadas**.
5. Na lista Tabela de condições, selecione **Item de configuração**.
6. No **campo Nome** do campo, insira o nome **Exposição de IC**.
7. No campo **Peso**, insira a importância relativa deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
8. No campo **Condição**, selecione **Nome** > **começa com**e insira o valor **externo**.

Condições personalizadas para a nova regra de risco



9. Clique em **Enviar**.

Nota:
Adicionar critérios condicionais à regra de risco pode prejudicar o desempenho.

Tópicos relacionados

Calculadoras do Vulnerability Response e regras da calculadora de vulnerabilidade

Criar uma calculadora do Vulnerability Response

Filtrar no Vulnerability Response

Vulnerability Response Calculadoras de Rollup

Após a avaliação inicial das calculadoras de risco no Assistente de configuração, use as calculadoras de acúmulo de vulnerabilidades para configurar como a pontuação de risco cumulativa é calculada para tarefas de correção e vulnerabilidades importadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use as calculadoras de acúmulo de vulnerabilidades para configurar como a pontuação de risco cumulativa é calculada para tarefas de correção e vulnerabilidades importadas. As seguintes calculadoras de rollup são enviadas com o sistema de base:

- *`Remediation Task Rollup`*: acumula as pontuações de risco de todos os itens vulneráveis em uma tarefa de correção para fornecer uma pontuação de risco geral para o grupo inteiro de itens vulneráveis.
- *`Patch Update Rollup`*: acumula as pontuações de risco para todos os itens vulneráveis com a mesma atualização de patch, para fornecer uma pontuação de risco geral para a atualização de patch.
- *`Organization Risk Score Rollup`*: acumula as pontuações de risco de todos os itens vulneráveis de host, itens vulneráveis de aplicação, itens vulneráveis de contêiner e problemas de configuração em uma organização, para fornecer uma pontuação de risco geral para toda a organização no painel unificado.
- *`Vulnerable Item Rollup`*: acumula as pontuações de risco de todos os itens vulneráveis de host em uma organização, para contribuir com a pontuação de risco geral de toda a organização para o painel unificado.
- *`Vulnerability Entry Rollup`*: acumula as pontuações de risco para todos os itens vulneráveis com a mesma entrada de vulnerabilidade, para fornecer uma pontuação de risco geral para a entrada de vulnerabilidade.
- *`Rollup EPSS Scores from NVD to TPEs`*: acumula as pontuações de EPSS de todos os itens vulneráveis/CVEs listados na tabela NVD para os TPEs existentes, para fornecer uma probabilidade geral da vulnerabilidade que está sendo explorada.
- *`Remediation Effort Rollup`*: acumula as pontuações de risco de todos os registros em um esforço de correção para fornecer uma pontuação de risco geral para o esforço de correção.

Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Calculadora de Rollup de Vulnerabilidade**.

Configure a calculadora de acúmulo para especificar quanto peso dar a cada um desses valores calculados na definição da pontuação de risco cumulativo. Quanto maior o peso, mais esse valor é usado para determinar a pontuação de risco acumulada nas tarefas de vulnerabilidade ou correção.

Nota:
Quando **Incluir adiado** é selecionado, todos os itens vulneráveis adiados são incluídos no cálculo de acúmulo para as tarefas de correção. Certifique-se de entender o impacto no cálculo total antes de selecionar esta opção.

As calculadoras de acúmulo executam o trabalho programado, *`Rollup vulnerable item values to vulnerability and groups`*, a cada 15 minutos para selecionar as mudanças e acumular os detalhes e as pontuações de risco para tarefas de correção e vulnerabilidades. Esses trabalhos programados também calculam valores cumulativos para o número de IVs, pontuação de risco máximo, data de destino da correção e status das tarefas de correção.

Nota:
Os valores calculados para entradas de vulnerabilidade não incluem dados de destino de correção.

A pontuação de risco é calculada quando:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A pontuação de risco, o destino de correção, o status de correção ou as mudanças de vulnerabilidade nos itens vulneráveis.
- O estado do item vulnerável muda para Aberto, Adiado, Encerrado ou muda de Encerrado ou Adiado.
- Itens vulneráveis são excluídos.
- Itens vulneráveis são adicionados ou removidos da tarefa de correção.

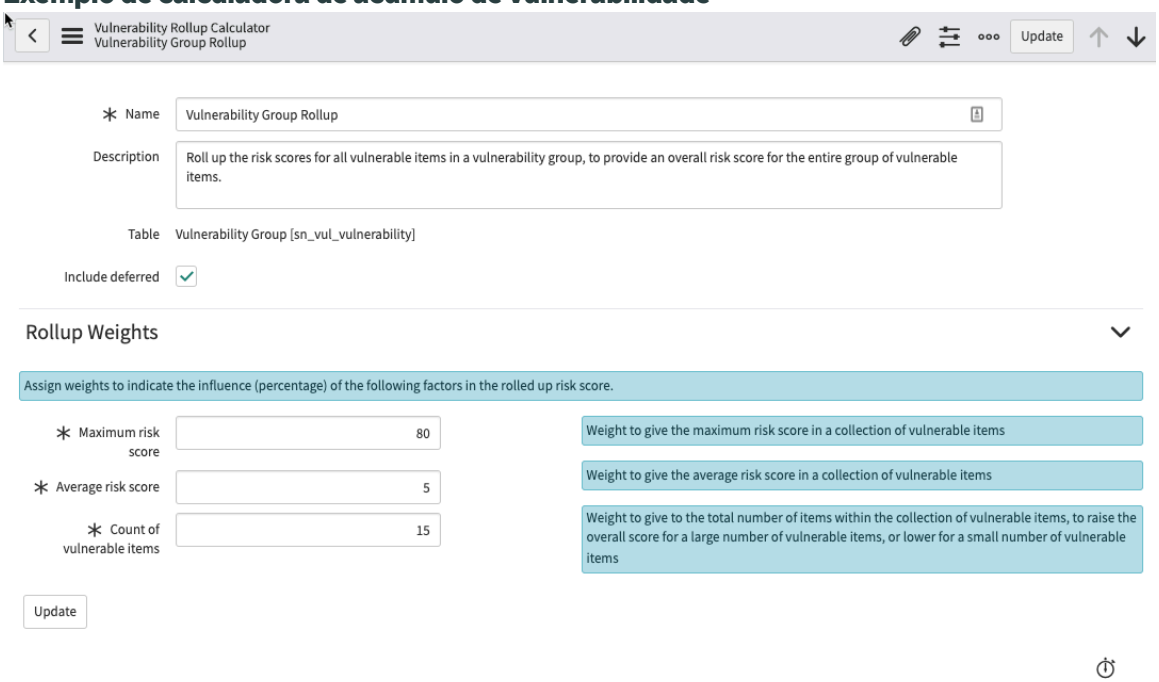
Exemplo de calculadora de acúmulo de vulnerabilidade: considere uma tarefa de correção VUL324567, que tem os seguintes itens vulneráveis:

- VIT1001 com pontuação de risco de 30
- VIT1002 com pontuação de risco de 40
- VIT1003 com pontuação de risco de 50

Além disso, considere os seguintes pesos na calculadora de acúmulo de vulnerabilidades:

- Pontuação de risco máximo: 80
- Pontuação de risco médio: 5
- Contagem de itens vulneráveis: 15

Exemplo de calculadora de acúmulo de vulnerabilidade



No exemplo de calculadora de acúmulo de vulnerabilidade, a fórmula para determinar a **pontuação de risco** da tarefa de correção é:

(**Pontuação de risco máximo**/100) * 80 + (**Pontuação de risco médio** /100) * 5 + (fator * 15)

O fator é determinado da seguinte forma:

Contagem de IV	Fator
< 10	0,2

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

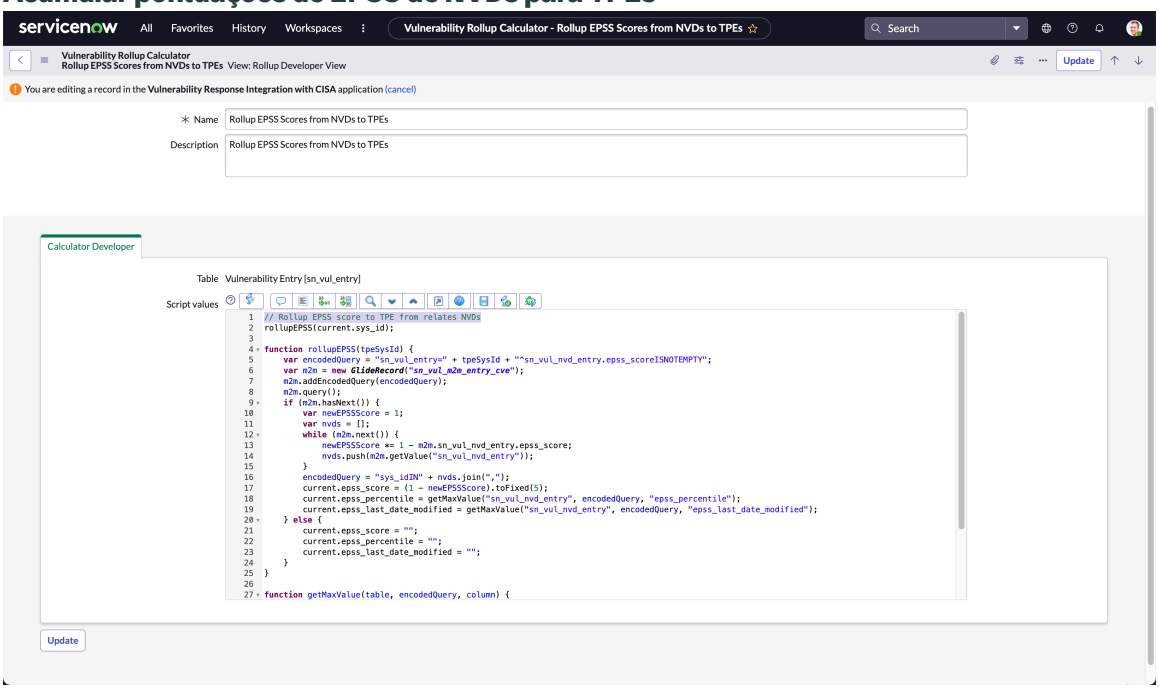
Contagem de IV	Fator
10 a 100	0,4
101–1000	0,6
1001–10000	0,8
> 10000	1

Portanto, para a tarefa de correção, VUL324567:

- A pontuação média de risco é 40
- A pontuação máxima de risco é 50
- 50 (pontuação de risco máximo)
- O fator é 0,2

A **pontuação de risco** seria 45 [(50/100) * 80 + (40/100) * 5 + 0,2 * 15 = 40 + 2 + 3 = 45]

Acumular pontuações de EPSS de NVDs para TPEs



Calculadora de acúmulo de EPSS - Exemplo

Por exemplo, considere uma organização com 100 vulnerabilidades, cada uma com 5% de chance de serem exploradas. A pergunta de grande interesse para um defesa de rede pode ser: qual é a probabilidade de que pelo menos uma dessas vulnerabilidades seja explorada e, portanto, qual é a minha ameaça geral? A probabilidade de pelo menos um evento ocorrer é simplesmente o complemento (oposto) de nenhum evento ocorrendo, ou seja:

```
P(at least one exploited vulnerability) = 1 - P(no vulnerabilities are exploited)
```

Em que a probabilidade de não haver vulnerabilidades é o produto linear de cada vulnerabilidade não explorada. Neste exemplo, como cada vulnerabilidade tem 5% de chance de ser explorada, cada uma tem 95% de chance de não ser explorada. E como há 100 deles, podemos escrever isso como:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
P(at least one vuln exploited) = 1 - P(no vulns are exploited) = 1 - P(one vuln not
 exploited)^100 = 1 - 0.95^100 = 0.994
```

O que indica que a probabilidade de pelo menos uma das vulnerabilidades serem exploradas é de 99,4%.

Importante:
Para modificar o `Rollup EPSS Scores from NVD to TPEs`, é necessário alternar a exibição do menu de contexto do formulário para a exibição de **desenvolvedor** de acúmulo da **exibição padrão**.

Criar ou editar Vulnerability Response regras de destino de correção

Após a avaliação inicial das regras de destino de correção no Assistente de configuração, os gerentes de vulnerabilidade podem configurar uma regra de destino de correção no nível de item vulnerável para orientar a correção de vulnerabilidades de alto risco em tempo hábil. Quando a data de correção de um item vulnerável se aproxima, uma notificação é enviada aos usuários ou grupos especificados na regra.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de destino de correção**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Nome	Nome da regra.
Meta (dias)	Especifique o número de dias em que os itens vulneráveis devem ser corrigidos, desde a última abertura.
V17.1: meta de (data)	Data a partir da qual os SLAs de destino são calculados. Você pode especificar somente a data ou os campos de tipo de data e hora. O valor padrão é Data da última abertura. Para personalizar os valores deste campo, consulte KB1185029 .
Ativo	Por padrão, a caixa de seleção **Ativo** está marcada, o que significa que a regra de destino de correção está ativa. Se esta caixa de seleção estiver desmarcada, esta regra não se aplicará aos novos itens vulneráveis criados no sistema.
Notificar (dias antes do vencimento)	Número de dias antes do tempo de correção direcionado para o envio de uma notificação. A data de notificação calculada usando este valor é usada para mostrar o status da correção e a codificação de cores. Se a data for anterior à data de notificação, o status da correção será "Em andamento". Se passar da data de notificação e antes da data de meta de correção, o status será mostrado como se aproximando da meta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Se este campo for definido como 0, somente uma notificação de **Meta** não atingida será enviada.
Descrição	Texto que descreve a regra de destino de correção.
Condição	Usando o filtro de condição, selecione os critérios para aplicar a regra aos itens vulneráveis. Para evitar impacto no desempenho, teste suas condições em escala de produção total. O teste permite determinar quanto tempo o trabalho **Avaliar destinos de correção** leva para ser executado, de acordo com as condições e o tamanho do seu Configuration Management Database (CMDB). A diferenciação de maiúsculas e minúsculas para o texto de pesquisa inserido no construtor de condição não é compatível com este registro ou formulário.
Notificações **Nota:** A contagem mostrada no e-mail de notificação não inclui itens vulneráveis no estado **Adiado**, **Resolvido**ou **Encerrado**.	
Usuários	As pessoas a serem notificadas quando o item vulnerável selecionado estiver se aproximando ou ultrapassar seu tempo de destino de correção direcionado.
Grupo	O grupo a ser notificado quando o item vulnerável selecionado estiver se aproximando ou ultrapassar seu tempo de destino de correção direcionado.
Atualizar Histórico	
	Não usado para a criação inicial de uma regra. Posteriormente, as anotações de trabalho do sistema são registradas aqui.

4. Clique em **Enviar**.
   Esta regra entra em vigor durante a próxima execução do trabalho programado, *`Evaluate remediation targets`* ou ao usar o botão **Aplicar mudanças** na exibição da lista Regras de destino de correção. O mesmo é verdadeiro quando uma regra existente é atualizada. Para obter mais informações sobre o trabalho programado e, **Aplicar mudanças**, consulte Vulnerability Response regras de destino de correção.

Configurar integrações de terceiros instaladas usando o Assistente de configuração

Configure o Vulnerability Response para funcionar com cada uma das implantações de aplicação de terceiros instaladas.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Assistente de configuração** > **Configuração de Integração**.
2. Selecione **Integrações de scanner** para configurar implantações de aplicações de terceiros instaladas.
3. Se Solução de gerenciamento do Vulnerability Response estiver instalado, você poderá selecionar **Integrações de solução** para configurar seus provedores de solução de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar integrações de soluções instaladas para Solução de gerenciamento de vulnerabilidade usando o Assistente de configuração

Depois de instalar a aplicação Vulnerability Solution Management, você pode configurar seus provedores de solução de vulnerabilidade usando o Assistente de configuração.

Antes de Iniciar

Funções necessárias: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) ou admin

Use as seções a seguir para complementar as instruções e os avisos fornecidos no Assistente de configuração para integrações de soluções instaladas para Solução de gerenciamento do Vulnerability Response.

- Verifique se você já instalou o Solução de gerenciamento de vulnerabilidade e as integrações de solução desejadas antes de começar. Para obter mais informações, consulte Instalar Vulnerability Response aplicações de terceiros usando o Assistente de configuração.
- Verifique se você tem credenciais de conta de terceiros disponíveis. Eles são necessários para editar algumas integrações de solução.
- Consulte Instalar a aplicação Solução de gerenciamento do Vulnerability Response para obter mais informações antes de configurar as soluções instaladas.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções**.

   O Integração com a solução Microsoft Security Response Center requer uma chave de API e um URL do Microsoft Security Response Center para configurá-lo.

   Nota:
   A inserção da chave de API é opcional para MSRC. Para obter a chave MSRC, você deve ter um ID da Microsoft de uma conta de e-mail live.com, outlook.com ou Microsoft.com, um número de telefone registrado na Microsoft ou um login do Skype.

2. Insira a URL.
   O URL no Assistente de configuração para MSRC é https://api.msrc.microsoft.com.
3. Clique em **Concluir**.
4. **Opcional:** Você pode executar importações sob demanda clicando **em Executar agora** na página de configuração depois de inserir suas credenciais.
5. O Red Hat Solution Integration também está disponível.
   Não requer uma chave de API.
6. No Assistente de configuração, à direita de Red Hat Solution Integration, clique em **Editar**.
7. Verifique se a URL no Assistente de configuração para RHSI é https://access.redhat.com/HR/rest
8. **Opcional:** Você pode executar importações sob demanda clicando **em Executar agora** na página de configuração.
9. Clique em **Concluir**, seguido por **Marcar como concluído** para concluir a configuração.
   Uma marca de seleção é exibida no Assistente de configuração para integrações de solução quando você conclui a configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar a integração de vulnerabilidade do MS TVM usando o Assistente de configuração

Configure a integração Vulnerability Response com a aplicação Microsoft Threat and Vulnerability Management (MS TVM) depois de instalá-la usando o Assistente de configuração.

Antes de Iniciar

Além das instruções e avisos fornecidos no Assistente de configuração para a integração Vulnerability Response com a integração do Microsoft Threat and Vulnerability Management, execute as seguintes ações:

- Verifique se você já instalou a aplicação antes de começar. Para obter mais informações, consulte Instalar Vulnerability Response aplicações de terceiros usando o Assistente de configuração.
- Consulte Preparando-se para o Microsoft Threat and Vulnerability Management Vulnerability Integration para obter mais informações antes de configurar a integração do Microsoft Threat and Vulnerability Management para Vulnerability Response.
- Verifique se você tem credenciais de conta do MS TVM disponíveis. Para obter essas credenciais, consulte Configurar o Microsoft Azure para a integração do MS TVM.

Funções necessárias: System Admin (admin) para instalação, Vulnerability Admin (sn_vul.vulnerability_admin) ou sn_vul.admin (preterido) e Configure Integration (sn_vul_msft_tvm.configure_integration) para configuração

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.

   O bloco Microsoft Threat & Vulnerability Management é exibido.

   O MS TVM é uma integração de várias origens, o que significa que você pode ter várias implantações da mesma integração de terceiros. As configurações da integração original de terceiros são usadas como modelo para as configurações de cada nova integração.

   Nota:
   Se você excluir a integração de vulnerabilidade original, precisará selecionar outra integração para usar como modelo. Considere desabilitar a integração em vez de excluí-la. As integrações criadas a partir de modelos desabilitados são desabilitadas por padrão.

   Os dados de cada integração de terceiros são identificados exclusivamente e estão disponíveis em uma única instância de Vulnerability Response.

2. Para configurar a integração do Microsoft Threat and Vulnerability Management, clique em **Editar**.
3. No formulário, preencha os campos.

Formulário Credenciais da conta

Campo	Descrição
Nome	Nome da instância.
Região de TVM	Região próxima ao local do servidor. Use o servidor mais próximo de sua localização para obter o desempenho ideal da API.
Tipo de autenticação	Método para verificar a identidade. A autenticação de usuário controla a visibilidade de ativos específicos para usuários específicos. O MS

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	TVM exporta os grupos de dispositivos que estão autorizados para este usuário. O valor padrão é Aplicação.
ID de locatário	Identidade de locatário da sua organização.
ID de cliente	Identidade do cliente gerada após o registro do MS TVM no Microsoft Azure.
Nome do usuário	Usuário que tem acesso ao grupo de dispositivos completo. Este campo é exibido somente quando Usuário é selecionado no tipo de autenticação.
Senha	Senha para o nome de usuário que tem acesso ao grupo de dispositivos completo. Este campo é exibido somente quando Usuário é selecionado no tipo de autenticação.
Segredo do cliente	Segredo do cliente gerado após o registro da aplicação MS TVM. Este campo é exibido somente quando a aplicação é selecionada no tipo de autenticação.

4. Para salvar suas mudanças e prosseguir para o primeiro formulário de integração, clique em **Avançar**.
   O formulário Configuração de importação de vulnerabilidades é exibido.
5. Habilite ou desabilite a importação de vulnerabilidades, determine a data de início das vulnerabilidades que você deseja importar e programe quando a importação de vulnerabilidades do MS TVM deve ser executada.
   Se você quiser importar todas as vulnerabilidades, deixe a data de início inicial em branco.
   a. Para importar dados sob demanda, clique em **Importar vulnerabilidades agora**.
   b. Para ver o registro de integração, clique **em Configurações avançadas**.
6. Para salvar suas mudanças e prosseguir para o primeiro formulário de integração, clique em **Avançar**.
   O formulário Configuração de importação de recomendações é exibido.
7. Habilite ou desabilite a importação de recomendações e determine a programação de quando a importação de vulnerabilidades do MS TVM deve ser executada.
   a. Para importar dados sob demanda, clique em **Importar recomendações agora**.
   b. Para ver o registro de integração, clique **em Configurações avançadas**.
8. Para salvar suas mudanças e prosseguir para o primeiro formulário de integração, clique em **Avançar**.
   O formulário Configuração de importação de máquinas é exibido.
9. Habilite ou desabilite a importação de máquinas, determine a data de início das máquinas que você deseja importar e programe quando a importação de máquinas MS TVM deve ser executada.
   Se você quiser importar todas as máquinas, deixe a data de início inicial em branco.

Nota:
Os marcadores de máquina são importados por padrão e usados para organizar e rastrear as máquinas listadas no ambiente MS TVM.

   a. Para exibir as regras de pesquisa do item de configuração (IC) padrão, clique em **Regras de pesquisa de IC**. As regras de pesquisa de IC definem como os dados da máquina de fontes de terceiros são usados para identificar itens de configuração (IC)s no Now Platform CMDB. Você tem a opção de adicionar regras de pesquisa ou modificar as regras de pesquisa de IC padrão nesta página. Para obter mais informações,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

consulte Regras de pesquisa de IC para identificar itens de configuração de Vulnerability Response integrações de vulnerabilidade de terceiros.

b. Para importar dados sob demanda, clique em **Importar máquinas agora**.

Nota:
As máquinas com o status integrado no MS TVM são recuperadas pela aplicação ServiceNow.

c. Para ver o registro de integração, clique **em Configurações avançadas**.

10. Para salvar suas mudanças e ir para o primeiro formulário de integração, clique em **Avançar**.
O formulário Configuração de importação de vulnerabilidades da máquina é exibido.

11. Habilite as seguintes integrações e determine a data de início das vulnerabilidades que você deseja importar.

Formulário de configuração de importação de vulnerabilidades da máquina

Integração	Descrição
Importação delta de vulnerabilidades da máquina com Microsoft TVM	Recupera vulnerabilidades que foram atualizadas durante a importação de vulnerabilidades completa, incluindo vulnerabilidades novas, corrigidas e atualizadas. Você só pode importar dados delta dos últimos 14 dias.
Importação completa de vulnerabilidades da máquina com Microsoft TVM	Recupera todas as vulnerabilidades em aberto. Devido ao alto volume de importação de dados, você pode programá-la para ser executada semanalmente.

Nota:

Execute a importação de máquinas antes da integração de vulnerabilidades de máquina. Caso contrário, os IVs não serão criados para as máquinas ausentes.

12. Para salvar suas mudanças e concluir a configuração no Assistente de configuração, clique em **Concluir**.

O que Fazer Depois

Se você quiser ativar um agrupamento de itens vulneráveis no ambiente clássico, navegue até > **Vulnerability Response** > **Administração** > **Regras de tarefa de correção** > **Recomendação do Microsoft TVM**.

No formulário exibido, selecione a opção **Ativo** para ativá-lo. Como alternativa, selecione **Novo** para criar uma nova regra.

Para obter mais informações, consulte Vulnerability Response tarefas de correção e regras de tarefa visão geral.

Configurar o Qualys Vulnerability Integration usando o Assistente de configuração

Depois de instalar a aplicação Qualys, configure-a usando o Assistente de configuração.

Antes de Iniciar

Use as seções a seguir para complementar as instruções e os prompts fornecidos no Assistente de configuração para configuração do Qualys Vulnerability Integration.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Verifique se você já instalou a aplicação antes de começar. Para obter mais informações, consulte Instalar Vulnerability Response aplicações de terceiros usando o Assistente de configuração.
- Consulte Preparando para o Qualys Vulnerability Integration para obter mais informações antes de configurar o Qualys Vulnerability Integration.
- Verifique se você tem credenciais de conta de terceiros disponíveis. Eles são necessários para editar alguns aplicativos de terceiros.

Funções necessárias: administrador do sistema (admin) para instalação, administrador de vulnerabilidade (sn_vul.vulnerability_admin) ou sn_vul.admin (obsoleto) para configuração.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
   As integrações instaladas são exibidas.
2. Clique em **Editar** à direita de Qualys Vulnerability Integration que você deseja configurar.
3. No formulário Credenciais da conta, insira suas credenciais Qualys Cloud Platform.
   Suas credenciais são necessárias para configurá-lo.
4. Use as anotações a seguir como guia ao continuar com a configuração.
   - O link **Configurações avançadas** aponta para o registro de integração Qualys. Você pode adicionar parâmetros que são compatíveis com o produto Qualys para suas consultas programadas para ajudá-lo a filtrar os dados de vulnerabilidade importados. Consulte Definir parâmetros de filtro adicionais para importações de Qualys para obter mais informações.
   - Se você atualizou de uma versão anterior do Vulnerability Response com uma versão do Qualys Vulnerability Integration que você já configurou, essa versão, com suas definições de configuração preservadas, ainda estará disponível.

     Em Configurações de importação em Configuração de detecção de host para Qualys Vulnerability Integration, há uma opção para exibir registros de detecção de vulnerabilidade Qualys fixos. Se habilitado, isso permite que você crie itens vulneráveis a partir de registros de detecção em um status fixo (estado =**Fixo**). Para obter mais informações sobre detecções de item vulnerável, consulte Vulnerability Response detecções de item vulnerável de integrações de terceiros.

     Você pode ativar a caixa de seleção **Pesquisar por partição de rede** na página Configuração de detecção de host para incluir o identificador da partição de rede na pesquisa de endereço IP. Para obter mais informações, consulte Atualizar itens de configuração com o identificador de partição de rede para Qualys Vulnerability Integration.

     Todos os marcadores de host são importados como parte da integração da lista de hosts Qualys. Os marcadores de host são usados principalmente para filtragem em Vulnerability Response Regras de tarefa de atribuição e correção. Eles são exibidos no formulário Item descoberto.

     Nota:
     A integração da lista de hosts Qualys deve ser executada antes de criar Regras de atribuição ou de tarefa de correção em Vulnerability Response para que todos os marcadores possam estar presentes nas regras e antes que os itens vulneráveis sejam importados e agrupados.

     As Qualys **etiquetas** do ativo são armazenadas no módulo Marcações do host no Qualys Vulnerability Integration.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O Qualys Vulnerability Integration oferece suporte a várias origens. Você pode ter várias implantações da mesma integração de terceiros. Para adicionar outra integração, na página Integrações do scanner, clique em **Adicionar integração**.

  As configurações da integração original de terceiros são usadas como modelo para as configurações de cada nova integração.

  Nota:
  Se você excluir a integração de vulnerabilidade original, precisará selecionar outra integração para usar como modelo. Considere desabilitar a integração em vez de excluí-la. As integrações criadas a partir de modelos desabilitados são desabilitadas por padrão.

  Os dados de cada integração de terceiros são identificados exclusivamente e estão disponíveis em uma única instância de Vulnerability Response.

- Você pode executar importações sob demanda clicando **em Executar agora** em uma página de configuração.

5. Clique em **Concluir** para concluir a configuração no Assistente de configuração.

Configurar a integração de vulnerabilidade da Tenable usando o assistente de configuração

Depois de instalar a aplicação Integração do Vulnerability Response com Tenable, configure-a usando o Assistente de configuração.

Antes de Iniciar

Use as seções a seguir para complementar as instruções e os avisos fornecidos no Assistente de configuração para a integração Integração do Vulnerability Response com Tenable.

- Verifique se você já instalou a aplicação antes de começar. Para obter mais informações, consulte Instalar Vulnerability Response aplicações de terceiros usando o Assistente de configuração.
- Consulte Preparando para a integração de vulnerabilidade da Tenable para obter mais informações antes de configurar o Tenable para Vulnerability Response.
- Verifique se você tem credenciais de conta de terceiros disponíveis. Eles são necessários para editar alguns aplicativos de terceiros.

Funções necessárias: System Admin (admin) para instalação, Vulnerability Admin (sn_vul.vulnerability_admin) ou sn_vul.admin (obsoleto) e Configure Integration (sn_vul_tenable.configure_integrations) para configuração.

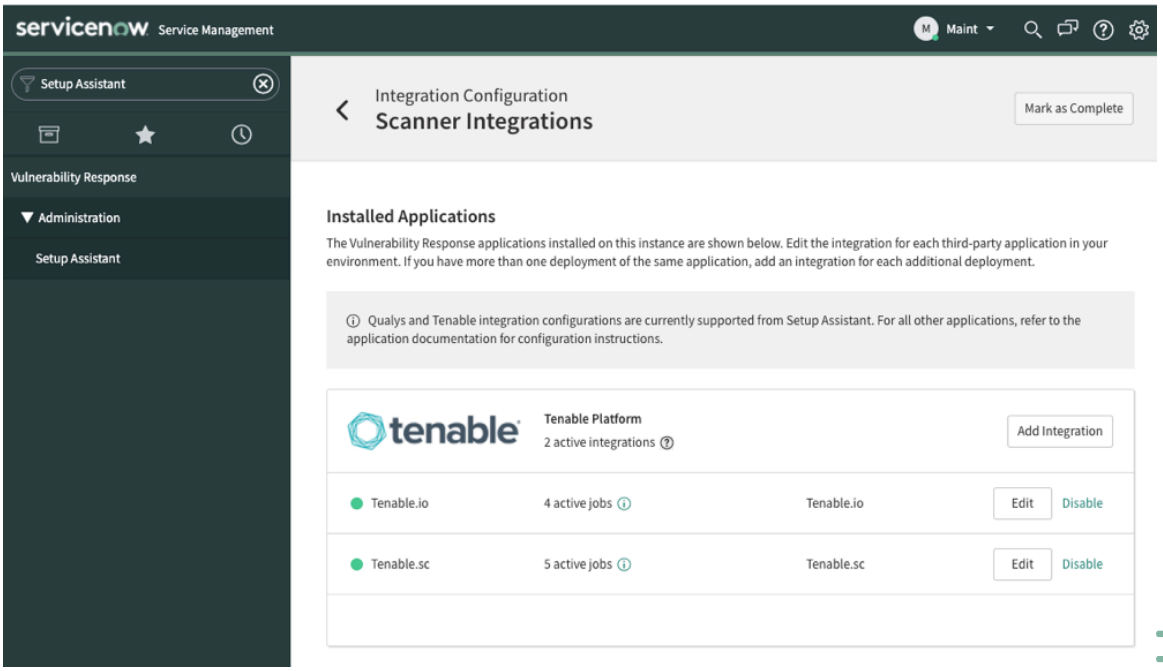
Procedimento

1. Se não for exibido, navegue até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.

   As integrações Tenable.io e Tenable.sc são exibidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A Tenable é uma integração de várias origens e você pode ter várias implantações da mesma integração de terceiros. As configurações da integração original de terceiros são usadas como modelo para as configurações de cada nova integração.

Nota:
Se você excluir a integração de vulnerabilidade original, precisará selecionar outra integração para usar como modelo. Considere desabilitar a integração em vez de excluí-la. As integrações criadas a partir de modelos desabilitados são desabilitadas por padrão.

Os dados de cada integração de terceiros são identificados exclusivamente e estão disponíveis em uma única instância de Vulnerability Response.

2. À direita da integração da Tenable que você deseja configurar, clique em **Editar**.
3. No formulário Credenciais da conta, preencha os campos.
   - Tenable.io requer acesso de administrador com um atributo de permissão maior ou igual a 64.

     Nota:
     A partir da v3.8 do Vulnerability Response Integration with Tenable, o acesso ao Tenable.io não precisa mais de privilégios de administrador. Um usuário básico com um atributo de permissão igual a 16 também pode acessar o produto.

   - Tenable.sc requer acesso de Analista de Segurança ou Gerente.

   a. Selecione seu produto Tenable.

   b. Insira o nome da sua conta da Tenable.

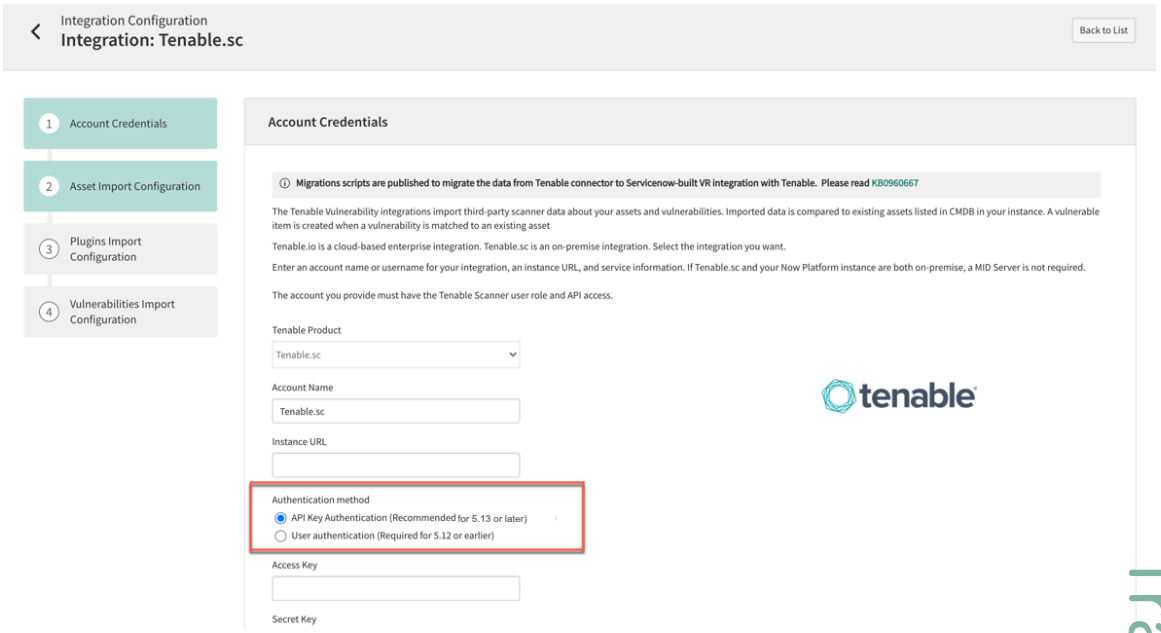
   c. No campo URL da instância, insira o URL da sua plataforma Tenable.

   d. Selecione um método de autenticação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Com base na sua versão de Tenable.sc, você tem duas opções de autenticação:



i. A partir da v5.13 de Tenable.sc, selecione **Autenticação de chave de API**. Insira suas chaves secretas e de acesso da Tenable.

ii. Antes da v5.13, a autenticação do usuário era compatível com sua instância Now Platform® e era obrigatória. Insira seu nome de usuário Now Platform e senha.

Somente a autenticação de chave de API é compatível com Tenable.sc. Insira suas chaves secretas e de acesso da Tenable.

e. Opcional: Selecione um MID Server.

(Optional) Se sua instância Now Platform e sua aplicação Tenable.sc não estiverem no mesmo local, escolha um MID Server configurado na lista de seleção. Para obter mais informações, consulte MID Server.

- Começando com v15.0 de Vulnerability Response e v3.0 de Tenable Vulnerability Integration, você tem a opção de habilitar o parâmetro `Async_request` conforme descrito em Configurações de recuperação de dados para a integração de vulnerabilidade da Tenable. Alguma configuração com o Tenable será necessária se você quiser fazer chamadas síncronas. Entre em contato com o produto Tenable para obter ajuda. Este parâmetro, uma vez ativado, é aplicável a todas as integrações da Tenable.sc e tem um tempo limite de 30 segundos. Para exibir os scripts de correção, navegue até **Definição do Sistema** > **Corrigir Scripts**.

- (Optional) Para os clientes existentes, um script de correção está disponível se você estiver usando chamadas assíncronas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se sua instância Now Platform e sua aplicação Tenable.sc estiverem no local, embora não sejam obrigatórias, você terá a opção de selecionar um MID Server configurado na lista de seleção.

Nota:
Quer você opte por empregar um MID Server ou não, as integrações expiram após cinco minutos e uma mensagem é exibida quando não há resposta do servidor.

(Optional) Se você receber um erro de tempo limite, no Assistente de configuração, verifique se você inseriu as credenciais e o URL corretos.

4. Clique em **Avançar** para salvar suas mudanças e prosseguir para o primeiro formulário de integração. O formulário Configuração de importação de ativo é exibido.
5. Neste formulário, ative ou desative a integração de importação de ativo, determine a data de início inicial dos ativos que você deseja importar e programe quando a importação de ativo da Tenable deve ser executada.

   Para Tenable.io

   - A integração de ativos pode ser usada com os resultados de conformidade Tenable.io e a integração de backfill de resultados de conformidade para importar dados de avaliação de configuração segura sobre seus ativos para a aplicação Configuration Compliance.
   - A versão 12.2 da aplicação Configuration Compliance será necessária em sua instância se você quiser importar e exibir esses dados de avaliação de configuração segura.

     Consulte Configuration Compliance dados importados para obter mais informações sobre quais dados são importados com essas integrações e onde eles são publicados.
   - Os resultados de conformidade Tenable.io e as integrações de preenchimento de resultados de conformidade não são ativados por padrão. Se você ativá-los, talvez prefira usar as configurações de programação padrão fornecidas. Consulte as etapas listadas abaixo para saber como localizar e ativar integrações para o Tenable Vulnerability Integration.
   - Você pode iniciar uma nova verificação sob demanda para itens vulneráveis para o produto Tenable.io de sua instância. A integração de modelo Tenable.io e a integração de credencial de verificação Tenable.io devem ser ativadas antes de iniciar novas verificações.

   Por padrão, essas integrações estão desativadas. Quando você insere suas credenciais para Tenable.io, todas as integrações Tenable.io são ativadas automaticamente. Para ativar ou desativar manualmente essas integrações:

   a. Navegar até **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
   b. Na lista exibida, localize os registros de integração Tenable.io desejados.
   c. Abra cada registro e marque a caixa de seleção **Ativo** para ativar a integração.
   d. Clique em **Atualizar** para salvar suas mudanças.
   e. Retorne ao Assistente de configuração para continuar com sua configuração para Tenable Vulnerability Integration com Vulnerability Response.

   - Para a integração Tenable.io, você também tem a opção de ativar e desativar a importação de etiquetas do ativo. As etiquetas do ativo são importadas por padrão e usadas para organizar e rastrear os ativos listados no seu CMDB no ambiente Tenable.io.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para os produtos Tenable.io e Tenable.sc, se você selecionar **Habilitar pesquisa por partição de rede** em Pesquisa por partição de rede, poderá criar ICs individuais usando o mecanismo de Identificação e Reconciliação (IRE) para seus ativos que têm o mesmo endereço IP. Para obter mais informações, consulte Atualizar itens de configuração com o identificador de partição de rede para Tenable Vulnerability Integration e Criando ICs para Vulnerability Response usando o mecanismo de Identificação e Reconciliação.
- Na parte superior da tela, ao lado do link Importação de ativo, clique no link **Regras de pesquisa de IC** para exibir as regras de pesquisa do item de configuração (IC) padrão. As Regras de pesquisa de IC definem como os dados de ativo de terceiros são usados para identificar itens de configuração (IC)s no Now Platform CMDB. Você tem a opção de adicionar regras de pesquisa ou modificar as regras de pesquisa de IC padrão nesta página. Para obter mais informações, consulte Regras de pesquisa de IC para identificar itens de configuração de Vulnerability Response integrações de vulnerabilidade de terceiros.
- Clique **em Importar ativos agora** para importar dados sob demanda.
- O link **Configurações avançadas leva** você ao registro de integração de ativos. A partir da v3.3, é possível adicionar parâmetros que são compatíveis com o produto Tenable.io para suas consultas programadas para ajudá-lo a filtrar os dados de vulnerabilidade importados com os Tenable.io Ativos e as integrações de vulnerabilidades fixas e abertas. Consulte Definir parâmetros de filtro adicionais para importações de Tenable.io para obter mais informações.

6. Clique em **Avançar** para salvar suas mudanças e prosseguir para o próximo formulário.
   O formulário Configuração de importação de plug-ins é exibido.
7. Neste formulário, habilite ou desabilite a importação de plug-ins (entradas de vulnerabilidade de terceiros), determine a data de início inicial dos plug-ins que você deseja importar e programe quando a importação de plug-ins da Tenable deve ser executada.

   Se você quiser importar todos os plug-ins, vulnerabilidades e ativos, deixe a data de início inicial em branco.

   - Clique **em Importar plug-ins agora** para importar dados sob demanda.
   - O link **Configurações avançadas direciona** você para o registro de integração de plug-ins.
   - Para a importação de vulnerabilidades, você pode programar e definir níveis de severidade para Tenable.io para as vulnerabilidades que deseja ingerir. Determine uma data para que somente as vulnerabilidades criadas ou atualizadas a partir de uma data específica sejam importadas.
   - Para a integração Tenable.sc, você pode determinar um filtro de consulta e uma data para que somente as vulnerabilidades criadas ou atualizadas a partir de uma data específica sejam importadas.
8. Clique em **Avançar** para salvar suas mudanças e prosseguir para o próximo formulário.
   O formulário Configuração de importação de vulnerabilidades é exibido. Habilite ou desabilite a integração e determine a data de início das vulnerabilidades que você deseja importar.

   Para o produto Tenable.io :

   - Importe somente as vulnerabilidades e os IVs associados que correspondam às condições escolhidas com o filtro de Severidade.
   - Para a integração de ativos [Tenable.io, `Last Scan Time` é importado e atualizado somente para ativos que têm vulnerabilidades.
   - Habilite a opção **Vulnerabilidades corrigidas** para exibir IVs para registros de detecção corrigidos. Se este sinalizador estiver habilitado no Assistente de configuração, novos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

IVs serão criados para detecções no estado **Fixo** que ainda não existem em sua instância. Quando habilitado, este recurso pode afetar negativamente o desempenho da ingestão.

- O link **Configurações avançadas** ao lado de Importar filtros direciona você para o registro de integração de vulnerabilidades.
- Clique no link **Importar programações** na parte superior para configurar a frequência com que as vulnerabilidades são ingeridas e habilitar a integração.

Para o produto Tenable.sc :

- Importe somente as vulnerabilidades e os IVs associados que correspondam aos filtros de condição definidos por uma consulta da Tenable na plataforma Tenable. Consulte a documentação da Tenable para obter mais informações sobre consultas da Tenable.

  O filtro de consulta da Tenable selecionado no Assistente de configuração também se aplica à Integração de ativos Tenable.sc. Somente os ativos com as vulnerabilidades que correspondem às condições do filtro de consulta são importados.

- Habilite a opção **Vulnerabilidades corrigidas** para exibir IVs para registros de detecção corrigidos. Se este sinalizador estiver ativo no Assistente de configuração, novos IVs serão criados para detecções no estado **Fixo** que ainda não existem em sua instância. Quando ativo, este recurso pode afetar negativamente o desempenho da ingestão.
- Para incluir o identificador de partição de rede na pesquisa de endereço IP, selecione **Habilitar pesquisa por partição de rede** caixa de seleção do **Pesquisa por partição de rede** seção. Para obter mais informações, consulte Atualizar itens de configuração com o identificador de partição de rede para Tenable Vulnerability Integration.
- Clique em **Importar programações** na parte superior para configurar a frequência com que as vulnerabilidades são ingeridas e habilitar a integração.
- O link **Configurações avançadas** ao lado de Importar filtros direciona você para o registro de integração de vulnerabilidades.
- A ServiceNow® Tenable.sc Integração de credencial de verificação é habilitada (Ativo) automaticamente no Assistente de configuração em sua instância quando você configura as Tenable.sc Integrações de vulnerabilidades (Tenable.sc Integrações de vulnerabilidades abertas e corrigidas).

  Esta integração importa e atualiza as credenciais do scanner do produto Tenable.sc em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais da Tenable. Navegar até **Integração de vulnerabilidade Tenable** > **Integrações** > **Integração de credencial de verificação da Tenable.sc** para exibir mais informações sobre a integração de credencial de verificação.

9. Clique em **Concluir** para salvar suas mudanças e concluir a configuração no Assistente de configuração.

O que Fazer Depois

(Opcional) Navegue até **Todos** > **Vulnerability Response** > **Administração** > **Calculadoras de vulnerabilidade** > **Calculadora de Risco Padrão** > **Regra de risco da Tenable** para habilitar a regra de risco da Tenable.

No formulário Regra da Calculadora de Vulnerabilidade exibido, marque a caixa de seleção Ativa para habilitá-la.

A Regra de risco da Tenable é instalada com a aplicação Integração do Vulnerability Response com Tenable como parte da Calculadora de risco padrão nas Calculadoras de vulnerabilidade da

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerability Response. A classificação de prioridade de vulnerabilidade (VPR) é um atributo do produto Tenable que é importado e usado com a nova calculadora de risco padrão. Esta regra de risco é desativada por padrão. Ao habilitar a regra da calculadora de risco da Tenable, os valores de VPR importados são usados para calcular a pontuação de risco dos itens vulneráveis. A distribuição de peso padrão para esta calculadora de risco: VPR = 70%, Ativo = 15% e Criticalidade dos negócios = 15%. Habilitar esta regra da Calculadora de risco da Tenable pode afetar o desempenho da ingestão de dados.

Veja Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade

Configurar provedores de soluções de vulnerabilidade

Depois de instalar a aplicação Vulnerability Solution Management, configure os provedores de solução de vulnerabilidade usando o Assistente de configuração.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (obsoleto) ou admin.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Configuração de Integração**.
2. Clique **em Integrações de solução**.
3. Na seção Common Vulnerability Response Framework, busque dados usando um URL, uma API ou uma importação.
   - Para buscar dados usando um URL ou API, clique em **Adicionar integração**.
   - Para buscar dados carregando um arquivo do Common Vulnerability Response Framework (CVRF), clique em **Importar arquivo**.

O que Fazer Depois
Dependendo de como você deseja importar os dados do CVRF, é possível executar uma das seguintes tarefas:

- Se você quiser importar um arquivo CVRF, consulte Importar dados do Common Vulnerability Reporting Framework por meio da importação de arquivo.
- Se você quiser importar dados CVRF usando as APIs, consulte Importar dados do Common Vulnerability Reporting Framework (CVRF) por meio do URL do CVRF.
- Se você quiser importar dados CVRF por meio de consultorias, consulte Importar dados do Common Vulnerability Reporting Framework de consultorias.

Importar dados do Common Vulnerability Reporting Framework por meio da importação de arquivo

Importe um arquivo CVRF para exibir dados no formato CVRF. A importação é uma atividade única.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) ou admin.

Por Que e Quando Desempenhar Esta Tarefa
Depois de importada, uma entrada de fila é criada com um anexo, que é analisado quando a entrada é processada. Os dados são preenchidos nas respectivas tabelas. Antes de analisar os dados CVRF, um registro de mapeamento de scanner é criado com base na configuração. Em seguida, os dados de mapeamento do scanner são transformados em dados de mapeamento do fornecedor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Vulnerability Response Framework**.
2. Clique **em Importar arquivo**.

   Nota:
   Você pode carregar apenas um arquivo XML de cada vez com um tamanho máximo de arquivo de 1 GB.

3. No campo **Nome**, insira um nome exclusivo para a integração.
   O programador é criado com este nome.
4. No campo **Fornecedor**, insira o nome do fornecedor.
   O campo **Origem** das soluções é preenchido com o nome do fornecedor.
5. Clique em **Concluir**.

Resultado

Uma fila de importação é criada. Clique no link na barra de informações para exibir as entradas da fila do fornecedor junto com a lista relacionada. Você também pode exibir o status do trabalho.

Depois que os dados são importados para o formato CVRF, os dados são processados da seguinte forma:

1. Quando a fila é processada, o arquivo é analisado com uma fonte de dados dedicada.
2. Depois que o processamento for concluído, o log da aplicação será atualizado.
3. Depois que o arquivo XML CVRF é analisado, ele preenche as tabelas a seguir na aplicação ServiceNow® Vulnerability Response.
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

Você pode ver as informações detalhadas relacionadas a erros ou exceções nos logs da aplicação.

Configurar aliases de conexão e credencial

Configure os aliases de conexão e credencial para autenticar fornecedores. Na análise de consultoria, os fornecedores de terceiros são autenticados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (obsoleto) ou admin

Procedimento

1. Criar autenticação OAuth.
   Consulte Criar um endpoint para que os clientes acessem a instância .
2. Crie um alias de conexão e credencial.
   Consulte Criar alias de conexão e credencial .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Crie uma conexão.
   a. Clique no nome do alias de conexão e credencial recém-criado.
   b. Na guia **Conexões**, clique em **Novo**.
   c. Se o tipo de autenticação for OAuth, selecione o Perfil de registro da aplicação criado na etapa 1 como **Perfil de entidade OAuth**.
   d. Crie um registro em Conexões a partir da lista relacionada do registro.
   e. No campo **Credencial**, selecione o registro de credencial criado na etapa 3d.
   f. No campo **URL de conexão**, insira o URL do fornecedor.
   g. Clique em **Enviar**.

Configurar um fornecedor do Common Vulnerability Reporting Framework que não seja a Cisco

Configure um fornecedor do Common Vulnerability Reporting Framework (CVRF) que não seja a Cisco com suporte de API.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (descontinuado) ou admin

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Conexão e Credencial** > **Aliases de conexão e credencial**.
2. Crie um registro com o tipo de autenticação compatível com o fornecedor.
   Para obter mais informações sobre como autenticar um fornecedor, consulte Configurar aliases de conexão e credencial.
3. Navegar até **Todos** > **Vulnerability Response** > **Flow Designer**.
4. Duplique o fluxo chamado "Análise de aconselhamento".

   Nota:
   - Se alguma das ações precisar ser alterada, copie a ação e use-a no novo fluxo.
   - Atualize a lógica relacionada à paginação de acordo com o fornecedor

5. Se a lógica do parâmetro de intervalo de datas não for igual à da Cisco, copie a ação **Atualizar parâmetros de paginação** e faça as mudanças necessárias para o fornecedor.
6. Navegar até **Todos** > **Vulnerability Response** > **Mapeamento de dados de aprimoramento**.
7. Crie um registro de acordo com a Cisco, alterando o valor **da chave de propriedade** de acordo com o fornecedor.
   Esta lógica é para mapear campos obrigatórios de uma carga de consultoria para uma tabela ServiceNow.
8. Mapeie os seguintes marcadores de API da carga da API.
   Esses marcadores precisam ser mapeados com detalhes a serem preenchidos na tabela Mapeamento de dados de aprimoramento. Por padrão, o mapeamento específico da Cisco é enviado.

   Nota:
   Você precisará criar um registro se precisar configurar vários fornecedores que publicam consultorias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Marcador de carga de consultoria	Coluna da tabela sn_vul_cvrf_solution_integration	Descrição
URL do CVRF	cvrf_URL	Nome do marcador que contém o URL do CVRF.
ID de consultoria (chave exclusiva para resposta)	Id	Nome do marcador que contém um identificador exclusivo.
Data da última modificação	last_modified_date	Nome do marcador que contém a data em que o registro foi atualizado pela última vez.

9. Com base no formato de resposta, altere a lógica de análise copiando a ação **Recuperar lista** do fluxo de análise de consultoria.

Importar dados do Common Vulnerability Reporting Framework de consultorias

Importe dados CVRF de recomendações configurando a URL do fornecedor com o tipo de importação como API.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (obsoleto) ou admin

Por Que e Quando Desempenhar Esta Tarefa

Quando a integração é executada, os avisos são obtidos. O URL do CVRF e o ID dos avisos são extraídos da carga útil. As chamadas de REST API são feitas para cada URL do CVRF e os dados são analisados e armazenados na tabela sn_vul_solution.

Procedimento

1. Navegar até **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Vulnerability Response Framework**.
2. Clique **em Adicionar integração**.
3. No formulário, preencha os campos.

Importar formulário de consultoria da solução

Campo	Descrição
Tipo de importação	Opção para selecionar o tipo de importação. Selecione **API**.
Nome	Nome exclusivo para a integração.
Fornecedor	Nome do fornecedor **Nota:** O campo **Origem** das soluções é preenchido com o nome do Fornecedor.
Alias de conexão	Opção para selecionar uma credencial autenticada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: A tabela sys_alias armazena credenciais e o URL base para consultas.
Programação	Frequência na qual os dados devem ser atualizados.
Dia	Dia da semana em que você deseja que os dados sejam atualizados.
Hora	Hora da semana em que você deseja que os dados sejam atualizados.
Configuração de API	
Fluxo	Opção para selecionar o fluxo. O fluxo é acionado quando o programador é executado. O fluxo se encarrega de analisar os avisos e extrai o URL do CVRF e armazena esses detalhes nas tabelas de atualização. Você pode copiar o fluxo existente e editar conforme necessário. Por exemplo, você pode fazer mudanças relacionadas à paginação.
Ação de fluxo	Opção para selecionar a ação de fluxo. As ações de fluxo cuidam da capacidade da janela deslizante. Você pode atualizar as ações de fluxo e adicionar o parâmetro de consulta diretamente à ação arrastando.
Tabela de Mapeamento	Opção para selecionar a tabela de mapeamento. O registro da tabela de mapeamento de dados de aprimoramento é usado para extrair o URL do CVRF e o ID de aconselhamento da carga de aconselhamento.
Consultas de resposta	Opção para inserir o nome do marcador da carga de recomendações de onde a lista de recomendações pode ser extraída.
Critérios de filtro	
Parâmetros de intervalo de tempo	Opção para selecionar o intervalo de tempo da solicitação e o formato de data das chamadas de API. O parâmetro Solicitação de data de início/ data de término é o nome do parâmetro usado para a data de início e a data de término durante as chamadas de API. Por exemplo, StartDate, start_date, endDate, end_date.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Formato de data	Opção para inserir o formato de data, como `mm/dd/aaaa`.. O formato de data é o formato que a API precisa para filtragem. Os formatos que não são compatíveis com o GlideDate não funcionam.
Intervalo inicial em dias	Einsira os dias para os quais os dados devem ser obtidos quando o programador é executado pela primeira vez. Para execuções subsequentes, o mecanismo de janela deslizante é seguido. **Nota:** Se você não quiser selecionar um intervalo de tempo, selecione **Sem parâmetros**.
Mapeamentos do scanner	
Origem do scanner	Opção para selecionar a origem da entrada de terceiros (TPE).
Coluna de vulnerabilidade	Opção para selecionar a palavra-chave.
Palavras-chave	Opção para inserir a palavra-chave para pesquisar a coluna de vulnerabilidade selecionada.

4. Clique em **Concluir**.

Importar dados do Common Vulnerability Reporting Framework (CVRF) por meio do URL do CVRF

Importe dados CVRF configurando o URL do fornecedor no Assistente de configuração.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin, sn_vul.admin (obsoleto) ou admin

Por Que e Quando Desempenhar Esta Tarefa

Quando a integração é executada, os dados são obtidos do URL que é analisado. Os dados são armazenados na tabela sn_vul_solution com origem como o nome do fornecedor.

Nota:
A Oracle publica diretamente o URL do CVRF para fornecer soluções. Portanto, se você quiser configurar a integração para importar dados do Oracle, certifique-se de ter o URL do CVRF para o Oracle e siga as etapas a seguir.

Procedimento

1. Navegar até **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Configuração de Integração** > **Integrações de soluções** > **Common Vulnerability Response Framework**.
2. Clique **em Adicionar integração**.
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importar formulário CVRF

Campo	Descrição
Tipo de importação	Tipo de importação. Selecione **URL**.
Nome	Nome exclusivo para a integração.
Fornecedor	Nome do fornecedor **Nota:** O campo **Origem** das soluções é preenchido com o nome do fornecedor.
URL	URL do qual você deseja buscar os dados da solução no formato CVRF.
Programação	Frequência na qual os dados devem ser atualizados. **Nota:** Se o marcador de status do CVRF mostrar "FINAL", o campo será definido automaticamente como **Sob demanda** para evitar execuções desnecessárias.
Dia	Dia da semana em que você deseja que os dados sejam atualizados.
Hora	Hora da semana em que você deseja que os dados sejam atualizados.

4. Clique em **Concluir**.

Importação de dados do Common Vulnerability Reporting Framework para solução de problemas

As ações de solução de problemas podem ajudar a resolver problemas comuns ao importar dados CVRF na aplicação Vulnerability Response.

Problema	Ação
A duração da execução da integração é longa	Se a integração for executada por um período maior do que o esperado, faça o seguinte: 1. Navegue até a tabela sn_vul_ds_import_q_entry. 2. Agrupar pelo campo **Status**. Você pode ver as entradas, que estão nos estados Concluído, Em andamento ou Na fila.
Falha na integração na importação baseada em API	Se a integração falhar na importação baseada em API, faça o seguinte: 1. Navegue até **Flow Designer**. 2. Abra o fluxo que foi selecionado na configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Problema	Ação
	Nota: No caso da Cisco, abra o fluxo de análise consultiva. 3. Clique **em Execuções**. 4. Abra a execução mais recente ou a execução que deve ser depurada. 5. Verifique o fluxo em cada fase.
Falha na integração na importação baseada em API com um erro de tempo limite	Se a integração falhar em uma importação baseada em API devido ao tempo limite no fluxo de análise de aconselhamento, faça o seguinte: 1. Aumente o tempo limite abrindo sys_properties.LIST. 2. Na coluna Nome, pesquise por sn_vul.CVRFFlowTimeout (inMiliSeconds). **Nota:** O tempo é mostrado em milissegundos. 3. Abra o registro e atualize o valor com um número grande. 4. Salve o registro e execute novamente a integração.
Falha na integração com o erro "O mapeamento do scanner para a transformação de dados de mapeamento do fornecedor está em andamento"	Verifique se a integração falha durante a importação baseada em API ou URL, com o seguinte erro:O mapeamento do scanner para a transformação de dados de mapeamento do fornecedor está em andamento. Os dados serão preenchidos somente após a conclusão da transformação. Tente executar após algum tempo. Se você tiver este erro, aguarde um pouco e execute a integração novamente.
A fila de importação não é criada durante a importação de arquivo	Durante uma importação de arquivo, às vezes a fila de importação não é criada. Esta falha significa que a transformação que mapeia os dados de mapeamento do scanner para os dados de mapeamento do fornecedor está em andamento. A entrada da fila é criada quando o processo é concluído.

Tarefas adicionais Vulnerability Response de instalação e configuração

Para ajudá-lo na correção, você pode executar essas tarefas de configuração administrativa adicionais como parte de sua configuração fora da configuração básica. Você executa essas tarefas fora do Assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode usar o relatório padrão fornecido com Vulnerability Response para supervisionar sua postura de segurança. Você pode editar esses relatórios se eles não se adequarem ao seu ambiente ou usá-los como modelos para criar o seu próprio.

Se a aplicação Performance Analytics para Vulnerability Response estiver instalada, você poderá criar relatórios, painéis dinâmicos e muito mais. Consulte Introdução a relatórios para obter mais informações.

As notificações por e-mail aumentam a produtividade e facilitam o fluxo de trabalho.

Com a Avaliação de exposição de software, pesquise o fornecedor, o nome do produto e o número da versão na Software Asset Management (SAM Foundation) para determinar sua exposição a software vulnerável.

A visibilidade das bibliotecas de vulnerabilidades pode fornecer flexibilidade com tarefas de agrupamento e correção.

Configure o Exception Management para ajudá-lo quando sua organização não puder cumprir uma gestão de vulnerabilidades ou política de segurança, padrão ou diretriz publicada, você poderá solicitar uma exceção.

Para obter mais tarefas de configuração adicionais, consulte os tópicos que seguem esta visão geral.

Testes de início rápido para Vulnerability Response

Valide se Vulnerability Response ainda funciona depois de fazer qualquer alteração na configuração, como aplicar um upgrade ou desenvolver um aplicativo. Copie e personalize esses testes de início rápido para aprovar ao usar seus dados específicos da instância.

A propriedade de execução de teste está desabilitada por padrão para impedir a execução de testes em um sistema de produção. Execute testes somente em instâncias de desenvolvimento, teste e outras que não sejam de produção. Se dados de demonstração ou contas de demonstração forem criados, todos os dados de demonstração deverão ser removidos antes de usar a instância em produção ou não produção. Consulte Executar o pacote de testes do Automated Test Framework (ATF) para Vulnerability Response para obter mais informações sobre como configurar e executar o pacote de testes para Vulnerability Response.

Os testes de início rápido Vulnerability Response exigem a ativação da aplicação Vulnerability Response (sn_vul) e o carregamento dos dados de demonstração.

Testes Vulnerability Response

Teste	Descrição	Versão de lançamento
VR: criar regras de destino de correção	Crie regras de destino de correção.	Madrid
VR: criar regras do grupo de vulnerabilidades	Crie regras do grupo de vulnerabilidades.	Madrid
VR: criar item vulnerável por meio de formulário	Determine se um usuário pode criar com êxito um item vulnerável a partir do formulário de Item vulnerável.	Madrid
VR: ciclo de vida do grupo de vulnerabilidades	Determine se um usuário pode resolver com êxito um grupo de vulnerabilidades.	Madrid

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes Vulnerability Response

Teste	Descrição	Versão de lançamento
VR: ciclo de vida do item vulnerável	Determine se um usuário pode mover com sucesso um item vulnerável durante o ciclo de vida e também se um item vulnerável encerrado pode ser reaberto.	Madrid
VR: calculadora de acúmulo	Determine se a calculadora de risco de acúmulo pode fornecer uma pontuação de risco geral para um grupo inteiro de itens vulneráveis usando as pontuações de todos os itens vulneráveis em um grupo de vulnerabilidade.	New York
VR: regras de atribuição de Vulnerability Response	Determine se um conjunto de exemplo de regras de atribuição pode atribuir automaticamente itens vulneráveis a um grupo de atribuição para correção.	New York
VR: calculadoras de vulnerabilidade	Teste as calculadoras de vulnerabilidade.	New York
VR: Pesquisa de IC - Qualys	Crie uma nova regra de pesquisa com o método "field_matching" chamada "Pesquisa por adaptador de rede" para Qualys. Determine se um item de configuração foi correspondido com êxito na tabela Item descoberto por adaptador de rede e endereço IP com a nova regra de pesquisa.	Orlando
VR: criar solicitação de mudança normal e de emergência	Determine se o usuário pode criar com êxito solicitações de mudança normais e de emergência a partir de um grupo de vulnerabilidades.	Orlando
VR: dividir grupo de vulnerabilidade	Determine se um usuário pode dividir com êxito um grupo de vulnerabilidades.	Orlando
VR: atualize o estado do VG quando um CHG é cancelado.	Determine se o campo Estado em um grupo de vulnerabilidades muda com êxito quando uma solicitação de mudança associada ao grupo de vulnerabilidades é cancelada.	Orlando
VR: atualize o estado do VG quando um CHG muda para revisão.	Determine se o campo Estado em um grupo de vulnerabilidades muda com êxito quando uma solicitação de mudança associada a ele é movida para o estado revisão.	Orlando

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes Vulnerability Response

Teste	Descrição	Versão de lançamento
VR: Pesquisa de IC - Rapid7	Teste a pesquisa de IC usando a regra de pesquisa Rapid7 Vulnerability Integration existente **IP Address**.	Orlando
VR: Pesquisa de IC - Qualys	Teste a pesquisa de IC criando uma nova regra de pesquisa para o Qualys Vulnerability Integration	Orlando
VR: fluxo de trabalho de aprovação de exceção para VI	Crie uma solicitação de exceção e verifique se o processo de aprovação está funcionando.	Orlando
VR: fluxo de trabalho de aprovação falso-positivo para VI	Crie uma solicitação de exceção de falso-positivo e verifique se o processo de aprovação está funcionando.	Orlando
VR: AVR (Application Vulnerability Response)	Determine se suas regras e calculadoras estão funcionando corretamente. Verifique se as atualizações estão funcionando.	Orlando
Regras de destino de correção: teste de importação de VI	Teste as regras de destino de correção de VR durante a importação.	Paris
VR: regra de classificação	Um exemplo de regra de classificação que classifica uma vulnerabilidade automaticamente.	Tokyo

Tópicos relacionados

Testes de início rápido

Executar o pacote de testes do Automated Test Framework (ATF) para Vulnerability Response

Execute o pacote de testes do Automated Test Framework (ATF) depois de instalar ou atualizar a aplicação Vulnerability Response.

Antes de Iniciar

Confirme uma instalação bem-sucedida e que sua instância funciona conforme projetado.

A propriedade de execução de teste está desabilitada por padrão para impedir a execução de testes em um sistema de produção. Execute testes somente em instâncias de desenvolvimento, teste e outras que não sejam de produção. Se dados de demonstração ou contas de demonstração forem criados, todos os dados de demonstração deverão ser removidos antes de usar a instância em produção ou não produção.

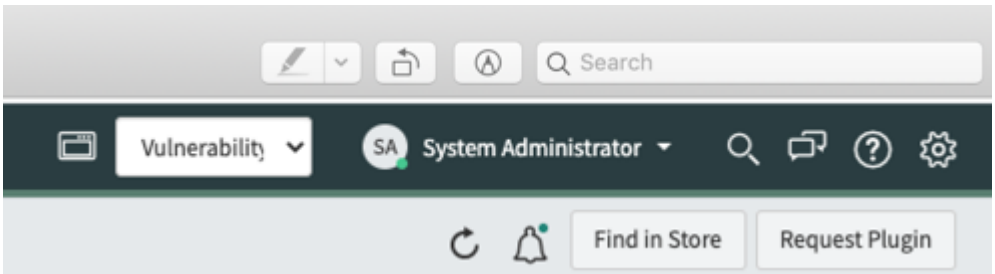
- Verifique se você instalou os dados de demonstração ao instalar o Vulnerability Response. Os dados de demonstração são necessários para executar o pacote de testes Vulnerability Response.
- Para habilitar o teste, siga estas etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegar até **Todos** > **Automated Test Framework (ATF)** > **Administração** > **Propriedades**.
2. Se não estiver selecionado, marque a caixa de seleção **Habilitar execução de teste/ pacote de testes**.
3. Clique em **Salvar**.
4. Se o escopo não estiver definido como **Vulnerability Response** no cabeçalho, ou o escopo não for exibido no cabeçalho, clique no ícone de configurações na parte superior da página na janela do navegador .
5. Na janela Configurações do sistema, clique em **Desenvolvedor**.
6. Se não estiver selecionado, clique em **Mostrar seletor de aplicações no cabeçalho** e feche a janela.
7. Na lista exibida ao lado de Administrador do sistema, clique em **Vulnerability Response** para o campo.

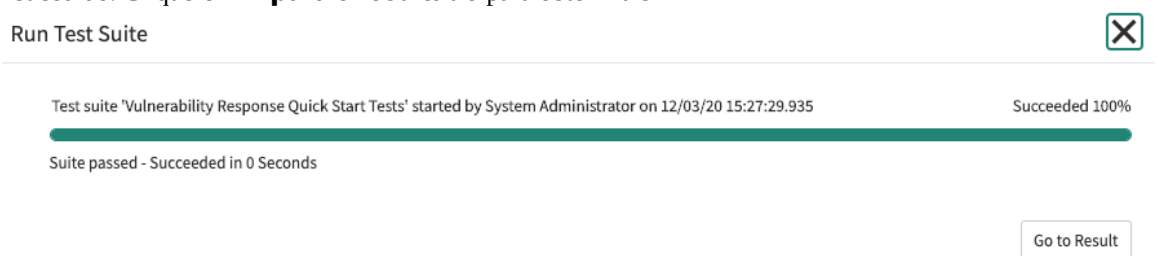
   O campo é exibido conforme mostrado na imagem a seguir.



Função necessária: admin ou atf_test_admin

Procedimento

1. Navegar até **Todos** > **Automated Test Framework (ATF)** > **Pacotes**.
2. Na lista de Pacotes de testes, localize **Testes de início rápido do Vulnerability Response**.
3. Selecione para abrir o registro.
4. No registro aberto, marque a caixa de seleção **Ativo**.
5. Clique em **Atualizar**.
6. Se o botão **Executar pacote de testes** não for exibido, atualize a tela, abra o registro novamente e clique em **Executar pacote de testes** para iniciar o teste.
   Após alguns momentos, a caixa de diálogo Executar Pacote de testes indica um teste bem-sucedido. Clique **em Ir para o resultado** para obter mais



   informações.

O que Fazer Depois

Parabéns! Você pode continuar com a configuração de Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre testes automatizados para Vulnerability Response e testes automatizados, pacotes de testes e criação de testes automatizados, consulte Automated Test Framework (ATF) .

Instalar Recomendações de atribuição de vulnerabilidade para Vulnerability Response

Instale o Recomendações de atribuição de vulnerabilidade para reduzir o tempo gasto na identificação de proprietários para descobertas de vulnerabilidade que não estão atribuídas ou foram atribuídas incorretamente. Esta aplicação está disponível como uma assinatura separada no ServiceNow Store.

Antes de Iniciar

Antes de executar o recurso [Recomendações de atribuição de vulnerabilidade de Vulnerability Response na sua instância Now Platform®, você deve primeiro baixar e instalar a aplicação Recomendações de atribuição de vulnerabilidade para Vulnerability Response. Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de não produção ou de desenvolvimento, não será necessário obter direitos. Para obter mais informações, consulte Ativação de uma aplicação da ServiceNow Store.

Função necessária: administrador

Tarefas de configuração	Ação
Verifique se a aplicação Vulnerability Response está instalada e ativada.	Navegar até **Todos** > **Aplicações do sistema** > **Todas as aplicações** > **Instalado em sua instância**. Vulnerability Response será mostrado nesta lista se estiver instalado. Se a aplicação não estiver instalada e ativada, consulte Como instalar Vulnerability Response.
Verifique se a aplicação Inteligência preditiva está instalada e ativada.	Navegar até **Aplicações do sistema** > **Todas as aplicações** > **Instalado em sua instância**. Inteligência preditiva será mostrado nesta lista se estiver instalado. Se a aplicação não estiver instalada e ativada, consulte Install Predictive Intelligence .
Verifique se você tem as funções ServiceNow necessárias para sua instância.	Verifique se você tem estas funções necessárias para instalação e verificação dos resultados esperados: • vulnerabilidade_admin: necessário para habilitar e configurar Recomendações de atribuição de vulnerabilidade. Você também pode usá-lo para exibir e selecionar

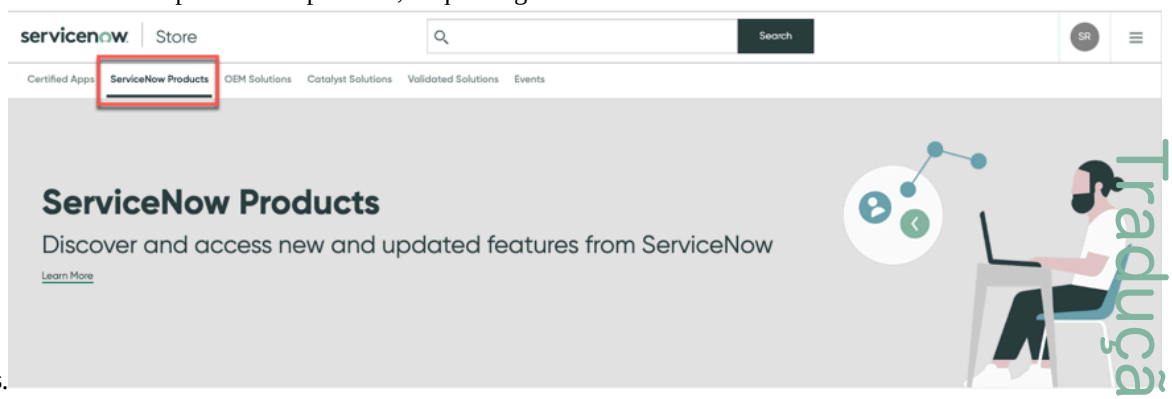
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Ação
	recomendações de atribuição para itens vulneráveis e tarefas de correção. • ServiceNow admin: necessário para instalar aplicações.

Procedimento

1. Navegue até o ServiceNow Store.
2. Clique **em Fazer login** e insira suas credenciais HI.
3. Para exibir os ServiceNow produtos disponíveis, clique na guia ServiceNow **Produtos**.



4. Para exibir todas as aplicações associadas que você está atribuindo para Recomendações de atribuição de vulnerabilidade, clique no produto Vulnerability Response.

   A página lista todas as aplicações para as quais você está qualificado se aceitar. Para obter informações sobre uma aplicação, clique no link da aplicação.

5. Para verificar se você tem direito a Recomendações de atribuição de vulnerabilidade, clique em **Aceitar**.
6. Para concordar com os termos e condições, no prompt, marque a caixa de seleção e clique em **Aceitar**.
   Uma mensagem é exibida indicando que você aceitou a aplicação com sucesso.
7. Pule para a etapa 10 para instalar a aplicação na sua instância Now Platform.
8. **Opcional:** Se você quiser gerenciar seu direito da aplicação Recomendações de atribuição de vulnerabilidade em outras instâncias Now Platform, clique em **Gerenciar direito**.

   Nota:

   (Optional) Se o botão **Gerenciar direito** não for exibido, clique na aplicação Recomendações de atribuição de vulnerabilidade na lista de produtos para exibi-lo.

   a. Escolha uma opção.

   b. Clique em **OK** ou em **Cancelar** para continuar.
   Você está pronto para ativar plug-ins e instalar a aplicação em suas instâncias Now Platform.
9. Faça login na instância Now Platform na qual você deseja instalar a aplicação Recomendações de atribuição de vulnerabilidade.
10. Navegar até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
11. Entre as aplicações listadas, localize a aplicação Recomendações de atribuição de vulnerabilidade (sn_vul_recom) e clique em **Instalar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A caixa de diálogo de instalação da aplicação é exibida e todas as dependências instaladas são exibidas.

12. **Opcional:** Se você quiser dados de demonstração, marque a caixa de seleção **Carregar dados de demonstração** e clique em **Instalar**.

    Nota:
    Se você não marcar a caixa de seleção **Carregar dados** de demonstração, os dados de demonstração não ficarão disponíveis para instalação no Gerenciador de aplicações posteriormente. Para obter informações sobre como instalar ou reinstalar os dados de demonstração após a instalação inicial, consulte o artigo Solução alternativa para instalar dados de demonstração se a aplicação já estiver instalada [KB0722909] na Base de conhecimento Now Support.

    Esta instalação pode levar algum tempo. Uma mensagem é exibida na caixa de diálogo Instalar depois que a aplicação e suas dependências são instaladas com sucesso.

13. Clique em **Fechar**.

14. Para configurar Recomendações de atribuição de vulnerabilidade, consulte Configurar recomendações de atribuição de vulnerabilidade para Vulnerability Response.

Configurar recomendações de atribuição de vulnerabilidade para Vulnerability Response

Habilite Recomendações de atribuição de vulnerabilidade para reduzir o tempo gasto na identificação dos responsáveis pelas descobertas de vulnerabilidade que não estão atribuídas ou foram atribuídas incorretamente.

Antes de Iniciar
Função necessária: sn_vul.manage_assignment_recom_config

Por Que e Quando Desempenhar Esta Tarefa
Esta aplicação não está habilitada por padrão.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Recomendações de atribuição**.
2. Selecione **Habilitar recomendações de atribuição**.
   O **campo de definição da solução Predictive Intelligence é** exibido. O valor padrão é **Atribuição de item vulnerável**.
3. Clique em **Salvar**.

Criar e treinar uma definição de solução para Vulnerability Response

Crie e treine um modelo de definição de solução para Vulnerability Response usando Inteligência preditiva. Você pode usar este modelo para prever o grupo de atribuição para um item vulnerável (IV) ou tarefa de correção (RT) com base nos dados existentes.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Predictive Intelligence** > **Classificação** > **Definições de solução**.
2. No formulário Definições de classificação, clique em **Atribuição de item vulnerável**.
   Esta é a definição de solução padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- A frequência de treinamento padrão é de 30 dias. Isso significa que a cada 30 dias, o modelo é treinado novamente automaticamente usando o conjunto de dados de IV que corresponde à condição do filtro configurada.
- Os campos da tabela Item vulnerável podem ser usados para treinamento. A definição de solução padrão é treinada em dois campos de IV: **Vulnerability.Summary** e **Configuration item.Name**. Você pode personalizar os campos usados para treinamento, dependendo de quais campos você considera úteis para prever a propriedade da vulnerabilidade em sua organização.

3. Para criar e treinar a solução de classificação, consulte Criar e treinar uma solução de classificação .

Nota:
Você também pode criar e treinar uma semelhança ou uma solução de clustering. Para obter mais informações, consulte:

- Crie e treine uma solução de semelhança .
- Crie e treine uma solução de clustering .

4. Clique em **Atualizar e treinar novamente**.

Nota:
Para definir configurações avançadas para soluções de ML, consulte Como definir configurações avançadas para suas soluções de ML .

Criar uma calculadora Vulnerability Response

Uma calculadora de vulnerabilidade é uma fórmula predefinida para calcular um campo de destino quando determinados critérios são atendidos. As calculadoras, que calculam a **pontuação de risco**do item vulnerável, podem conter **regras de risco**.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Nota:
Você pode observar uma degradação no desempenho ao executar calculadoras de vulnerabilidade que contêm scripts.

Ordene que suas regras executem as regras mais simples primeiro e execute somente scripts nos itens que não podem ser tratados com uma condição e valor de modelo ou uma regra de risco.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Calculadoras de vulnerabilidade**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Calculadora de vulnerabilidade

Campo	Descrição
Nome	O nome da calculadora de vulnerabilidade.
Tabela	Preenchido automaticamente com o nome da tabela de item vulnerável.
Aplicação	Preenchido automaticamente com Vulnerability Response.
Campo de destino	Campo a ser calculado.
Descrição	Descrição de texto da calculadora.
Ativo	Liga ou desliga a calculadora.

4. Clique com o botão direito do mouse no cabeçalho para **Salvar**.
   A seção **Regras da calculadora de vulnerabilidade** é exibida.
5. Crie uma regra para a calculadora clicando em **Novo**.

> **Nota:**
> Para obter o formulário **Novas regras de risco** (disponível somente quando o **campo Destino** for **Pontuação de risco**), consulte a etapa 10.

6. Preencha os campos, se for o caso.

Formulário Regra da Calculadora de Vulnerabilidade

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual a calculadora de vulnerabilidade será executada. Uma calculadora com uma entrada de ordem de 100 é executada antes de uma calculadora com uma entrada de ordem de 200.
Calculadora	Preenchido automaticamente com a calculadora primária.
Ativo	Por padrão, a caixa de seleção **Ativa** está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará aos novos itens vulneráveis criados no sistema.
Exibição avançada	Quando selecionadas, as condições de script e os valores de script podem ser selecionados em Tipo de **condição** e **Tipo de valor**.

7. Preencha os campos na guia **Quando esta condição for atendida**, conforme apropriado.

Guia Quando esta condição for atendida

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual a calculadora de vulnerabilidade será executada. Uma calculadora com uma entrada de ordem de 100 é executada antes de uma calculadora com uma entrada de ordem de 200.
Calculadora	Preenchido automaticamente com a calculadora primária.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ativo	Por padrão, a caixa de seleção **Ativa** está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará aos itens vulneráveis criados no sistema.
Exibição avançada	Quando selecionado, selecione condições de script e valores de script em Tipo de **condição e Tipo** de **valor**.
Tipo de condição	Disponível quando você seleciona a **exibição Avançado**. As opções incluem: ○ Filtro: usa condições de filtro. ○ Grupo de filtros: consulte Criar um novo grupo de filtros para definir os critérios da calculadora. ○ Script: condição de script usada para determinar quando aplicar esta calculadora. **Nota:** Antes de escrever scripts para determinar quando aplicar as calculadoras, retorne à lista **Calculadoras de vulnerabilidade**. Explore os registros da calculadora de vulnerabilidade enviados com o sistema de base.
Condição	Define condições básicas de filtro para determinar se a calculadora deve ser usada ou não. Selecionar o **grupo de filtros** ou os tipos de condição de **script** oculta este campo. A diferenciação de maiúsculas e minúsculas para o texto de pesquisa inserido no construtor de condição não é compatível com este registro ou formulário.

8. Clique na guia **Definir estes valores** e preencha os campos no formulário, conforme apropriado.

Guia Definir estes campos

Campo	Descrição
Tipo de valor	Disponível quando você seleciona a **exibição Avançado**. As opções incluem: ○ Modelo: defina os valores a serem definidos em cada campo. ○ Script: usado para definir os valores em cada campo.
Valores de Script	Disponível se você selecionou o tipo de valor de **Script**. Define a quais valores os cálculos serão aplicados.
Modelo	Selecione os campos e valores que você deseja usar para a calculadora. Selecionar o tipo de valor de **Script** oculta este campo.

9. Quando tiver concluído todas as entradas, clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Ao editar uma calculadora existente e quiser atualizar todas as pontuações existentes, você pode usar o botão **Reaplicar Calculadora**. Ele é executado em todos os itens vulneráveis (IVs) ativos e, se essa calculadora for usada para definir seu valor, recalcula o valor desses IVs. Como a reaplicação de uma calculadora pode levar muito tempo, um trabalho programado lida com isso.

10. Para o formulário **Novas regras de risco**, preencha os campos conforme apropriado.

Defina cada peso de acordo com a porcentagem do resultado que deve vir desse valor. Para quaisquer dados que o seu scanner não forneça, ou para dados que não devam fazer parte da pontuação de risco, defina o peso como zero.

Você pode adicionar, excluir ou atualizar os campos. Você também pode configurar a porcentagem de ponderação dos valores de campo. Para obter mais informações, consulte Definir campos e pesos para a regra de risco das Calculadoras de risco do Vulnerability Response.

Conforme você atualiza os pesos, os cenários exibem os pesos restantes, bem como os resultados da **Pontuação de risco** antecipada.

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual a calculadora de vulnerabilidade será executada. Uma calculadora com uma entrada de ordem de 100 é executada antes de uma calculadora com uma entrada de ordem de 200.
Calculadora	Preenchido automaticamente com a calculadora primária.
Ativo	Por padrão, a caixa de seleção **Ativa** está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará aos novos itens vulneráveis criados no sistema.
Condição	Define condições básicas de filtro para determinar se a calculadora deve ser usada. Selecionar o **grupo de filtros** ou os tipos de condição de **script** oculta este campo.
Ponderações	
Severidade da Vulnerabilidade	Percentual do resultado proveniente da severidade.
Pontuação de EPSS de vulnerabilidade	Probabilidade da vulnerabilidade ser explorada. Por padrão, o peso desses critérios é zero. Se você quiser usar isso para o cálculo da pontuação de risco, defina um peso apropriado em relação a esses critérios.
Explorar itens existentes	Percentual do resultado proveniente da existência de uma exploração. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.
Nível de habilidade Exploit	Porcentagem do resultado que vem do nível de habilidade exigido pela exploração. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.
Vetor de ataque Exploit	Percentual do resultado que vem de onde o ataque é direcionado. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.

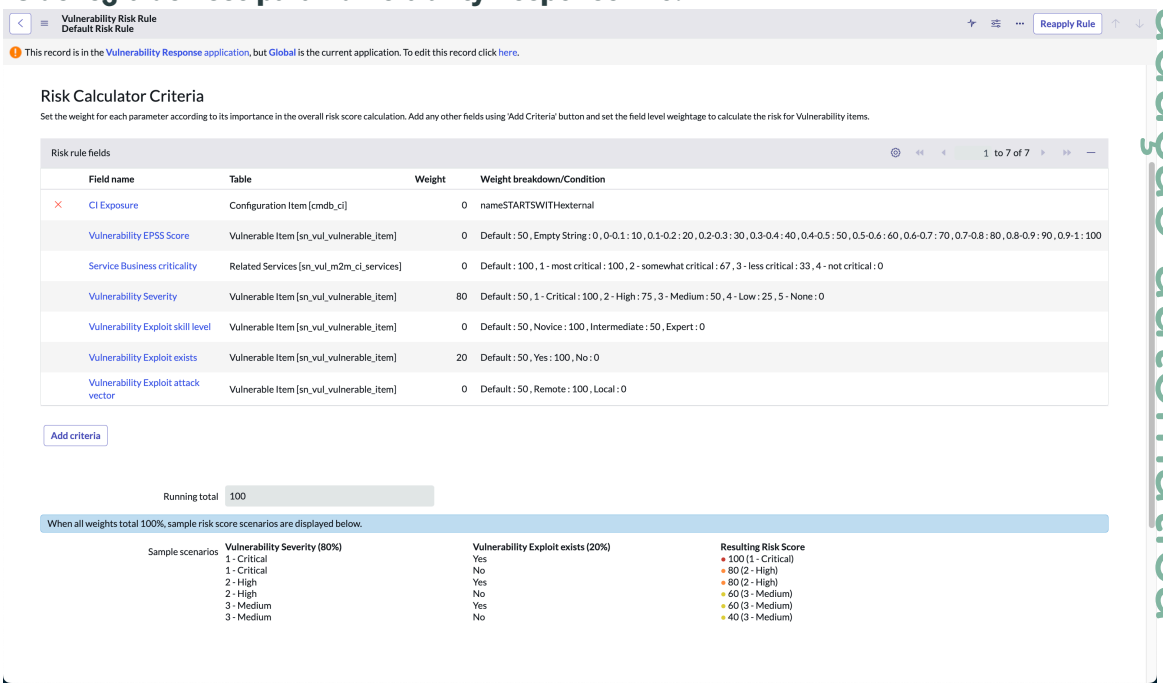
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Criticalidade dos negócios de serviço	Percentual do resultado proveniente da criticidade dos negócios. Se você não vinculou seus ICs aos serviços de negócios, defina o peso como zero.
Exposição de IC	Porcentagem do resultado que vem de se o IC é voltado para a internet. Se o peso for diferente de zero, um filtro de condição será exibido para definir quais ICs estão voltados para a Internet. Defina o filtro para selecionar os itens de configuração voltados para a Internet. Você pode visualizar quais registros correspondem à condição.
Total da execução	Percentuais totais calculados automaticamente. Quando esse valor atinge 100, a visualização de cenário mostra amostras de pontuações de risco em diferentes cenários.
Cenários de pontuação de risco	Quando todos os pesos totalizam 100%, os cenários de pontuação de risco são exibidos, fornecendo uma visualização da pontuação de risco em alguns dos cenários possíveis.

Você pode adicionar ou remover critérios e ajustar o peso de cada critério usando a lista integrada.

IC de regra de risco para Vulnerability Response v20.x



Tradução automática

11. Clique em **Enviar**.

Desabilitar a calculadora de vulnerabilidade padrão se não for usada

Se você não usar calculadoras de vulnerabilidade, desabilite a calculadora padrão, além de todas as outras que você definiu. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é criado ou atualizado e podem afetar o desempenho da importação inicial.

Antes de Iniciar

Função necessária: administrador

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Calculadoras de vulnerabilidade**.
2. Abra a calculadora relevante.
3. Desmarque a caixa de seleção **Ativo** para desativar a calculadora.
4. Clique em **Atualizar**.

Criar, habilitar ou modificar Vulnerability Response regras de exclusão automática

Você pode criar, habilitar ou modificar as regras de exclusão do item de vulnerabilidade (IV) e da tarefa de correção (RT). Use a exclusão automática para remover registros mais antigos das tabelas IV e RT.

Antes de Iniciar

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Funções necessárias:

- administrador: modificar as regras de exclusão automática
- sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto): exibir o módulo de exclusão automática

Por Que e Quando Desempenhar Esta Tarefa

Com o tempo, uma grande quantidade de registros encerrados provavelmente se acumulará nas tabelas IV e VUL da sua instância. Muitos desses registros podem ter sido encerrados por mais de 365 dias, mas não foram removidos. Use regras de exclusão automática para remover muitos desses registros encerrados mais antigos. A remoção desses registros não apenas reduz significativamente o número de registros nas tabelas IV e VUL, como também ajuda a manter o alto desempenho.

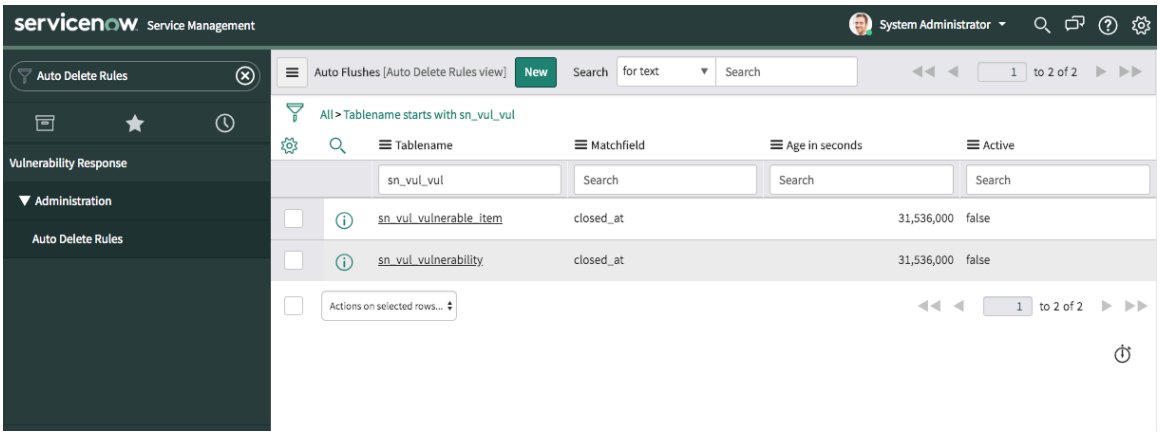
Embora os registros de destino da exclusão automática por padrão tenham sido encerrados por 365 dias, a primeira execução pode tentar limpar muitos registros em uma única transação. Dependendo do tamanho do seu ambiente, talvez você prefira escalonar o processo de exclusão para limitar o escopo da consulta. Por exemplo, você pode iniciar sua primeira execução para registros encerrados com mais de 450 dias. Depois que a execução for concluída, você poderá trabalhar em incrementos menores (425, 400, 375) até reduzir o número de registros com mais de 365 dias.

Há duas regras fornecidas com o Now Platform® que excluem automaticamente os registros encerrados que atendem às condições especificadas junto com todos os registros que se referem a eles. Uma regra exclui itens vulneráveis e a outra regra exclui tarefas de correção. Por padrão, essas regras de exclusão automática estão desabilitadas, portanto, você precisa ativá-las manualmente antes de excluir qualquer registro. Você pode escolher as duas regras pré-configuradas fornecidas com sua instância ou pode criar a sua própria.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de exclusão automática**.
   A exibição de lista é exibida.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



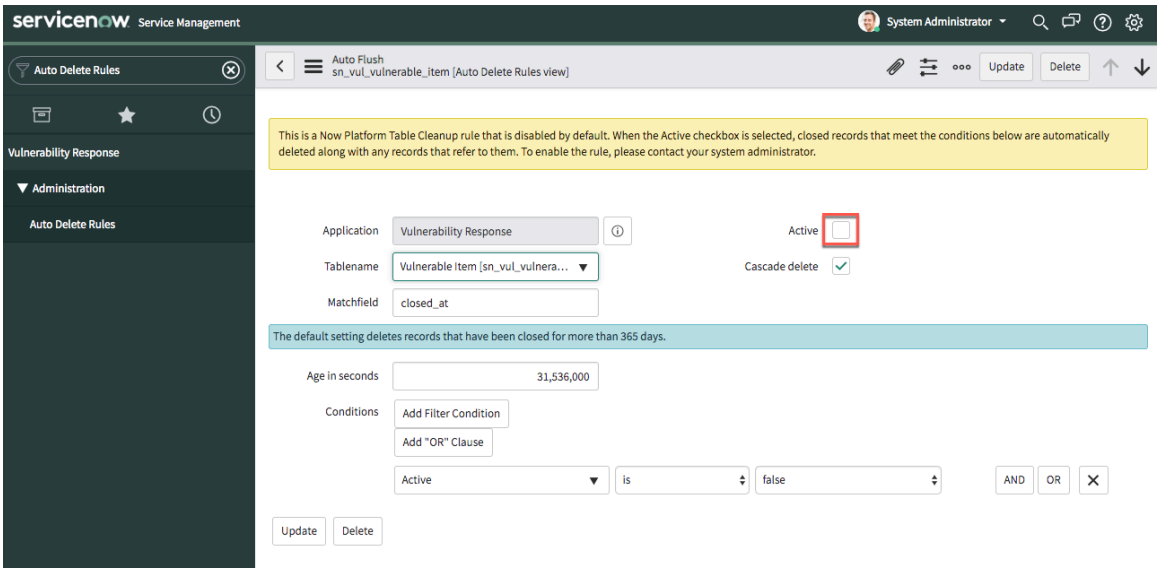
2. Para editar, selecione a regra de exclusão para itens vulneráveis (sn_vul_vulnerable_item) ou a regra para tarefas de correção (sn_vul_vulnerability).
3. Para criar uma nova regra, clique em **Novo**.
4. Preencha ou edite os campos no formulário, conforme apropriado.

Campo	Descrição
Aplicação	Nome da aplicação na qual os registros estão sendo excluídos. O valor padrão é Vulnerability Response.
Nome da tabela	Nome da tabela para a qual a regra está sendo aplicada.
Campo de correspondência	Campo para o qual o sistema monitora a duração.
Ativo	Opção para ativar a regra. Depois de ativado, o registro pode ser excluído.
Exclusão em cascata	Opção para excluir todos os registros correspondentes, além de todos os registros que se referem a eles. Se esta opção não for selecionada, somente os registros correspondentes serão excluídos, mas não os registros que se referem a eles.
Idade em segundos	Idade do registro de vulnerabilidade a ser excluído. Para as regras de IV e RT, a idade é de 365 dias. Essa idade é exibida em segundos.
Condições	Condições de filtro que definem os registros nas tabelas IV e RT (VUL) às quais as regras se aplicam.

5. Marque a caixa de seleção **Ativa** para ativar uma regra.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Depois que a regra é ativada, a função da plataforma por hora, **Limpeza automática**, exclui os registros da tabela para a qual a regra está ativada.

Se o seu ambiente tiver milhões ou dezenas de milhões de registros que correspondam aos seus critérios de exclusão, consulte o suporte ao cliente ServiceNow antes de habilitar as regras de exclusão automática para ajudá-lo a excluir registros usando um processo em fases.

Adicionar gráficos de significância da vulnerabilidade à página inicial do Vulnerability Response

Você pode adicionar gráficos de definição de significância de vulnerabilidade e outras visualizações à Visão geral.

Antes de Iniciar

- Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.
- O plug-in Vulnerability Analytics deve ser ativado.

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Visão geral**.
   Alguns relatórios são adicionados ao painel por padrão. Para obter mais informações sobre esses relatórios, consulte Usando os painéis padrão Vulnerability Response.
2. Próximo ao cabeçalho do painel, clique no ícone de exibição do cartão ícone + de adição **Adicionar conteúdo** para abrir a caixa de diálogo e adicionar mais widgets.
3. Nas listas da caixa de diálogo **Adicionar widgets**, selecione **Relatórios** para exibir mais relatórios Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique no local na tela que você deseja adicionar o medidor.
5. Feche a caixa **Adicionar conteúdo**.

Definir Vulnerability Response notificações por e-mail

Configure notificações por e-mail para compartilhar informações úteis sobre atualizações e atividades importantes, como aprovação e rejeição de solicitações de falso-positivos. Criar uma notificação por e-mail envolve especificar quando enviá-la, quem a recebe e o que ela contém.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Modelos de e-mail**.
2. Selecione **Novo**.

Para obter instruções detalhadas para criar notificações por e-mail, consulte Create an email notification .

Resultado

A partir da v21.0 do Vulnerability Response, quando um destinatário clica nos links de uma notificação por e-mail, os registros são abertos no Vulnerability Manager Workspace ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos no Vulnerability Manager Workspace para os usuários com as funções, sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager ou sn_vul_container.vulnerability_admin.
- Links abertos no Espaço de correção de problemas de TI para os usuários com funções, sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_ownerou sn_vul.app_developer.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Definir modelos de e-mail do Vulnerability Response

Criar uma notificação por e-mail envolve especificar quando enviá-la, quem a recebe e o que ela contém.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Modelos de e-mail**.
2. Selecione **Novo**.

Para obter instruções detalhadas para criar modelos de e-mail, consulte Construct an email message with a template .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar ou editar notificações de destino de correção

Os administradores de vulnerabilidade podem editar a notificação de destino de correção ou adicionar novas, especificando quando enviar a notificação, quem recebe a notificação e qual conteúdo está na notificação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Notificações**.
2. Selecione o registro de notificação de destino de correção ou selecione **Novo**.
3. Preencha os campos no formulário, conforme apropriado.
   Para obter mais informações sobre os campos de formulário, consulte Create an email notification .
4. Selecione **Visualizar notificação** para exibir a mensagem.

Resultado

A partir da v21.0 do Vulnerability Response, quando um destinatário clica nos links de uma notificação por e-mail, os registros são abertos no Vulnerability Manager Workspace ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos no Vulnerability Manager Workspace para os usuários com as funções, sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager ou sn_vul_container.vulnerability_admin.
- Links abertos no Espaço de correção de problemas de TI para os usuários com funções, sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_owner, ou sn_vul.app_developer.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Configurar avaliação de exposição

Para avaliar a exposição de dia zero (dia atual) de seus ativos a software vulnerável com a aplicação Avaliação de exposição, primeiro verifique se a aplicação Gestão de ativos de software ITSM está instalada.

Com a função de gravação de vulnerabilidade, (sn_vulnerability_write), você pode exibir o módulo Avaliação de exposição e criar e editar registros de avaliação de exposição sob demanda para software vulnerável em sua instância com a aplicação Vulnerability Response.

Requisitos de compatibilidade e sistema

A aplicação Vulnerability Response está disponível no ServiceNow Store. A aplicação Gestão de ativos de software ITSM (com.snc.asset_management) é necessária para o módulo Avaliação de exposição. Esta aplicação gerencia todos os seus ativos e licenças de software, e a versão SAM Foundation desta aplicação faz parte da aplicação Vulnerability Response que você baixou do ServiceNow Store. A aplicação Exposure Assessment funciona com as aplicações SAM Foundation ou SAM Pro Now Platform®.

A aplicação SAM Pro não faz parte do produto principal Vulnerability Response da ServiceNow Store e requer uma assinatura separada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para verificar se a aplicação SAM Foundation está instalada em sua instância, navegue até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e pesquise por com.snc.asset_management. Se a aplicação não estiver instalada, clique em **Instalar**.

Como a aplicação de avaliação de exposição requer acesso aos dados de ativos em sua instância Now Platform®, as aplicações de gestão de ativos devem ter dados para referência. A tabela de modelos de descoberta de software (cmdb_sam_sw_discovery_model) e as instalações de software (cmdb_sam_sw_install) exigem dados.

Tópicos relacionados

Avalie sua exposição a software vulnerável

Configurar Gestão de exceções para Vulnerability Response

Quando sua organização não pode estar em conformidade com uma gestão de vulnerabilidades ou política de segurança, padrão ou diretriz publicada, você pode solicitar uma exceção. A gestão de exceções envolve solicitar, revisar, aprovar ou rejeitar exceções a um item vulnerável (IV) ou tarefa de correção (RT) que não pode ser corrigida de acordo com a política.

Antes de Iniciar

Limite a duração de uma exceção solicitada e adicione um questionário à exceção ou à solicitação de falso-positivo usando o módulo Vulnerability Response. Por padrão, uma exceção é solicitada usando o módulo ServiceNow® Vulnerability Response. Você também pode solicitar uma exceção usando a integração GRC: Policy and Compliance Management.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Função necessária: sn_vul.manage_exception_configuration

Por Que e Quando Desempenhar Esta Tarefa

Se Vulnerability Response estiver habilitado, você poderá limitar a duração pela qual uma exceção pode ser solicitada. Da mesma forma, se o módulo GRC: Policy and Compliance Management estiver instalado, você poderá selecionar GRC: Policy and Compliance Management na tela de configuração. Habilitar esta opção permite solicitar uma exceção que especifica a política e o objetivo de controle de GRC.

Se você adicionar um questionário, ele será enviado para a pessoa que gerou a exceção ou a solicitação de falso-positivo. Você pode usar o questionário padrão ou criar um com base em seus requisitos.

É útil que o aprovador de exceção entenda o motivo da solicitação da exceção.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Gestão de exceção**.
2. No formulário Configuração de gestão de exceções, selecione como você deseja gerenciar uma exceção selecionando uma opção na lista **Gerenciar exceções usando**.
   Você pode selecionar Vulnerability Response ou GRC: Policy and Compliance Management. Você deve ativar o plug-in GRC para usar GRC: Policy and Compliance Management para solicitar uma exceção. Alterar a configuração não afeta os dados existentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Se você selecionou a opção Vulnerability Response, insira as seguintes informações:

Configurações do formulário de gestão de exceções de VR

Campo	Descrição
Duração	Período para o qual uma exceção pode ser solicitada.
Unidade	Unidade de tempo para o período especificado.
Habilitar questionário para solicitar exceção	Opção para adicionar um questionário à solicitação de exceção que está sendo gerada.
Questionário para solicitar exceção	Exibe o questionário selecionado por você para solicitar uma exceção. O **Questionário de exceção** é exibido por padrão. **Nota:** Este campo é exibido somente quando você marca a caixa de seleção **Habilitar questionário para solicitar exceção**.
Questionário para controle de compensação	Exibe o questionário que um proprietário de correção deve responder para solicitações de redução de risco. A partir da v20.0 de Vulnerability Response, você pode definir questionário para solicitações de redução de risco. O **Questionário de controle de remuneração** é selecionado por padrão. **Nota:** Este campo é exibido somente quando você marca a caixa de seleção **Habilitar questionário para solicitar exceção**.
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso-positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Exibe o questionário selecionado por você para marcar como falso positivo. O questionário para solicitação de falso-positivo é exibido por padrão. **Nota:** Este campo é exibido somente quando a caixa de seleção **Habilitar questionário para marcar como falso-positivo** está marcada.

Se você personalizou o questionário existente e atualizou para v20.0, esse questionário personalizado aparecerá para a solicitação de redução de risco em vez do **Questionário de controle de compensação**padrão.

4. Se você selecionou a opção GRC: Policy and Compliance Management, insira as seguintes informações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações do formulário de gestão de exceções de VR

Campo	Descrição
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso-positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Exibe o questionário selecionado por você para marcar como falso positivo. O questionário para solicitação de falso-positivo é exibido por padrão.

5. Para configurar questionários com base em condições para solicitações de exceção e falso-positivo:

   a. Na seção Configuração do questionário de VR, selecione **Novo**.

   b. No formulário Configuração de questionário - Novo registro, preencha os campos e selecione **Enviar**.
   Para obter mais informações sobre os campos de formulário de Configuração de questionário, consulte Campos de formulário de configuração de questionário.
   O questionário criado aparece na seção Configuração do questionário de VR do formulário Configurações para gestão de exceções de VR.

   Por exemplo, se você quiser configurar o questionário para solicitações de falso-positivos para itens vulneráveis críticos, selecione a regra de aprovação **Falso-positivo para itens vulneráveis**, forneça a condição como Classificação de `risco é 1 - Crítico` e selecione o questionário desejado no formulário Configuração do questionário.

6. Selecione **Salvar**.

Adicionar um aprovador de exceção

Adicione usuários aos grupos de aprovadores para que você possa solicitar uma exceção.

Antes de Iniciar

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa

Até Vulnerability Response v14.0, uma solicitação de exception para um item vulnerável ou tarefa de correção é aprovada usando o fluxo de trabalho de aprovação de dois níveis padrão. A solicitação deve ser aprovada por dois níveis de aprovadores.

Nota:
Até Vulnerability Response v14.0, se não houver nenhum aprovador de primeiro nível, uma exceção não poderá ser solicitada. No entanto, a partir de Vulnerability Response v15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Grupos**.
2. Na coluna Nome, pesquise por **Exceção**e clique em **Aprovador de exceção - Nível 1**.

> **Nota:**
> A partir de Vulnerability Response v12.8.1, você pode usar as propriedades do sistema fornecidas no sistema de base para aprovações de exceção por meio do fluxo de trabalho na tabela Propriedades do sistema [sys_properties]. Portanto, quando uma solicitação de falso-positivo ou exceção é gerada por meio do fluxo de trabalho, ela é enviada para aprovação dos IDs de grupo definidos na propriedade do sistema. Navegar até **Todos** > **Propriedades do sistema** e selecione *`sn_vul.exception_approver_L1`*, *`sn_vul.exception_approver_L2`*ou *`sn_vul.false_positive_approver_group`* para mudar o valor da propriedade.

3. No formulário Aprovador de exceção do grupo - Nível 1, clique na lista relacionada Membros do grupo.
4. Clique em **Novo** para criar uma lista.
5. No formulário, preencha os campos.

Formulário do usuário

Campo	Descrição
ID do usuário	Identificador exclusivo do usuário.
Nome	Nome do usuário.
Sobrenome	Sobrenome do usuário.
Título	Cargo do usuário. Insira um título ou descrição do trabalho ou selecione um na lista.
Departamento	Departamento do usuário.
Senha	Senha atribuída ao usuário. Esta senha pode ser permanente ou temporária.
A senha precisa ser redefinida	Opção para permitir que o usuário redefina a senha para garantir a segurança.
Bloqueado	Opção para bloquear a saída do usuário da instância e encerrar todas as sessões ativas do usuário. O sistema evita que usuários com a função de administrador se bloqueiem.
Ativo	Opção para tornar este usuário ativo. Somente você pode ver um usuário inativo nestas áreas: ○ Listas de usuários ○ Lista de seleção nos campos de referência (ícone de lupa) ○ Lista de preenchimento automático que aparece quando você digita em um campo de referência
Acesso somente ao serviço Web	Opção para designar este usuário como um usuário não interativo.
Usuário de integração interna	Opção para designar este usuário como um usuário de integração interna.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
E-mail	Endereço de e-mail do usuário.
Idioma	Idioma preferencial do usuário.
Integração de calendário	Calendário usado para gerenciar a programação de trabalho. Por exemplo, Outlook.
Fuso horário	Fuso horário para a localização deste usuário.
Formato de data	Formato preferencial do usuário para datas.
Telefone comercial	Telefone comercial do usuário.
Telefone celular	Telefone celular do usuário.
Foto	Foto que você pode carregar clicando em **Clique para adicionar...**.

6. Clique em **Enviar**.
7. Repita as etapas 1 a 5 para criar um Aprovador de exceção - Nível 2.
   O aprovador deve navegar até **Vulnerability Response** > **Minhas aprovações** e aprovar as solicitações.

Nota:
Para aprovar uma exceção para GRC: Policy and Compliance Management, consulte Configuração opcional do Policy and Compliance Management .

Configurar regras de aprovação para Gestão de exceções

A partir da Vulnerability Response v15.0, use o Flow Designer para aprovar solicitações de exceção para gestão de exceções, regras de exceção e gestão de falsos positivos. Se você estiver implantando Vulnerability Response (VR) pela primeira vez, o Flow Designer será habilitado por padrão.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Se você for um usuário de VR existente, a opção padrão será fluxo de trabalho.
Se você implantou Vulnerability Response v15.0 ou posterior, o valor da propriedade do sistema *sn_vul.flow_designer_activation* será definido como verdadeiro. Isso significa que o Flow Designer está habilitado por padrão.

Se você já estiver usando Vulnerability Response antes da v15.0, o valor desta propriedade do sistema será definido como falso. Você pode ativar o Flow Designer alterando o valor para verdadeiro.

Nota:
Você não pode reverter para usando o fluxo de trabalho depois de ativar o Flow Designer. Para obter uma comparação detalhada entre o fluxo de trabalho e o Flow Designer, consulte Fluxo de trabalho de gestão de exceções versus Flow Designer.

Para usar o Flow Designer, crie regras usando o módulo Regras de aprovação. Usando este módulo, você pode configurar regras de aprovação para cada um dos seguintes fluxos de trabalho de gestão de exceções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Solicitação de exceção para tarefas de correção
- Solicitação de exceção para itens vulneráveis
- Regra de exceção
- Falso-positivo para tarefas de correção
- Falso positivo para itens vulneráveis

Nota:
Você também pode definir condições que contenham vários níveis de aprovação em uma regra. O Flow Designer herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente. Para obter informações sobre como configurar níveis de aprovação, consulte Criar níveis de aprovação para a Gestão de exceções.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de aprovação**.
2. Na página Regras de aprovação, selecione o grupo para o qual você deseja definir a regra de aprovação.
3. No formulário, preencha os campos.

Formulário Regra de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Tabela	Tabela na qual a regra é aplicada.
Aplicação	O valor padrão é Vulnerability Response.
Tipo de regra	Especifica o tipo de regra. Por exemplo, gestão de exceções, falso-positivo ou regra de exceção.
Ativo	Habilitado por padrão, o que significa que a regra de aprovação está em uso.
Descrição	Descrição resumida das regras de aprovação.
Expiração da aprovação (dias) A partir da v21.0 de Vulnerability Response	Data até quando o aprovador pode aprovar a solicitação.
Aprovador do Notify (dias) A partir da v21.0 de Vulnerability Response	Data após a qual o aprovador é notificado para agir.

4. Selecione **Atualizar**.
   Na guia Configurações de aprovação, há dois níveis de aprovadores configurados por padrão. Você pode selecionar uma regra para definir as condições com base em diferentes casos de uso em uma regra. Para obter mais informações, consulte Criar configurações para uma regra de aprovação.

Nota:
Em cada página de configuração, você pode criar vários níveis de aprovação. Para obter mais informações, consulte Criar níveis de aprovação para a Gestão de exceções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example:
Com base em diferentes casos de uso, você pode definir diferentes processos de aprovação para as mesmas vulnerabilidades encontradas em diferentes itens de configuração.

Criar configurações para uma regra de aprovação

Defina as condições para filtrar itens vulneráveis correspondentes, tarefas de correção ou regras de exceção para um nível de aprovação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
No módulo Configurações de aprovação, você pode configurar vários níveis de aprovação para diferentes configurações. Defina regras baseadas em condição, com cada regra contendo vários níveis de aprovação.

Nota:
Use o módulo Regras de aprovação para configurar regras de aprovação para os fluxos de trabalho de gestão de exceções. Para obter informações sobre como configurar regras de aprovação, consulte Configurar regras de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de aprovação**.
2. Selecione uma regra de aprovação e navegue até a guia **Configurações de aprovação**.
3. Selecione uma configuração.
4. No formulário, preencha os campos.

Formulário Configuração de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Ativo	Habilitado por padrão, o que significa que a configuração de aprovação está em uso.
Descrição	Descrição resumida dos níveis de configuração de aprovação.
Condição	Identifica os itens vulneráveis correspondentes ou as tarefas de correção.

5. Selecione **Atualizar**.
   Você pode definir condições que contêm vários níveis de aprovação em uma regra. O Flow Designer herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente. Para obter informações sobre como configurar níveis de aprovação, consulte Criar níveis de aprovação para a Gestão de exceções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example:
Você pode definir diferentes caminhos de aprovação para diferentes tipos de vulnerabilidades ou itens de configuração (voltados para a Internet ou internos).

Criar níveis de aprovação para a Gestão de exceções

Defina os níveis de usuários e grupos de usuários que aprovarão as solicitações de exceção.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de aprovação**.
2. Selecione uma regra de aprovação e navegue até a guia **Configurações de aprovação**.
3. Selecione uma configuração.
4. Na seção Níveis de aprovador, selecione um nível de aprovador.
5. No formulário, preencha os campos.

Formulário de nível de aprovação

Campo	Descrição
Nome	Nome do nível de aprovação.
Aprovação obrigatória	Selecione quantas aprovações são necessárias para o nível selecionado: ○ Um aprovador necessário ○ Todos os usuários devem aprovar
Ativo	Habilitado por padrão, o que significa que o nível de aprovação está em uso.
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Configuração de aprovação	Contém as configurações de aprovação.
Atribuir usando	Selecione uma opção de: ○ Usuário e grupo de usuários ○ Campo da tabela de aprovação ○ Script
Grupos	Grupo de nível de aprovador que consiste em vários usuários. O usuário deve ter uma das seguintes funções:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ sn_vul.exception_approver: para gestão de exceções e regras de exceção ○ sn_vul.false_positive_approver: para falso-positivo
Usuários	Edite os usuários listados nos grupos.

6. Para salvar as mudanças, selecione **Atualizar**.

Nota:
Antes da v15.0, o processo de fluxo de trabalho é funcional se houver usuários somente no nível de exceção 1. No entanto, a partir da v15.0, deve haver pelo menos um usuário em cada nível.

Antes da v15.0, no fluxo de trabalho, se não houvesse nenhum usuário no segundo nível, o item de vulnerabilidade ou o grupo vulnerável era adiado. No entanto, da v15.0 em diante, se não houver usuário no segundo nível, a solicitação de aprovação será rejeitada automaticamente.

Example:
Pode haver diferentes níveis de aprovação para vulnerabilidades para servidores Linux e Windows.

Fluxo de trabalho de gestão de exceções versus Flow Designer

A partir do Vulnerability Response v15.0, se você estiver implantando Vulnerability Response (VR) pela primeira vez, o Flow Designer para aprovar solicitações de exceção na gestão de exceções será habilitado por padrão. Se você for um usuário de VR existente, a opção padrão será fluxo de trabalho.

Nota:
A partir da Vulnerability Response v19.0, somente o Flow Designer é compatível com novos clientes. Se você for um usuário existente e atualizar para Vulnerability Response v19.0, o designer de fluxo e o fluxo de trabalho de gestão de exceções serão compatíveis.

Fluxo de trabalho versus designer de fluxo

Considerações	Fluxo de trabalho	Flow Designer
Versão	Antes da v15.0 de Vulnerability Response.	A partir da v15.0 de Vulnerability Response.
Opção padrão	Opção padrão se você for um usuário de VR existente.	Opção padrão para novos usuários de VR a partir da v15.0.
Configuração do processo de aprovação	O gerenciamento de exceções inclui solicitações de falso-positivo e exceção junto com regras de exceção.	Inclui a definição de vários níveis e a adição de diferentes aprovadores para diferentes casos de uso. Mais fácil de implementar do que o fluxo de trabalho. O gerenciamento de exceções inclui solicitações de falso-positivo e exceção junto com regras de exceção.
Atualizando para o Flow Designer	Você pode atualizar para o Flow Designer a partir do fluxo de trabalho. No entanto, as	O Flow Designer está habilitado por padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho versus designer de fluxo

Considerações	Fluxo de trabalho	Flow Designer
	solicitações existentes só podem ser aprovadas usando o fluxo de trabalho.	
Propriedade do sistema `sn_vul.flow_designer_activation`	Se você estiver usando o fluxo de trabalho para gerenciamento de exceções antes da v15.0, a propriedade do sistema será definida como falsa. Para ativar o Flow Designer, defina esta propriedade como verdadeira. **Nota:** Você não pode reverter para usando o fluxo de trabalho depois de ativar o Flow Designer.	Se você estiver usando o VR pela primeira vez para v15.0 ou posterior, o valor da propriedade do sistema será definido como verdadeiro por padrão.
Módulo de regras de aprovação	Depois de definir a propriedade do sistema como verdadeira, o trabalho programado **Habilitar regras de aprovação do módulo** é executado em 24 horas. Este trabalho programado habilita o módulo **Regras de aprovação**. Para ativar este módulo instantaneamente, execute este trabalho manualmente.	Se você implantou o VR pela primeira vez a partir do VR v15.0, este módulo está disponível por padrão.
Níveis de aprovação	Fornece a opção de definir apenas dois níveis de aprovadores.	Fornece várias opções, como definir qualquer número de configurações, níveis de aprovador e adicionar dinamicamente aprovadores para cada regra.

Tradução automática

Adicionar um aprovador de falso positivo

Somente usuários adicionados ao grupo de aprovadores de falso-positivo podem aprovar falsos-positivos para itens vulneráveis (IVs) e tarefas de correção (VULs). A concessão de um falso positivo é um processo de aprovação de nível único.

Antes de Iniciar

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

A partir do Vulnerability Response v15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > > **Administração de usuários** > **Grupos**.
2. Na coluna **Nome**, pesquise por **Falso-positivo** e clique na opção.
3. No formulário Grupo, navegue até **Membros do grupo** > **Novo** (ou **Editar**).
4. No formulário Usuário, crie um registro inserindo os detalhes do usuário e clique em **Enviar**.
   Todas as funções são concedidas ao usuário. Os usuários selecionados são adicionados à lista Membros do grupo. Esses membros podem aprovar solicitações para marcar IVs ou tarefas de correção como falso-positivos. Depois de aprovado, o estado do registro é atualizado para Encerrado e ele é reaberto somente na data especificada.

Configurar questionário para redução de risco

A partir da Vulnerability Response v20.0, você pode personalizar o questionário da solicitação de redução de risco para um conjunto de itens vulneráveis filtrados ou tarefas de correção.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

O **Questionário para controles de compensação para itens vulneráveis** e **o Questionário para controles de compensação para regras de aprovação de grupo vulnerável** são enviados com o sistema de base.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Gestão de exceção**.
2. No formulário Configurações para gestão de exceções de VR, marque a caixa de seleção Habilitar questionário para solicitar exceção.
3. Para configurar questionários com base em condições para solicitações de redução de risco:

   a. Na seção Configuração do questionário de VR, selecione **Novo**.

   b. No formulário Configuração de questionário - Novo registro, selecione a regra de aprovação **Questionário para controles de compensação para grupos vulneráveis** ou **Questionário para controles de compensação para itens vulneráveis** e forneça a condição.

   c. Selecione o questionário desejado e selecione **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre os campos de formulário de Configuração de questionário, consulte Campos de formulário de configuração de questionário.
O questionário criado aparece na seção Configuração do questionário de VR do formulário Configurações para gestão de exceções de VR.

4. Selecione **Salvar** no formulário Configurações para gestão de exceções de VR.

Exibir ANS do Vulnerability Response para tarefas de correção

Para garantir que os itens vulneráveis sejam processados corretamente, você pode definir um Acordo de nível de serviço (ANS) para Vulnerability Response tarefas de correção.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa
As definições do ANS nesta lista são um subconjunto da lista de ANS da plataforma, específica para Vulnerability Response.

Para obter instruções detalhadas, consulte Create an SLA definition .

Se você estiver rastreando o tempo que leva para corrigir IVs, talvez prefira usar Vulnerability Response regras de destino de correção. As regras de destino de correção definem os intervalos de tempo esperados para corrigir itens vulneráveis (IV) especificamente no contexto do Vulnerability Response, enquanto os SLAs podem fornecer um intervalo de tempo para corrigir a própria vulnerabilidade.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Definições do ANS**.
2. Clique em uma definição.
   Os SLAs de tarefa são mostrados nas listas relacionadas de **Tarefas**de correção.

Configurar watchdog

Use a página de configuração do watchdog para criar novos ou atualizar os existentes com as condições que você deseja especificar. Você pode habilitar a notificação para cada watchdog e ser notificado quando as condições forem atendidas.

Antes de Iniciar
Função necessária: sn_sec_cmn.admin

Procedimento

1. Navegar até **Todos** > **Security Operations** > **WatchDog** > **Configuração**.
2. Selecione o watchdog que você deseja implementar.
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de integração do Watchdog

Campo	Descrição
Nome	Nome do watchdog.
Ativo	Defina a caixa de seleção como `true` para habilitar o watchdog.
Tipo de condição	Escolha entre Filtro ou Script.
Condição avançada	Este campo é exibido somente quando Script é selecionado em Tipo de condição.
Tabela	Selecione a tabela para executar a condição de watchdog.
Condição	Condição para avaliar o watchdog.
Notificar	Caixa de seleção para notificar os grupos ou usuários se a condição de watchdog for atendida.
Usuários	Lista de usuários a serem informados se a condição de watchdog for atendida.
Grupos	Grupo a ser informado se a condição de watchdog for atendida.
Log de observação	
Cão de guarda	Referência à tabela de monitoramento.
Contagem	Número de registros que atendem aos critérios do watchdog.
Anotações	Anotações adicionais para os logs de watchdog.

4. Selecione **Atualizar**.

Tarefas de configuração avançadas Vulnerability Response

As tarefas de configuração a seguir exigem codificação ou conhecimento avançado ServiceNow e não são consideradas parte da configuração básica.

Talvez você prefira executar essas tarefas somente se tiver experiência avançada em codificação ou conhecimento especializado do Now Platform.

Criar importações separadas por domínio para uma integração

Se você exigir que os dados importados estejam em um domínio específico, o usuário atribuído para executar as integrações deverá pertencer a esse domínio.

Antes de Iniciar

Função necessária:

import_admin e a função de integração de configuração para sua integração específica, por exemplo, sn_vul.configure_r7_integration ou sn_vul_tenable.configure_integration.

Por Que e Quando Desempenhar Esta Tarefa

Este conjunto de tarefas requer codificação ou conhecimento avançado ServiceNow.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As filas de importação contêm anexos de dados que os trabalhos programados (integrações) processam. Em um ambiente separado por domínio, você deve corresponder o trabalho programado à fila de importação correta.

Procedimento

1. Crie um domínio.
2. Para cada domínio criado, crie um usuário e atribua o usuário a esse domínio.

   Pense neste usuário como um espaço reservado **run_as** para o domínio em sua integração de vulnerabilidade. É o equivalente ao usuário **VR.System** no domínio global. Este usuário precisa de acesso a fontes de dados, mapas de transformação e dados de vulnerabilidade.

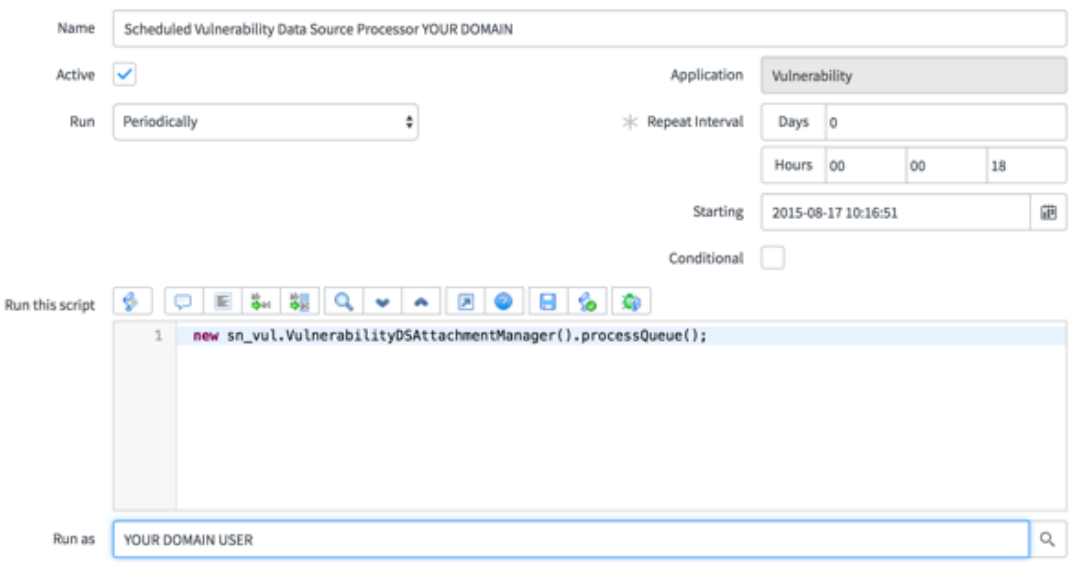
   Nota:
   Não use este usuário para qualquer outra finalidade.

3. Crie um trabalho programado em cada domínio.
   Para obter mais informações sobre precauções e configurações adicionais, consulte Configurações adicionais para Domain Separation.

   a. Navegar até **Todos** > **Definição do Sistema** > **Trabalhos programados**.

   b. Copie o **processador da fonte de dados de vulnerabilidade programada** para o domínio.

   c. Para identificar o trabalho programado, anexe o domínio ao nome.



   d. No campo **Executar como**, altere o usuário **run_as** para o usuário que você criou na Etapa 2.

   A partir da v20.1 de Vulnerability Response, as seguintes mudanças de script são enviadas com o sistema de base.

4. **Nota:**
   Edite a seguinte ação de IU para que a integração seja executada no domínio do usuário **run_as**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

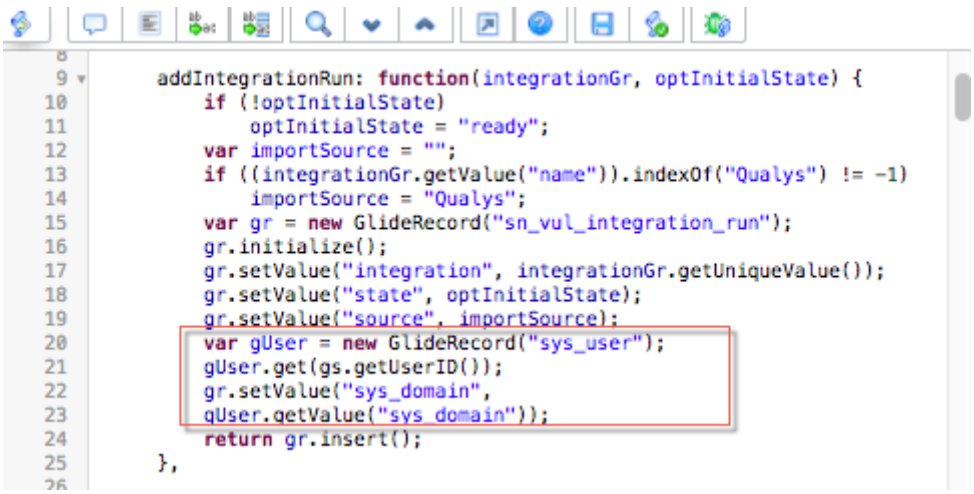
Edite a ação de IU **Executar agora** no trabalho de integração do **Qualys Host Detection Integration** para adicionar este bloco de código à parte superior do arquivo.

Example

```
//sys id below is of host detection integration
if(current.sys_id == "5d9cf0daff540300c68c9f783894fa4d"){
current.run_as = gs.getUserID
();
}
```

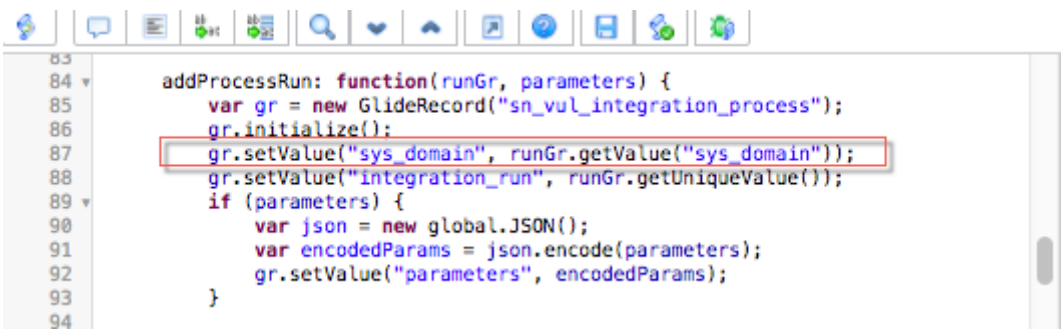
5. **Nota:**
   Edite as inclusões de script a seguir para que a integração seja executada no domínio do usuário **run_as**.

   Edite o método de inclusão de script **VulnerabilityIntegrationUtilsaddIntegrationRun** para adicionar o código realçado



```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

6. Edite o método de inclusão de script **VulnerabilityIntegrationUtils**, **addProcessRun** para adicionar o código realçado na imagem a seguir.
   Código addProcessRun



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

7. Edite o método de inclusão de script **VulnerabilityIntegrationUtils**, **copyProcess** para adicionar o código realçado na imagem a seguir.
   Código de copyProcess

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Script

```
325
326     _copyProcess: function(intProcGr, isProcessErrored) {
327         var copy = new GlideRecord('sn_vul_integration_process');
328         copy.initialize();
329         copy.setValue('integration_run', intProcGr.getValue('integration_run'));
330         copy.setValue('parameters', intProcGr.getValue('parameters'));
331         copy.setValue('state', 'new');
332         copy.setValue('notes', '');
333         copy.setValue('sys_domain', intProcGr.getValue('sys_domain'));
334         if (isProcessErrored) {
335             copy.setValue('errored_retries', parseInt(intProcGr.getValue('errored_retries')) + 1);
336             var nextRetryDueOn;
337             if (intProcGr.getValue('next_retry_due_on') != '')
338                 nextRetryDueOn = new GlideDateTime(intProcGr.getValue('next_retry_due_on'));
339             else
340                 nextRetryDueOn = new GlideDateTime();
341
342             var intgInstance = new sn_vul.VulnerabilityIntegrationHelper().getIntScriptInstance(intProcGr);
343             var nextRetryDelay = intgInstance.getNextRetry(intProcGr.errored_retries);
344             nextRetryDueOn.addSeconds(nextRetryDelay * 60);
345             if (parseInt(intProcGr.getValue('errored_retries')) + 1 < intgInstance.getMaxRetry())
346                 copy.setValue('next_retry_due_on', nextRetryDueOn.getValue());
347         } else
348             copy.setValue('retries', intProcGr.retries + 1);
349
350         copy.insert();
351         return copy;
352     },
```

8. Edite o método de inclusão de script **DataSourceVulnReportRefreshProcessor_processFromDataSourceGroups** para mudar este código original:
Código original de _processFromDataSourcesGroups

```
23
24     _processFromDataSourceGroups: function(payload, fileName) {
25         var gr = new GlideRecord("sn_vul_int_data_src");
26         gr.addQuery("sn_vul_integration", this.integrationGr.sys_id + "");
27         gr.orderBy("ds_group_number");
28         gr.orderBy("last_used");
29         gr.query();
30         var lastGroup;
31         if (gr.getRowCount() == 0) {
32             throw new Error("There are no data sources to provide data to.");
33         }
34         while (gr.next()) {
35             var thisGroup = gr.getValue("ds_group_number");
36             if (lastGroup == thisGroup && lastGroup !== undefined) {
37                 continue;
38             } else {
39                 var ds = new GlideRecord("sys_data_source");
40                 if (!ds.get(gr.sys_data_source + ""))
41                     continue;
42
43                 var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                 mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue());
45                 gr.setValue("last_used", new GlideDateTime().getValue());
46                 gr.update();
47                 lastGroup = thisGroup;
48             }
```

Para:

Código _processFromDataSourcesGroups editado

```
43                 var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                 mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue(),this.integrationProcessGr.getValue("sys_domain"));
45                 gr.setValue("last_used", new GlideDateTime().getValue());
46                 gr.update();
47                 lastGroup = thisGroup;
```

9. Edite o método de inclusão de script **VulnerabilityDSAttachmentManager**, **queueItem** para adicionar os seguintes blocos de código realçados
item da fila

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
queueItem: function(dataSource, attachmentName, reportData, optIntegrationProcess,optDomain) {
    var gr = new GlideRecord(this._QUEUE_TABLE);
    gr.initialize();
    gr.setValue("status", "NEW");
    gr.setValue("data_source", dataSource);
    if (optIntegrationProcess)
        gr.setValue("integration_process", optIntegrationProcess);
    if(optDomain){
            gr.setValue("sys_domain", optDomain);
    }
    var sysId = gr.insert();
```

_getNext

```
_getNext: function() {
    // First go through the retries, if any
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    var sysDomainUser = gUser.getValue("sys_domain");
    var gr = new GlideRecord(this._QUEUE_TABLE);
    gr.addQuery("status", "RETRY");
    gr.addQuery("sys_domain", sysDomainUser);
    gr.orderBy("queued_on");
    gr.query();
    if (gr.next()) {
        return gr;
    }

    // Then handle the regular queued items
    gr = new GlideRecord(this._QUEUE_TABLE);
    gr.addQuery("status", "QUEUED");
    gr.orderBy("queued_on");
    gr.addQuery("sys_domain", sysDomainUser);
    gr.query();
    if (gr.next()) {
        return gr;
    }
```

Função _processQueueEntry

```
_processQueueEntry: function(entry) {
    var schedGrId = this._getScheduledImportSet(entry.data_source);
    if (gs.nil(schedGrId)) {
        return;
    }

    var dataSourceGr = new GlideRecord("sys_data_source");
    if (!dataSourceGr.get(entry.data_source)) {
        gs.warn("Non existent data source - marking as complete");
        entry.setValue("status", "COMPLETE");
        entry.setValue("processing_notes", "Data source does not exist, could not process.");
        entry.update();
        return;
    }

    try {
        this._deleteDataSourceAttachments(entry.data_source);
        if (!this._verifyDataSourceAttachmentsDeleted(entry.data_source)) {
            gs.error("VulnerabilityDSAttachmentManager._processQueueEntry: Attachments not deleted for queue
entry " + entry.sys_id);
            throw "Attachments not deleted";
        }
        var attachmentApi = new GlideSysAttachment();
        attachmentApi.copy(this._QUEUE_TABLE, entry.sys_id + "", this._DATA_SOURCE, dataSourceGr.sys_id + "");
        var schedGr = new GlideRecord("scheduled_import_set");
        schedGr.get(schedGrId);
        schedGr.setValue("data_source", entry.data_source);
        schedGr.setValue("run_as", gs.getUserID());
        schedGr.update();
```

Neste ponto, você está pronto para importações separadas por domínio.

Nota:
Se você tiver várias implantações de uma integração Vulnerability Response ou Application Vulnerability Response, repita este processo para cada implantação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar e oferecer suporte a vários domínios na estrutura de trabalhos em segundo plano

Os trabalhos em segundo plano em produtos de resposta de vulnerabilidade são projetados para serem executados por longos períodos para executar vários processos em seus registros. Os processadores de trabalho em segundo plano são enviados com o sistema de base que é executado por meio do usuário do sistema e cria registros no domínio global.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Administrador de Domínio** > **Domínios**.
2. Crie um domínio.

   Para obter mais informações sobre como criar um domínio, consulte Create a domain .

   Para cada domínio criado, crie um usuário e atribua o usuário ao domínio. Suponha que este usuário seja um espaço reservado run_as para o domínio. É o equivalente ao usuário VR.System no domínio global. Este usuário precisa de acesso aos dados de vulnerabilidade.

3. Altere o run_as dos trabalhos programados *`Scheduled Background Job Manager`* e *`Close the parent background job`*.

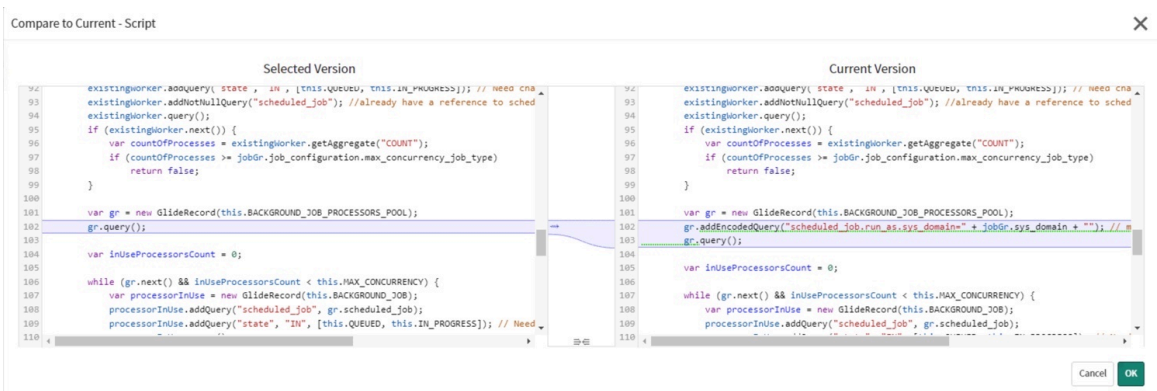
   Se você tiver vários domínios criados, duplique este trabalho e altere o usuário run_as de acordo. Você também pode manter uma cópia dos trabalhos anteriores com o usuário run_as do domínio global em um modo inativo.

   Dez trabalhos de processador (por exemplo, *`Background job processor 10`*) são enviados com o sistema de base. Altere a execução a partir desses trabalhos para o usuário separado por domínio. Se vários domínios estiverem presentes, dois trabalhos por domínio serão suficientes, mas esses trabalhos também podem ser duplicados, se necessário. Mantenha dois trabalhos de processador com o usuário run_as no domínio global.

   A partir da v20.0 de Vulnerability Response, as seguintes mudanças de script são enviadas com o sistema de base.

4. Modifique a inclusão de script *`BackgroundJobManager`* e adicione a seguinte linha, conforme mostrado na imagem a seguir.

```
gr.addEncodedQuery("scheduled_job.run_as.sys_domain=" + jobGr.sys_domain + "");
```



Nota:
Acione a reaplicação sob demanda de qualquer regra do domínio correto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar uma regra de pesquisa de IC do Vulnerability Response

O módulo **Regras de pesquisa de IC** contém regras que são usadas para encontrar o registro correspondente às informações do host recebidas durante as importações de integração de vulnerabilidade de terceiros. As informações do host são correspondidas aos itens descobertos, às classes de item de configuração incompatíveis e ao Configuration Management Database (CMDB).

Antes de Iniciar

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Criar regras de pesquisa de IC requer conhecimento avançado de ServiceNow e Vulnerability Response. Em vez de modificar uma das regras de pesquisaexistentes , considere copiá-la e modificar a cópia. Quando você estiver satisfeito com o fato de a nova regra fazer o que você deseja, desative a original.

Nota:
As regras, depois de removidas, não podem ser recuperadas. Em vez de remover as regras existentes, desative-as ao criar novas.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **CMDB** > **Regras de Pesquisa de IC**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de regra de pesquisa de IC

Campo	Descrição
Nome	Nome da regra.
Método de pesquisa	Método usado para correspondência. As opções são: ○ **Script**: script pré-criado (endereço IP, nome DNS e assim por diante) ou personalizado. ○ **Correspondência de campo**: pesquise na tabela ou no campo no CMDB.
Tipo	Tipo usado com o **método Pesquisa**de script.
Ordem	Ordem de precedência da regra. Regras com a ordem mais baixa são avaliadas primeiro.
Ativo	Caixa de seleção para saber se a regra está ativa ou desabilitada.
Fonte	Origem usada como entrada para esta regra.
Campo de origem	Campo de origem usado como entrada para esta regra. Selecione qualquer campo, mas ele será tratado como um valor de cadeia de caracteres.
Condição	Condição baseada na qual a regra de pesquisa de IC é aplicada. Esta condição depende do atributo do scanner de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: O atributo do ativo faz parte da carga útil. Ele é recebido do scanner de terceiros. Consulte a tabela Itens descobertos para obter exemplos de carga útil.
Script	Um exemplo de script editável, com base no **Tipo**, é mostrado. Implemente o script personalizado seguindo os comentários incluídos no modelo da função padrão. **Nota:** A função de processo tem três parâmetros: `rule`, `sourceValue`e `sourcePayload`
Pesquisar na tabela	Tabela a ser pesquisada no CMDB. Usado com o campo correspondente ao **Método de pesquisa**.
Pesquisar no campo	Campo que contém informações que podem ser usadas para localizar um IC. Usado com o campo correspondente ao **método de pesquisa**. Este campo pode estar no registro de IC ou em um registro relacionado, como um adaptador de rede.

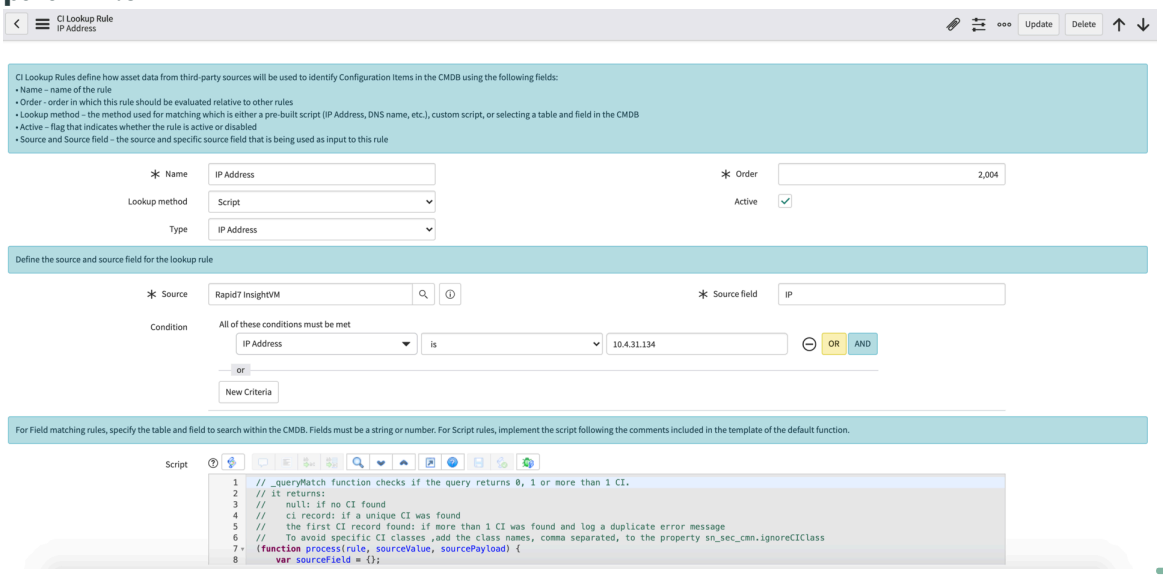
4. Clique em **Enviar**.

Para obter mais informações sobre implementação de regras de pesquisa de IC, consulte Etapas para ajudar a evitar registros duplicados ou órfãos após a execução de Vulnerability Response regras de pesquisa de IC.

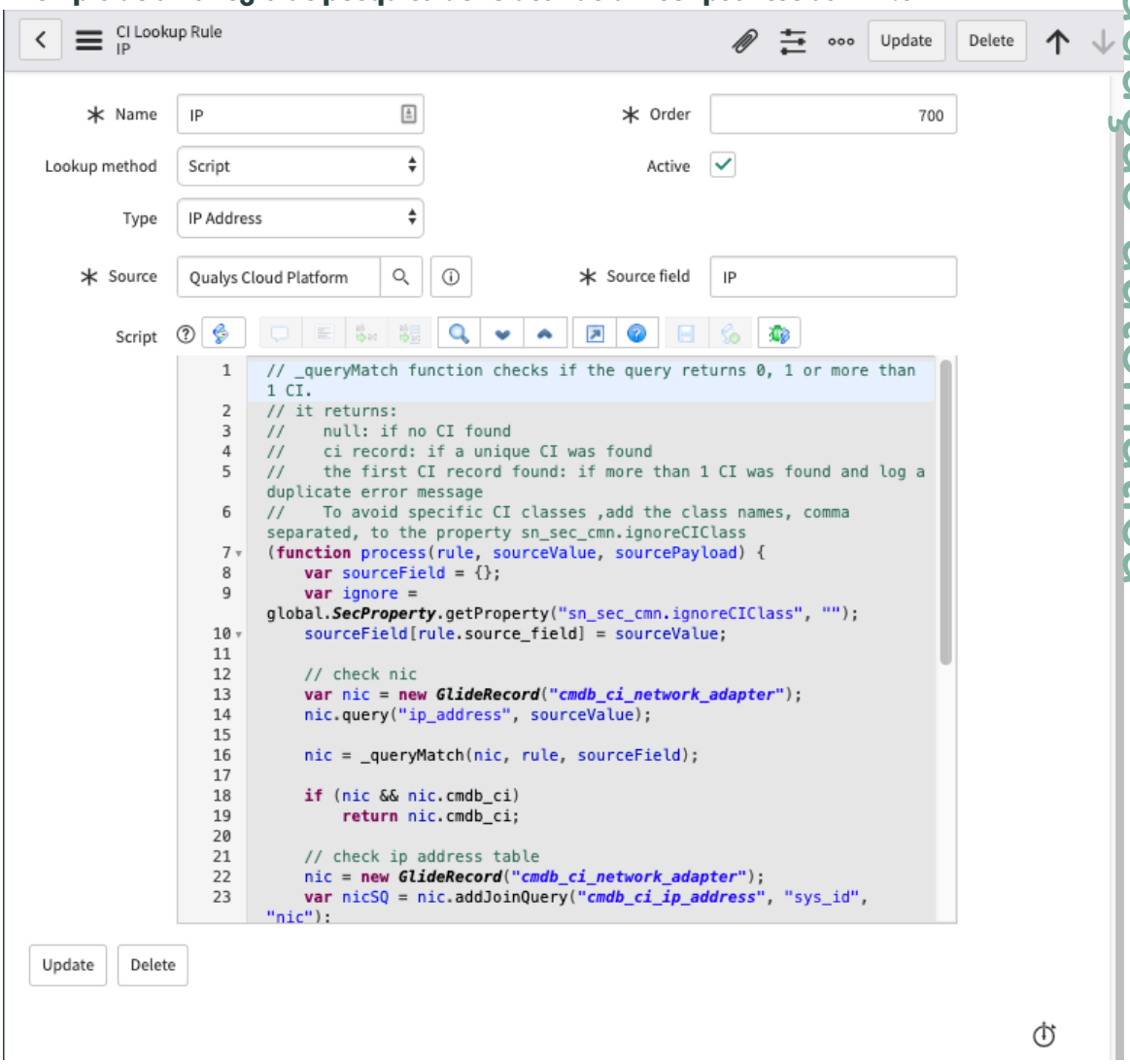
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de uma regra de pesquisa de IC usando um construtor de condição para V12.0



Exemplo de uma regra de pesquisa de IC usando um script antes da V12.0



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Vulnerability Response campos de formulário de item vulnerável

Ignorar classes de IC

Para ignorar algumas classes de item de configuração (IC), por exemplo, Balanceador de carga [cmdb_ci_lb], ao executar Regras de pesquisa de IC, defina a propriedade do sistema **ignoreCIClass** [*sn_sec_cmn.ignoreCIClass*.

Antes de Iniciar

Função necessária: administrador

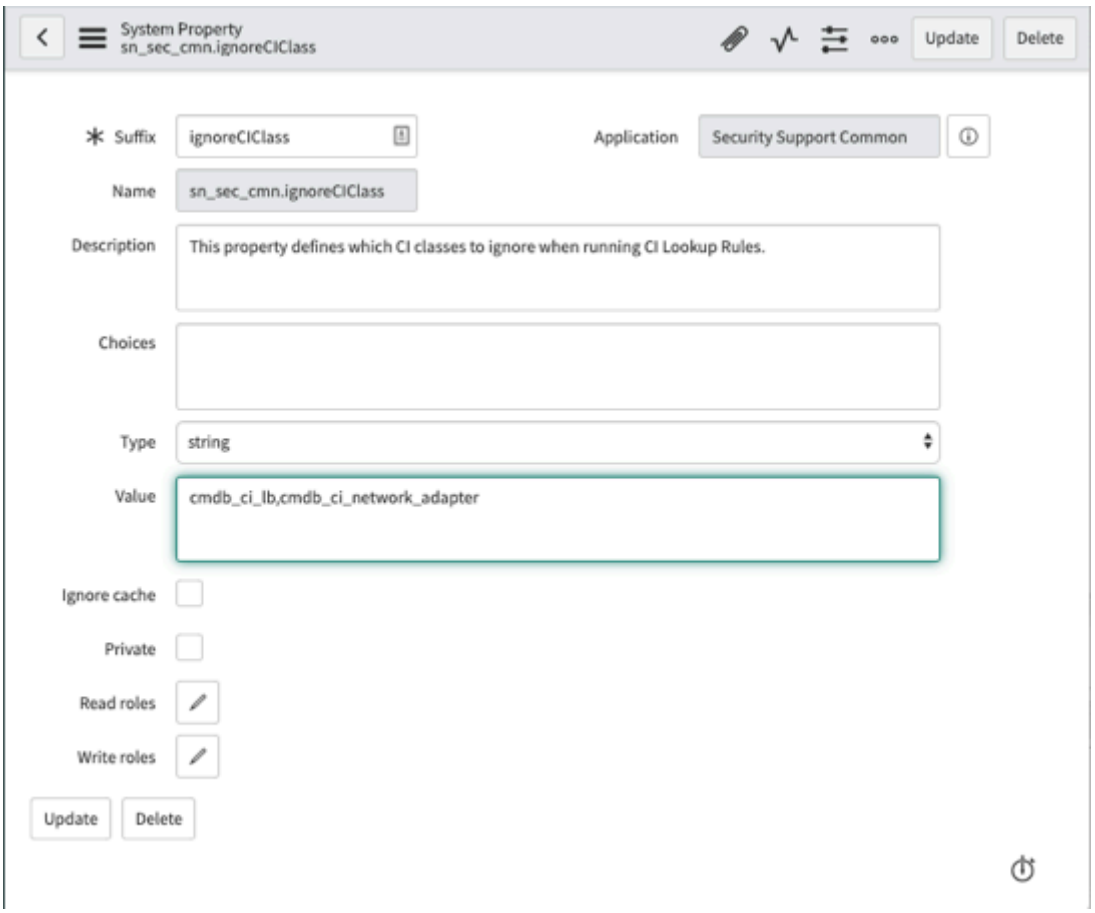
Nota:

A propriedade do sistema **ignoreCIClass** está disponível a partir de Vulnerability Response v9.0, no entanto, a funcionalidade da propriedade não está disponível na atualização de qualquer versão anterior.

Se você atualizou de qualquer aplicação Security Operations, antes da versão 9.0, consulte KB0788209 para obter instruções sobre como habilitar esta funcionalidade.

Procedimento

1. Insira sys_properties.list na barra de navegação à esquerda.
2. Clique **em Enter**.
3. No menu **Pesquisar**, em **Nome**, insira sn_sec_cmn.ignoreCIClass.
4. Na caixa de texto **Valor**, insira as classes de IC a serem excluídas em uma lista separada por vírgulas.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Atualizar**.
   Esta lista é usada pelas Regras de pesquisa de IC durante a próxima importação. Itens vulneráveis criados durante a importação não são associados a um IC de qualquer tipo listado no campo **Valor** da propriedade do sistema sn_sec_cmn.ignoreCIClass.

Filtrar ICs desativados

Filtrar itens de configuração (ICs) desativados ao executar as regras de pesquisa de IC. Para filtrar ICs desativados ao executar as regras de pesquisa de IC do CMDB do Security Operations, defina a propriedade do sistema **filterOutDecommissionedCI** [**sn_sec_cmn.filterOutDecommissionedCI**] como verdadeira.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
O valor padrão da propriedade do sistema é verdadeiro. Esta propriedade é aplicável somente para regras de pesquisa de IC em Vulnerability Response e não afeta a lógica de pesquisa do IRE.

Procedimento

1. Insira sys_properties.list na barra de navegação à esquerda.
2. Selecione **Enter**.
3. No menu **Pesquisar**, em **Nome**, insira sn_sec_cmn.filterOutDecommissionedCI para filtrar os ICs desativados.
4. Na caixa de texto **Valor**, insira o valor verdadeiro ou falso.
   O valor padrão é verdadeiro.
5. Selecione **Atualizar**.
   Este valor é usado pelas Regras de pesquisa de IC durante a próxima importação. A propriedade do sistema sn_sec_cmn.filterOutDecommissionedCI filtra os ICs desativados ao executar essas regras de pesquisa.

Promover ICs automaticamente

Edite a cadeia de caracteres JSON na propriedade do sistema **autoPromoteFields** [**sn_sec_cmn.autoPromoteFields**] para que suas regras de pesquisa de item de configuração (IC) promovam automaticamente todos os ICs do Security Operations do CMDB para entradas correspondentes na tabela [cmdb_ci].

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
O tipo de propriedade do sistema é "cadeia de caracteres" e requer que você insira uma cadeia de caracteres JSON. Esta propriedade é ativada por padrão e promove a correspondência de ICs ao executar as regras de pesquisa de IC.

Scripts de pesquisa personalizados podem retornar registros de tabela secundária do script. Para esta propriedade, a função *_autoPromoteCI* em *CIIdentify Script Include* usa o IC retornado pelo script de pesquisa e percorre automaticamente os relacionamentos para chegar à entrada *cmdb_ci* e retorná-la.

Para substituir a lógica de promoção automática, ou seja, para adicionar ou atualizar novas classes de IC, adicione o objeto JSON ao campo Valor na propriedade do sistema [**sn_sec_cmn.autoPromoteFields**].

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Insira sys_properties.list na barra de navegação à esquerda.
2. Selecione **Enter**.
3. Localize a propriedade do sistema [**sn_sec_cmn.autoPromoteFields**] e selecione o registro para abri-lo.

   Cadeia de caracteres padrão:

```
{
 "dscy_switchport":"cmdb_ci",
 "cmdb_ci_network_adapter":"cmdb_ci",
 "cmdb_ci_nic":"cmdb_ci",
 "cmdb_ci_ip_address":"nic"
}
```

4. Na caixa de texto **Valor**, edite a cadeia de caracteres usando o formato de emparelhamento padrão.
5. Selecione **Atualizar**.
   Este valor é usado pelas Regras de pesquisa de IC durante a próxima importação. A propriedade do sistema [sn_sec_cmn.autoPromoteFields] promove os ICs ao executar essas regras de pesquisa.

Configurar a chave do item vulnerável

Configure a granularidade da chave do item vulnerável (IV) na aplicação Vulnerability Response para definir o que torna um item vulnerável (IV) em sua organização.

Antes de Iniciar

Função necessária: administrador

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Termos-chave

IC (Configuration Item, item de configuração)

Um ativo existente listado no seu CMDB.

Vulnerabilidade

Um registro de uma vulnerabilidade conhecida importada do National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CWE) ou integrações de terceiros com Vulnerability Response.

Item vulnerável

Um item vulnerável é criado quando uma vulnerabilidade importada corresponde a um item de configuração no seu CMDB.

Detecção

Uma ocorrência única e distinta de uma vulnerabilidade, conforme relatado pelos verificadores de suas integrações de terceiros. As detecções são importadas e exibidas na detecção e nos registros de item vulnerável em sua instância. Também conhecido como Detecção de item vulnerável.

Por padrão, um item vulnerável é uma combinação exclusiva de um item de configuração (IC), uma vulnerabilidade e uma instância de integração. Para criar itens vulneráveis com mais granularidade, adicione portas exclusivas de detecções de item vulnerável para ajudá-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

lo a gerenciar a correção de vulnerabilidades no nível que você considera mais eficaz para sua organização.

Se você quiser criar itens vulneráveis com mais granularidade, configure a chave do item vulnerável para que ela inclua a porta. Quando a porta Incluir está habilitada, os itens vulneráveis são criados por portas exclusivas a partir de detecções de item vulnerável.

A partir do Vulnerability Response V17.1, você pode identificar e corrigir vulnerabilidades do Rapid7 adicionando a prova como a chave IV. Para obter mais informações, consulte Adicionando prova às chaves de item vulnerável do Rapid7.

Escolha uma opção na tabela a seguir para habilitar a opção Incluir porta.

Três cenários para habilitar a opção Incluir porta com a chave IV pela primeira vez

Se...	Descrição
Uma ou mais das seguintes condições são verdadeiras: • Você está atualizando de uma versão de Vulnerability Response anterior à v10.0 que não era compatível com detecções de item vulnerável. • Você é um novo cliente e não tem dados do Vulnerability Response (itens vulneráveis ou detecções de item vulnerável) em sua instância Now Platform®. • Você já excluiu todos os registros de item vulnerável e dados relacionados em sua instância e está pronto para criar todos os dados do Vulnerability Response começando com uma nova importação para incluir IVs diferenciados por porta exclusiva.	Habilite Incluir porta. Depois que a porta de inclusão estiver habilitada, as detecções importadas criarão itens vulneráveis que incluem IVs diferenciados por uma porta exclusiva que começa com a próxima importação.
Ambas as condições são verdadeiras: • Você tem a v10.0 ou posterior de Vulnerability Response e os dados do Vulnerability Response existentes (itens vulneráveis ou detecções de itens vulneráveis) em sua instância que você deseja preservar. • Você deseja começar a criar novos itens vulneráveis para incluir IVs diferenciados por porta exclusiva.	Habilitar Incluir porta. Suas detecções existentes e os itens vulneráveis associados serão preservados. Depois que a porta de inclusão estiver habilitada, novas detecções criarão novos itens vulneráveis que incluem IVs diferenciados por uma porta exclusiva que começa com a próxima importação.
Ambas as condições são verdadeiras: • Você tem v10.0 ou posterior de Vulnerability Response. • Você tem dados do Vulnerability Response (itens vulneráveis ou detecções de item vulnerável) existentes,	1. Exclua todos os registros de item vulnerável e dados relacionados da sua instância. 2. Habilitar Incluir porta. Depois que a porta de inclusão estiver habilitada, novas detecções criarão

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Três cenários para habilitar a opção Incluir porta com a chave IV pela primeira vez

Se...	Descrição
mas não deseja preservar os dados existentes, pois prefere criar seus dados de vulnerabilidade a partir de uma nova importação e deseja incluir IVs diferenciados por porta exclusiva.	novos itens vulneráveis que incluem IVs diferenciados por uma porta exclusiva que começa com a próxima importação.

Nota:

Se a opção Incluir porta estiver habilitada, mais de um item vulnerável poderá ser criado para um item de configuração. Por exemplo, se houver uma vulnerabilidade para duas portas em um item de configuração, portas 80 e 443, dois IVs exclusivos serão criados, um para cada porta que inicia com a próxima importação.

Nota:

Certifique-se de criar IVs para incluir IVs por portas exclusivas antes de habilitar este recurso. Depois de habilitar a chave de IV para incluir a porta, você deve primeiro excluir os dados do Vulnerability Response antes de desabilitar a porta de inclusão e retornar à importação de dados de vulnerabilidade usando a granularidade de chave de IV padrão, ou seja, em que os IVs são criados para a porta, mas não são diferenciados por uma porta exclusiva. Para obter mais informações sobre como excluir seus dados de vulnerabilidade, consulte Exclua todos os seus registros de item vulnerável e dados relacionados em Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Configurar granularidade de IV**.

   O campo Última atualização exibe a data em que a chave IV foi configurada pela última vez.

2. Clique na caixa de seleção Incluir porta para habilitá-la.

3. Clique em **Salvar**.
   A caixa de diálogo de confirmação é exibida.

   Se você não tiver registros de detecção de item vulnerável em sua instância, as detecções de item vulnerável e os itens vulneráveis serão criados por porta exclusiva, começando com sua próxima importação.

   Se você tiver detecções de item vulnerável e itens vulneráveis em sua instância, as detecções existentes e os itens vulneráveis associados serão preservados. Novas detecções criam novos vulneráveis que incluem IVs diferenciados por porta exclusiva que começam com a próxima importação.

O que Fazer Depois

Verifique se os itens vulneráveis por porta são exibidos na detecção de item vulnerável e nos registros de item vulnerável. Para obter mais informações, consulte Exibir Vulnerability Response dados de detecção de item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionando prova às chaves de item vulnerável do Rapid7

Adicione a prova como uma chave de item vulnerável (IV) para os Rapid7 IVs. Incluir a prova de vulnerabilidades específicas permite que a integração do scanner Rapid7 crie IVs para cada prova recebida de Rapid7.

Uma chave de IV é a combinação de vulnerabilidade, item de configuração (IC) e instância de integração. Dividir as detecções em diferentes IVs com base na prova cria vários IVs. Você pode atribuir as vulnerabilidades aos responsáveis pela correção apropriados.

Por exemplo, pode haver duas detecções com a mesma vulnerabilidade e IC, mas com provas diferentes, levando à criação de um IV. A partir da Vulnerability Response V17.1, você pode identificar e corrigir vulnerabilidades adicionando a prova como a chave IV.

Você pode adicionar a prova como uma chave IV da seguinte forma:

Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Configurar granularidade de IV** e selecione a opção para incluir prova.

Caso de uso: inclusão de prova na chave de IV para IVs existentes ou divisão de IVs existentes com base na prova de detecção

Para criar IVs com base na prova, você pode usar as vulnerabilidades R7 log4j. Por exemplo, você pode usar uma das várias vulnerabilidades R7 log4j, como `R7-apache-log4j-core-cve-2021-44228`, `R7-amazon_linux-cve-2021-44228`ou `R7-amazon-linux-ami-2-cve-2021-44228`.

Se todas as detecções em um IV tiverem a mesma prova, o IV existente será atualizado para incluir "Prova na chave de IV (external_id)". Se houver várias detecções com provas diferentes, o IV existente será encerrado. As detecções são divididas nos novos IVs com "Prova na chave de IV (external_id)".

Nota:

Se você fornecer o ID da vulnerabilidade, os IVs existentes serão divididos com base na prova. As novas vulnerabilidades para este ID de vulnerabilidade também têm prova como uma das chaves IV.

Exclua todos os seus registros de item vulnerável e dados relacionados em Vulnerability Response

Remova permanentemente todos os dados do Vulnerability Response (itens vulneráveis ou detecções de itens vulneráveis) e dados e registros relacionados da aplicação Vulnerability Response na sua instância Now Platform®.

Antes de Iniciar

Exclua registros de detecção de item vulnerável, itens vulneráveis, grupos de vulnerabilidades e todos os registros relacionados na aplicação Vulnerability Response da sua instância. Use este processo para limpar sua instância para importar dados com um novo início de suas integrações de terceiros ou, como um pré-requisito para retornar a configuração de chave do item vulnerável (IV) à configuração padrão. Para obter mais informações sobre como configurar a chave IV, consulte Configurar a chave do item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Esta ação exclui todos os registros de item vulnerável e todos os dados relacionados da sua instância. Depois de excluídos, esses dados não podem ser recuperados. Também requer que você suspenda a importação de dados e desabilite suas integrações de terceiros ativas com Vulnerability Response.

É necessário excluir seus dados de item vulnerável com este processo antes de mudar a configuração da chave IV. A remoção de todos os dados garante que todos os itens vulneráveis e detecções de itens vulneráveis sejam mapeados e atualizados com os dados mais atuais, começando com a próxima importação.

Verifique se as seguintes condições se aplicam antes de excluir seus dados:

- Você tem a v10.0 ou posterior de Vulnerability Response instalada. Para obter mais informações, consulte Vulnerability Response detecções de item vulnerável de integrações de terceiros.
- Você deseja desabilitar a porta de inclusão e retornar a configuração da chave IV à configuração padrão.
- Você tem itens vulneráveis existentes e detecções de item vulnerável, mas não deseja ou precisa atualizá-los e mantê-los.
- Você determinou que deseja remover todos os dados existentes do Vulnerability Response e registros relacionados para limpar sua instância.

Função necessária: sn_vul.vulnerability_admin

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Integrações de Vulnerabilidade**.
2. Registre todas as integrações ativas exibidas.

   Todas as integrações ativas listadas com trabalhos programados são desabilitadas antes da exclusão de todos os itens vulneráveis e dados relacionados para que nenhum dado novo seja importado durante a remoção de dados. Registrar esta lista ajuda a ativar suas integrações após a conclusão da exclusão.

3. Revise o artigo Como excluir dados do Vulnerability Response existentes para reimportação na Base de conhecimento HI.
4. Se for exibida uma mensagem de aviso que o impeça de gravar na coluna Ativa, para desabilitar as integrações ativas, siga estas etapas.

   a. Na coluna Nome, clique em um item para abrir o registro.

   b. Se você não puder editar a caixa de seleção Ativo, clique no link **aqui** para editar o registro.

   c. Clique na caixa de seleção **Ativa** para desabilitar a integração e cancelar o próximo trabalho programado.

   d. Clique em **Atualizar** para salvar suas mudanças e retornar à lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e. Verifique se você desabilitou todas as integrações ativas da lista de integrações.
Depois de desabilitar uma integração, ela não será mais exibida na lista de integrações ativas. Para exibir uma lista de integrações inativas e localizar todas as integrações desabilitadas depois de excluir todos os dados de vulnerabilidade, na coluna Ativa na parte superior, insira `=false`.

5. Continue com as etapas no artigo da base de conhecimento para excluir seus dados de vulnerabilidade existentes.
6. Depois de confirmar que todos os dados foram excluídos com sucesso, navegue até **Vulnerability Response** > **Administração** > **Configurar granularidade de IV**.
7. No formulário:
   - Se você excluiu dados porque prefere criar seus dados de vulnerabilidade para incluir a porta de uma nova importação, habilite Incluir porta e clique em **Salvar**.
   - Se você excluiu dados porque deseja retornar a chave de IV à sua configuração padrão, desabilite Incluir porta e clique em **Salvar**.

   Para obter mais informações, consulte Configurar a chave do item vulnerável.

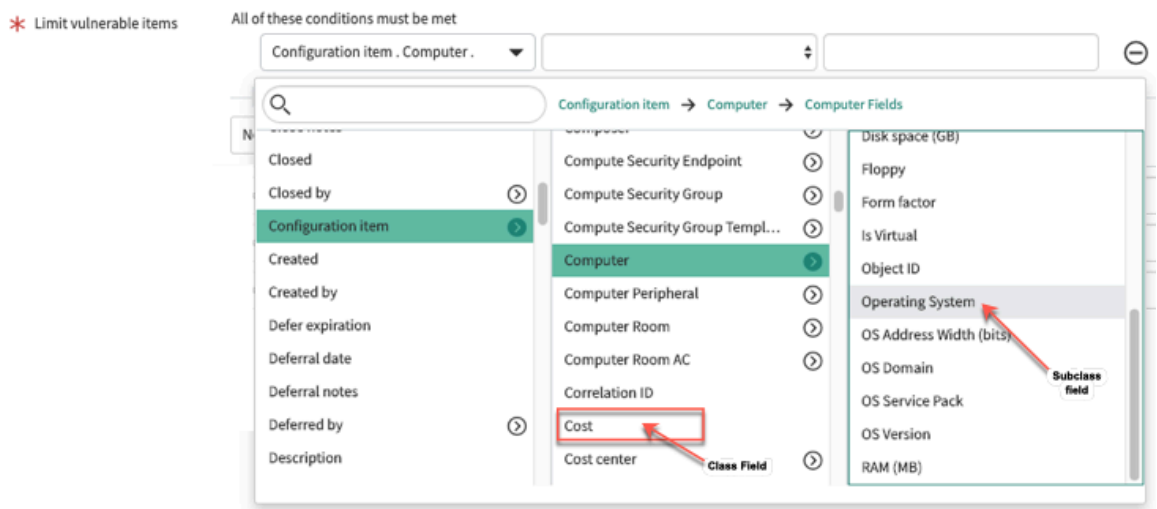
Filtragem em Vulnerability Response

Regras de tarefa de correção, Calculadoras e Regras de atribuição usam condições durante a importação, criadas usando o **Construtor de condição**. Mudanças em seus critérios podem afetar o desempenho, já que cada registro é avaliado usando esses filtros.

As regras e calculadoras enviadas com o sistema básico são otimizadas para desempenho. Editar ou criar regras ou calculadoras é cuidadoso e pode exigir experiência em ServiceNow e Vulnerability Response.

Evite filtrar com base em campos de subclasse

Algumas tabelas oferecem suporte à extensão. Um exemplo disso é a tabela IC do CMDB [cmdb_ci]. Tabelas como cmdb_ci_hardware e cmdb_ci_computer estendem esta tabela. Se você filtrar com base em um campo que não está na tabela primária, esse filtro poderá ser caro de construir e avaliar.



Por exemplo, filtrar em **Item de Configuração** > **Custo** não afetaria negativamente o desempenho porque **Custo** é um campo de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

classe, e não um campo de subclasse, de **Item de configuração**.

Item de Configuração > **Computador**, no entanto, é uma subclasse que requer uma referência com pontos para outro campo, neste caso, **Sistema operacional**. Esse processo pode levar muitos milissegundos, o que aumenta rapidamente, quando milhões de itens vulneráveis estão sendo importados e afeta o desempenho.

Nota:
Usar a condição [contém] é como uma pesquisa de caractere curinga e pode causar impacto no desempenho. Usar [is] sempre que possível é mais eficiente.

Criar um mapa de severidade Vulnerability Response

Vulnerability Response mapeamento de severidade transforma campos de severidade de origem de terceiros em campos reconhecíveis em Vulnerability Response.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa

Vulnerability Response é enviado com o banco de dados de vulnerabilidades nacional (NVD) para mapeamento de severidade ServiceNow normalizado. ServiceNow integrações de terceiros, como Qualys Vulnerability Integration fornecem mapeamentos de severidade após a instalação. Esses mapas podem ser ajustados alterando os campos nos mapas existentes.

Criar ou editar um mapa de severidade destina-se somente a mapeamentos de terceiros personalizados ou não padrão em seu ambiente.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Mapeamento de severidade normalizado**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Mapeamento de campo

Campo	Descrição
Fonte	O nome da origem do mapeamento de severidade.
Valor de origem	O valor de severidade de origem.
Valor de meta	O valor de severidade da meta. As opções são: ○ 1- Crítico ○ 2 - Alta

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ 3 – Médio ○ 4 - Baixo(a) ○ 5 - Nenhum

4. Repita a etapa 3 para cada nível de severidade de origem.
5. Clique em **Enviar**.

Definir classificações de serviço para relatórios Vulnerability Response e listas relacionadas

Traga mais foco para relatórios e listas relacionadas em Vulnerability Response definindo classificações de serviço. Além disso, a redução do número de classificações de serviço solicitadas pode melhorar o desempenho da Vulnerability Response coleta de dados.

Antes de Iniciar

Função necessária: administrador

Nota:

A edição das propriedades do sistema requer experiência em ServiceNow e Vulnerability Response.

Procedimento

1. Insira `sys_properties_list.do` na barra de navegação à esquerda.
2. Clique **em Enter**.
3. No menu **Pesquisar**, em **Nome**, insira `sn_vul.service_classifications`.
4. Abra a propriedade do sistema *`sn_vul.service_classifications`*.
5. Na caixa de texto **Valor**, insira a lista separada por vírgulas das classificações de serviço desejadas.

   Nota:
   Quando esta configuração está vazia, todos os serviços são listados.

   Exemplos:

   Para ver Serviços de negócios, Serviços técnicos e Serviços de aplicações e excluir Ofertas de serviço, Serviços compartilhados e serviços não classificados, defina o valor como: **Serviço de negócios, Serviço técnico, Serviço de aplicações**.

   Para ver os Serviços de aplicações, defina o valor como: **Serviço de aplicações**.

6. Clique em **Atualizar**.
   Os dados em cada relatório e lista relacionada de item vulnerável são filtrados por classificação de serviço durante a próxima execução do trabalho noturno do Performance Analytics.

Auditar campos selecionados na tabela de itens vulneráveis

Habilite a auditoria para os campos especificados na tabela Item vulnerável [sn_vul_vulnerable_item]. Este método de auditoria é útil quando você deseja auditar campos que não podem ser auditados por padrão.

Antes de Iniciar

Função necessária: administrador

Tradução automática

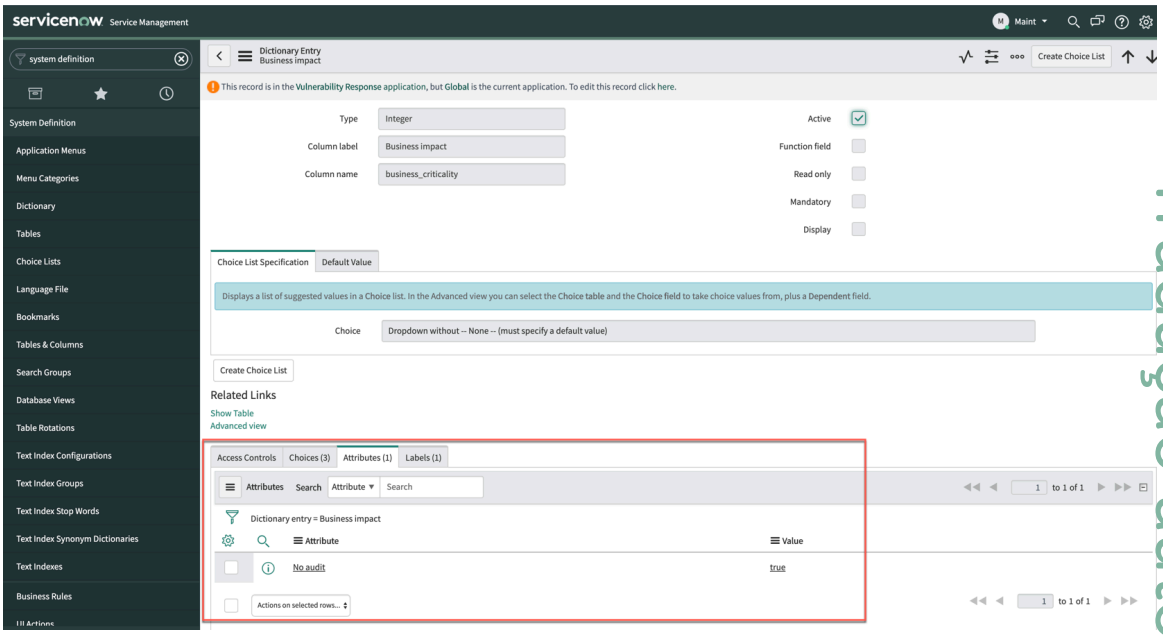
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

A tabela sn_vul_vulnerable_item é auditável por padrão. Campos que têm o atributo no_audit definido como verdadeiro não são auditáveis. Para obter mais informações sobre auditoria de tabelas, consulte Habilitar auditoria para uma tabela .

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Definição do Sistema** > **Tabelas** e pesquise a tabela sn_vul_vulnerable_item.
   A lista de entradas do dicionário para a tabela é exibida.
2. Para habilitar a auditoria para um campo, clique no nome da entrada.
   A página de entrada do dicionário para essa entrada é exibida.



3. Navegar até **Atributos** > **Nenhuma auditoria**.
   A página Atributo de dicionário é exibida.
4. Para remover o atributo no audit=true, clique em **Excluir**.
   A auditoria para este campo está habilitada.

Vulnerability Response configuração da estrutura de trabalho em segundo plano

Defina a estrutura de trabalho em segundo plano na sua instância Now Platform®. Essas mudanças de configuração podem ajudar a melhorar o desempenho, reduzindo a quantidade de recursos do sistema usados para executar seus trabalhos em segundo plano.

O que você pode editar na estrutura de trabalho em segundo plano

Com o módulo Configuração de trabalho em segundo plano, você tem as seguintes opções de configuração na estrutura:

- Você pode definir o número de trabalhos em segundo plano que são executados simultaneamente para Vulnerability Response processos.
- Para trabalhos longos que são executados em segundo plano e processam grandes quantidades de dados, você pode criar partições para processar dados em partes menores.
- Você pode cancelar um trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por que configurar a estrutura de trabalho em segundo plano

Os trabalhos em segundo plano em Now Platform® foram projetados para serem executados por longos períodos para executar vários processos em seus registros em Vulnerability Response. Anteriormente, esses trabalhos eram baseados em regras de negócios executadas de forma assíncrona. Não há limite para o número desses trabalhos que podem ser executados em segundo plano em sua instância para que as grandes quantidades de registros afetados por esses trabalhos possam ser processadas. Quando vários trabalhos que demoram muito para serem concluídos são executados simultaneamente em segundo plano, os recursos do sistema usados para executar os trabalhos programados são afetados, o que pode afetar negativamente o desempenho.

Configurar a estrutura de trabalho em segundo plano pode ajudar a melhorar seu desempenho, reduzindo a quantidade de recursos do sistema usados para executar seus trabalhos em segundo plano.

Termos-chave

Capacidade do trabalho

Descreve os trabalhos específicos. Por exemplo, um trabalho específico pode incluir os seguintes recursos:

- O trabalho pode ser executado em paralelo com outro trabalho do mesmo tipo.
- O trabalho pode ser particionado.
- O trabalho pode ser cancelado durante a execução.

Simultaneidade

Refere-se a trabalhos ou partes de trabalhos executados em paralelo.

Partição

Partições são partes de trabalhos que podem ser divididas para que possam ser processadas em paralelo para obter melhor desempenho. Normalmente, se refere a trabalhos com tempos de execução longos.

Configuração do trabalho

Refere-se às configurações de um trabalho programado específico.

Trabalho programado

Trabalhos programados são trabalhos automatizados que podem ser realizados em um horário específico ou em uma programação recorrente.

Recursos do sistema

Refere-se à quantidade de recursos do sistema que você deve oferecer suporte a um determinado número de trabalhos em segundo plano e trabalhos programados em seu ambiente.

Propriedade do sistema

As propriedades do sistema armazenam informações de configuração que raramente ou nunca mudam. Cada vez que você altera ou adiciona uma propriedade do sistema, o sistema limpa o cache para manter todos os nós do cluster sincronizados. Essa limpeza de cache afeta o desempenho.

Regra de negócios

Uma regra de negócios é um script do lado do servidor que é executado quando um registro é exibido, inserido, atualizado ou excluído, ou quando uma tabela é consultada. As regras de negócios realizam tarefas como alterar automaticamente valores em campos de formulário

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

quando determinadas condições são atendidas ou criar eventos para notificações por e-mail e ações de script.

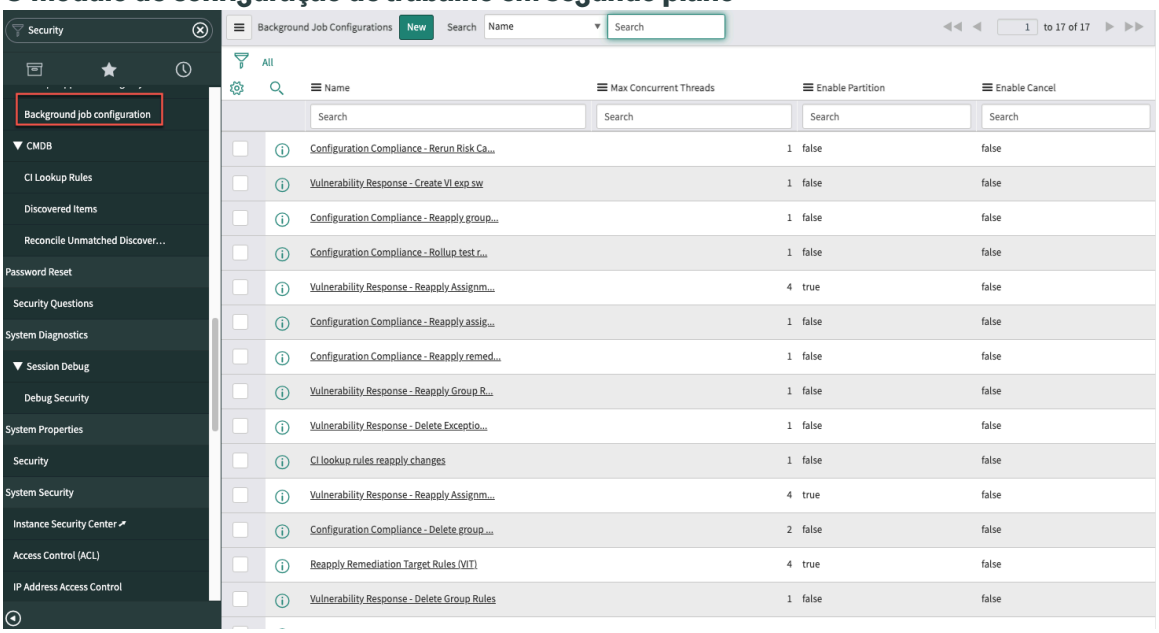
Caso de uso para definir a estrutura de trabalho em segundo plano

Por exemplo, o trabalho em segundo plano que aplica regras de destino de correção para registros de item vulnerável (VITs) e registros de item vulnerável do Application Vulnerability Response (AVITs) processa simultaneamente grandes quantidades de registros com várias tarefas.

Dependendo do tamanho da importação e do número de registros que você tem em seu ambiente, este trabalho pode usar uma grande quantidade de recursos do sistema disponíveis e levar muito tempo para ser concluído com êxito. Os trabalhos de manutenção do sistema ou outros trabalhos programados podem ser executados mais lentamente.

No módulo de configuração de trabalho em segundo plano, os trabalhos são listados por nome e um ID de configuração exclusivo. Nesses registros, você pode definir quantas tarefas deseja executar simultaneamente para um determinado trabalho em segundo plano. Você também pode definir o trabalho para processar partições de dados para que as tarefas sejam concluídas com mais rapidez e facilidade e usem menos recursos do sistema. Você também pode cancelar um trabalho se determinar que ele está sendo executado por muito tempo.

O módulo de configuração de trabalho em segundo plano



Para obter mais informações sobre as etapas necessárias para definir as configurações do trabalho em segundo plano, consulte Definir configurações de trabalho em segundo plano em Vulnerability Response.

Definir configurações de trabalho em segundo plano em Vulnerability Response

Defina quantas tarefas você deseja executar simultaneamente para um determinado trabalho em segundo plano. Você também pode definir o trabalho para importar partições de dados para que as tarefas sejam concluídas com mais rapidez e facilidade e usem menos recursos do sistema. Você também pode cancelar um trabalho se determinar que ele está sendo executado por muito tempo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

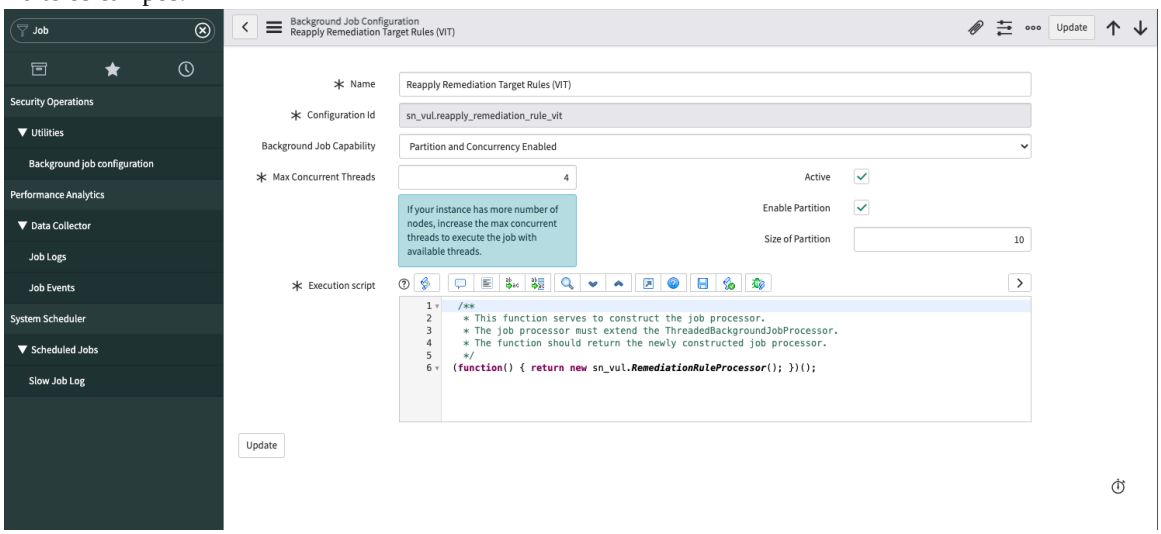
Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou gerenciadores de vulnerabilidade com a função granular sn_sec_cmn.manage_background_job

Consulte a seção abaixo das etapas para obter um exemplo.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Configurações de trabalho em segundo plano**.
2. Na coluna Nome, clique em um registro para abri-lo.
3. Edite os campos.



4. Clique em **Atualizar** para salvar suas mudanças.
   Consulte o exemplo a seguir para saber como verificar os resultados das mudanças de configuração.

   Há duas configurações de trabalho de Regras de destino de correção incluídas com a aplicação, uma para itens vulneráveis, uma para itens vulneráveis da aplicação:

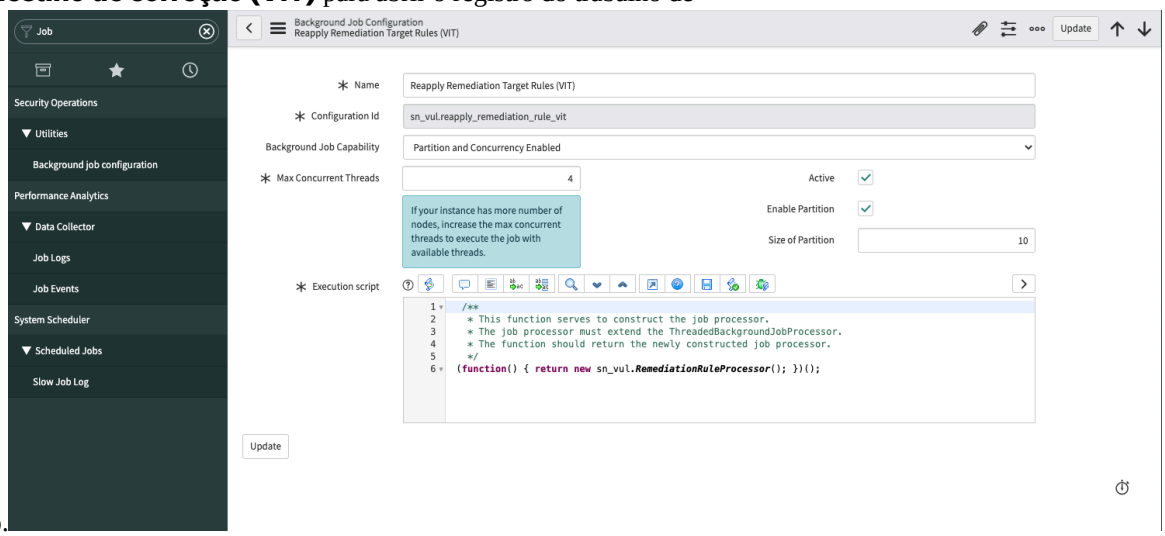
   - Reaplicar regras de destino de correção (VIT)
   - Reaplicar regras de destino de correção (AVIT)

   Suponha que você altere para as regras de destino de correção e queira reaplicá-las sem usar a maioria dos recursos de processamento do sistema disponíveis. Para ajudá-lo a limitar os recursos de processamento, você pode controlar o número de trabalhos em segundo plano executados e o número de itens processados por trabalho no módulo Configurações de trabalho em segundo plano.
5. Para definir essas configurações, navegue até **Security Operations** > **Configurações de trabalho em segundo plano** e clique em **Reaplicar**

Tradução automática

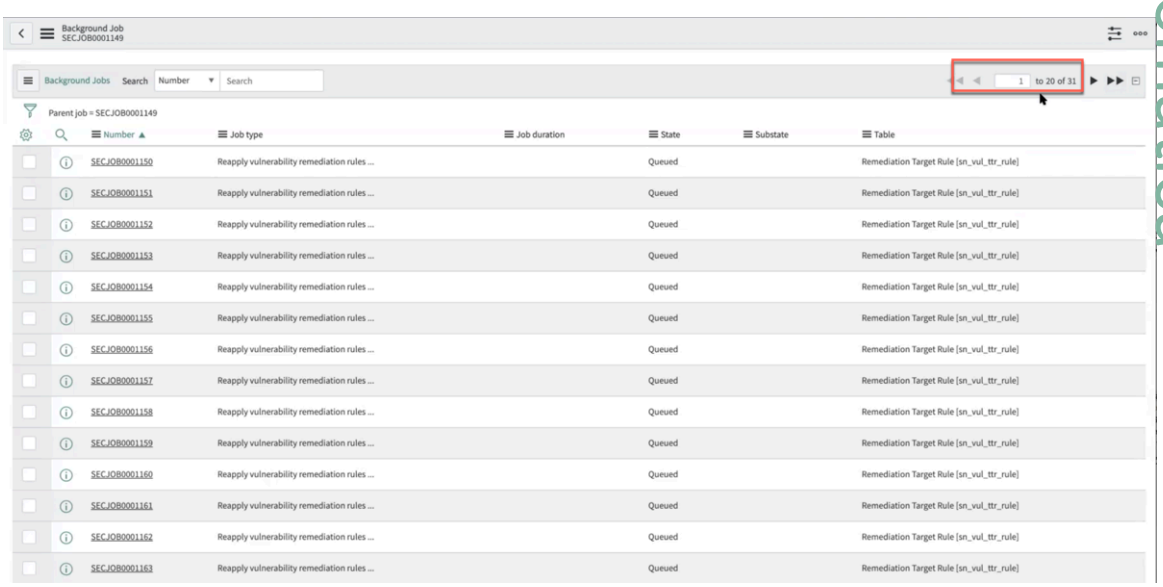
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

regras de destino de correção (VIT) para abrir o registro do trabalho de configuração.



Para fins de exemplo, digamos que você saiba que tem pouco mais de 300 IVs.

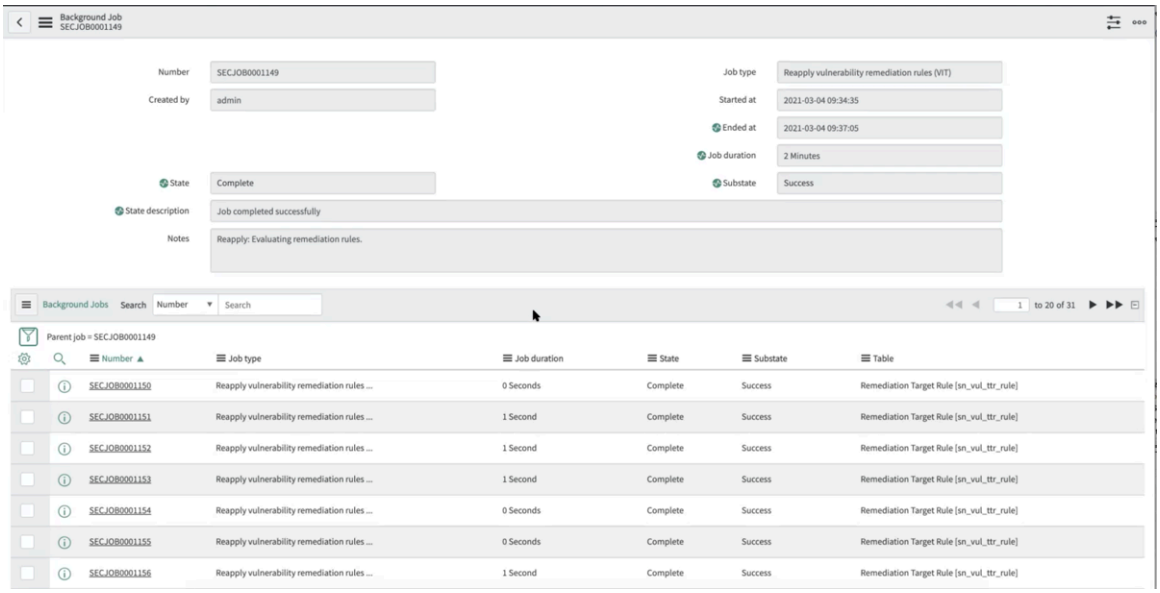
6. No registro do trabalho de configuração aberto, altere o valor do Tamanho da partição de **4** para **10**.
7. Navegar até **Vulnerability Response** > **Regras de destino de correção**, localize a regra de correção de vulnerabilidade Reaplicar que você alterou, selecione o registro na lista e clique em **Aplicar mudanças** para reavaliar as regras de destino para os IVs existentes.
   O trabalho Reaplicar regras de correção de vulnerabilidade (VIT) está na fila.
8. Clique no link **Exibir status** para exibir o registro do trabalho em segundo plano e verificar se os trabalhos estão enfileirados, conforme mostrado na imagem a seguir.
   Para este exemplo, 31 trabalhos são criados para processar regras de destino para 307 IVs (máximo de 10 itens por trabalho). Esses trabalhos são secundários do trabalho em segundo plano primário. Os trabalhos secundários processam os registros sequencialmente.



Quando todos os trabalhos forem concluídos com sucesso, os campos serão atualizados no registro do trabalho em segundo plano.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Navegue até seus itens vulneráveis e verifique se eles refletem sua nova mudança de regra.

Processamento paralelo avançado para trabalhos em segundo plano no Vulnerability Response

Com esta configuração avançada, controle o número total de trabalhos em segundo plano que estão sendo processados em paralelo, independentemente do tipo de trabalho.

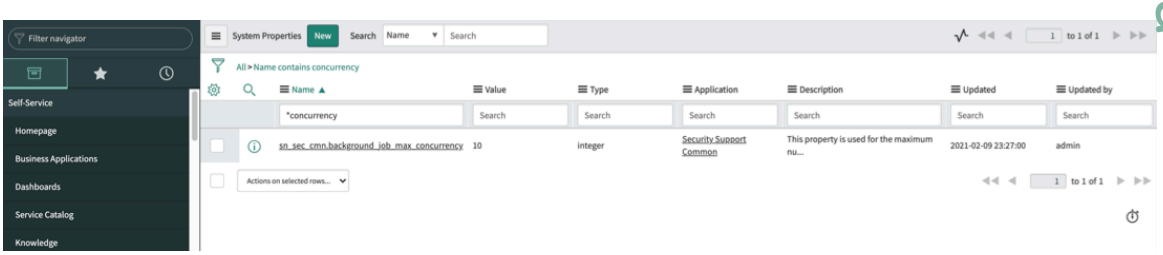
Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou gerenciadores de vulnerabilidade com a função granular sn_sec_cmn.manage_background_job

Nota:
Este procedimento requer conhecimento avançado de programação.

Procedimento

1. No Navegador de filtro, insira **sys_properties.list** e localize a propriedade do sistema *sn_sec_cmn.background_job_max_concurrency*.



2. Clique para abrir o registro.

Por padrão, a propriedade do sistema *sn_sec_cmn.background_job_max_concurrency* executa no máximo 10 trabalhos em segundo plano em paralelo.

Se sua instância tiver um número baixo de nós, você poderá reduzir esse valor na propriedade do sistema. Por exemplo, digamos que você tenha sete regras de atribuição em sua lista de Regras de grupo. No registro de configuração do trabalho Reaplicar regras de atribuição, três trabalhos são definidos para o máximo de threads simultâneos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

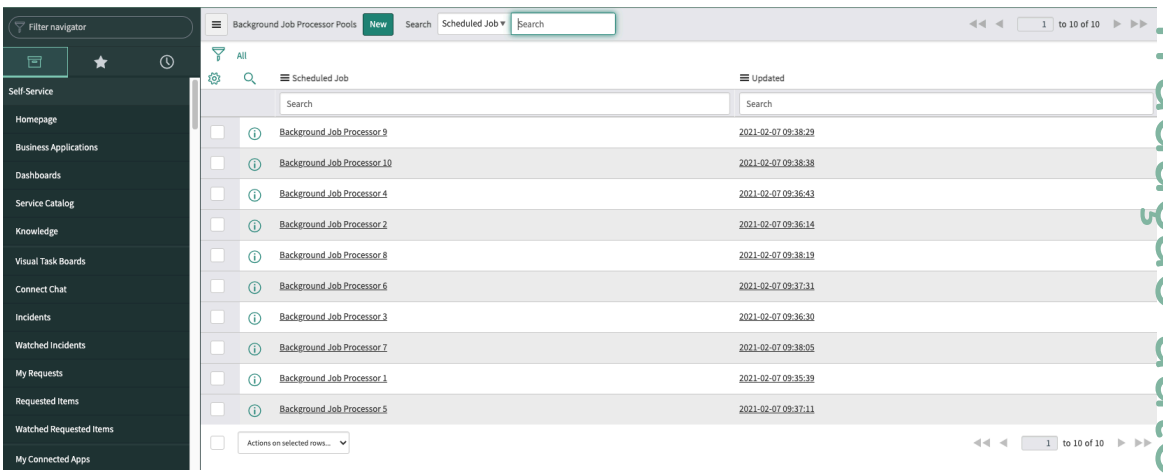
O valor de simultaneidade da sua estrutura é 10, mas o sistema é uma instância de nó único, portanto, você pode processar dois trabalhos particionados do trabalho Reaplicar regras de atribuição simultaneamente. Se você definir o Máximo de threads simultâneos como um registro de trabalho de Regras de atribuição, todos os tipos de trabalho Reaplicar regras de atribuição serão processados sequencialmente.

Por outro lado, se sua instância tiver mais nós, você poderá aumentar esse valor, mas também deverá adicionar mais trabalhos programados para fazer essa mudança.

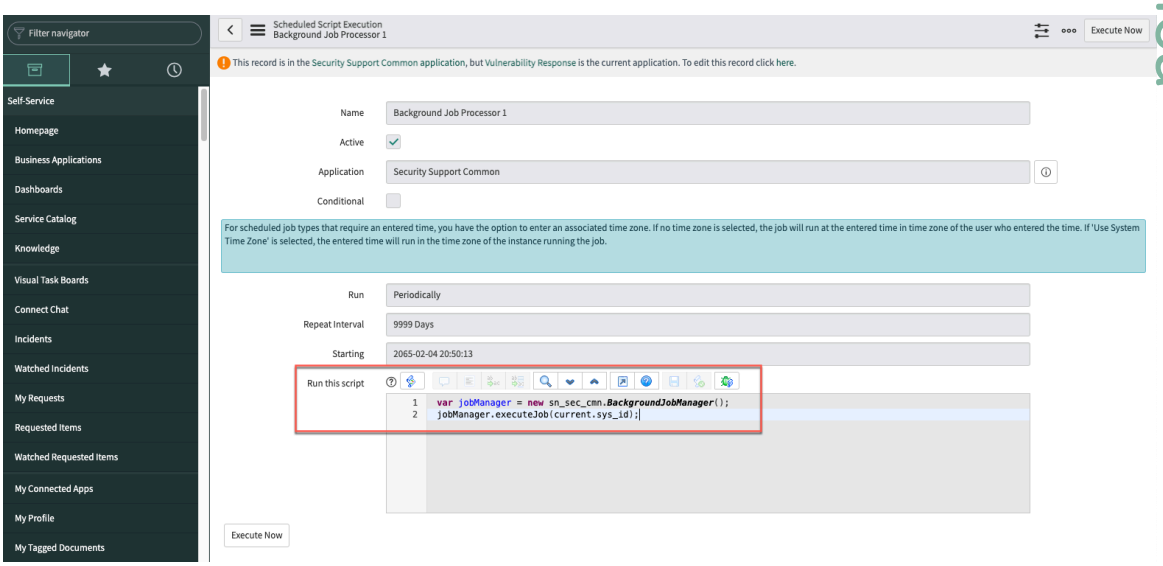
Para aumentar o número de trabalhos programados, duplique um trabalho programado quantas vezes forem necessárias para corresponder ao valor pelo qual você aumentou a propriedade do sistema. Por exemplo, por padrão, há 10 trabalhos programados. Portanto, se você quiser 20 trabalhos, deverá duplicar um trabalho 10 vezes.

Os dez trabalhos programados incluídos com Now Platform® para processamento são exibidos na tabela sn_sec_cmn_background_job_processor_pool.

3. No Navegador de filtro, insira **sn_sec_cmn_background_job_processor_pool.list**



4. Clique em um trabalho para copiá-lo e duplicá-lo quantas vezes forem necessárias para que o número de trabalhos corresponda ao valor pelo qual você aumentou a propriedade do sistema.



5. Depois que o trabalho programado for definido, adicione uma referência clicando em **Novo** na lista sn_sec_cmn_background_job_processor_pool para o trabalho que você copiou.

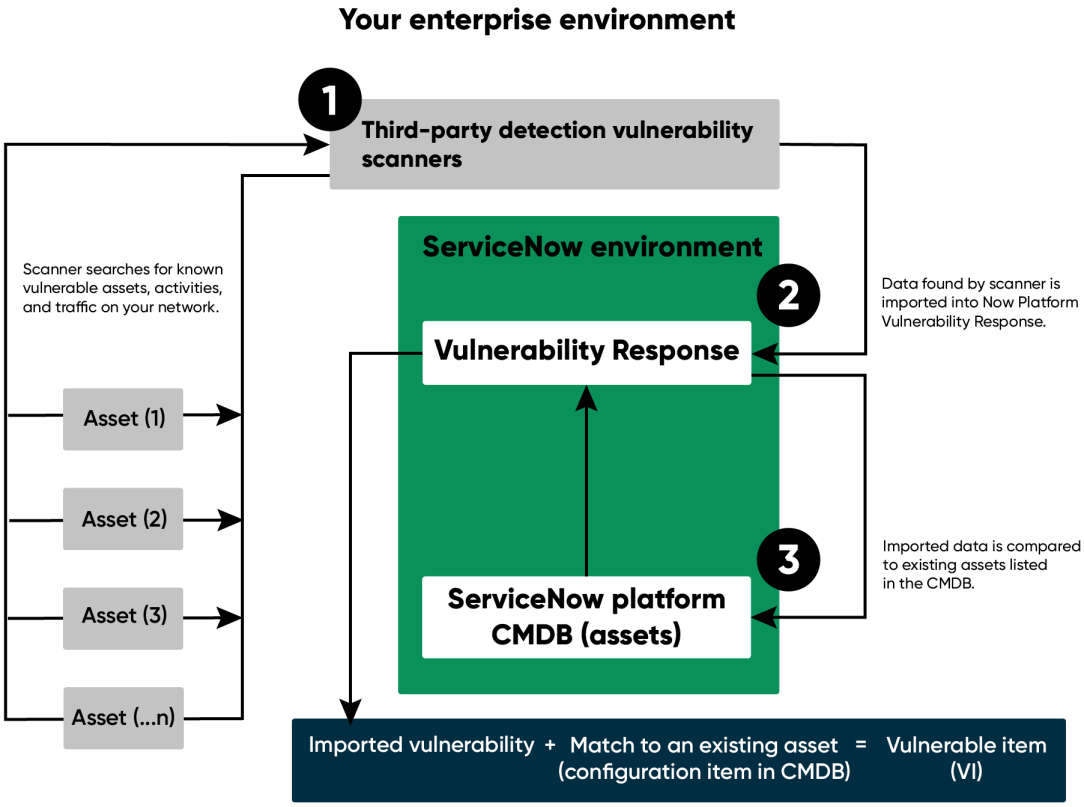
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Vulnerability Response

Vulnerability Response inclui suporte para integrações de terceiros. Esta seção inclui algumas diretrizes básicas para o desenvolvimento de suas próprias integrações.

Integrações de terceiros



As vulnerabilidades importadas do National Vulnerability Database (NVD) e os dados de detecção de scanners de terceiros são reconciliados com os ativos no seu CMDB. Quando uma vulnerabilidade importada corresponde a um ativo existente, um item vulnerável é criado. Itens vulneráveis são agrupados automaticamente em tarefas para correção, pontuados de risco com contexto de negócios, priorizados e atribuídos às equipes apropriadas para correção.

Nota:

Integrações de terceiros são tratadas separadamente. Se mais de uma aplicação de integração de terceiros estiver em uso em seu ambiente, não haverá desduplicação de item vulnerável (IV) entre as integrações. Por exemplo, a desduplicação de IV entre Rapid7 e Qualys não está disponível.

No entanto, são esperadas incompatibilidades na contagem de detecção entre um scanner de terceiros (por exemplo, Qualys) para IVs em sua instância ServiceNow, já que deduplicamos em IPs, portas e assim por diante.

Para obter informações sobre integrações de terceiros compatíveis com Application Vulnerability Response, consulte, Integração do Application Vulnerability Response a outras aplicações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Integração de Vulnerabilidade de Exploração Conhecida (KEV) da CISA
- Noções básicas sobre a integração de vulnerabilidade do Microsoft Threat and Vulnerability Management
- Noções básicas sobre a integração de orquestração de patches do BigFix HCL com Vulnerability Response
- Noções básicas sobre a integração de orquestração de patches [Vulnerability Response com Microsoft SCCM
- Noções básicas sobre as integrações do NVD
- Integração da vulnerabilidade da Qualys
- Noções básicas sobre o Rapid7 Vulnerability Integration
- Shodan Exploit Integration
- Noções básicas sobre a integração de vulnerabilidade da Tenable
- Integrações da Solução do Microsoft Security Response Center Solution Integration

O Integração com a solução Microsoft Security Response Center está disponível com Solução de gerenciamento de vulnerabilidade. Para obter informações sobre a instalação e configuração de Integração com a solução Microsoft Security Response Center e Red Hat Solution Integration, consulte Instalar a aplicação Solução de gerenciamento do Vulnerability Response. Você pode configurar, editar, programar e iniciar sob demanda o Integração com a solução Microsoft Security Response Center e o Red Hat Solution Integration de dentro do Assistente de configuração.

Anotações adicionais para integrações

Se várias implantações forem compatíveis com uma integração, consulte Criar importações separadas por domínio para uma integração.

- Você pode instalar, configurar, programar e iniciar sob demanda muitos dos aplicativos de integração de dentro do Assistente de configuração.
- Você pode instalar a aplicação Rapid7 Vulnerability Integration do Assistente de configuração, mas a configuração não é compatível com esta integração de dentro do Assistente de configuração. Para obter mais informações, consulte Instalar o Rapid7 Vulnerability Integration.
- A aplicação Tenable para Vulnerability Response da Tenable é criada e mantida pela Tenable. Consulte a documentação em Tenable para Vulnerability Response.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

A partir do VR v17.1, os seguintes nomes de estado do processo de integração foram atualizados:

Nome do estado antes da V17.1	Nome do estado V17.1 em diante
Processando	Recuperando
Aguardar conclusão	Aguardando/Processando

Nota:
Você pode exibir os anexos que foram baixados e processados. Quando o status da execução da integração é esperaconcluída, ele exibe a porcentagem da integração que está concluída.

Integrações criadas manualmente

Você pode adicionar outras integrações que não estão disponíveis como aplicações ServiceNow Store, conforme necessário. Para obter mais informações, consulte Criar manualmente uma integração de vulnerabilidade.

Noções básicas sobre as integrações do NVD

As integrações do NVD usam dados importados do produto National Vulnerability Database (NVD) do National Institute of Standards and Technology (NIST) para ajudar a determinar o impacto e a prioridade das falhas no seu código. Execute esta integração como parte de sua configuração inicial de Vulnerability Response e antes de importar dados de vulnerabilidade para sua instância com um scanner de terceiros.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

O NIST NVD coleta dados de vulnerabilidades e exposições comuns (CVE) e enumeração de plataforma comum (CPE) e disponibiliza esses dados para o Now Platform®. Ele se integra facilmente a Vulnerability Response para mapear vulnerabilidades de CVE e CPE, enriquecendo os dados em sua instância.

Importante:
Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Depois de instalada, a integração do NIST National Vulnerability Database Integration - API (somente CVE) é invocada automaticamente como um trabalho programado e é executada diariamente. Você também pode executar trabalhos programados individuais manualmente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os trabalhos programados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Dica:
A ativação desse plug-in em instâncias de produção pode exigir uma licença separada.

Versões disponíveis

Versão de lançamento	Notas de versão
Vulnerability Response Integração com NVD v1.2	

Importação inicial de dados de vulnerabilidade com as integrações de NVD e CWE

1. Execute uma importação inicial de dados do CWE com a Integração abrangente do CWE 2000.

   Consulte Configurar e executar o trabalho programado para atualizar registros CWE. Você executa atualizações do CWE **sob demanda** a partir do registro de integração por padrão e deve configurá-lo.

   Nota:
   Programe a atualização do CWE para ser executada antes da atualização do banco de dados do NVD. O dia padrão para a atualização do NVD é **Semanalmente** na segunda- **feira**.

2. Verifique se a aplicação Vulnerability Response Integration with NVD está instalada e se uma importação de dados inicial da integração de banco de dados de vulnerabilidades do NIST - API (somente CVE) ou da integração de banco de dados de vulnerabilidades do NIST - API (CVE e CPE) foi bem-sucedida.

   Para CPEs, verifique se uma importação de dados inicial da API do NIST National Vulnerability Database Integration (somente CPE) foi bem-sucedida.

   A ativação desse plug-in em instâncias de produção pode exigir uma licença separada. Depois que o plug-in é instalado, a API do NIST National Vulnerability Database Integration (somente CVE) é ativada por padrão. Ele é executado diariamente. Para obter mais informações, consulte Instalar a integração Vulnerability Response com o banco de dados nacional de vulnerabilidades do NIST.

3. Bibliotecas de terceiros são atualizadas como trabalhos programados. Consulte a documentação de integração em Integrações do Vulnerability Response para obter mais informações sobre integrações de terceiros.

Noções básicas sobre dados de vulnerabilidade importados e itens vulneráveis

Na sua instância Now Platform, cada vulnerabilidade importada é representada por uma entrada de vulnerabilidade nas bibliotecas de origem de produtos de varredura de terceiros como Qualys, por exemplo. Os itens vulneráveis (IV) que são importados e atualizados em sua instância são referências a bibliotecas de terceiros, como a biblioteca Qualys. Uma biblioteca de terceiros pode, por sua vez, fazer referência ao NVD.

Por exemplo, ao ingerir dados de vulnerabilidade de terceiros de um produto como Qualys, você está ingerindo IVs que fazem referência a um QID (Qualys Identificador). No caso de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Qualys, esse QID por sua vez faz referência a um CVE da biblioteca NVD. Ao clicar nesse QID em uma tarefa de correção ou registro de item vulnerável na aplicação Vulnerability Response e executar as integrações de NVD e CWE para ingerir dados, você está exibindo dados de vulnerabilidade atuais e aprimorados que permitem ver os relacionamentos existentes entre seus IVs e CVEs, CWEs e CPEs.

Antes de executar um produto de varredura de terceiros como Qualys que tem sua própria biblioteca, você deve primeiro instalar e executar, pelo menos, a integração do NIST National Vulnerability Database Integration- API (somente CVE) (também inclui detalhes relacionados ao CISA) , integração do CWE para ingerir dados de vulnerabilidade. Essas importações de dados de NVD e CWE aprimoram seus dados Vulnerability Response ou Application Vulnerability Response antes de importar dados com um produto de terceiros.

Para obter mais informações sobre como gerenciar o NVD, CWE e bibliotecas de terceiros e exibi-las, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros e Exibir Vulnerability Response bibliotecas de vulnerabilidade.

Depois de verificar a importação de NVD bem-sucedida, para aprimorar ainda mais seus dados de vulnerabilidade, Configurar e executar o trabalho programado para atualizar registros CWE.

Execute as importações de NVD e CWE antes de importar dados de vulnerabilidade com um produto de terceiros. Bibliotecas de terceiros são atualizadas como trabalhos programados. Consulte a documentação de integração em Integrações do Vulnerability Response para obter mais informações sobre integrações de terceiros.

Localizando as integrações do NVD

Para exibir as integrações do NVD, navegue até **Vulnerability Response ou Application Vulnerability Response** > **Administração** > **Integrações**.

As integrações a seguir estão incluídas no sistema de base.

Nota:
Somente a integração do NIST National Vulnerability Database Integration - API (somente CVE) está ativa, por padrão.

Integrações do NVD

Integração	Descrição
NIST National Vulnerability Database Integration - API (somente CVE)	Recupera somente dados de vulnerabilidade do NIST NVD (CVE). Por padrão, esta integração é definida automaticamente para ser executada diariamente.
NIST National Vulnerability Database Integration API (somente CPE)	Recupera dados de CPE do NIST NVD. Esta integração está inativa por padrão. Ative esta integração se quiser capturar dados de CPE que incluem um formato de nome formal, um método para verificar nomes em relação a um sistema e um formato de descrição para vincular texto e testes a um nome. Essas informações são armazenadas em Software vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do NVD

Integração	Descrição
	Esta integração é definida para ser executada diariamente e está inativa por padrão. Para ativar esta integração, consulte Ativar o NIST National Vulnerability Database–API (somente CPE).
NIST National Vulnerability Database Integration API (CPE não mapeado)	Recupera dados de CPE associados ao CVE buscado do NIST NVD. Esta integração está inativa por padrão. Ative esta integração se quiser capturar dados de CPE que incluem um formato de nome formal, um método para verificar nomes em relação a um sistema e um formato de descrição para vincular texto e testes a um nome. Essas informações são armazenadas em uma lista relacionada de registro de entrada de vulnerabilidade do NVD. Esta integração é definida para ser executada sob demanda e está inativa por padrão. Para ativar esta integração, consulte Ativar a API do banco de dados nacional de vulnerabilidades do NIST (CPE não mapeado).

Importante:
A integração "NIST National Vulnerability Database Integration-API (CVE e CPE)" está obsoleta.

Para obter os status de execução da integração, consulte Exibir o status da execução de importação da integração do NVD (National Vulnerability Database).

Preparando para as integrações do NVD

Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. As integrações do NVD pressupõem que você esteja familiarizado com o NIST National Vulnerability Database (NVD).

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Nota:
Antes de executar as integrações do NVD, faça as mudanças de configuração necessárias com base em seus requisitos.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Configurar e executar o trabalho programado para atualizar registros CWE

Dimportações de dados do CWE enriquecem ainda mais os dados de vulnerabilidade em sua instância. Use registros de enumeração de pontos fracos comuns (CWE) baixados do banco de dados do CWE para referência ao decidir se uma vulnerabilidade deve ser escalonada. Execute esta integração como parte de sua configuração inicial de Vulnerability Response e antes de importar dados de vulnerabilidade para sua instância com um scanner de terceiros.

Antes de Iniciar
Funções necessárias: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)
Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Nota:
Programe a atualização do CWE para ser executada antes da atualização do banco de dados do NVD. O dia padrão para a atualização do NVD é **Semanalmente** na segunda- **feira**.

Atualize os registros de fraqueza comuns do banco de dados de Enumeração de Pontos Fracos Comuns em uma programação regular. Você também pode atualizar o script padrão ou escrever seus próprios scripts, conforme necessário.

Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco. Você não pode escalar uma vulnerabilidade na página Enumerações de Pontos Fracos Comuns.

- Se você tiver a função de administrador, poderá adicionar repositórios ao trabalho programado.
- Se você tiver sn_vul.vulnerability_read, poderá executar o trabalho programado.
- Se você tiver sn_vul.vulnerability_write, poderá editar os detalhes do trabalho programado.

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Integrações**.
2. Selecione o trabalho programado **Integração abrangente do CWE 2000**.
3. Modifique os campos, conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Integração de vulnerabilidade

Campo	Descrição
Nome	Nome do trabalho programado.
Ativo	Se o trabalho programado está ativo. Se você não quiser que o trabalho seja executado por um período específico, poderá configurar os parâmetros que deseja usar e desativar o trabalho.
Executar	Frequência com que você deseja que o trabalho seja executado. Os campos subsequentes são exibidos ou ocultos com base na sua configuração neste campo. **Nota:** A atualização do CWE é **Sob demanda** por padrão. Defina como um período programado anterior às atualizações do NVD. As opções incluem: ○ Diariamente: escolha um **horário** ○ Semanalmente: (opção mais comum) escolha um **dia** e**hora** ○ Mensalmente: escolha **dia** e **hora** ○ Periodicamente: escolha um **intervalo de repetição**, data e hora de **início** ○ Uma vez: escolha uma data e hora de **início**
Dia	O dia em que você deseja que o trabalho programado seja executado. Se você selecionou **Semanalmente** no campo **Executar**, este campo exibirá os dias da semana. Se você selecionou **Mensalmente** no campo **Executar**, este campo exibirá os dias do mês. **Nota:** Programe a atualização do CWE para ser executada antes da atualização do banco de dados do NVD. O dia padrão para a atualização do NVD é **Semanalmente** na segunda- **feira**.
Hora	A hora em que você deseja que o trabalho programado seja iniciado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Programe a atualização do CWE para ser executada antes da atualização do banco de dados do NVD. O tempo padrão para a atualização do NVD é 01:00:00
Script de integração	O script para extrair dados das fontes de dados especificadas na lista relacionada **Fontes de dados**.
Integração de origem	[Somente leitura]
Instância de origem	[Somente leitura]
Aplicação	[Somente leitura] O nome da aplicação para a qual você está executando o trabalho programado.
Intervalo de repetição	O número de dias e horas antes que o trabalho programado seja executado novamente. Este campo aparece quando **Periodicamente** é selecionado na lista **Executar**.
Iniciando	A data e a hora de início das atualizações periódicas. Este campo aparece quando **Periodicamente** é selecionado na lista **Executar**.
Condicional	A caixa de seleção para adicionar parâmetros condicionais.
Condição	As condições para executar o trabalho programado. Este campo aparece quando a caixa de seleção **Condicional** está marcada.
Estratégia do processador de relatórios	A estratégia para extrair dados e processar o trabalho programado. ○ Para extrair dados das fontes de dados na lista relacionada **Fontes** de dados usando o script no campo Script de **integração**, selecione **Anexo de fonte de dados**. ○ Para selecionar um processador personalizado no campo de **script Processador de relatório**, selecione o **Processador de relatório personalizado**.
Processador de relatórios	O script a ser executado quando o trabalho programado for executado. Este campo aparece quando o **Processador de relatório personalizado** é selecionado na lista de **Estratégia do processador de relatório**.
Script de fábrica do processador	O script para criar o processador de relatório. Este campo aparece quando o **Processador de relatório personalizado** é selecionado na lista de **Estratégia do processador de relatório**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique com o botão direito do mouse no cabeçalho para **Salvar** suas mudanças.
5. Para executar o trabalho programado imediatamente, clique em **Executar agora**.
   Você retornará à exibição Integrações de vulnerabilidade.
6. Para observar o andamento da importação, selecione o trabalho programado **Integração abrangente do CWE 2000** novamente e selecione a guia **Execuções de integração de vulnerabilidade**.

   Consulte Exibir Vulnerability Response bibliotecas de vulnerabilidade para ver as entradas importadas.

Instalar a integração Vulnerability Response com o banco de dados nacional de vulnerabilidades do NIST

Antes de executar a integração em sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto NIST National Vulnerability Database (NVD) se integre corretamente a Vulnerability Response. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Tarefas de configuração	Descrição
Verifique se a aplicação Vulnerability Response está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Vulnerability Response.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o administrador do sistema [admin] instalará a aplicação e atribuirá usuários ao Gerenciador de vulnerabilidades em Vulnerability Response ou ao grupo Gerenciador de App-Sec em Application Vulnerability Response. Para obter informações sobre as funções do grupo em Vulnerability Response, consulte Gerenciar persona e funções granulares para Vulnerability Response. Para obter informações sobre funções de grupo em Application Vulnerability Response, consulte Application

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	Vulnerability Response grupos de usuários e funções. • O Gerenciador de vulnerabilidade ou o Gerenciador de App-Sec supervisiona a configuração e verifica os resultados esperados.

Função necessária: administrador

Nota:
Antes de executar as integrações do NVD, faça as mudanças de configuração necessárias com base em seus requisitos.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não mude este valor.

Procedimento

1. Faça login na instância na qual você deseja instalar as integrações do NVD.
2. Navegue até o ServiceNow Store.
3. No ServiceNow Store, pesquise a aplicação Vulnerability Response Integration with NVD.
4. Selecione o bloco da aplicação.
   Informações detalhadas sobre a aplicação que você está instalando são exibidas.

   Nota:
   Considere ler as seções **Outros requisitos** e **Dependências**, conforme aplicável.

5. Selecione **Solicitar app** e insira suas Now Support credenciais de login.
6. Selecione **Obter**.
7. Insira o **Nome da instância** e **o Motivo da instância**e selecione **Validar instância**.
8. Selecione **Solicitação**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Todos** > **Aplicações do sistema** > **Candidaturas** > **Todos**.
10. Localize a aplicação, selecione-a e selecione **Instalar**.
    Sua aplicação é instalada automaticamente na sua instância.

O que Fazer Depois

Após a instalação inicial, consulte as modificações em Modificação e atividades opcionais de integração do NVD.

Ativar a API do banco de dados nacional de vulnerabilidades do NIST (CPE não mapeado)

Para ingerir dados de enumeração de plataforma comum (CPE) para dados de vulnerabilidades e exposições comuns (CVE), você pode executar uma importação de dados completa com um trabalho programado sob demanda.

Antes de Iniciar

A integração do National Vulnerability Database Integration (NVD)–API (CPE não mapeada) captura dados (CPE) que incluem um formato de nome formal, um método para verificar nomes em relação a um sistema e um formato de descrição para vinculando texto e testes

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a um nome. Essas informações são armazenadas em uma lista relacionada de registro de entrada de vulnerabilidade do NVD.

Função necessária: sn_vul.vulnerability_admin ou App-Sec Manager

Procedimento

1. Navegar até **Todos** > **Vulnerability Response ou Application Vulnerability Response** > **NVD** > **Integrações**.
2. Selecione a integração NIST National Vulnerability Database Integration–API (CPE não mapeada).
3. Marque a caixa de seleção **Ativo**.

Nota:
A integração é pré-configurada para ser executada sob demanda. Ao ativar a integração, ela será executada automaticamente após a integração da API de integração do NIST NVD (somente CVE). Alterar qualquer outro parâmetro de integração requer ServiceNow e Vulnerability Response e experiência e pode resultar em dados incompletos.

   a. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Integrações**.
   b. Selecione Integração do banco de dados de vulnerabilidades do NIST – Integração de API (CPE não mapeada).
   c. Selecione a guia **Detalhes da integração**.
   Independentemente do valor do campo **Importar desde**, os CPEs de todos os CVEs recuperados são recuperados.
4. Selecione **Executar agora** para realizar uma execução inicial de integração de suporte completo.
   Depois que a importação inicial for concluída, as importações programadas de dados delta serão retomadas.
   Para obter status de execução de integração, consulte Exibir o status da execução de importação da integração do NVD (National Vulnerability Database).

Ativar o NIST National Vulnerability Database–API (somente CPE)

Para ingerir dados de enumeração de plataforma comum (CPE), você pode executar uma importação de dados completa com um trabalho programado diariamente.

Antes de Iniciar

A integração do National Vulnerability Database Integration (NVD)–API (somente CPE) do Instituto Nacional de Padrões e Tecnologia (NIST) captura dados (CPE) que incluem um formato de nome formal, um método para verificar nomes em relação a um sistema e um formato de descrição para vinculando texto e testes a um nome. Essas informações são armazenadas em uma tabela de software vulnerável.

Função necessária: sn_vul.vulnerability_admin ou App-Sec Manager

Procedimento

1. Navegar até **Todos** > **Vulnerability Response ou Application Vulnerability Response** > **NVD** > **Integrações**.
2. Selecione a integração do NIST National Vulnerability Database Integration–API (somente CPE).
3. Marque a caixa de seleção **Ativo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A integração é pré-configurada para ser executada diariamente. Alterar qualquer outro parâmetro de integração requer experiência ServiceNow e pode resultar em dados incompletos.
- A ativação desta integração ativará automaticamente as integrações NIST National Vulnerability Database Integration - API (somente CVE) e NIST National Vulnerability Database Integration - API (CPE não mapeado) e definirá seu campo de execução como sob demanda.
- Além disso, uma execução bem-sucedida da integração do NIST National Vulnerability Database Integration- API (somente CPE) acionará automaticamente o NIST National Vulnerability Database Integration- API (somente CVE). E a conclusão bem-sucedida da API do NIST National Vulnerability Database Integration (somente CVE) acionará automaticamente a API do NIST National Vulnerability Database Integration (CPE não mapeado).

Nota:
O campo Importar desde a data na integração do NIST National Vulnerability Database Integration - API (somente CPE) está vazio por padrão. Mantenha em branco para buscar dados dos últimos 357 dias.

Para recuperar dados históricos durante a importação inicial da verificação do NVD, defina uma data de início no registro de integração do NIST National Vulnerability Database Integration - API (somente CPE).

a. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Integrações**.

b. Selecione Integração do banco de dados de vulnerabilidades do NIST – Integração de API (somente CPE).

c. Selecione a guia **Detalhes da integração**.

d. Defina o valor do campo **Importar desde** como a data mais antiga que você deseja recuperar. Cada importação bem-sucedida redefine esta data para a data e a hora do dia selecionado.

4. Selecione **Executar agora** para realizar uma execução inicial de integração de suporte completo. Depois que a importação inicial for concluída, as importações programadas de dados delta serão retomadas. Para obter status de execução de integração, consulte Exibir o status da execução de importação da integração do NVD (National Vulnerability Database).

Modificação e atividades opcionais de integração do NVD

Configure modificações opcionais especificamente para as integrações do NVD.

Nota:
Alterar outras configurações de integração do NVD, além das listadas aqui, requer conhecimento avançado ServiceNow e Vulnerability Response e está além do escopo da documentação do produto.

Executar uma importação manual de integração do NVD

Se sua importação inicial falhar ou você não quiser aguardar a importação inicial programada, poderá executar uma importação de dados completa independentemente do trabalho programado diário ou semanal.

Antes de Iniciar

Nota:
As integrações NIST National Vulnerability Database Integration - API (somente CPE) e NIST National Vulnerability Database Integration - API (CPE não mapeadas) estão inativas por padrão. Para obter mais informações, consulte Ativar o NIST National Vulnerability Database–API (somente CPE) e Ativar a API do banco de dados nacional de vulnerabilidades do NIST (CPE não mapeado).

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Vulnerability Response ou Application Vulnerability Response** > **Administração** > **Integrações**.
2. Escolha uma integração, por exemplo, a integração do NIST National Vulnerability Database Integration - API (somente CVE).
3. Selecione **Executar agora**.

> **Nota:**
> Se a integração do NIST National Vulnerability Database Integration-API (CPE não mapeada) estiver ativada, os dados de CPE associados serão armazenados na lista relacionada de software vulnerável da entrada de vulnerabilidade do NVD. Consulte Vulnerability Response campos de formulário de vulnerabilidade.

4. Para obter os status de execução da integração, consulte Exibir o status da execução de importação da integração do NVD (National Vulnerability Database).

Exibir o status da execução de importação da integração do NVD (National Vulnerability Database)

Use a lista relacionada Execuções de integração de **vulnerabilidade** para verificar o sucesso de suas execuções de integração, localizar problemas e informar suas decisões de correção.

Antes de Iniciar

Para exibir o status de execução da importação da integração do NVD:

- Vulnerability Response e a aplicação Vulnerability Response integration with NVD integration deve ser instalada e configurada.
- As importações de integração do NVD devem estar em execução. A integração do NIST National Vulnerability Database Integration-API (somente CVE) é executada por padrão.

> **Nota:**
> As integrações NIST National Vulnerability Database Integration-API (apenas CPE) e NIST National Vulnerability Database Integration-API (CPE não mapeadas) estão inativas por padrão. Para obter mais informações, consulte Ativar o NIST National Vulnerability Database–API (somente CPE) e Ativar a API do banco de dados nacional de vulnerabilidades do NIST (CPE não mapeado).

Função necessária: sn_vul.vulnerability_admin ou App-Sec Manager

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite.

Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. O último registro processado com mais de uma hora indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Se você não estiver usando o gráfico de status de execução de integração do NVD, Navegar até **Todos** > **Vulnerability Response ou Application Vulnerability Response** > **Administração** > **Integrações**.
2. Selecione um **link** para uma integração.
3. Selecione a lista relacionada **Execuções de integração de vulnerabilidade**.
4. Verifique se todas as importações foram bem-sucedidas.

Trouble?

As causas mais comuns para uma execução com falha incluem:

- Interrupção de rede.
- Um problema na transferência de dados que resulta em dados corrompidos durante a transformação.

Se você encontrar qualquer uma dessas condições, selecione **Executar agora**e execute novamente a integração.

Tópicos relacionados

Vulnerability Response campos de formulário de vulnerabilidade

Adicionar CVEs a entradas de terceiros

As informações de vulnerabilidade e exposição comuns (CVE) podem ser relacionadas a uma única vulnerabilidade de terceiros. Geralmente, ele é adicionado durante uma importação de integração de terceiros. No entanto, você pode adicionar vários CVEs (vulnerabilidades) manualmente.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

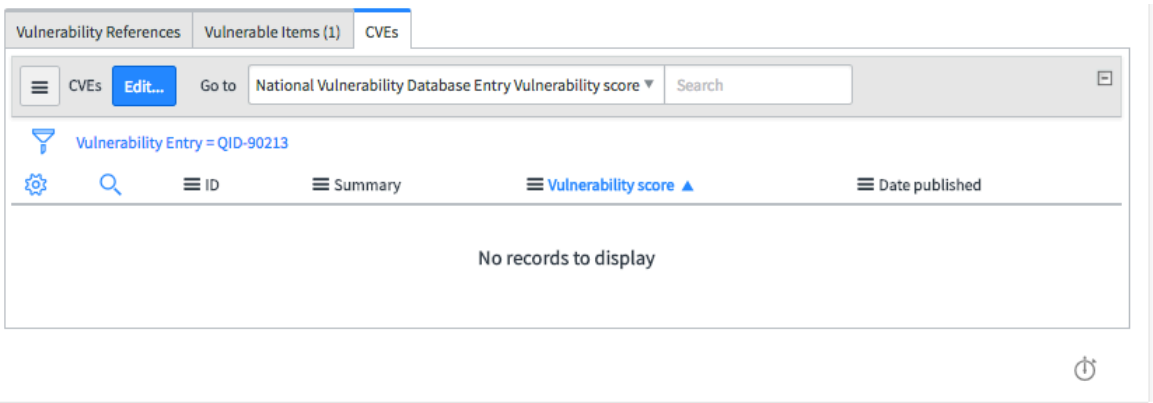
Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Bibliotecas** > **Terceiros**.
2. Abra um registro.
3. Clique na guia da lista relacionada de **CVEs**.



4. Clique em **Editar**.
5. Escolha quais CVEs adicionar.

> **Nota:**
> Você pode usar filtros de condição para refinar a coleção de CVE.

6. Clique em **Salvar**.

Tópicos relacionados

Vulnerability Response campos de formulário de vulnerabilidade

Exibir Vulnerability Response bibliotecas de vulnerabilidade

Você pode exibir dados de vulnerabilidade importados do National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) ou de terceiros para decidir se deve escalar uma tarefa de correção.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Bibliotecas**.

   Para obter informações sobre campos específicos, consulte Vulnerability Response campos de formulário de vulnerabilidade.

   As seguintes bibliotecas estão disponíveis:

Bibliotecas	Descrição
NVD	Lista de vulnerabilidades encontradas pelo NVD e inclui check-lists de segurança, falhas de software relacionadas à segurança, configurações incorretas, nomes de produtos e métricas de impacto, incluindo explorações.

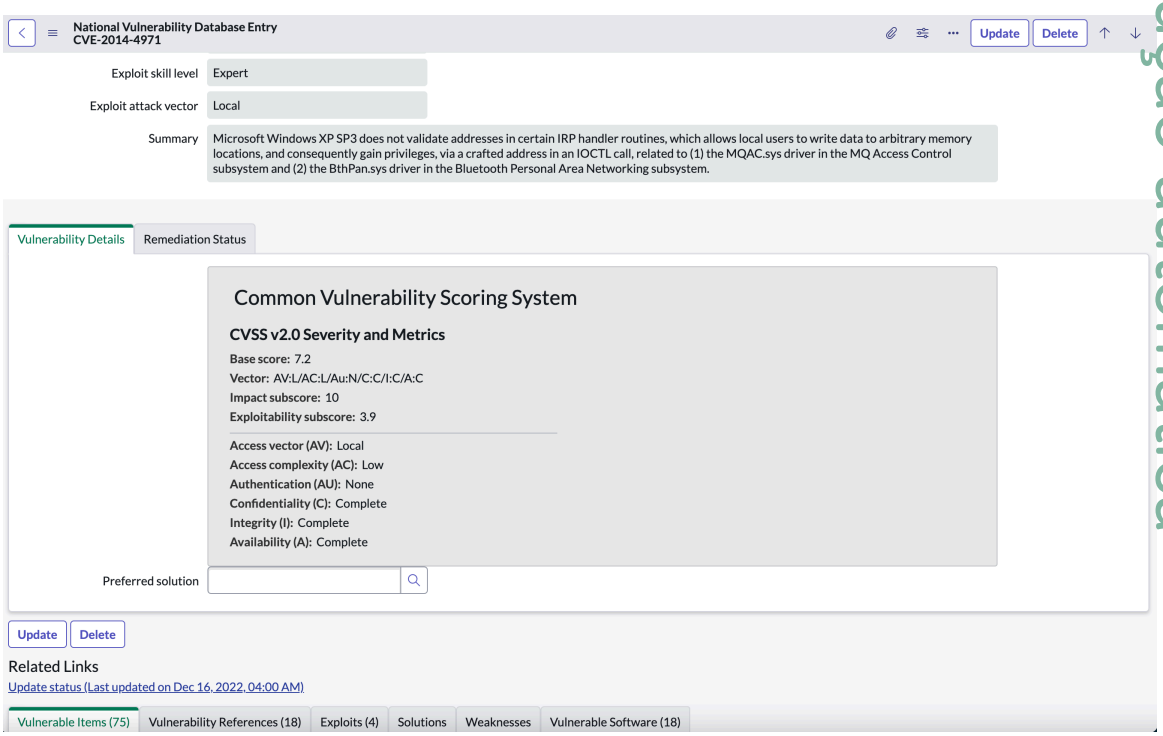
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Bibliotecas	Descrição
CWE	Lista de tipos de pontos fracos de software desenvolvidos pela comunidade. Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco. Você não pode escalar uma vulnerabilidade na tela Enumerações de Pontos Fracos Comuns, é apenas para referência.
Terceiros	Lista de vulnerabilidades de terceiros importadas em sua instância. Contém uma lista de referências relacionadas, itens vulneráveis, explorações e CVEs.

2. Escolha uma biblioteca para exibir as vulnerabilidades.
3. Clique em um link na lista para abrir um registro.

   Um registro CVE na biblioteca de entradas do banco de dados de vulnerabilidades nacionais. Mais informações estão disponíveis nos **Links relacionados**. Após uma importação de dados, você pode escolher uma vulnerabilidade e explorar seus relacionamentos com itens vulneráveis, explorações, possíveis soluções, possíveis patches e quaisquer referências a artigos da base de conhecimento na Base de conhecimento HI. Se Solução de gerenciamento de vulnerabilidade estiver instalado, você poderá exibir uma solução preferencial em registros NVD, se houver uma disponível.



Integração de Vulnerabilidade de Exploração Conhecida (KEV) da CISA

A integração Vulnerability Response com o catálogo de vulnerabilidades exploradas conhecidas (KEVs) da CISA ingere dados para ajudá-lo a priorizar e corrigir essas vulnerabilidades com eficácia.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A CISA permite a correção urgente e priorizada de vulnerabilidades ativamente exploradas para agências governamentais e empresas.

Sobre a CISA

A Cybersecurity & Infrastructure Security Agency (CISA) é uma agência de segurança cibernética e de infraestrutura dos EUA que publica um relatório sobre as vulnerabilidades mais exploradas. Ele se integra facilmente com Vulnerability Response para mapear vulnerabilidades de Vulnerabilidades e exposições comuns (CVE), enriquecendo os dados em sua instância. Essas informações são acumuladas na tabela Entradas de vulnerabilidade de terceiros. A data de vencimento mais antiga é considerada para o acúmulo dos itens vulneráveis.

Nota:
A caixa de seleção **CISA existe** para CVEs recuperados pela CISA.

Valores recuperados da integração CISA:

- ID do CVE
- Prazo
- Data adicionada
- Fornecedor/projeto
- Produto
- Ransomware conhecido (a partir da v21.0 de Vulnerability Response, um novo campo **conhecido por ser usado em campanhas de ransomware** é ingerido do catálogo de vulnerabilidades exploradas conhecidas (KEVs) da CISA. É indicado pela sinalização do campo **Ransomware conhecido** na tabela de banco de dados de entrada de vulnerabilidade nacional. O sinalizador é definido no nível de vulnerabilidades e exposições comuns (CVE) e acumulado para a entrada de terceiros (TPE).

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Trabalhos programados

A integração CISA é invocada automaticamente como um trabalho programado diariamente. Você também pode executar trabalhos programados individuais manualmente. Os trabalhos programados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Versões disponíveis

Versão de lançamento	Notas de versão
Vulnerability Response v16.5, v18.0 Vulnerability Response Integração com CISA v1.0, v1.2	

Exibição da integração CISA

Para exibir a integração CISA, navegue até **Vulnerability Response** > **Administração** > **Integrações** > **Integração de vulnerabilidade de exploração conhecida da CISA**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As integrações a seguir estão incluídas no sistema de base.

Nota:
Somente a integração CISA está ativa, por padrão.

Integração CISA

Integração	Descrição
Integração de Segurança Cibernética e Agência de Segurança de Infraestrutura (CISA)	Recupera dados de vulnerabilidade CISA (CVE) e enriquece os dados de vulnerabilidade existentes. Esta integração é definida automaticamente para ser executada diariamente.

Para exibir dados em vulnerabilidades de terceiros, consulte Exibir Vulnerability Response bibliotecas de vulnerabilidade.

Preparando para a integração CISA

Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. A integração de vulnerabilidade conhecida explorada da CISA pressupõe que você esteja familiarizado com a Cybersecurity & Infrastructure Security Agency (CISA).

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Nota:
Antes de executar a integração do CISA, faça as mudanças de configuração necessárias com base em seus requisitos.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Instalar a aplicação Vulnerability Response Integration with CISA ServiceNow®

Antes de executar a integração na sua instância, as etapas de instalação e configuração devem ser concluídas para que o consultor de vulnerabilidades conhecidas da Cybersecurity & Infrastructure Security Agency (CISA) se integre ao Vulnerability Response. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Tarefas de configuração	Descrição
Verifique se a aplicação Vulnerability Response está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Vulnerability Response.
Verifique se a aplicação Vulnerability Response Integration with NVD está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar a integração Vulnerability Response com o banco de dados nacional de vulnerabilidades do NIST.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o administrador do sistema [admin] instalará a aplicação e atribuirá usuários ao gerenciador de vulnerabilidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	em Vulnerability Response. Para obter informações sobre as funções do grupo em Vulnerability Response, consulte Gerenciar persona e funções granulares para Vulnerability Response. • O gerenciador de vulnerabilidades supervisiona a configuração e verifica os resultados esperados.

Função necessária: administrador

Procedimento

1. Faça login na instância na qual você deseja instalar o Vulnerability Response Integration with CISA.
2. Navegue até o ServiceNow Store.
3. No ServiceNow Store, pesquise a aplicação Vulnerability Response Integration with CISA.
4. Selecione o bloco da aplicação.
   Informações detalhadas sobre a aplicação que você está instalando são exibidas.

   Nota:
   Considere ler as seções **Outros requisitos** e **Dependências**, conforme aplicável.

5. Selecione **Solicitar app** e insira suas Now Support credenciais de login.
6. Selecione **Obter**.
7. Insira o **Nome da instância** e **o Motivo da instância**e selecione **Validar instância**.
8. Selecione **Solicitação**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Candidaturas**.
10. Localize a aplicação, selecione-a e selecione **Instalar**.
    Sua aplicação é instalada automaticamente na sua instância.

O que Fazer Depois

Nota:
Nenhuma configuração é necessária para a integração CISA.

Noções básicas sobre a integração do Sistema de pontuação de previsão de exploração (EPSS)

Visão geral da integração de EPSS com Vulnerability Response.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral

A integração do Sistema de pontuação de previsão de exploração (EPSS) importa dados de EPSS relacionados a vulnerabilidades e exposições comuns (CVEs) do First.org para priorizar e corrigir vulnerabilidades. Para obter mais informações, consulte https://www.first.org . O Sistema de pontuação de previsão de exploração (EPSS) é um esforço orientado por dados para estimar a probabilidade (probabilidade) de que uma vulnerabilidade de software será explorada na natureza. O modelo de EPSS produz uma pontuação de probabilidade entre 0 e 1 (0 e 100%). Quanto maior a pontuação, maior a probabilidade de uma vulnerabilidade ser explorada.

As importações de dados da integração de EPSS enriquecem ainda mais os dados de NVD em sua instância. Se os registros de NVD não estiverem presentes, ele criará um espaço reservado na tabela CVE e adicionará detalhes de EPSS na mesma tabela. Execute esta integração como parte de sua configuração inicial de Vulnerability Response e antes de importar dados de vulnerabilidade para sua instância com um scanner de terceiros.

Importante:
Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é VR.System. Não altere este valor.

Importação inicial de dados com a integração de EPSS

1. Realize uma importação inicial de dados de EPSS com a integração de EPSS First.org. Para obter mais informações, consulte Configure e execute um trabalho programado para atualizar registros CVE com dados EPSS.

   Importante:
   Você executa atualizações de EPSS **diariamente** a partir do registro de integração por padrão e deve configurá-lo se quiser que ele seja executado como um trabalho programado.

2. Bibliotecas de terceiros são atualizadas como trabalhos programados. Para obter mais informações, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

   Importante:
   É recomendável executar integrações do NIST National Vulnerability Database Integration - API (somente CVE) antes do EPSS.

Execute as importações de EPSS antes de importar dados de vulnerabilidade com um produto de terceiros. Bibliotecas de terceiros são atualizadas como trabalhos programados. Consulte a documentação de integração em Integrações do Vulnerability Response para obter mais informações sobre integrações de terceiros.

Importante:
A integração a seguir está incluída no sistema de base. A integração está ativa por padrão.

Após a execução inicial, os trabalhos programados do sistema de base executam as integrações automaticamente na ordem. Você também pode executar trabalhos programados individuais manualmente. Os trabalhos programados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Na ativação da integração de EPSS, os campos Pontuação de EPSS, Percentual de EPSS e Última modificação de EPSS são adicionados à tabela Entradas de vulnerabilidade. Para CVEs existentes, esses campos são atualizados automaticamente na conclusão bem-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

sucedida do trabalho de importação inicial. Se houver novos CVEs adicionados à tabela Entradas de vulnerabilidade após a conclusão do trabalho programado do EPSS, os CVEs recém-adicionados indicarão sua origem como EPSS. As pontuações são acumuladas para TPEs existentes de CVEs da tabela NVD, usando o sistema de base `Rollup EPSS score from NVD to TPEs calculator`. Você também pode modificar a calculadora. Para obter mais informações, consulte Vulnerability Response Calculadoras de Rollup.

Tópicos relacionados

Criar uma calculadora Vulnerability Response

Configure e execute um trabalho programado para atualizar registros CVE com dados EPSS

Personalize o trabalho programado do sistema de base para atualizar registros CVE com dados EPSS.

Antes de Iniciar

Importante:
Você precisa baixar e ativar o plug-in Vulnerability Response Integration with CISA (com.snc.vulnerability.cisa) para habilitar a integração de EPSS.

A seguir está a lista de novos campos adicionados à tabela NVD para armazenar dados de EPSS.

- Pontuação de EPSS
- Percentual de EPSS
- Última modificação de EPSS

Nota:
Configure a exibição de lista ou a exibição de formulário de acordo com o requisito para exibir os campos recém-adicionados.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

As importações de dados da integração de EPSS enriquecem ainda mais os dados de NVD em sua instância. Se os registros de NVD não estiverem presentes, ele criará um espaço reservado na tabela CVE e adicionará detalhes de EPSS na mesma tabela. Execute esta integração como parte de sua configuração inicial do Vulnerability Response e publique para importar dados de vulnerabilidade para sua instância.

Nota:
Por padrão, a integração de EPSS do First.org está no estado **Ativo**. O trabalho programado do sistema de base é configurado, por padrão, para ser executado diariamente.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Integrações**.
2. Localize e selecione First.org EPSS Integration.
3. Modifique os campos, conforme necessário.
4. Clique com o botão direito do mouse no cabeçalho para **Salvar** suas mudanças.
5. Selecione **Executar agora**para executar o trabalho programado imediatamente.
   Você retornará à exibição Integrações de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Selecionar **EPSS do First.org** > **Guia Execuções de integração de vulnerabilidade** para exibir o andamento da importação.
   Na conclusão bem-sucedida do trabalho programado, as pontuações de EPSS, o percentil e os carimbos de data/hora da pontuação de EPSS da última modificação são atualizados nos CVEs.

O que Fazer Depois

- Consulte Adicionar condição de pontuação de EPSS na regra de negócio da calculadora de risco.
- Consulte Exibir Vulnerability Response bibliotecas de vulnerabilidade para ver as entradas importadas.

Adicionar condição de pontuação de EPSS na regra de negócio da calculadora de risco

Modifique a regra de negócios para adicionar a condição de pontuação de EPSS à calculadora de risco.

Antes de Iniciar

Nota:
O procedimento a seguir é necessário para que as atualizações de EPSS em vulnerabilidades sejam distribuídas para os itens vulneráveis.

Função necessária: sn_vul.manage_risk_score_configuration

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Regra de negócios**.
2. Pesquise por **Definir sinalizador de recálculo**.

   Nota:
   Há duas `Set recalculate flag` regras de negócio. Você pode usar qualquer um deles.

3. Navegue até a guia **Quando executar**.
4. Selecione **Adicionar cláusula "OR"** e selecione `Pontuação de EPSS` em **Escolher campo** e `mudanças` no campo **Escolher operador**.
5. Selecione **Atualizar**.

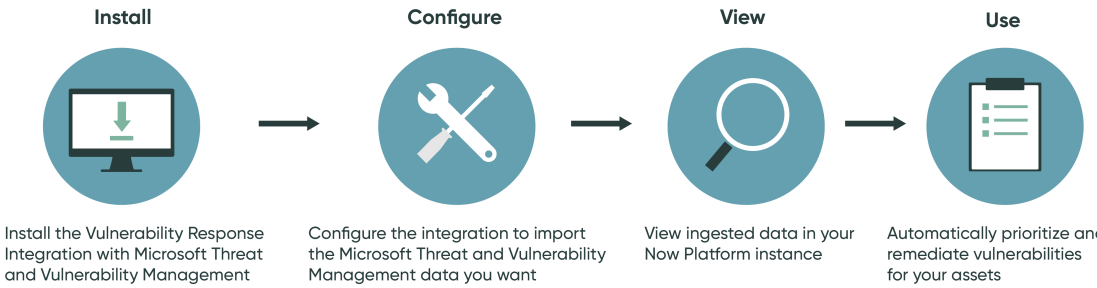
Noções básicas sobre a integração de vulnerabilidade do Microsoft Threat and Vulnerability Management

A integração do Vulnerability Response com a aplicação Microsoft Threat and Vulnerability Management (MS TVM) usa dados importados do MS TVM para ajudá-lo a priorizar e corrigir vulnerabilidades de seus ativos. A aplicação está disponível com uma assinatura separada do ServiceNow Store.

Você pode usar a integração de vulnerabilidade do MS TVM para importar dados do scanner de terceiros sobre seus ativos e vulnerabilidades. Você pode exibir relatórios sobre vulnerabilidades e itens vulneráveis nos painéis Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Versões disponíveis

Versão de lançamento	Notas de versão
Vulnerability Response Integração com MS TVM v2.2	Para obter mais informações sobre as versões lançadas da aplicação Vulnerability Response, compatibilidade e mudanças de esquema, consulte o artigo Matriz de compatibilidade do Vulnerability Response e mudanças de esquema de versão [KB0856498] na Base de conhecimento HI .

Domain Separation e MS TVM

Importe dados de integração de vulnerabilidade para um domínio especificado atribuindo um usuário nesse domínio para executar as integrações. Para criar importações separadas por domínio para a integração de vulnerabilidade do MS TVM, consulte Criar importações separadas por domínio para uma integração.

Termos e principais recursos das integrações

Itens vulneráveis e vulnerabilidades

Um item vulnerável é criado na sua instância Now Platform quando:

- Uma vulnerabilidade importada de um scanner de terceiros é correspondida a um ativo existente (item de configuração) no seu CMDB). O produto MS TVM se refere a essas correspondências como vulnerabilidades.
- Uma vulnerabilidade importada de um scanner de terceiros não corresponde a um ativo existente no seu CMDB. Nesse caso, um item de configuração (IC) incompatível também é criado com um item vulnerável.

  Use o Mecanismo de Identificação e Reconciliação (IRE) para criar ICs em duas novas classes quando um IC existente não puder ser correspondido com um host. Caso contrário, ICs incompatíveis serão criados nas classes de IC incompatíveis. Para obter mais informações, consulte Criando ICs para Vulnerability Response usando o mecanismo de Identificação e Reconciliação.

Entradas de vulnerabilidade de terceiros

As entradas de vulnerabilidade de terceiros são importadas de scanners de terceiros, como o MS TVM, e são listadas na tabela Entradas de vulnerabilidade de terceiros na instância Now Platform. Além disso, as entradas do banco de dados de vulnerabilidades nacionais (CVEs) são

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

importadas do MS TVM. As informações de exploração associadas a esses dois tipos de entradas vêm do MS TVM. Essas informações de exploração podem ser usadas para cálculo de risco.

Nota:
Uma vulnerabilidade de terceiros é recuperada somente para vulnerabilidades que não têm um CVE atribuído a elas. O MS TVM pode adicionar um nome temporário para a vulnerabilidade, por exemplo, TVM-XXXX-XXXX. Este nome é atualizado depois que um ID de CVE é atribuído.

IC (Configuration Item, item de configuração)

ICs são os ativos existentes listados em CMDB.

Item descoberto

Itens descobertos são os ativos ingeridos da importação da máquina MS TVM que correspondem aos ICs existentes no seu CMDB.

Se uma correspondência não for encontrada, um IC será criado na classe de IC incompatível do CMDB. Habilite o plug-in CMDB CI Class Models, o Mecanismo de Identificação e Reconciliação (IRE) cria ICs usando novas classes. Para obter mais informações, consulte Criando ICs para Vulnerability Response usando o mecanismo de Identificação e Reconciliação. Se o IC original incompatível for reclassificado, os registros do item descoberto serão atualizados para refletir esse estado. Os itens descobertos fornecem visibilidade de como os ativos são identificados e mapeados para ICs no CMDB.

Regras de pesquisa de IC

Quando os dados são importados do MS TVM, Vulnerability Response usa automaticamente os dados da máquina (ativo) para pesquisar correspondências no CMDB. As regras de pesquisa de IC são usadas para identificar ICs e adicioná-los aos registros de IV quando os IVs são criados.

Instância

Uma instância se refere a várias contas do MS TVM. Cada conta pode ser uma instância na aplicação MS TVM.

Integração

Uma integração é um trabalho programado que recupera informações de uma fonte de terceiros, como a integração das máquinas MS TVM.

Implantação

Quando uma integração oferece suporte a várias origens, uma única existência de integração é chamada de implantação da sua integração. Uma implantação se refere às integrações e produtos em seu ambiente. Por exemplo, você pode ter várias implantações do MS TVM em seu ambiente.

A integração do MS TVM também inclui os seguintes recursos principais:

- Você pode identificar os ativos em seu ambiente e atualizar os ICs em seus itens descobertos existentes, itens vulneráveis e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.
- Você pode programar quando deseja que os trabalhos sejam executados para todas as integrações do MS TVM. Você também pode executar trabalhos programados sob demanda.
- Você pode agrupar itens vulneráveis.
- Você pode configurar regras de pesquisa de IC para definir como os dados de ativo de fontes de terceiros são usados para identificar ICs em seu CMDB.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções necessárias de Now Platform

As tarefas de integração exigem as seguintes funções na sua instância Now Platform.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

admin

O administrador do sistema usa o Assistente de configuração para instalar a aplicação MS TVM. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração.

sn_vul.vulnerability_admin

Depois de atribuído, o administrador de vulnerabilidade conclui a configuração das integrações do MS TVM no Assistente de configuração. Esta função tem acesso completo à aplicação Vulnerability Response e seus registros. O administrador de vulnerabilidades configura todas as Vulnerability Response aplicações e regras para integrações de terceiros instaladas.

sn_vul_msft_tvm.configure_integration

Esta função contém a função granular sn_vul_msft_tvm.read_integration. Usuários com esta função podem configurar a integração do Vulnerability Response com a aplicação Microsoft Threat and Vulnerability Management.

sn_vul_msft_tvm.read_integration

Usuários com esta função só podem exibir a integração do Vulnerability Response com os registros da aplicação Microsoft Threat and Vulnerability Management.

Grupo do Vulnerability Response

Por padrão, o grupo do Vulnerability Response está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Vulnerability Response herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente.

Integrações do MS TVM

Várias origens são compatíveis com todas as integrações do MS TVM. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente do Assistente de configuração em Vulnerability Response. Você também instala e configura a integração Vulnerability Response com a aplicação MS TVM no Assistente de configuração.

Para exibir as integrações do MS TVM, navegue até **Integração de vulnerabilidade Microsoft VTM** > **Administração** > **Integrações**. Vulnerability Response fornece integrações com endpoints do MS TVM para importar os dados de acordo com os intervalos de tempo programados. As integrações a seguir estão incluídas no sistema de base.

Integrações do MS TVM

Sequência de execução	Programação	Integração	Descrição
1	Diariamente	Integração de recomendações do Microsoft TVM	Recupera uma lista de todas as recomendações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do MS TVM

Sequência de execução	Programação	Integração	Descrição
			de segurança acionáveis para corrigir as vulnerabilidades.
2	Diariamente	Integração de vulnerabilidade do Microsoft TVM (CVE)	Recupera uma lista das entradas do banco de dados de vulnerabilidades nacionais e entradas de vulnerabilidades de terceiros, bem como suas informações de exploração.
3	Diariamente	Integração de máquinas com Microsoft TVM	Recupera todos os dados do ativo (máquina), incluindo marcadores de máquina, do Microsoft TVM e os processa em sua instância.
4	Semanalmente **Nota:** Após a instalação, esta integração é executada automaticamente após a importação das máquinas.	Integração de vulnerabilidades de máquinas com Microsoft TVM (importação completa)	Recupera todas as vulnerabilidades em aberto em todos os ativos.
5	Diariamente	Integração de vulnerabilidades de máquinas com Microsoft TVM (importação delta)	Recupera todas as informações que foram alteradas na importação de vulnerabilidades completa da organização, incluindo as vulnerabilidades novas, corrigidas e atualizadas.

Itens vulneráveis são agrupados em tarefas de correção de acordo com as regras de grupo que você definiu e são atribuídos para correção com base em suas regras de atribuição. Para obter mais informações, consulte Vulnerability Response tarefas de correção e regras de tarefa visão geral e Vulnerability Response visão geral de regras de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de pesquisa de IC

Quando os dados são importados do MS TVM, Vulnerability Response usa automaticamente os dados da máquina (ativo) para pesquisar correspondências no Configuration Management Database (CMDB). As regras de pesquisa de IC são usadas para identificar ICs e adicioná-los aos registros de IV quando os IVs são criados. Para obter mais informações sobre como funcionam as regras de pesquisa de IC, consulte Regras de pesquisa de IC para identificar itens de configuração de Vulnerability Response integrações de vulnerabilidade de terceiros.

Nota:
Depois de remover uma regra, não será possível recuperá-la. Em vez de remover uma regra existente, você deve desabilitá-la.

As seguintes regras de pesquisa do MS TVM são enviadas com o sistema de base:

- MAC_ADDRESS
- FQDN
- IP

Nota:
Você pode usar vários valores para o IP_ADDRESS e o MAC_ADDRESS de um ativo. Uma regra de pesquisa de IC considera todos os valores para correspondência.

Itens descobertos

Você pode ver os ICs que foram detectados durante uma importação da integração do MS TVM Machines.

Nota:
O filtro padrão desta lista é definido como Incompatível. Você pode exibir todos os itens descobertos de uma importação removendo o filtro.

Para obter mais informações, consulte Itens Descobertos.

Marcadores de máquina

Os marcadores de máquina, também conhecidos como marcadores de host, são usados para organizar e rastrear os ativos em sua organização. Você atribui marcadores às suas máquinas.

Todos os marcadores de máquina são importados como parte da integração de máquinas MS TVM. Os marcadores de máquina geralmente são usados para filtragem em regras de atribuição Vulnerability Response e regras de grupo de vulnerabilidade. Os marcadores são exibidos no formulário Item descoberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Execute a integração do MS TVM Machine antes de criar Vulnerability Response regras de tarefa de atribuição ou correção na aplicação Vulnerability Response para que todos os marcadores estejam disponíveis para essas regras antes que os itens vulneráveis sejam importados e agrupados. Observe também os seguintes pontos sobre marcadores:

- O armazenamento de marcador não faz distinção entre maiúsculas e minúsculas. Se um marcador Paris for criado, um marcador PARIS não poderá ser armazenado na tabela de marcadores da máquina. Paris e PARIS são considerados o mesmo marcador de máquina pelo sistema. O marcador que for importado primeiro será o marcador armazenado e reconhecido.
- Usar marcadores de máquina como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. As chaves de grupo são colunas na tabela de tarefas de correção, enquanto os marcadores de máquina devem ser usados somente no construtor de condição.
- Os marcadores de máquina são controlados pela propriedade do sistema global sn_vul.import_host_tags. Esta propriedade é definida como verdadeira por padrão. Desabilitar os marcadores os desabilita em todas as Now Platform® instâncias.

O que fazer a seguir

Depois de baixar a integração Vulnerability Response com o Microsoft Threat and Vulnerability Management do ServiceNow® Store, a instalação e a configuração são compatíveis com o Assistente de configuração em Vulnerability Response. Para obter mais informações, consulte Instalar e configurar a aplicação Vulnerability Response Integration with the MS TVM usando o Assistente de configuração.

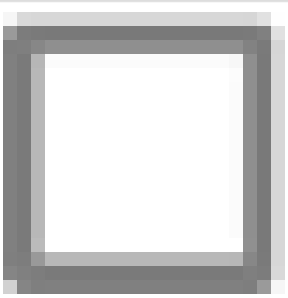
Preparando-se para o Microsoft Threat and Vulnerability Management Vulnerability Integration

Você pode se preparar para a integração de vulnerabilidade do ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) executando tarefas de configuração.

Antes de começar a usar uma check-list

Para instalar e configurar a integração Vulnerability Response com a aplicação MS TVM, você pode imprimir a check-list a seguir e verificar se os itens listados foram concluídos antes de instalar a aplicação e importar dados de vulnerabilidade para sua instância Now Platform®.

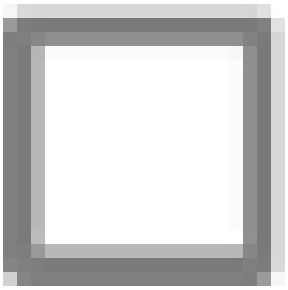
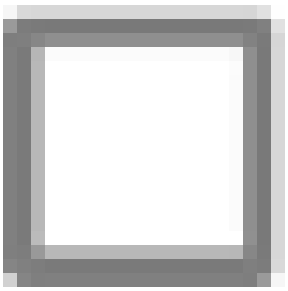
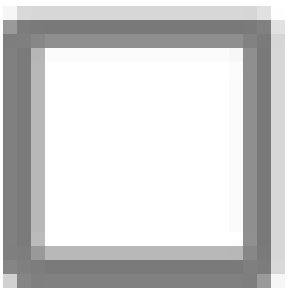
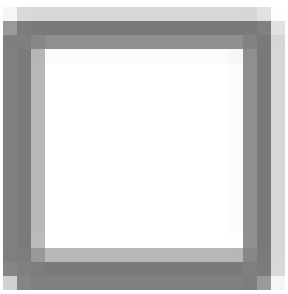
Check-list de preparação da integração

Tarefa	Descrição
	Verifique se você tem um dos seguintes conjuntos de informações: • ClientSecret, ClientId e TenantId para sua conta do MS TVM • Nome de usuário, senha, ClientId e TenantId da sua conta do MS TVM. Para obter essas informações, consulte Configurar o Microsoft Azure para a integração do MS TVM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

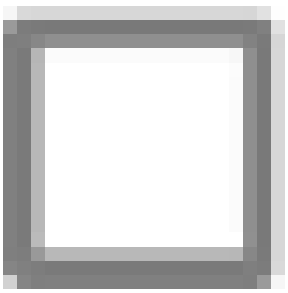
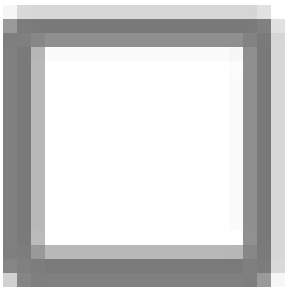
Check-list de preparação da integração

Tarefa	Descrição
	Se ainda não estiver instalado e ativado, instale a aplicação Vulnerability Response antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar a aplicação Vulnerability Response, consulte Como instalar Vulnerability Response. Esta integração requer a versão 14.0 de Vulnerability Response ou posterior.
	Se você ainda não tiver a aplicação em sua instância, obtenha direitos e baixe a integração Vulnerability Response com a aplicação MS TVM para sua instância Now Platform®. Consulte .
	Estime o número de itens vulneráveis que você espera importar. Verifique se sua instância pode aceitar o número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a longos tempos de carregamento. Se você não souber o tamanho da sua instância ou se precisar de assistência, entre em contato com o ServiceNow® Suporte técnico.
	Verifique se você tem os seguintes grupos ou usuários para gerenciar as integrações e para corrigir itens vulneráveis: **admin** Usa o Assistente de configuração para instalar a integração do Vulnerability Response com a aplicação MS TVM. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração. **sn_vul.vulnerability_admin** Conclui a configuração da integração do MS TVM. Esta função tem acesso completo à aplicação Vulnerability Response (VR) e seus registros. Este administrador configura todas as aplicações e regras de VR e configura integrações de terceiros. **sn_vul_msft_tvm.configure_integration** Configura a integração de vulnerabilidade do MS TVM. Esta função contém a função granular sn_vul_msft_tvm.read_integration. **sn_vul_msft_tvm.read_integration** Exibe (lê) registros da integração de vulnerabilidade do MS TVM. **Grupo do Vulnerability Response**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
	Por padrão, o grupo do Vulnerability Response está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Vulnerability Response herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente. Se ainda não tiver sido criado, talvez você prefira criar grupos adicionais e adicionar usuários com o módulo Administração de usuários em sua instância antes de usar o Assistente de configuração. Para obter mais informações, consulte Criar um grupo de usuários . Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que os usuários podem fazer e ver na aplicação Vulnerability Response. Para obter a atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração.
	Instale a integração Vulnerability Response com o NVD e execute a API do NIST National Vulnerability Database Integration (somente CVE).
	Para promover um desempenho aprimorado para sua primeira importação, você pode desabilitar determinados recursos, regras ou trabalhos em sua instância. • Desabilite as calculadoras de vulnerabilidade se você não as usar. Essas calculadoras, além de qualquer outra que você tenha definido, são executadas sempre que um registro de item vulnerável é criado ou atualizado. Para obter mais informações, consulte Desabilitar a calculadora de vulnerabilidade padrão se não for usada. • Durante a importação inicial de registros, determinadas regras de negócios relacionadas à notificação podem fazer com que muitas notificações sejam geradas, o que pode afetar o desempenho da ingestão.

Você está pronto para Instalar e configurar a aplicação Vulnerability Response Integration with the MS TVM usando o Assistente de configuração.

Configurar o Microsoft Azure para a integração do MS TVM

Configure sua conta no portal do Azure Microsoft para acessar a API do Microsoft Threat and Vulnerability Management (MS TVM) remotamente. Você precisa desta conta para acessar o locatário do MS TVM e coletar informações de máquinas, vulnerabilidades e recomendações de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: Microsoft Administrador do portal do Azure.

Por Que e Quando Desempenhar Esta Tarefa

Conclua as seguintes tarefas de configuração no portal do Azure Microsoft antes de instalar a aplicação ServiceNow® para esta integração.

Para verificar se você tem acesso ao conteúdo mais atual, consulte o site de documentos da Microsoft . Se você não criou um ID de aplicação para autenticação OAuth 2.0 no portal do Azure Microsoft, siga as etapas deste procedimento.

Procedimento

1. Faça login no portal do Azure Microsoft usando suas credenciais de administrador do portal do Azure.
2. No painel de navegação esquerdo do painel inicial, clique em **Azure Active Directory**.
3. No painel Visão geral, clique em **Registros do app (Visualização)**.
4. No painel Registros do aplicativo (Visualização), clique em **Novo registro**.
   O formulário Registrar uma aplicação é exibido.
5. No formulário, preencha os campos.

Registrar um formulário de aplicação

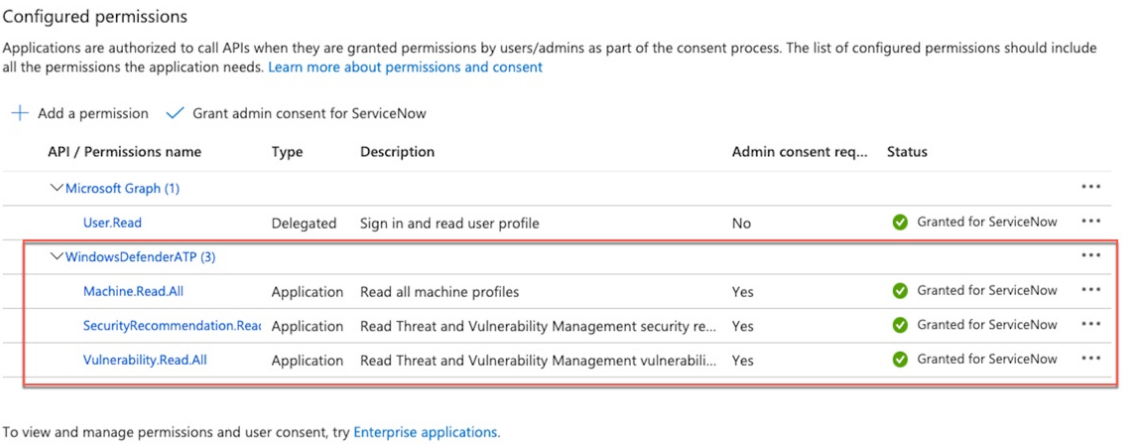
Campo	Descrição
Nome	Nome da aplicação. Neste exemplo, a integração ServiceNow MS TVM é inserida.
Tipos de conta compatíveis	Para esta conta, em Tipos de conta compatíveis, clique **em Contas somente neste diretório organizacional (somente ServiceNow - locatário único)**.
URL de redirecionamento (opcional)	Se você inserir um valor para este campo, ele não será usado pela integração.

6. Clique em **Registrar**.
   O ID da aplicação (cliente) e o ID do diretório (locatário) são criados. Insira esses valores na página de configuração nos campos ID do **cliente e ID** do **locatário** durante a etapa de configuração no ServiceNow Assistente de configuração da integração VR-TVM. Esta etapa foi descrita em Instalar e configurar a aplicação Vulnerability Response Integration with the MS TVM usando o Assistente de configuração.
7. Quando vir o ID da aplicação (cliente) exibido no ServiceNow painel de integração do MS TVM, clique em **Exibir permissões de API**.
8. Navegar até **Solicitar permissões de API** > **APIs que minha organização usa**e, em seguida, clique em **Windows Defender ATP**.
9. No painel Integração MS TVM da ServiceNow - Permissões de API, clique em **Adicionar uma permissão**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

10. Forneça acesso de leitura a máquinas, vulnerabilidades e recomendações de



segurança.

11. Clique **em Conceder consentimento do administrador para**<your organization name> .

Nota:
Para autenticar como uma aplicação de uma instância ServiceNow, execute as seguintes ações:

a. Navegar até **ServiceNow MS TVM Integration** > **Certificados e segredos**e, em seguida, clique em **Novo segredo do cliente**.

b. No formulário, preencha os campos.

Formulário de segredos do cliente

Campo	Descrição
Descrição	Nome da aplicação.
Expira	Data de vencimento.

c. Clique em **Adicionar**.

O campo **Valor** é preenchido com o novo segredo do cliente, que é sua nova senha.

Nota:
Você precisará desta senha ao configurar a integração na sua instância Now Platform. Para obter mais informações, consulte Instalar e configurar a aplicação Vulnerability Response Integration with the MS TVM usando o Assistente de configuração.

d. Salve esta senha em um local seguro. Depois de sair desta página, esta senha não estará disponível.

Você criou com sucesso um ID de aplicação para autenticação no portal do Azure Microsoft.

O que Fazer Depois

Você está pronto para configurar sua instância Now Platform® para a integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instalar e configurar a aplicação Vulnerability Response Integration with the MS TVM usando o Assistente de configuração

Instale e configure a integração Vulnerability Response com a aplicação Microsoft Threat and Vulnerability Management (MS TVM) para que você possa usar os dados importados do MS TVM para priorizar e corrigir vulnerabilidades de seus ativos.

Antes de Iniciar

Antes de executar a ServiceNow® Microsoft Threat and Vulnerability Management Vulnerability Integration, você deve baixar a aplicação Vulnerability Response Integration with Microsoft Threat and Vulnerability Management na aplicação ServiceNow Store e instalá-la e configurá-la usando o Assistente de configuração na aplicação Vulnerability Response.

Antes de instalar a aplicação MS TVM, verifique se você concluiu todos os itens na check-list Preparando-se para o Microsoft Threat and Vulnerability Management Vulnerability Integration. Para obter informações sobre como configurar sua Microsoft conta do Azure, consulte Configurar o Microsoft Azure para a integração do MS TVM.

Funções necessárias: administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação Microsoft Threat and Vulnerability Management no Assistente de configuração. Administrador de vulnerabilidade (sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) para configurar a aplicação no Assistente de configuração depois que ele for instalado.

Por Que e Quando Desempenhar Esta Tarefa

Execute o procedimento a seguir antes de instalar e configurar a integração do MS TVM.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Instalação da aplicação de integração**.

   Após alguns momentos, as aplicações disponíveis para instalação em sua instância serão exibidas.

2. Localize o bloco **Microsoft Threat and Vulnerability Management** e clique em **Instalar**.

   A aplicação Vulnerability Response Integration with Microsoft Threat and Vulnerability Management que você baixou do ServiceNow Store está instalada.

3. Siga os prompts do Assistente de configuração para continuar com a instalação.
   Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Vulnerability Response aplicações de terceiros usando o Assistente de configuração.

O que Fazer Depois

Depois de concluir a instalação no Assistente de configuração, navegue até **Configuração de Integração** > **Integrações do Scanner** no Assistente de configuração para continuar com a configuração. Para obter mais informações para complementar os prompts fornecidos no Assistente de configuração, consulte Configurar a integração de vulnerabilidade do MS TVM usando o Assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de recuperação de dados para o Microsoft Threat and Vulnerability Management Integration

Você pode usar as configurações de recuperação de dados para ajudá-lo a determinar o tipo e o escopo dos dados que deseja importar da integração de vulnerabilidade do ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) para sua instância Now Platform®.

As configurações de recuperação de dados ajudam a controlar os dados que você deseja importar. Você pode definir os valores desses filtros em instâncias de integração. Para exibir as instâncias de integração, navegue até **Microsoft Threat and Vulnerability Management Vulnerability Integration** > **Instâncias de Integração** e clique na integração do MS TVM.

Na página Instância de integração, clique em **Parâmetros** de instância de integração para exibir uma lista de parâmetros ou clique na guia **Integrações de vulnerabilidade** para obter uma programação, detalhes de REST, detalhes de integração, fontes de dados e informações de execução de integração.

Configurações e filtros de recuperação de dados para as integrações do MS TVM na sua instância Now Platform

As configurações a seguir estão disponíveis para as integrações do MS TVM na sua instância Now Platform. Essas e outras definições de configuração são exibidas na página Instância de integração da sua instância Now Platform. Você pode preferir deixar essas configurações em suas configurações padrão para as primeiras execuções de integração.

MS-TVM.

vi_size_limit

Define o número de registros de item vulnerável a serem incluídos no conjunto de resultados da integração de vulnerabilidades da máquina MS TVM. Esta configuração deve estar no formato int32. O valor padrão é 2.000.

vulnerability_size_limit

Define o número de registros de vulnerabilidade a serem incluídos no conjunto de resultados da integração MS TVM Vulnerability (CVE). Esta configuração deve estar no formato int32. O valor padrão é 2.000.

recomendações_tamanho_limite

Define o número de registros de vulnerabilidade a serem incluídos no conjunto de resultados da integração de recomendações do MS TVM. Esta configuração deve estar no formato int32. O valor padrão é 2.000.

ativo_tamanho_limite

Define o número de registros de vulnerabilidade a serem incluídos no conjunto de resultados da integração de máquinas MS TVM. Esta configuração deve estar no formato int32. O valor padrão é 2.000.

machine_filter

Filtra as máquinas provenientes do MS TVM. Este filtro é aplicado à integração de máquinas MS TVM. O valor padrão é trazer máquinas em que onBoardingStatus seja onBoarded.

Mensagens REST para o Microsoft Threat and Vulnerability Management Vulnerability Integration

Você pode usar as mensagens REST para a integração de vulnerabilidade ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) para fazer chamadas para a API do MS TVM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Token de acesso do MS TVM

Você também pode usar as mensagens REST do token de acesso do MS TVM para recuperar o token de acesso da API do MS TVM para que possa autenticar as solicitações da REST API. As mudanças no método de registro da mensagem REST afetam as solicitações de autenticação feitas ao MS TVM.

Integração do MS TVM

Você pode usar a mensagem REST para a integração do MS TVM para recuperar informações do MS TVM. As mudanças no método de registro da mensagem REST afetam as solicitações feitas ao MS TVM para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Métodos REST

Método REST	Descrição do método
GET vulnerabilidades	Recupera informações de vulnerabilidade e exploração do MS TVM.
GET Vulnerabilidades de software por máquina	Recupera todas as vulnerabilidades em aberto.
OBTER recomendações	Recupera a lista de todas as recomendações de segurança acionáveis que afetam a organização.
GET máquinas	Recupera a coleção de ativos.
OBTER mudanças de vulnerabilidades de software por máquina	Recupera todas as informações que foram alteradas na importação de vulnerabilidades completa da organização, incluindo vulnerabilidades novas, corrigidas e atualizadas.

Transformação de dados para o Microsoft Threat and Vulnerability Management Vulnerability Integration

Depois de identificar os dados que deseja importar, os dados são recuperados da aplicação ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM), processados por meio de um conjunto de fontes de dados e transformados em sua instância.

Durante a instalação, os mapas de severidade normalizados são instalados no módulo Mapeamento de severidade normalizado. Esses mapas transformam níveis de severidade de vulnerabilidade de terceiros importados Microsoft em níveis de severidade padrão para processamento em sua instância. Para obter informações sobre como criar mapas de severidade, consulte Criar um mapa de severidade Vulnerability Response.

Importação de máquinas MS TVM

Os dados das máquinas importadas são carregados primeiro na tabela Importação de máquinas MS TVM [sn_vul_msft_tvm_machines_import].

A Transformação de máquinas do MS TVM é usada para transformar as informações das máquinas importadas.

Nota:
As mudanças neste mapa de transformação alteram como os dados da importação de máquinas MS TVM são processados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação** e pesquise por **Microsoft TVM Machines Transform**.

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação das máquinas MS TVM

Campo de origem	Campo de destino	Descrição
u_id	source_id	ID exclusivo para ativos. Este ID é mapeado para o source_id do registro do item descoberto.
u_ipaddresses.macAddress	mac_address	Endereço MAC que é mapeado da API para o campo de endereço MAC do host do registro cmdb_ci.
u_ipaddresses.ipAddress	ip_address	Campo de endereço IP que é mapeado para o campo de endereço IP do registro cmdb_ci.
u_lastseen	data_última_verificação	Campo que é mapeado para o campo last_scan_date no registro do item descoberto.
u_machinetags		Marcadores que são salvos em sn_sec_cmn_host_tag. O mapeamento de marcadores para ativos é salvo em sn_sec_cmn_m2m_src_ci_tag.
u_osplatform	os	Campo que é mapeado para o campo os no registro cmdb_ci.
u_computerdnsname	fqdn	Campo que mapeia o campo dnsname da API para o campo fqdn no registro cmdb_ci.

Os scripts de transformação a seguir são executados durante o processo de transformação.

As máquinas MS TVM transformam o tempo e a finalidade do script de mapa

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação).	Script usado para inicializar os valores na variável de escopo (sn_vul_msft_tvm) para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto de importação concluir a transformação).	Script usado para atualizar valores no host e verificar se o host existe. Com base nos resultados, este script modifica os valores na variável de escopo (sn_vul_msft_tvm). Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de ICs criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O script include MicrosoftTVMMachinesProcessor é chamado a partir do script de transformação onBefore. Ele obtém a saída da integração das máquinas Microsoft TVM e a transforma em um IC. Quaisquer mudanças nesta inclusão de script podem alterar a transformação dos dados das máquinas do Microsoft TVM na tabela de IC e item descoberto.

Integração de vulnerabilidades do MS TVM

Os dados de vulnerabilidades importados são carregados primeiro na tabela de importação do Microsoft TVM CVE (Vulnerabilidades) [sn_vul_msft_tvm_vulnerabilities_import].

Nota:
As mudanças neste mapa de transformação alteram como os dados da importação de vulnerabilidades do MS TVM são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação** e pesquise por **Transformação de vulnerabilidades do Microsoft TVM**.

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de vulnerabilidades do Microsoft TVM

Campo de origem	Campo de destino	Descrição
u_id	id	Mapeia para a coluna ID do registro sn_vul_entry.
u_severidade	source_severity	Mapeia o campo Gravidade para a severidade. O valor padrão é 5.
u_publishedon	date_published	Mapeia o campo u_publishedon para a data de publicação.
u_publicexploit	public_exploit	Mapeia o u_publicexploit fornecido pelo scanner para a coluna de exploração pública na tabela de entrada de vulnerabilidade.
u_cvssv3	v3_base_score	Mapeia a pontuação do cvssv3 para a pontuação base do v3 no registro de entrada da vulnerabilidade.
u_description	resumo	Mapeia a descrição para o campo de resumo no registro de entrada da vulnerabilidade.
u_exploitink	malware_kit	Mapeia o campo u_exploitinkit para o kit de malware na tabela de exploração.
u_exploittypes	tipo	Mapeia o tipo de exploração para o tipo na tabela de exploração.
u_exploitverified	is_exploit_verified	Mapeia o campo u_exploitverified para a exploração verificada na tabela Explorar.
u_exploituris	explore_links	Mapeia o campo u_exploituris para os links de exploração na tabela de exploração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os scripts de transformação a seguir são executados durante o processo de transformação.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação).	Script usado para inicializar os valores na variável de escopo (sn_vul_msft_tvm) para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto de importação concluir a transformação).	Script usado para criar ou atualizar os valores no NVD ou na tabela de entrada de terceiros. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir os valores dos novos itens que foram criados e os itens que foram atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de recomendações do MS TVM

Os dados de recomendação importados são carregados primeiro na tabela Importação de recomendações do MS TVM [sn_vul_msft_tvm_recom_import].

Nota:
As mudanças neste mapa de transformação alteram como os dados da importação do MS TVM Recommendations são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação** e pesquise por **Transformação de recomendação do MS TVM**.

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação da recomendação do MS TVM

Campo de origem	Campo de destino	Descrição
u_recommendedvendor	recomendado_vendor	Mapeia o campo u_recommendedvendor para a coluna Fornecedor.
u_weaknesses	pontos fracos	Mapeia o campo u_weaknesses para a coluna Pontos fracos.
u_exponentmachinescount	src_expos_máquinas_cnt	Mapeia o campo u_ex openedmachinescount para a coluna Contagem de máquinas expostas.
u_status	status	Mapeia o status para o campo Status no registro de recomendação.
u_productname	product_name	Mapeia o campo u_productname para o nome do produto no registro de recomendação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação da recomendação do MS TVM

Campo de origem	Campo de destino	Descrição
u_nonproductiv_impactedassets	não_prod_impacted_assets	Mapeia o campo u_nonproductiv_impactedassets para a coluna Ativos afetados no registro de recomendação.
u_activealert	active_alert	Mapeia o campo u_activealert para a coluna Alerta ativo no registro de recomendação.
u_recommendedversion	recomendado_versão	Mapeia o campo u_recommendedversion para a coluna Versão recomendada no registro de recomendação.
u_totalmachinecount	total_machine_count	Mapeia o campo u_totalmachinecount para a coluna Contagem total de máquinas no registro de recomendação.
u_exposureimpact	exposition_impact	Mapeia o campo u_exposureimpact para a coluna Impacto da exposição no registro de recomendação.
u_recommendationname	recomendação_name	Mapeia o campo u_recommendationname para a coluna Nome da recomendação no registro de recomendação.
u_subcategoria	subcategoria	Mapeia o campo u_subcategory para a coluna Subcategoria no registro de recomendação.
u_id	source_id	Mapeia o ID de recomendação do MS TVM para a coluna ID de origem.
u_remediationtype	correção_tipo	Mapeia o campo u_remediationtype para a coluna Tipo de correção no registro de recomendação.
u_relatedcomponent	related_component	Mapeia o campo u_relatedcomponent para a coluna Componente relacionado no registro de recomendação.
u_recommendedprogram	recomendado_programa	Mapeia o campo u_recommendedprogram para a coluna Programa recomendado no registro de recomendação.
u_recommendationcategory	recomendação_categoria	Mapeia o campo u_recommendationcategory para a coluna Categoria de recomendação no registro de recomendação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação da recomendação do MS TVM

Campo de origem	Campo de destino	Descrição
u_publicexploit	public_exploit	Mapeia o campo u_publicexploit para a coluna Exploração pública no registro de recomendação.
u_vendor	fornecedor	Mapeia o campo u_vendor para a coluna Fornecedor no registro de recomendação.
[Script]	integration_instance	Nome da instância da qual a recomendação é importada.
[Script]	sys_domain	Domínio no qual este registro é importado.

Os scripts de transformação a seguir são executados durante o processo de transformação.

Script de mapa de transformação de recomendação do MS TVM

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação).	Script usado para inicializar os valores na variável de escopo (sn_vul_msft_tvm) para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto de importação concluir a transformação).	Script usado para atualizar valores nas recomendações e verificar se as recomendações existem. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir os valores de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de vulnerabilidades da máquina com MS TVM

O mapa de transformação de vulnerabilidades de máquina do MS TVM é usado para transformar informações de vulnerabilidades abertas e fixas que são importadas do MS TVM.

Nota:
As mudanças neste mapa de transformação alteram como os dados da importação de vulnerabilidades da máquina MS TVM são processados.

Para acessar os mapas de transformação de vulnerabilidades em aberto e corrigidas do MS TVM, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação** e pesquise por **Transformação de vulnerabilidades da máquina MS TVM**.

A tabela a seguir lista os campos do mapa de transformação por integração.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de vulnerabilidades da máquina MS TVM

Campo de origem	Campo de destino	Descrição
u_id	detecção_chave	Mapeia o campo u_id para a coluna Chave de detecção na tabela de detecção.
u_diskpaths	prova	Mapeia o campo u_diskpaths para a coluna Prova na tabela de detecção.
u_registrypaths	prova	Mapeia o campo u_registrypaths para a coluna Prova na tabela de detecção.
u_recommendedsecurityupdateid	solução_preferencial	Mapeia o campo u_recommendedsecurityupdateid para a coluna Solução preferencial na tabela de itens vulneráveis, se a solução existir com o mesmo ID na tabela sn_vul_solution.
u_recommendationreference	recomendação	Mapeia o campo u_recommendationreference para a coluna Recomendação na tabela de itens vulneráveis.
u_cveid	vulnerabilidade	Mapeia o campo u_cveid para a coluna Vulnerabilidade na tabela de itens vulneráveis.
u_status	source_status	Mapeia o campo u_status para a coluna Status de origem na tabela de detecção.
u_eventtimestamp	temporal_score	Mapeia o campo u_eventtimestamp para a última coluna encontrada na tabela de itens vulneráveis.
u_lastseentimestamp	last_seen	Mapeia o campo u_lastseentimestamp para a coluna Visto pela última vez na tabela de itens vulneráveis.
u_firstseentimestamp	first_seen	Mapeia o campo u_firstseentimestamp para a coluna Visto pela primeira vez na tabela de itens vulneráveis.
u_recommendedsecurityupdate	solution_summary	Mapeia o campo u_recommendedsecurityupdate

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de vulnerabilidades da máquina MS TVM

Campo de origem	Campo de destino	Descrição
		para a coluna Resumo da solução na tabela de itens vulneráveis.
u_recommendedsecurityupdateurl	solution_summary	Mapeia o campo u_recommendedsecurityupdateurl para a coluna Resumo da solução na tabela de itens vulneráveis.

Os scripts de transformação a seguir são executados durante o processo de transformação.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação).	Script usado para inicializar os valores na variável de escopo (sn_vul_msft_tvm) para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto de importação concluir a transformação).	Script usado para verificar se a entrada de vulnerabilidade e as detecções existem. Caso contrário, esses registros serão criados em suas respectivas tabelas. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para atualizar a contagem de IVs e detecções conforme importados do MS TVM. Este script é para uso interno e não deve ser modificado ou excluído.

Gráfico de status de execução da integração para a integração de vulnerabilidade do Microsoft Threat and Vulnerability Management

Você pode usar o módulo Status de execução da integração do Microsoft Threat and Vulnerability Management (MS TVM) para fornecer uma exibição gráfica do status das execuções de integração do MS TVM.

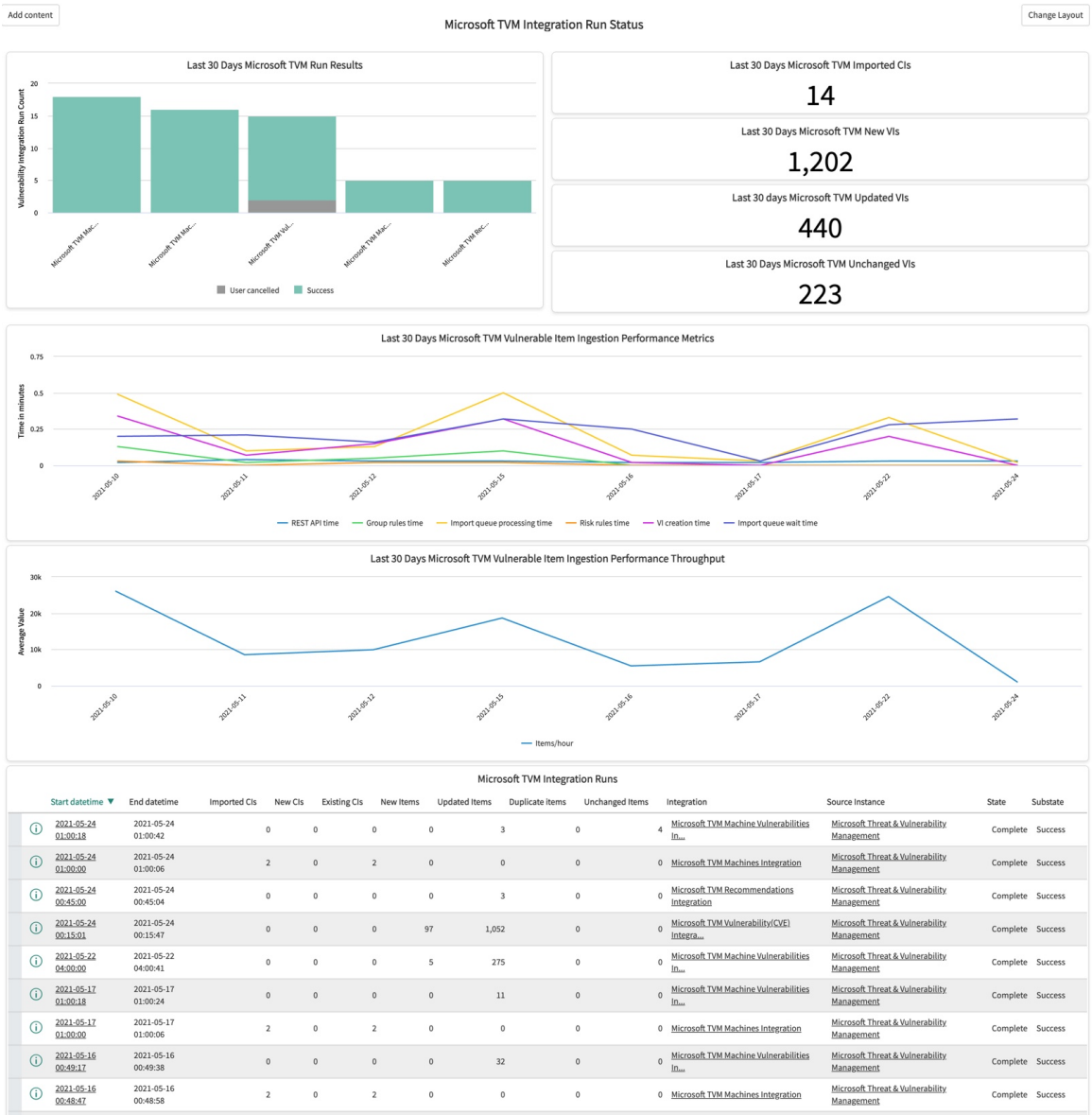
A partir da versão 19.0 do Vulnerability Response, este painel está disponível na IU da nova experiência.

Nota:
Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

No gráfico, você pode apontar para qualquer parte do gráfico para exibir um resumo dos dados específicos dessa parte. Se você clicar em qualquer parte do gráfico de barras, uma lista será aberta para fornecer informações mais detalhadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Relatórios do gráfico de status de execução da integração do MS TVM

Nome	Descrição
Resultados do Microsoft TVM nos últimos 30 dias	Número de execuções de integração que foram concluídas para cada integração. Este relatório mostra as execuções bem-sucedidas e com falha. Cada execução é exibida como uma barra no gráfico.
Novos IVs do Microsoft TVM nos últimos 30 dias	Número de novos itens vulneráveis que foram importados nos últimos 30 dias.
IVs atualizados do Microsoft TVM nos últimos 30 dias	Número de itens vulneráveis atualizados que foram importados nos últimos 30 dias.
VIs inalterados do Microsoft TVM nos últimos 30 dias	Número de itens vulneráveis duplicados que foram importados nos últimos 30 dias.
Execuções de integração do MS TVM	Registros de execução de integração em uma lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Descrição
	Nota: **V16.1:** para verificar as detecções para esta integração, compare as detecções ou descobertas com os dados de detecção ServiceNow`sn_vul_detection`] na tabela . Enquanto a integração está em andamento, pode haver uma mudança na detecção ou na contagem de descobertas. Este relatório exibe a contagem de detecções na coluna "Contagem até a data" na instância, após a conclusão da execução da integração.
Métricas de desempenho de ingestão de item vulnerável do Microsoft TVM nos últimos 30 dias	Métricas de desempenho diárias para itens vulneráveis comparadas nos últimos 30 dias.
Taxa de transferência de desempenho de ingestão de item vulnerável do Microsoft TVM nos últimos 30 dias	Taxa de transferência diária de ingestão de item vulnerável que foi medida para a integração de detecção de host do Microsoft TVM nos últimos 30 dias.
ICs importados do Microsoft TVM nos últimos 30 dias	Número de novos itens de configuração que foram importados nos últimos 30 dias.

Verificar o status de execução da importação da integração da Gestão de ameaças e vulnerabilidades da Microsoft

Use o status de execução de importação do Microsoft Threat and Vulnerability Management (MS TVM) para verificar o sucesso das execuções de integração e para localizar quaisquer problemas.

Antes de Iniciar

Este procedimento faz as seguintes suposições:

- Você tem Vulnerability Response e o MS TVM Vulnerability Integration instalado e configurado.
- As importações de integração de vulnerabilidade do MS TVM são programadas e estão em execução.

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Gestão de ameaças e vulnerabilidades da Microsoft** > **Integrações**.
   a. Escolha uma integração.
   b. Clique na lista relacionada Execuções de integração de vulnerabilidade.
2. Verifique se o estado das importações está Concluído, com o Subestado como Êxito.
   As causas mais comuns para uma execução com falha são as seguintes:
   - Interrupção de rede.
   - Deterioração de bits na transferência de dados, resultando em dados corrompidos durante a transformação.
3. **Opcional:** Se você vir uma dessas condições que causaram uma execução com falha, clique em **Executar agora** e execute novamente a integração.

Noções básicas sobre a integração de orquestração de patches do BigFix HCL com Vulnerability Response

Você pode gerenciar patches e implantações de patch para vulnerabilidades críticas para grandes grupos de ativos com a integração de orquestração de patches Vulnerability Response com o produto HCL BigFix.

Orquestração de patches com Vulnerability Response

A orquestração de patches com Vulnerability Response usa importações programadas de integrações de soluções de terceiros, fornecedores de patches e scanners de vulnerabilidade. Os dados de detecção do scanner correspondem aos ativos em seu ambiente com vulnerabilidades e atualizações de patch que podem corrigi-los. Envie solicitações de patch para aprovação, programe atualizações de patch para resolver itens vulneráveis e monitore o andamento da correção de todos os registros na aplicação Vulnerability Response em seu Now Platform®.

Vulnerability Response Patch Orchestration with HCL BigFix

Quando a aplicação Vulnerability Response Patch Orchestration with HCL BigFix integration é usada com as aplicações ServiceNow® Solução de gerenciamento de vulnerabilidade, Patch Orchestration e Vulnerability Response, os gerentes e analistas de vulnerabilidade podem executar as seguintes tarefas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Consulte mais contexto e informações sobre os tipos de patches e soluções de fornecedores (patches).
- Exiba e monitore os dados de vulnerabilidade e solução, bem como o andamento da correção de vulnerabilidades de registros nos espaços Vulnerability Response.

Especialistas em TI e proprietários de correção podem executar as seguintes tarefas:

- Implante patches compatíveis com o produto BigFix para seus Windows, CentOS, MAC, Oracle e outros ativos em intervalos regulares e programados fora do horário de expediente para evitar conflitos de trabalho.
- Identifique ativos sem patch com vulnerabilidades ou ativos que foram ou não atualizados com sucesso por patches programados a partir de dados de detecção importados de scanners de terceiros.
- Programe os patches disponíveis no Espaço de correção de TI ou no ambiente clássico para ativos vulneráveis sem patch de atualização de patch, tarefa de correção e registros de item descoberto.

Termos-chave nas aplicações Vulnerability Response e BigFix

IC (Configuration Item, item de configuração)

ICs são os ativos existentes listados em Configuration Management Database (CMDB). Chamadas do BigFix ICs, computadores.

Grupos de computadores

Terminologia usada no produto BigFix que se refere a um grupo de ativos.

Item vulnerável

Uma vulnerabilidade importada que corresponde a um ativo existente no seu CMDB.

Instância

Uma conta distinta da aplicação BigFix. Cada conta de usuário pode ser uma instância na aplicação BigFix. Este termo também se refere a um endereço da Web exclusivo e seguro para uma instância Now Platform.

Integração

Uma integração é um trabalho programado no Now Platform que recupera informações de uma fonte de terceiros, como a integração com as máquinas BigFix.

Solução

Existem dois tipos de soluções no contexto desta integração, potenciais e preferenciais. Uma possível solução é aquela que pode solucionar uma vulnerabilidade. As vulnerabilidades geralmente têm muitas soluções potenciais. Uma solução preferencial corresponde à solução mais eficaz para uma vulnerabilidade específica detectada.

Patch

Atualizações de software que corrigem vulnerabilidades. Na aplicação BigFix, os patches são chamados de Fixlets. Por exemplo, o BigFix tem Fixlets para Windows, CentOS, MAC, Oracle e outros produtos.

Patch preferencial

Patches preferenciais são atualizações de software que têm como objetivo corrigir vulnerabilidades específicas. Os patches, uma vez implantados, são mapeados para os itens vulneráveis que estão relacionados a vulnerabilidades específicas e os corrigem.

Tarefa de correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas de itens vulneráveis na aplicação Vulnerability Response de ações que são necessárias para corrigir vulnerabilidades.

Implantação

Para fins desta integração, a implantação se refere a quando você aplica, inicia ou programa um patch para uma máquina. O BigFix chama essas implantações de ações. Você pode implantar (criar ações) para os patches que baixou do BigFix no seu Now Platform. Navegue até itens descobertos, patches ou tarefas de correção de registros individuais em Vulnerability Response. Você pode implantar patches com trabalhos programados em máquinas individuais ou em grupos de computadores.

A implantação no Now Platform também pode se referir a uma integração que oferece suporte a várias origens. Uma única existência de integração é chamada de implantação da sua integração. Uma implantação se refere às integrações e produtos em seu ambiente. Por exemplo, você pode ter várias implantações da integração do BigFix Vulnerability em seu ambiente.

Vulnerability Solution Management e Vulnerability Response Patch Orchestration com HCL BigFix Integration

O gerenciamento de soluções é fornecido pela aplicação Solução de gerenciamento de vulnerabilidade, uma aplicação Now Platform que correlaciona suas descobertas de vulnerabilidade com o detalhamento das soluções (patches) que as corrige. Identifique os patches de software de terceiros para produtos e serviços, atualizações de configuração e outros controles que têm o maior impacto para sua organização. Junto com as informações do scanner de terceiros, as aplicações Solução de gerenciamento do Vulnerability Response, Vulnerability Responsee Vulnerability Response Patch Orchestration com HCL BigFix trabalham juntos para instalar patches preferenciais da solução, para a vulnerabilidade, para o item vulnerável para ajudá-lo a corrigir e fechar vulnerabilidades ao seu ambiente.

O Solução de gerenciamento do Vulnerability Response, Vulnerability Responsee o Vulnerability Response Patch Orchestration com HCL BigFix Integration estão disponíveis no ServiceNow® Store.

Funções necessárias de Now Platform

As tarefas de instalação, configuração e correção de integração exigem as funções a seguir em sua instância Now Platform.

admin

Usuários com esta função obtêm direitos para aplicações nas instâncias ServiceNow Store e os baixam para Now Platform instâncias.

sn_vul.vulnerability_admin

Usuários com esta função ativam aplicações na instância Now Platform e concluem a configuração da aplicação Vulnerability Response. Esta função tem acesso completo à aplicação Vulnerability Response (VR) e seus registros. Este usuário administrador configura todas as aplicações de VR, regras e integrações de terceiros.

sn_vul_bigfix.configure_integration

Usuários com esta função configuram a aplicação BigFix Patch Orchestration Integration. Esta função contém a função granular sn_vul_bigfix.read_integration.

sn_vul_bigfix.read_integration

Usuários com esta função podem exibir (somente leitura) os registros da aplicação Vulnerability Response e do BigFix Patch Orchestration Integration e os dados de orquestração de patches.

sn_vul_patch_orch.configure_patch

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuários com esta função podem configurar e aplicar patches.

sn_vul_patch_orch.read_patch

Usuários com esta função podem exibir (somente leitura) informações do patch.

Aprovadores

Atribua usos aos grupos de aprovadores de nível 1 e aprovador de nível 2 se quiser que as solicitações de patch enviadas sejam aprovadas antes da implantação.

Para obter mais informações sobre como atribuir essas funções usando o Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre as funções Vulnerability Response em seu Now Platform, consulte Vulnerability Response personas e funções granulares.

Regras de pesquisa de IC

Quando os dados são importados da aplicação BigFix, a aplicação Vulnerability Response pesquisa automaticamente correspondências no Configuration Management Database (CMDB) usando dados de máquina (ativo). As regras de pesquisa de IC são usadas para identificar ICs (ativos) e adicioná-los automaticamente aos registros de item vulnerável (IV) quando os IVs são criados.

As seguintes regras de pesquisa de IC são enviadas com o sistema de base e são usadas para identificar ICs (ativos) e adicioná-los à aplicação Vulnerability Response :

- MAC_ADDRESS
- IP_ADDRESS
- DNS_NAME

Você pode usar vários valores para o IP_ADDRESS de um ativo. Uma regra de pesquisa de IC considera todos os valores para correspondência. Para obter mais informações sobre como as regras de pesquisa de IC e como elas funcionam, consulte Regras de pesquisa de IC para identificar itens de configuração de Vulnerability Response integrações de vulnerabilidade de terceiros.

MID Server

A integração do Vulnerability Response Patch Orchestration com HCL BigFix é uma integração no local. Requer um MID Server autônomo que não faça parte de um cluster de MID Server. O MID Server é necessário para executar scripts em máquinas remotas de sua instância para importar dados do servidor BigFix. As APIs para esta integração são chamadas usando MID Servers que você configurou em sua instância Now Platform. Para obter mais informações, consulte Preparar para a integração do Patch Orchestration Vulnerability Response com HCL BigFix.

Integrações e dependências da Vulnerability Response Integração do Patch Orchestration com HCL BigFix

As aplicações de produto e dependência a seguir são necessárias para o Vulnerability Response Patch Orchestration com integração do HCL BigFix. Essas aplicações estão disponíveis na ServiceNow® Store.

Versões disponíveis de aplicações e dependências necessárias para a integração de orquestração de patches

Para exibir dados de orquestração de patches e atualizações disponíveis (patches) nos espaços em Vulnerability Response, os aplicativos a seguir são necessários. Todas as

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

aplicações listadas estão disponíveis no ServiceNow® Store. Algumas aplicações exigem assinaturas separadas.

Para obter mais informações sobre a compatibilidade de versão com as aplicações e versões da família necessárias, consulte o artigo KB0856498 Vulnerability Response Compatibility Matriz e mudanças de esquema de versão na Base de conhecimento HI.

Aplicação e versão de lançamento
Vulnerability Response
Solução de gerenciamento de vulnerabilidade
Aplicação Vulnerability Response Patch Orchestration
Vulnerability Response Orquestração de patches com aplicação HCL BigFix
Security Support Common
Orquestração de suporte de segurança
Uma aplicação de scanner de vulnerabilidade de terceiros compatível

Vulnerability Response Tabelas da aplicação Patch Orchestration

A aplicação Vulnerability Response Patch Orchestration contém as seguintes tabelas:

Tabela	Descrição
Atualização de patch [sn_vul_patch_orch_update]	Armazena informações sobre os patches que estão disponíveis em instâncias distintas.
Atualização de dispositivo [sn_vul_patch_orch_m2m_src_ci_update]	Armazena dados sobre os patches implantados, junto com o status da implantação, que são exibidos em registros de item descoberto.
Coleção [sn_vul_patch_orch_collection]	Armazena dados de coleta de instâncias distintas.
Coleção de dispositivos [sn_vul_patch_orch_m2m_src_ci_collection]	Armazena dados de coleções sobre itens descobertos.
Implantação de patch [sn_vul_patch_orch_deployment]	Armazena informações sobre patches implantados sobre Coleções e ICs.
Possível patch [sn_vul_patch_orch_m2m_vuln_patch]	Armazena dados sobre patches e vulnerabilidades que identificam os patches que podem ser usados para resolver uma vulnerabilidade.

Integrações de orquestração de patches do Vulnerability Response com HCL BigFix

As integrações desenvolvidas pela engenharia ServiceNow® compõem a implantação da solução orquestrada com o produto BigFix. As integrações a seguir estão incluídas na aplicação Vulnerability Response Patch Orchestration Integration with HCL BigFix que você baixa do ServiceNow® Store.

Depois de instalar a aplicação de integração na sua instância Now Platform, para exibir essas integrações, navegue até **Integrações** > **Integração da Orquestração de patches do BigFix**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

> **Integrações**. A aplicação Vulnerability Response processa dados em intervalos de tempo programados importados por essas integrações com endpoints do BigFix.

Integração	Descrição
Integração de coleção do BigFix	• Esta integração está programada para ser executada diariamente e é executada primeiro na execução da integração encadeada. • Recupera os computadores e grupos de computadores que compõem os grupos de computadores (itens de configuração) da aplicação BigFix.
BigFix Fixlet Integration	• Quando programada, essa integração é acionada pela conclusão da integração do BigFix Collection. Você também pode executá-lo sob demanda. • Recupera informações sobre todos os fixlets disponíveis (patches) do servidor BigFix.
BigFix Device Fixlet Integration	• Quando programada, essa integração é acionada pela conclusão da integração do BigFix Fixlet. Você também pode executá-lo sob demanda. • Recupera informações sobre os fixlets que estão atualmente nos computadores (ativos) do servidor BigFix.
Integração do BigFix Actions	• Quando programada, essa integração é acionada pela conclusão da integração do BigFix Device Fixlet. Você também pode executá-lo sob demanda. • Recupera informações sobre os patches programados pela equipe de TI no servidor BigFix.

Preparar para a integração do Patch Orchestration Vulnerability Response com HCL BigFix

Prepare-se para a integração executando as tarefas de configuração a seguir.

Antes de Iniciar

Funções necessárias: administrador para instalar as aplicações e atribuir funções. Outras funções estão listadas na tabela a seguir.

Por Que e Quando Desempenhar Esta Tarefa

Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração.

Você está pronto para Instalar a aplicação Vulnerability Response Patch Orchestration with HCL BigFix.

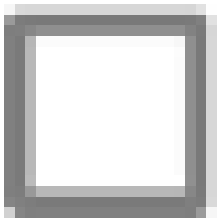
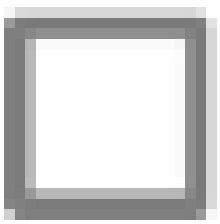
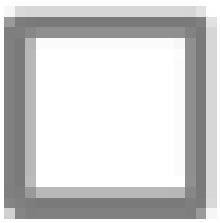
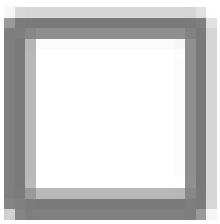
Procedimento

1. Para uma instalação e configuração sem problemas da aplicação Vulnerability Response Patch Orchestration with HCL BigFix, siga a check-list fornecida.
2. Você pode preferir imprimir a check-list a seguir e verificar se os itens listados foram concluídos antes de instalar a aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Após a instalação e a configuração, importe as informações relacionadas ao patch e à vulnerabilidade para sua instância Now Platform®.

Tarefa	Descrição
	(Opcional) Se ainda não estiver instalado e ativado, talvez você prefira instalar a aplicação Vulnerability Response antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar a aplicação Vulnerability Response, consulte Como instalar Vulnerability Response. Esta integração requer a versão 16.0 de Vulnerability Response ou posterior.
	Se ainda não estiver instalado, obtenha os direitos e instale um aplicativo scanner de terceiros para importar dados de vulnerabilidade. Consulte Integrações do Vulnerability Response para obter mais informações sobre scanners de terceiros compatíveis com Vulnerability Response. Consulte .
	Se ainda não estiver instalado, obtenha os direitos e baixe a aplicação Vulnerability Response Patch Orchestration com HCL BigFix para sua instância Now Platform®. Consulte .
	Obter credenciais do BigFix. Verifique se você tem nomes de conta, senhas e outras informações de serviço exigidas pelos seus produtos BigFix para que você tenha acesso a eles.
	Verifique se você tem grupos ou usuários para gerenciar as integrações e corrigir itens vulneráveis. **admin** O administrador do sistema obtém direitos, baixa e instala a aplicação BigFix Patch Orchestration e as outras aplicações necessárias para a integração. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração em Vulnerability Response ou no módulo Administração de usuário. **sn_vul.vulnerability_admin** Depois de atribuído, o administrador de vulnerabilidades conclui a configuração das integrações do BigFix e de outras aplicações de terceiros. Esta

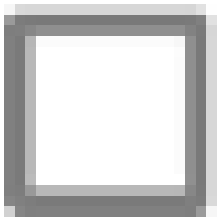
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	função tem acesso completo à aplicação Vulnerability Response (VR) e seus registros. Esta função configura todas as aplicações de VR, regras, integrações de terceiros, Vulnerability Response Patch Orchestration e aplicações de Vulnerability Solution Management. **sn_vul_bigfix.configure_integration** Usuários com esta função configuram a aplicação BigFix Patch Orchestration Integration. Esta função contém as funções granulares sn_vul_bigfix.read_integration e connection_admin que permitem ao usuário se conectar ao console do BigFix e configurar as instâncias de integração em seu Now Platform. **sn_vul_bigfix.read_integration** Usuários com esta função podem exibir (somente leitura) os registros da aplicação Vulnerability Response e do BigFix Patch Orchestration Integration e os dados de orquestração de patches. **sn_vul_patch_orch.configure_patch** Usuários com esta função podem configurar e aplicar patches. Os patches solicitados por este usuário do item vulnerável e os registros de atualização de patch serão enviados para aprovação se a gestão de mudanças estiver ativa e os aprovadores estiverem atribuídos. **sn_vul_patch_orch.read_patch** Usuários com esta função podem exibir (somente leitura) informações de patch em registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para o IT Remediation e Vulnerability Manager Workspaces. **Aprovadores** Usuários atribuídos ao nível de aprovador 1 e, opcionalmente, nível de aprovador 2, grupos de aprovadores aprovam as solicitações de patch enviadas. Por padrão, os patches são enviados ao grupo de Aprovador de nível 1 para aprovação antes da implantação. Para obter mais informações sobre o processo de aprovação, consulte Orquestração de patches com Vulnerability Response. Para obter mais informações sobre como configurar aprovadores e grupos, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. O administrador do sistema executa a atribuição inicial de funções a usuários e grupos para a integração. Por padrão, o grupo Vulnerability Response está disponível. Se ainda não tiver sido criado, talvez você prefira criar grupos adicionais para as funções de especialista em

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	correção e analista de vulnerabilidade e adicionar usuários com o módulo de Administração de usuários em sua instância. Consulte Criação de um grupo de usuários .
	Verifique se você habilitou todos os recursos, regras, plug-ins de dependência ou trabalhos em sua instância necessários para a integração. ○ O Vulnerability Response Patch Orchestration com HCL BigFix é uma integração no local que requer o uso de um MID Server autônomo. Para obter mais informações sobre MID Servers em sua instância, consulte MID Server . ○ Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e localize o plug-in. Se não estiver instalado em sua instância, instale-o e ative-o.

O que Fazer Depois

Agora você está pronto para Instalar a aplicação Vulnerability Response Patch Orchestration with HCL BigFix.

Instalar a aplicação Vulnerability Response Patch Orchestration with HCL BigFix

Baixe a aplicação Vulnerability Response Patch Orchestration com HCL BigFix em ServiceNow® Store.

Antes de Iniciar

Funções necessárias: administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação. Administrador de vulnerabilidade (sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)) para configurar o Vulnerability Response Patch Orchestration com HCL BigFix e outros aplicativos depois que eles forem instalados.

Por Que e Quando Desempenhar Esta Tarefa

Antes de instalar a aplicação, verifique se você concluiu todos os itens da check-list em Preparar para a integração do Patch Orchestration Vulnerability Response com HCL BigFix.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Procedimento

1. Navegar até **Todos** > **Aplicações do sistema** > **todas as aplicações disponíveis** > **Todos**.
2. Localize a aplicação **Vulnerability Response Patch Orchestration with HCL BigFix** e clique em **Instalar**.

   Esta ação instala a aplicação que você baixou do ServiceNow Store.
3. Como alternativa, você pode instalar aplicações do Assistente de configuração.
   Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Vulnerability Response aplicações de terceiros usando o Assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Depois de concluir a instalação, navegue até **Todos** > **Integração da Orquestração de patches do BigFix** > **Configuração** para continuar com a configuração.

Configurar a integração de orquestração de patches Vulnerability Response com HCL BigFix

Depois de instalar a aplicação, configure-a com as informações da sua conta do BigFix e valide suas credenciais.

Antes de Iniciar

Funções necessárias: sn_vul.vulnerability_admin e sn_vul_bigfix.configure_integration

Procedimento

1. Navegar até **Integração da Orquestração de patches do BigFix** > **Configuração**.
2. Preencha os campos com suas informações e credenciais do BigFix.

Campo	Descrição
Instância de integração	O nome da conta da instância do BigFix que você deseja usar, por exemplo, BigFix Patch Management integration.
Nome do host	Insira o URL do host do BigFix.
Nome do usuário	Insira o nome de usuário da sua conta do BigFix.
Senha	Insira a senha da sua conta do BigFix.
MID Server	Insira o nome do MID Server autônomo da lista que você deseja usar. Consulte Preparar para a integração do Patch Orchestration Vulnerability Response com HCL BigFix para obter mais informações sobre MID Servers e configurar tarefas em seu Now Platform®.

3. Clique em Salvar e testar credenciais.
   O status da sua conexão entre o BigFix e sua instância Now Platform® é exibido no campo Status de validação. Se você não vir um teste bem-sucedido, siga os prompts.
4. **Opcional:** A separação de domínio é compatível com esta integração.
   Você pode adicionar várias configurações de à sua instância. Para adicionar configurações adicionais:
   a. Navegar até **Integração da Orquestração de patches do BigFix Instâncias de integração**.
   b. Verifique se o escopo da aplicação, Vulnerability Response Patch Orchestration com HCL BigFix, é exibido no campo Escopo da aplicação.
   c. Clique em **Nova**.
   d. Preencha o formulário.

Campo	Descrição
Nome	Nome da instância de integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aplicação	Vulnerability Response Patch Orchestration with HCL BigFix
Integração	[Somente leitura] O gerenciamento de patches do BigFix é o padrão.
Ativo	O padrão é ativado (selecionado). Se desmarcada, a instância não está ativa.

e. Clique em **Enviar**.
Sua nova instância de integração é exibida na lista Instâncias de integração.

f. Repita as etapas 1 a 3 para configurar sua instância de integração e testar suas credenciais.

5. Configure aprovações para solicitações de patch.
Por padrão, uma propriedade do sistema [**sn_vul_patch_orch.patch_approval_required**] é ativada para que, quando as implantações de patch forem programadas, elas sejam enviadas para revisão e aprovação para usuários atribuídos ao nível 1 - grupo de aprovação de atualização de patch.

Se você quiser que os usuários com a função sn_vul_patch_orch.configure_patch programem patches sem aprovação, desative a propriedade [**sn_vul_patch_orch.patch_approval_required**]. Você pode preferir deixar as aprovações ativadas para que os patches programados não entrem em conflito com o horário normal de trabalho.

Nota:
Se você desativar a propriedade do sistema de aprovação, qualquer usuário com a função sn_vul_patch_orch.configure_patch poderá programar e implantar patches sem revisão e aprovação.

Como um usuário com a função sn_vul.vulnerability_admin, para desativar a propriedade do sistema:

a. Navegar até **sys.properties.list**.

b. Localize **sn_vul_patch_orch.patch_approval_required** e clique nele para abrir o registro.

c. No campo Valor, digite `false`.

d. Clique em **Atualizar**.

6. Se você não desativar esta propriedade, deverá atribuir aprovadores para solicitações de patch.
Como um usuário com a função sn_vul.vulnerability_admin, siga estas etapas.

a. Navegar até **Vulnerability Response** > **Administração** > **Regras de aprovação**.

b. Se a Regra de **aprovação Implantar aprovação de atualização de patch** não for exibida na lista, clique em **Todos** à direita do ícone de filtro verde no canto superior esquerdo da tela para exibir a lista inteira.

c. Na lista, clique em **Implantar aprovação de atualização de patch**.

d. No registro, com a guia Configuração de aprovação selecionada, clique em **Configuração padrão Aprovação de atualização de patch**.

e. No registro, clique em **Nível 1 - Aprovação de atualização de patch**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

f. Adicione usuários a este grupo.

Os usuários atribuídos a este grupo aprovam as solicitações de patch enviadas por usuários com a função sn_vul_patch_orch.configure_patch. Navegue até **Minhas aprovações** para exibir e processar as solicitações.

7. Clique em**Atualizar** para salvar suas mudanças.

8. **Opcional:** Você pode configurar aprovações em vários níveis para que mais de uma aprovação seja necessária antes da implantação de solicitações de patch programadas.

a. Com o registro de aprovação da atualização de patch de configuração padrão exibido, clique em **Novo**.

b. Preencha os campos.

Campo	Descrição
Nome	Nome do nível de aprovação, por exemplo, **Nível 2 – Aprovação de atualização de patch**.
Ativo	Ativado por padrão, o que significa que o nível de aprovação está em uso.
Aprovação obrigatória	Selecione quantas aprovações são necessárias para o nível selecionado: ▪ Um aprovador necessário ▪ Todos os usuários devem aprovar
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Função	Selecione uma função para o grupo na lista.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Configuração de aprovação	Contém as configurações de aprovação.
Atribuir usando	Selecione uma opção: ▪ Usuário e grupo de usuários ▪ Campo da tabela de aprovação ▪ Script
Grupos	Grupo de nível de aprovador que consiste em vários usuários. O usuário deve ter uma das seguintes funções que você especificar.
Usuários	Edite os usuários listados nos grupos.

c. Clique em **Enviar** para salvar suas edições.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de dados de patch para a integração de orquestração de patches Vulnerability Response com HCL BigFix

Os dados de patch e os dados de rollup de patch, bem como as informações de vulnerabilidade e o status de correção de suas vulnerabilidades, são exibidos em registros em sua instância.

Exibição de dados de patch nos espaços Vulnerability Response

Funções necessárias:

- Função sn_vul_patch_orch.configure_patch para configurar e programar patches
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para o IT Remediation and Vulnerability Manager Workspaces

No Espaço de correção de TI, você pode exibir os patches:

- Na exibição inicial, é possível clicar nos cartões de pontuação para exibir registros de soluções preferenciais em IVs, ICs vulneráveis e patches preferenciais em IVs.
- Na exibição de lista, é possível exibir todos os registros de atualização de patch (VPUs) dos links de patches e os itens vulneráveis (VITs) atribuídos a você que têm patches.

Você pode programar patches dos seguintes registros:

- Da atualização de patch (VPU)
- Tarefa de correção (RT)
- Registros de item descoberto (SDI)

No Vulnerability Manager Workspace, você pode exibir os patches:

- Na exibição inicial dos tópicos de observação, é possível exibir os patches preferenciais e potenciais, as datas programadas do patch e se todos os patches foram baixados na guia **Itens vulneráveis**.
- Na exibição de lista nos esforços de correção, onde você pode exibir dados de patch em registros de IV na guia**Itens vulneráveis**.

Na exibição clássica do ambiente, navegue até **Todos** > **Vulnerability Response** > **Patches**.

Registros de atualização de patch nos espaços de VR e na exibição do ambiente clássico

Os dados de patch e os dados e status de rollup de patch são exibidos nos registros em sua instância. Os registros de patch são incluídos como parte do recurso de orquestração de patches desta integração com Vulnerability Response. Exiba registros de patch (VPU) em espaços Vulnerability Response na exibição de lista no espaço de correção de TI. Os registros de atualização de patch na exibição clássica e nos espaços Vulnerability Response incluem os seguintes dados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Dados de solução de vulnerabilidade e informações de fornecedores de patch importados pela aplicação Vulnerability Solution Management.
- Status de correção de origem que inclui o número total de dispositivos que têm uma determinada vulnerabilidade que pode ser corrigida por um patch e todos os dispositivos que não tenham atualizações.
- Status de correção que inclui % de IVs corrigidos e o total de IVs que têm um patch como preferencial.
- Dispositivos associados, itens vulneráveis, implantações de patch e solicitações de patch nos links relacionados em registros na exibição de classe. Esses dados são exibidos em guias em registros nos espaços Vulnerability Response.
- Solicitações de patch que os responsáveis pela correção enviaram para aprovação.

Rollup de estado em registros de item vulnerável

Para obter mais informações sobre acúmulo de estado para registros, consulte Dados de patch e acúmulo de estado para orquestração de patches no Vulnerability Response.

Registros que acumulam contagens de IV ativas

Para evitar o acúmulo de todos os patches para todas as vulnerabilidades, o trabalho programado seleciona somente as mudanças na contagem de IV ativa. Essas mudanças de contagem e dados relacionados são acumulados para os seguintes registros em Vulnerability Response:

- VIT
- RT
- Solução de vulnerabilidade
- Atualização de patch

Exibição de dados de patches sem soluções

Para obter mais informações sobre como exibir patches sem soluções, consulte Exibir patches sem soluções em Vulnerability Response.

Dados de patch no Vulnerability Response

Os painéis do Vulnerability Management (PA) e do CISO estão incluídos com uma assinatura com o Performance Analytics para a aplicação Vulnerability Response. Se você tiver uma assinatura do Performance Analytics, mas não tiver uma integração de orquestração de patches instalada, a guia de correção será exibida no painel do CISO, mas não será preenchida com dados.

Para o painel Vulnerability Management (PA), navegue até **Todos** > **Vulnerability Response** > **Visão geral**. Clique na guia **Correção** e role até a parte inferior da página para exibir os dados de atualizações de patch: patches programados e não programados, patches sem data de destino e contagens semanais.

No Painel do CISO, navegue até **Todos** > **Vulnerability Response** > **Painel do CISO**. Com a guia Visão geral selecionada, role até a parte inferior da página para exibir os dados de cobertura do patch: criticidade, patches programados e não programados e patches sem datas de destino.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre os painéis Vulnerability Response, consulte Usando os painéis padrão Vulnerability Response, Orquestração de patches com os espaços Vulnerability Responsee Exibição de dados de orquestração de patches nos painéis Vulnerability Response.

Programe patches com a integração de orquestração de patches Vulnerability Response HCL BigFix

Programe patches de registros de tarefa de Atualização de Patch e Correção na aplicação Vulnerability Response em sua instância Now Platform.

Antes de Iniciar

A partir da versão 16.1, você pode programar patches nos Espaços Vulnerability Response ou no ambiente clássico.

Funções necessárias:

- Função sn_vul_patch_orch.configure_patch para configurar e programar patches
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para o IT Remediation and Vulnerability Manager Workspaces

Procedimento

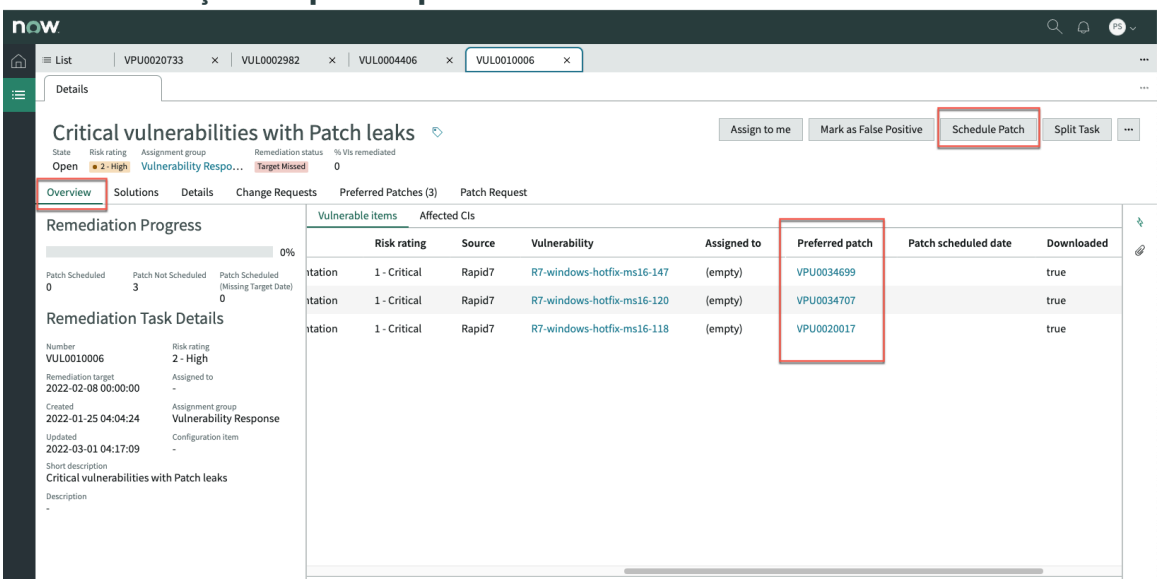
1. Nos espaços de vulnerabilidade Vulnerability Response, como um usuário com a função sn_vul.remediation_owner, navegue até **Todos** > **Vulnerability Response** > **Espaço de correção de TI**.
2. Na página inicial, clique **em Patch preferencial em IVs**.
   A lista de registros de atualização de patch para os IVs com patches preferenciais atribuídos a você é exibida.
3. Localize um registro que você deseja abrir e clique para abri-lo.
4. Como alternativa, na exibição de lista no espaço de trabalho, clique em **Patches** > **Todos** e localize um registro de atualização de patch.
   O registro de atualização de patch é exibido. Talvez você prefira revisar os dados antes de programar um patch, pois pode haver outros patches já programados.
5. Consulte a tabela a seguir sobre os dados exibidos e o que você pode fazer.
6. Clique **em Programar patch**.
7. Na caixa de diálogo, preencha os campos.
8. Clique em **Implantar**.
   A solicitação de patch é enviada para para revisão. Você pode exibir o status de todas as solicitações enviadas de **Solicitações de exceção** > **Minhas solicitações** na exibição de lista.
9. Como alternativa, você pode programar patches de tarefas de correção (RT) que são atribuídas a você ou ao seu grupo.

Nota:
A opção de programar um patch de um registro de tarefa de correção está disponível somente se houver patches mapeados para (associados aos) IVs na tarefa. Esses patches serão exibidos na coluna Patch preferencial se você rolar para a direita de um registro de tarefa de correção com a guia Visão geral selecionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de correção com patches preferenciais



10. Clique em **Programar patch** no registro RT e siga as etapas listadas acima para programá-lo na caixa de diálogo.
11. Você pode programar patches para as etapas listadas anteriormente no ambiente clássico.
    Para localizar esses registros, siga estas etapas.

    a. No ambiente clássico, navegue até **Vulnerability Response** > **Patches** > **Todos**.

    b. Na lista exibida, localize um registro de atualização de patch.

    c. Para tarefas de correção, navegue até **Vulnerability Response** > **Tarefas de correção** e localize um registro.
    O rastreia o status da correção na guia Status da correção. Na parte inferior do registro, os dados do patch são exibidos nos Links relacionados.

    d. Clique em Programar patch e preencha os campos.

Campo	Descrição
Nome da implantação	Insira um nome para esta implantação de patch. Este nome ajuda a rastrear suas atualizações.
Atualização de patch	Escolha um dos patches disponíveis na lista.
Ativos	Selecione um: ▪ Grupo de computadores: selecione esta opção se quiser escolher uma coleção (um grupo de ativos) para este patch. Os grupos são compostos pelos itens de configuração que são importados da aplicação BigFix. ▪ Lista de computadores: selecione esta opção se quiser escolher computadores individuais (ativos) para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	este patch. Você pode ver dados sobre o fabricante, local, classe, quando foi atualizado pela última vez e a programação de manutenção na caixa de diálogo exibida.
Hora de início e hora de término	Insira as horas de início e de término da janela de tempo. Insira quando você deseja que o patch inicie sua implantação e o último dia em que o patch pode ser instalado.

Mensagens REST para a integração de orquestração de patches do Vulnerability Response com HCL BigFix

A integração de orquestração de patches Vulnerability Response com mensagens HCL BigFix REST são usadas para fazer chamadas para a API do BigFix.

Login do BigFix

Você também pode usar as mensagens REST para o login do BigFix para autenticar as solicitações de REST API. As mudanças no método de registro da mensagem REST afetam as solicitações de autenticação feitas ao BigFix.

Nome do parâmetro	Valor	Descrição
sourceType	cumulativo	Indica de onde a integração de origem extrai dados. Usado por código. Mudanças não são recomendadas.
classificaçãoDIR	desc	Indica a direção da classificação dos dados extraídos da integração. Mudanças não são recomendadas.
campo de classificação	severidade	Indica o campo no qual a classificação de dados se baseia. Mudanças não são recomendadas.
tipo	vulnerabilidade	Indica o tipo de dados a serem obtidos da integração para a integração de ativos. Mudanças não são recomendadas.

Integração do BigFix

Você pode usar a mensagem REST para a integração do BigFix para recuperar informações do BigFix. As mudanças no método de registro da mensagem REST afetam as solicitações feitas ao BigFix para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Métodos REST

Método REST	Descrição
Obter dados de busca	Recupera as informações do BigFix sobre um dos seguintes com base na consulta fornecida:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Métodos REST

Método REST	Descrição
	• Computador/Grupos de computadores • Fixlets • Fixlets relevantes em computadores • Ação/ Comportamento

Nome do parâmetro	Valor	Descrição
url	Valores dinâmicos com base no usuário	Indica o endpoint do console do BigFix

Patch de implantação do BigFix

Você pode usar a mensagem REST para a integração do BigFix para programar patches do Now Platform® para o BigFix. As mudanças no método de registro da mensagem REST afetam as solicitações feitas ao BigFix para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Método REST	Descrição
Patch de implantação POST	Programa o patch para o console do BigFix em um ou vários computadores.

Nome do parâmetro	Valor	Descrição
url	Valores dinâmicos com base no usuário	Indica o endpoint do console do BigFix.
título	Valores dinâmicos com base no usuário	Título da implantação.
configurações_tag	Configurações de nome de marcador XML com valores	Indica configurações que têm parâmetros diferentes e são enviadas para o BigFix ao programar o patch.
computer_tag	Computadores nomeados com marcador XML com valores	Indica a lista de computadores nos quais o patch será programado.
site_name	Valor da atualização do patch	Nome do site onde o Fixlet está presente.
fixlet_id	Valor da atualização do patch	ID do Fixlet.

Transformação de dados para a integração de orquestração de patches com HCL BigFix

Os dados são recuperados da orquestração de patches Vulnerability Response com integração do HCL BigFix, processados por meio de um conjunto de fontes de dados e transformados em sua instância Now Platform®.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importação de coleção do BigFix

Os dados dos ativos importados (computadores e grupos de computadores) são carregados na tabela BigFix Collection Import [sn_vul_bigfix_collection_import]. O computador BigFix e a TM de importação de grupos de computadores (mapa de transformação?) são usados para transformar as informações importadas.

Nota:
As mudanças neste mapa de transformação alteram a forma como os dados da importação da coleção do BigFix são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação** e localize o Computador BigFix e o TM de importação de grupos de computadores. A tabela a seguir lista os campos do mapa de transformação por integração.

Tempo do script do mapa de transformação da importação do computador BigFix e dos grupos de computadores

Script	Descrição
OnStart (quando um conjunto de importação criou uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_bigfix] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto de importação concluir a transformação).	Script usado para criar e atualizar ICs com base nas regras de pesquisa de IC e coleções, bem como na relação entre elas. Com base nos resultados, este script modifica os valores na variável de escopo [sn_vul_bigfix]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de ICs criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de fixlet do BigFix

Os dados dos fixlets importados são carregados na tabela BigFix Fixlet Import [sn_vul_bigfix_patch_update_import].

O BigFix Fixlet Import TM é usado para transformar as informações importadas.

Nota:
As mudanças neste mapa de transformação alteram como os dados da importação de Fixlet do BigFix são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação** e localize o BigFix Fixlet Import TM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de importação de Fixlet do BigFix

Campo de origem	Campo de destino	Descrição
u_id	artigo_id	ID exclusivo de um fixlet em um site.
u_id	source_id	ID exclusivo de um fixlet em um site.
U_site_name	Sn_vul_bigfix_site_name	Nome do site no BigFix do qual o Fixlet depende.
U_display_name	Título	Título do Fixlet.
[Script]	ID do boletim	ID de origem da solução.
[Script]	Sn_vul_solution	Solução baseada no ID de origem.
U_source	informativo_origem	Fornecedor de origem da solução.
[Script]	Data_versão	Data de lançamento do fixlet.
U_category	Update_category	Categoria do fixlet.
[Script]	Is_highest_supersedence	Booliano para se o fixlet for a substituição mais alta ou não.
[Script]	Is_downloaded	Booliano de se o fixlet foi baixado ou não.
[Script]	Integration_instance	Nome da instância da qual o fixlet é importado.
U_source_severity	Source_severity	Severidade do fixlet.
U_applicable_count	Num_total	Número total de dispositivos com fixlets ausentes.
[Script]	Last_modified	Data da última modificação do fixlet.

Tempo do script do mapa de transformação de importação do Fixlet do BigFix

Script	Descrição
OnStart (quando um conjunto de importação criou uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_bigfix] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto de importação concluir a transformação).	O script usado para atualizar os valores na variável de escopo [sn_vul_bigfix]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de fixlets criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importação de fixlet do dispositivo do BigFix

Os dados dos fixlets relevantes importados nos computadores são carregados na tabela BigFix Device Fixlet Import [sn_vul_bigfix_device_patch_import].

O BigFix Device Fixlet TM é usado para transformar as informações importadas.

Nota:
As mudanças neste mapa de transformação alteram como os dados da importação do Fixlet do dispositivo do BigFix são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação** e localize o BigFix Device Fixlet TM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Tempo do script do mapa de transformação do Fixlet do dispositivo do BigFix

Script	Descrição
OnStart (quando um conjunto de importação criou uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_bigfix] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto de importação concluir a transformação).	Script usado para criar e atualizar ICs com base nas regras de pesquisa de IC e nas coleções, bem como na relação entre elas. Com base nos resultados, este script modifica os valores na variável de escopo [sn_vul_bigfix]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de ICs criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de ações do BigFix

Os dados das ações importadas são carregados na tabela Importação de ações do BigFix [sn_vul_bigfix_deployment_import].

O BigFix Actions Import TM é usado para transformar as informações importadas.

Nota:
As mudanças neste mapa de transformação alteram como os dados da importação do BigFix Actions são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação** e localize o BigFix Fixlet Import TM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de importação de ações do BigFix

Campo de origem	Campo de destino	Descrição
u_id	source_id	ID exclusivo de uma ação.
U_name	nome	Nome da ação
[Script]	Sn_vul_bigfix_discovered_item	Referência do item descoberto no qual o patch está implantado
U_status	status	Status da ação
[Script]	Sn_vul_patch_orch_update	Referência do patch
U_apply_count	Contagem_success	Contagem de sucesso da ação.
U_retry_count	tentar novamente	Contagem de novas tentativas da ação.
[Script]	Deployment_time	Hora de início da ação.
[Script]	prazo	Hora de término da ação.
[Script]	Origem_criada	Hora de criação da ação.
[Script]	Integration_instance	Nome da instância da qual a ação é importada.

Tempo do script do mapa de transformação de importação do BigFix Actions

Script	Descrição
OnStart (quando um conjunto de importação criou uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_bigfix] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto de importação concluir a transformação).	O script usado para atualizar os valores na variável de escopo [sn_vul_bigfix]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de ações criadas, atualizadas e ignoradas. Este script é para uso interno e não deve ser modificado ou excluído.

Exemplo de fluxo de trabalho para a integração de orquestração de patches do Vulnerability Response com o HCL BigFix

Um exemplo de como a orquestração de patches funciona com o produto HCL BigFix.

Antes de Iniciar

Digamos, por exemplo, que todo o seu ambiente seja corrigido uma vez a cada três semanas. A janela de patch mais recente foi concluída há uma semana, mas você deseja aplicar um patch para corrigir uma vulnerabilidade crítica que se tornou conhecida recentemente. Devido à natureza crítica desta vulnerabilidade, você não pode esperar mais duas semanas pelo próximo patch programado.

Funções necessárias:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para o Vulnerability Manager Workspace.
- sn_vul.remediation_owner para exibir o espaço do proprietário de correção de TI.
- Função sn_vul_patch_orch.configure_patch para configurar e programar patches.
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para o IT Remediation e Vulnerability Manager Workspaces.

Por Que e Quando Desempenhar Esta Tarefa

Como gerente de vulnerabilidade ou analista que trabalha no Vulnerability Manager Workspace, você pode considerar a criação de tópicos de observação ou a edição de tópicos de observação existentes para ajudá-lo a capturar IVs importados com vulnerabilidades críticas. Com a integração de orquestração de patches, você também pode ver os patches que deseja usar para corrigir e rastrear essas vulnerabilidades. A tabela a seguir lista alguns exemplos com as condições que você pode definir para tópicos de observação para orquestração de patches. Use esses exemplos para ajudá-lo a determinar as configurações que funcionam melhor para o seu ambiente. Consulte Criar um tópico de observação no Vulnerability Manager Workspace para obter mais informações sobre como configurar o tópico de observação.

Amostra de tópicos de observação para orquestração de patches no Vulnerability Manager Workspace

Nome do tópico de observação	Descrição
Vulnerabilidades críticas com vazamentos de patch	A classificação de risco é 1 - crítico E O motivo é o patch não programado
Vulnerabilidades críticas com patches programados (ANS ausente)	O motivo é patch programado (data de destino ausente)
Vulnerabilidades críticas com patches programados	A classificação de risco é 1 - crítico E A data programada do patch não está vazia E O motivo é Patch programado

- Como gerente ou analista de vulnerabilidade, depois de criar os tópicos de observação e os esforços de correção, você gera tarefas de correção. Em registros de IV e tarefas de correção, você pode fazer uma busca detalhada na guia Detecções e localizar registros de itens descobertos que têm a vulnerabilidade que você está rastreando, junto com os ativos importados pelo produto BigFix.
- Como analista de vulnerabilidade ou administrador, você pode monitorar os dados de patch associados à vulnerabilidade. Você também pode implantar um patch ou vários patches em um ativo específico (item de configuração) de um registro de item descoberto.

Como especialista em correção de TI, você tem opções de como lidar com a vulnerabilidade com uma implantação de patch.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você pode programar o patch a partir de um registro de atualização de patch (VPU#).
- Se os itens vulneráveis (IV) tiverem soluções preferenciais mapeadas para eles e forem atribuídos a você ou aos seus grupos, você poderá programar os patches de uma tarefa de correção que tenha esses itens vulneráveis.

Procedimento

1. Como Especialista em correção de TI, no Espaço de correção de TI, clique na exibição inicial.
2. Na exibição inicial, clique no cartão de pontuação **Tarefas de correção atribuídas** para exibir os registros.

   Para fins deste exemplo, você pode verificar o campo Descrição resumida na tarefa de correção (VUL#) para qualquer texto relacionado à sua vulnerabilidade crítica. Digamos, por exemplo, que você saiba que seu gerenciador de vulnerabilidades criou um tópico de observação chamado Vulnerabilidades críticas com vazamentos de patch para capturar IVs (VIT#) com esta vulnerabilidade crítica.

   Com o registro aberto, você também pode revisar os IVs, os patches preferenciais e ver se você ou alguém do seu grupo já enviou solicitações de patch para aprovação.
3. Se você tiver informações suficientes, talvez prefira enviar uma solicitação de patch agora a partir desta tarefa de correção.

   Nota:
   Se os IVs associados ao registro não tiverem patches mapeados para eles, o botão **Programar patch** não estará disponível no registro.
4. Clique em **Programar patch** e preencha os campos na caixa de diálogo.
   Para obter mais informações sobre como programar um patch, consulte Programe patches com a integração de orquestração de patches Vulnerability Response HCL BigFix.
5. Como alternativa, na exibição de lista no Espaço de correção de TI, você pode clicar nos links Tarefas de correção, Itens vulneráveis, Soluções e Patches para exibir esses registros.

   No caso deste exemplo, em vez de um nome de tópico de observação, você pode saber o ID do artigo ou o ID do boletim e o título do patch. Em caso afirmativo, convém verificar se algum dos IVs com esta vulnerabilidade está atribuído a você ou aos seus grupos. Em registros de atualização de patch, você pode enviar solicitações de patch. Em registros de IV, você pode verificar possíveis patches e abrir a tarefa de correção associada se quiser enviar uma solicitação de patch.
6. Se você não tiver acesso aos espaços ou se preferir exibir dados e programar patches no ambiente clássico, siga estas etapas.

   a. Navegar até **Todos** > **Vulnerability Response** > **Patches** > **Todos**.

   b. Localize o registro de atualização de patch desejado.
   Você pode preferir filtrar os registros com pontuações de risco crítico.

   c. Revise os campos de IVs associados e % de IVs corrigidos na guia Status de correção.
   Se os IVs tiverem patches disponíveis, o botão **Programar patch** será exibido no canto superior direito do registro.

   d. Se você decidir enviar uma solicitação, clique em **Programar patch**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como programar um patch, consulte Programe patches com a integração de orquestração de patches Vulnerability Response HCL BigFix.

e. Como alternativa, digamos que você não tenha as informações do ID do patch, mas verifique o campo Descrição resumida nas tarefas de correção atribuídas ao seu grupo para qualquer texto relacionado à sua vulnerabilidade crítica.

f. Navegar até **Todos** > **Vulnerability Response** > **Tarefas de correção** > **Atribuído aos Meus grupos**.

g. Localize o registro desejado e clique nele para abri-lo.
No registro aberto, revise a guia Status de correção para IVs e % de IVs corrigidos. Clique nos Links relacionados para registros IV, Soluções preferenciais, Patches preferenciais e Solicitações de patch.

Nota:
Se os IVs associados ao registro não tiverem patches mapeados para eles, o botão **Programar patch** não estará disponível no registro.

h. Clique em **Programar patch** no registro se quiser enviar uma solicitação de patch.

Noções básicas sobre a integração de orquestração de patches [Vulnerability Response com Microsoft SCCM

Gerencie patches e implantações de patch para as vulnerabilidades críticas em seus ativos com a integração Vulnerability Response com o produto Microsoft System Center Configuration Manager (SCCM).

Orquestração de patches com Vulnerability Response

A orquestração de patches com Vulnerability Response usa importações programadas de integrações de soluções de terceiros, fornecedores de patches e scanners de vulnerabilidade. Os dados de detecção do scanner correspondem aos ativos em seu ambiente com vulnerabilidades e atualizações de patch que podem corrigi-los. Você envia solicitações de patch para aprovação, programa atualizações de patch para resolver itens vulneráveis e monitora o andamento da correção, tudo a partir da sua instância Now Platform®.

Vulnerability Response orquestração de patches com Microsoft SCCM

Quando o Vulnerability Response Patch Orchestration com a aplicação SCCM Microsoft é usado com as aplicações ServiceNow® Solução de gerenciamento de vulnerabilidade, Patch Orchestration e Vulnerability Response, os gerentes e analistas de vulnerabilidade podem executar as seguintes tarefas:

- Consulte mais contexto e informações sobre os tipos de patches e soluções de fornecedores (patches).
- Exiba e monitore os dados de vulnerabilidade e solução, bem como o andamento da correção de vulnerabilidades de registros nos espaços Vulnerability Response.

Especialistas em TI e proprietários de correção podem executar as seguintes tarefas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Implante patches compatíveis com o produto Microsoft SCCM para seus Windows, CentOS, macOS, Oracle e outros ativos em intervalos regulares e programados fora do horário de expediente para evitar conflitos com o trabalho.
- Identifique ativos sem patch com vulnerabilidades ou ativos que foram ou não atualizados com sucesso por patches programados a partir de dados de detecção importados de scanners de terceiros.
- Programe os patches disponíveis no Espaço de correção de TI ou na IU clássica para ativos vulneráveis sem patch de atualização de patch, tarefa de correção e registros de item descoberto.

Termos-chave nas aplicações SCCM Vulnerability Response e Microsoft

IC (Configuration Item, item de configuração)

ICs são os ativos existentes listados em Configuration Management Database (CMDB). Microsoft SCCM chama ICs, dispositivos.

Coleções e coleções de dispositivos

Terminologia usada no produto SCCM Microsoft que se refere a um grupo de ativos.

Item vulnerável

Uma vulnerabilidade importada que corresponde a um ativo existente no seu CMDB.

Instância

Uma conta distinta da aplicação SCCM Microsoft. Cada conta de usuário pode ser uma instância na aplicação Microsoft SCCM. Este termo também se refere a um endereço da Web exclusivo e seguro para uma instância Now Platform.

Integração

Uma integração é um trabalho programado no Now Platform que recupera informações de uma fonte de terceiros, como a integração com as Microsoft máquinas SCCM.

Solução

Existem dois tipos de soluções no contexto desta integração, potenciais e preferenciais. Uma possível solução é aquela que pode solucionar uma vulnerabilidade. As vulnerabilidades geralmente têm muitas soluções possíveis. Uma solução preferencial corresponde à solução mais eficaz para uma vulnerabilidade específica detectada.

Patches

Atualizações de software que corrigem vulnerabilidades. Na aplicação Microsoft SCCM, os patches são chamados de Patches. Por exemplo, o Microsoft SCCM tem patches para Windows, CentOS, MAC, Oracle e outros produtos.

Patch preferencial

Patches preferenciais são atualizações de software que têm como objetivo corrigir vulnerabilidades específicas. Os patches, uma vez implantados, são mapeados para os itens vulneráveis que estão relacionados a vulnerabilidades específicas e os corrigem.

Tarefa de correção ou, antes da v15.0 de Vulnerability Response, grupos de vulnerabilidade

Listas de itens vulneráveis na aplicação Vulnerability Response de ações que são necessárias para corrigir vulnerabilidades.

Implantação

Para fins desta integração, a implantação se refere a quando você aplica, inicia ou programa um patch para uma máquina. Você pode implantar os patches que baixou do Microsoft SCCM no seu Now Platform navegando até itens descobertos, patches ou tarefas de correção de registros individuais em Vulnerability Response. Você pode implantar patches com trabalhos programados em máquinas individuais ou em grupos de computadores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A implantação no Now Platform também pode se referir a uma integração que oferece suporte a várias origens. Uma única existência de integração é chamada de implantação da sua integração. Uma implantação se refere às integrações e produtos em seu ambiente. Por exemplo, você pode ter várias implantações da integração de vulnerabilidade SCCM Microsoft em seu ambiente.

Solução de gerenciamento de vulnerabilidade e Vulnerability Response integração de orquestração de patches com Microsoft SCCM

A aplicação Solução de gerenciamento de vulnerabilidade é uma aplicação Now Platform que correlaciona suas descobertas de vulnerabilidade com o detalhamento das soluções (patches) que as corrigem. Identifique os patches de software de terceiros para produtos e serviços, atualizações de configuração e outros controles que têm o maior impacto para sua organização. Junto com as informações do scanner de terceiros, as aplicações Solução de gerenciamento do Vulnerability Response, Vulnerability Responsee Vulnerability Response Patch Orchestration com Microsoft SCCM trabalham juntos para instalar patches preferenciais da solução, para a vulnerabilidade, para o item vulnerável para ajudá-lo a corrigir e feche vulnerabilidades para o seu ambiente. As aplicações de integração Solução de gerenciamento do Vulnerability Response, Vulnerability Responsee Vulnerability Response Patch Orchestration Microsoft SCCM estão disponíveis no ServiceNow® Store.

Funções necessárias de Now Platform

As tarefas de instalação, configuração e correção de integração exigem as funções a seguir em sua instância Now Platform.

admin

Usuários com esta função obtêm direitos para aplicações nas instâncias ServiceNow Store e os baixam para Now Platform instâncias.

sn_vul.vulnerability_admin

Usuários com esta função ativam aplicações na instância Now Platform e concluem a configuração da aplicação Vulnerability Response. Esta função tem acesso completo à aplicação Vulnerability Response (VR) e seus registros. Este usuário administrador configura todas as aplicações de VR, regras e integrações de terceiros.

sn_vul_sccm.configure_integration

Usuários com esta função configuram a aplicação Microsoft SCCM Patch Orchestration Integration. Esta função contém a função granular sn_vul_sccm.read_integration.

sn_vul_sccm.read_integration

Usuários com esta função podem exibir (somente leitura) os registros da aplicação Vulnerability Response e Microsoft SCCM Patch Orchestration Integration e os dados de orquestração de patches.

sn_vul_patch_orch.configure_patch

Usuários com esta função podem configurar e aplicar patches.

sn_vul_patch_orch.read_patch

Usuários com esta função podem exibir (somente leitura) informações do patch.

Aprovadores

Atribua usos aos grupos de aprovadores de nível 1 e aprovador de nível 2 se quiser que as solicitações de patch enviadas sejam aprovadas antes da implantação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como atribuir essas funções usando o Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração.

Regras de pesquisa de IC

Quando os dados são importados da aplicação Microsoft SCCM, a aplicação Vulnerability Response pesquisa automaticamente correspondências no Configuration Management Database (CMDB) usando dados de ID de recurso. As regras de pesquisa de IC são usadas para identificar ICs (ativos) e adicioná-los automaticamente aos registros de item vulnerável (IV) quando os IVs são criados. As regras de pesquisa de IC a seguir são enviadas com o sistema de base e são usadas para identificar ICs (ativos) e adicioná-los aos itens descobertos.

Esta regra de pesquisa depende dos dados trazidos pelo Service Graph Connector with SCCM. Você deve instalar e executar a integração do CMDB antes de executar as integrações do SCCM. Se você tiver várias instalações do servidor SCCM, poderá configurar o alias de conexão do Service Graph Connector na página de configuração de orquestração de patches do SCCM.

MID Server

O Vulnerability Response Patch Orchestration com Microsoft SCCM é uma integração no local. Requer um MID Server autônomo Windows que não faça parte de um cluster de MID Server. O MID Server é necessário para executar scripts em máquinas remotas de sua instância para importar dados do servidor SCCM. As APIs para esta integração são chamadas usando MID Servers que você configurou em sua instância Now Platform. Preparar para a integração de orquestração de patches [Vulnerability Response com o Microsoft SCCM.

Integrações e dependências do Vulnerability Response Patch Orchestration com a aplicação SCCM Microsoft

As aplicações de produto e dependência a seguir são necessárias para a integração do Vulnerability Response Patch Orchestration com o Microsoft System Center Configuration Manager (SCCM). Essas aplicações estão disponíveis no ServiceNow® Store

Versões disponíveis de aplicações e dependências necessárias para a integração de orquestração de patches

Para exibir dados de orquestração de patches e atualizações disponíveis (patches) nos espaços e na IU clássica em Vulnerability Response, os aplicativos a seguir são necessários. Todas as aplicações listadas estão disponíveis no ServiceNow® Store. Algumas aplicações exigem assinaturas separadas.

Para obter mais informações sobre a compatibilidade de versão com as aplicações e versões da família necessárias, consulte o artigo KB0856498 Vulnerability Response Compatibility Matriz e mudanças de esquema de versão na Base de conhecimento HI.

Aplicação e versão de lançamento
Vulnerability Response
Solução de gerenciamento de vulnerabilidade
Aplicação Vulnerability Response Patch Orchestration
Vulnerability Response Patch Orchestration com aplicação Microsoft SCCM

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação e versão de lançamento
Security Support Common
Orquestração de suporte de segurança
Service Graph Connector with SCCM

Vulnerability Response orquestração de patches tabelas da aplicação

A aplicação Vulnerability Response Patch Orchestration contém as seguintes tabelas:

Tabela	Descrição
Atualização de patch [sn_vul_patch_orch_update]	Armazena informações sobre os patches que estão disponíveis em instâncias distintas.
Atualização de dispositivo [sn_vul_patch_orch_m2m_src_ci_update]	Armazena dados sobre os patches implantados, junto com o status da implantação, que são exibidos em registros de item descoberto.
Coleção [sn_vul_patch_orch_collection]	Armazena dados de coleta de instâncias distintas.
Coleção de dispositivos [sn_vul_patch_orch_m2m_src_ci_collection]	Armazena dados de coleções sobre itens descobertos.
Implantação de patch [sn_vul_patch_orch_deployment]	Armazena informações sobre patches implantados sobre Coleções e ICs.
Possível patch [sn_vul_patch_orch_m2m_vuln_patch]	Armazena dados sobre patches e vulnerabilidades que identificam os patches que podem ser usados para resolver uma vulnerabilidade.

Vulnerability Response Patch Orchestration com integrações SCCM Microsoft

As integrações desenvolvidas pela engenharia ServiceNow® compõem a implantação da solução orquestrada com o produto Microsoft SCCM. As integrações a seguir estão incluídas com a aplicação Microsoft SCCM Patch Orchestration Integration que você baixa em ServiceNow® Store.

Depois de instalar a aplicação de integração na sua instância Now Platform, para exibir essas integrações, navegue até **Integrações** > **SCCM Patch Orchestration Integration** > **Integrações**. A aplicação Vulnerability Response processa dados em intervalos de tempo programados importados por essas integrações com Microsoft endpoints SCCM.

Integração	Descrição
Microsoft Integração de coleta do SCCM	• Esta integração está programada para ser executada diariamente e é executada primeiro na execução da integração encadeada. • Recupera as coleções de dispositivos das Coleções SCCM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
Microsoft SCCM Device Collection Integration	• Quando programada, essa integração é acionada pela conclusão da integração de coleta do SCCM. Você também pode executá-lo sob demanda. • Esta integração busca os dispositivos em cada coleção. Esta integração cria registros na tabela de itens descobertos e na tabela de coleção de dispositivos.
Microsoft Integração de atualização de patch do SCCM	• Quando programada, esta integração é acionada pela conclusão da integração da coleção de dispositivos SCCM. Você também pode executá-lo sob demanda. • Recupera informações do servidor SCCM sobre os patches que estão instalados ou ausentes nos dispositivos (ativos).
Microsoft Integração de implantações do SCCM	• Quando programada, essa integração é acionada pela conclusão da integração de atualização de patch. Você também pode executá-lo sob demanda. • Recupera informações sobre os patches programados pela equipe de TI no servidor SCCM.

Preparar para a integração de orquestração de patches [Vulnerability Response com o Microsoft SCCM

Prepare-se para a integração executando as tarefas de configuração a seguir.

Antes de Iniciar

Funções necessárias: administrador para instalar as aplicações e atribuir funções. Outras funções estão listadas na tabela a seguir.

Por Que e Quando Desempenhar Esta Tarefa

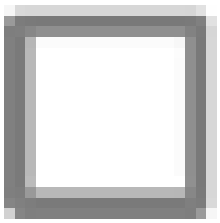
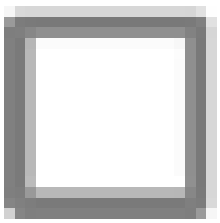
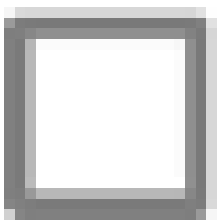
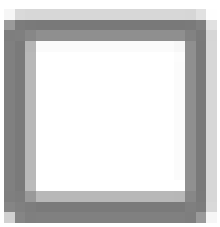
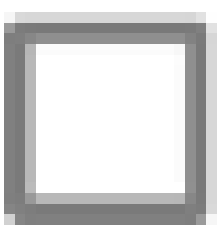
Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração.

Procedimento

1. Para uma instalação e configuração sem problemas da aplicação Vulnerability Response Patch Orchestration com Microsoft SCCM, siga a check-list fornecida abaixo.
2. Você pode preferir imprimir a check-list a seguir e verificar se os itens listados estão concluídos antes de instalar a aplicação e importar informações relacionadas a patches e vulnerabilidades para sua instância Now Platform®.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	(Opcional) Se ainda não estiver instalado e ativado, talvez você prefira instalar a aplicação Vulnerability Response antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar a aplicação Vulnerability Response, consulte Como instalar Vulnerability Response. Esta integração requer a versão 16.1 de Vulnerability Response ou posterior.
	Se ainda não estiver instalado, obtenha os direitos e instale um aplicativo scanner de terceiros para importar dados de vulnerabilidade. Consulte Integrações do Vulnerability Response para obter mais informações sobre scanners de terceiros compatíveis com Vulnerability Response. Consulte .
	Se ainda não estiver instalado, obtenha os direitos e baixe a aplicação Vulnerability Response Patch Orchestration com Microsoft SCCM para sua instância Now Platform®. Consulte .
	Obtenha Microsoft credenciais SCCM. Verifique se você tem nomes de conta, senhas e outras informações de serviço exigidas por seus produtos Microsoft para que você tenha acesso a eles.
	Verifique se você tem grupos ou usuários para gerenciar as integrações e corrigir itens vulneráveis. **admin** O administrador do sistema obtém direitos, baixa e instala a aplicação Microsoft SCCM Patch Orchestration e as outras aplicações necessárias para a integração. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração em Vulnerability Response ou no módulo Administração de usuário. **sn_vul.vulnerability_admin** Depois de atribuído, o administrador de vulnerabilidade conclui a configuração das Microsoft integrações

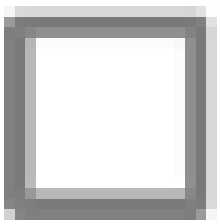
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	do SCCM e de outras aplicações de terceiros. Esta função tem acesso completo à aplicação Vulnerability Response (VR) e seus registros. Esta função configura todas as aplicações de VR, regras, integrações de terceiros, Vulnerability Response aplicações de Patch Orchestration e Vulnerability Solution Management. **sn_vul_sccm.configure_integration** Usuários com esta função configuram a aplicação Microsoft SCCM Patch Orchestration Integration. Esta função contém as funções granulares sn_vul_sccm.read_integration e connection_admin que permitem ao usuário se conectar ao console do SCCM e configurar as instâncias de integração em seu Now Platform. **sn_vul_sccm.read_integration** Usuários com esta função podem exibir (somente leitura) os registros da aplicação Vulnerability Response e Microsoft SCCM Patch Orchestration Integration e os dados de orquestração de patches. **sn_vul_patch_orch.configure_patch** Usuários com esta função podem configurar e aplicar patches. Os patches solicitados por este usuário do item vulnerável e os registros de atualização de patch serão enviados para aprovação se a gestão de mudanças estiver ativa e os aprovadores estiverem atribuídos. **sn_vul_patch_orch.read_patch** Usuários com esta função podem exibir (somente leitura) informações de patch em registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para o IT Remediation e Vulnerability Manager Workspaces. **Aprovadores** Usuários atribuídos ao nível de aprovador 1 e, opcionalmente, nível de aprovador 2, grupos de aprovadores aprovam as solicitações de patch enviadas. Por padrão, os patches são enviados ao grupo de nível 1 de aprovadores para aprovação antes da implantação. Para obter mais informações sobre o processo de aprovação, consulte Configurar a Orquestração de patches do Vulnerability Response com a integração do SCCM Microsoft. Para obter mais informações sobre como configurar aprovadores e grupos, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. O administrador do sistema executa a atribuição inicial de funções a usuários e grupos para a integração. Por padrão, o grupo Vulnerability Response está disponível. Se ainda não tiver sido criado, talvez você prefira criar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	grupos adicionais para as funções de especialista em correção e analista de vulnerabilidade e adicionar usuários com o módulo de Administração de usuários em sua instância. Consulte Criação de um grupo de usuários .
	Verifique se você habilitou todos os recursos, regras, plug-ins de dependência ou trabalhos em sua instância necessários para a integração. ○ O Vulnerability Response Patch Orchestration com Microsoft SCCM é uma integração no local que requer o uso de um MID Server Windows autônomo. Para obter mais informações sobre MID Servers em sua instância, consulte MID Server . ○ Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e localize o plug-in. Se não estiver instalado em sua instância, instale-o e ative-o.

Instalar a aplicação Vulnerability Response Patch Orchestration com Microsoft SCCM

Baixe a aplicação do ServiceNow Store.

Antes de Iniciar

Antes de instalar a aplicação, verifique se você concluiu todos os itens da check-list em Preparar para a integração de orquestração de patches [Vulnerability Response com o Microsoft SCCM.

Funções necessárias: administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação. Administrador de vulnerabilidade (sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) para configurar o Vulnerability Response Patch Orchestration Microsoft SCCM e outros aplicativos depois que eles forem instalados.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter o direito de prosseguir para Ativar uma aplicação ServiceNow Store.

Procedimento

1. Navegar até **Todos** > **Aplicações do sistema** > **todas as aplicações disponíveis** > **Todos**.
2. Localize a aplicação **Vulnerability Response Patch Orchestration with Microsoft SCCM** e clique em **Instalar**.

   Esta ação instala a aplicação que você baixou do ServiceNow Store.
3. Como alternativa, você pode instalar aplicações do Assistente de configuração.
   Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Vulnerability Response aplicações de terceiros usando o Assistente de configuração.

O que Fazer Depois

Depois de concluir a instalação, navegue até **Todos** > **Integração do Orquestração de patches do Microsoft SCCM** > **Configuração** para continuar com a configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar a Orquestração de patches do Vulnerability Response com a integração do SCCM Microsoft

Depois de instalar o aplicativo, configure-o com as informações da sua conta e valide suas credenciais.

Antes de Iniciar

Funções necessárias: sn_vul.vulnerability_admin e sn_vul_sccm.configure_integration

Procedimento

1. Navegar até **Todos** > **Integração do Orquestração de patches do Microsoft SCCM** > **Configuração**.
2. Preencha os campos com suas Microsoft informações e credenciais do SCCM.

Campo	Descrição
Instância de integração	O nome da Microsoft conta de instância do SCCM que você deseja usar, por exemplo, Microsoft SCCM Patch Management integration.
Nome do host	Insira o URL do host SCCM Microsoft.
Nome do usuário	Insira o nome de usuário da sua conta do SCCM Microsoft.
Senha	Insira a senha da sua conta do SCCM Microsoft.
MID Server	Insira o nome do MID Server autônomo da lista que você deseja usar. Consulte Preparar para a integração de orquestração de patches [Vulnerability Response com o Microsoft SCCM para obter mais informações sobre MID Servers e configurar tarefas em seu Now Platform®.

3. Clique em Salvar e testar credenciais.
   O status da sua conexão entre o Microsoft SCCM e sua instância Now Platform® é exibido no campo Status de validação. Se você não vir um teste bem-sucedido, siga os prompts.
4. **Opcional:** A separação de domínio é compatível com esta integração.
   Você pode adicionar várias configurações de à sua instância. Para adicionar configurações adicionais:
   a. Navegar até **Todos** > **Integração do Orquestração de patches do Microsoft SCCM Instâncias de integração**.
   b. Verifique se o escopo da aplicação, Vulnerability Response Patch Orchestration with Microsoft SCCM, é exibido no campo Escopo da aplicação.
   c. Clique em **Nova**.
   d. Preencha o formulário.

Campo	Descrição
Nome	Nome da instância de integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aplicação	Vulnerability Response Patch Orchestration com Microsoft SCCM
Integração	[Somente leitura] Microsoft O gerenciamento de patches do SCCM é o padrão.
Ativo	O padrão é ativado. Se desmarcada, a instância não está ativa.

e. Clique em **Enviar**.
Sua nova instância de integração é exibida na lista Instâncias de integração.

f. Repita as etapas 1 a 3 para configurar sua instância de integração e testar suas credenciais.

5. Configure aprovações para solicitações de patch.
Por padrão, uma propriedade do sistema [**sn_vul_patch_orch.patch_approval_required**] é ativada para que, quando as implantações de patch forem programadas, elas sejam enviadas para revisão e aprovação para usuários atribuídos ao nível 1 - grupo de aprovação de atualização de patch.

Se você quiser que os usuários com a função sn_vul_patch_orch.configure_patch programem patches sem aprovação, desative a propriedade [**sn_vul_patch_orch.patch_approval_required**]. Você pode preferir deixar as aprovações ativadas para que os patches programados não entrem em conflito com o horário normal de trabalho.

Nota:
Se você desativar a propriedade do sistema de aprovação, qualquer usuário com a função sn_vul_patch_orch.configure_patch poderá programar e implantar patches sem revisão e aprovação.

Como um usuário com a função sn_vul.vulnerability_admin, para desativar a propriedade do sistema:

a. Navegar até **Todos** > **sys.properties.list**.

b. Localize **sn_vul_patch_orch.patch_approval_required** e clique nele para abrir o registro.

c. No campo Valor, digite `false`.

d. Clique em **Atualizar**.

6. Se você não desativar esta propriedade, será necessário atribuir aprovadores para solicitações de patch.
Como um usuário com a função sn_vul.vulnerability_admin, siga estas etapas.

a. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de aprovação**.

b. Se a Regra de **aprovação Implantar aprovação de atualização de patch** não for exibida na lista, clique em **Todos** à direita do ícone de filtro verde no canto superior esquerdo da tela para exibir a lista inteira.

c. Na lista, clique em **Implantar aprovação de atualização de patch**.

d. No registro, com a guia Configuração de aprovação selecionada, clique em **Configuração padrão Aprovação de atualização de patch**.

e. No registro, clique em **Nível 1 - Aprovação de atualização de patch**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

f. Adicione usuários a este grupo.

Os usuários atribuídos a este grupo aprovam as solicitações de patch enviadas por usuários com a função sn_vul_patch_orch.configure_patch. Navegue até **Minhas aprovações** para exibir e processar as solicitações.

7. Clique em**Atualizar** para salvar suas mudanças.

8. Opcional: Você pode configurar aprovações em vários níveis para que mais de uma aprovação seja necessária antes da implantação de solicitações de patch programadas.

a. Com o registro de aprovação da atualização de patch de configuração padrão exibido, clique em **Novo**.

b. Preencha os campos.

Campo	Descrição
Nome	Nome do nível de aprovação, por exemplo, **Nível 2 – Aprovação de atualização de patch**.
Ativo	Ativado por padrão, o que significa que o nível de aprovação está em uso.
Aprovação obrigatória	Selecione quantas aprovações são necessárias para o nível selecionado: ▪ Um aprovador necessário ▪ Todos os usuários devem aprovar
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Função	Selecione uma função para o grupo na lista.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Configuração de aprovação	Contém as configurações de aprovação.
Atribuir usando	Selecione uma opção: ▪ Usuário e grupo de usuários ▪ Campo da tabela de aprovação ▪ Script
Grupos	Grupo de nível de aprovador que consiste em vários usuários. O usuário deve ter uma das seguintes funções que você especificar.
Usuários	Edite os usuários listados nos grupos.

c. Clique em **Enviar** para salvar suas edições.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de dados de patch e acúmulo de dados de patch para a integração do Patch Orchestration [Vulnerability Response com Microsoft SCCM

Os dados de patch e os dados de rollup de patch, bem como as informações de vulnerabilidade e o status de correção de suas vulnerabilidades são exibidos em registros em sua instância.

Exibição de dados de patch nos espaços Vulnerability Response

Funções necessárias:

- Função sn_vul_patch_orch.configure_patch para configurar e programar patches
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para o IT Remediation and Vulnerability Manager Workspaces

No Espaço de correção de TI, você pode exibir os patches:

- Na exibição inicial, é possível clicar nos cartões de pontuação para exibir registros de soluções preferenciais em IVs, ICs vulneráveis e patches preferenciais em IVs.
- Na exibição de lista, é possível exibir todos os registros de atualização de patch (VPUs) dos links de patches e os itens vulneráveis (VITs) atribuídos a você que têm patches.

Você pode programar patches dos seguintes registros:

- Da atualização de patch (VPU)
- Tarefa de correção (RT)
- Registros de item descoberto (SDI)

No Vulnerability Manager Workspace, você pode exibir os patches:

- Na exibição inicial dos tópicos de observação, é possível exibir os patches preferenciais e potenciais, as datas programadas do patch e se todos os patches foram baixados na guia **Itens vulneráveis**.
- Na exibição de lista nos esforços de correção, onde você pode exibir dados de patch em registros de IV na guia**Itens vulneráveis**.

Na exibição clássica do ambiente, navegue até **Todos** > **Vulnerability Response** > **Patches**.

Registros de atualização de patch nos espaços de VR e na exibição do ambiente clássico

Os dados de patch e os dados e status de rollup de patch são exibidos nos registros em sua instância. Os registros de patch são incluídos como parte do recurso de orquestração de patches desta integração com Vulnerability Response. Exiba registros de patch (VPU) em espaços Vulnerability Response na exibição de lista no espaço de correção de TI. Os registros de atualização de patch no ambiente clássico e nos espaços Vulnerability Response incluem os seguintes dados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Dados de solução de vulnerabilidade e informações de fornecedores de patch importados pela aplicação Vulnerability Solution Management.
- Status de correção de origem que inclui o número total de dispositivos que têm uma determinada vulnerabilidade que pode ser corrigida por um patch. Além disso, ele também inclui e todos os dispositivos que não tenham atualizações.
- Status de correção que inclui % de IVs corrigidos e o total de IVs que têm um patch como preferencial.
- Dispositivos associados, itens vulneráveis, implantações de patch e solicitações de patch nos links relacionados em registros na exibição de classe. Esses dados são exibidos em guias em registros nos espaços Vulnerability Response.
- Solicitações de patch que os responsáveis pela correção enviaram para aprovação.

Acúmulo de estado em registros de item vulnerável

Para obter mais informações sobre acúmulo de estado para registros, consulte Dados de patch e acúmulo de estado para orquestração de patches no Vulnerability Response.

Registros que acumulam contagens de IV ativas

Para evitar o acúmulo de todos os patches para todas as vulnerabilidades, o trabalho programado seleciona somente as mudanças na contagem de IV ativa. Essas mudanças de contagem e dados relacionados são acumulados para os seguintes registros em Vulnerability Response:

- VIT
- RT
- Solução de vulnerabilidade
- Atualização de patch

Exibição de dados de patches sem soluções

Para obter mais informações sobre como exibir patches sem soluções, consulte Exibir patches sem soluções em Vulnerability Response.

Dados de patch no Vulnerability Response

Os painéis do Vulnerability Management (PA) e do CISO estão incluídos com uma assinatura com o Performance Analytics para a aplicação Vulnerability Response. Se você tiver uma assinatura do Performance Analytics, mas não tiver uma integração de orquestração de patches instalada, a guia de correção será exibida no painel do CISO, mas não será preenchida com dados.

Para o painel Vulnerability Management (PA), navegue até **Todos** > **Vulnerability Response** > **Visão geral**. Clique na guia **Correção** e role até a parte inferior da página para exibir os dados de atualizações de patch: patches programados e não programados, patches sem data de destino e contagens semanais.

No Painel do CISO, navegue até **Todos** > **Vulnerability Response** > **Painel do CISO**. Com a guia Visão geral selecionada, role até a parte inferior da página para exibir os dados de cobertura do patch: criticidade, patches programados e não programados e patches sem datas de destino.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre os painéis Vulnerability Response, consulte Usando os painéis padrão Vulnerability Response, Orquestração de patches com os espaços Vulnerability Responsee Exibição de dados de orquestração de patches nos painéis Vulnerability Response.

Programar patches com a integração do SCCM [Microsoft com Vulnerability Response

Programe patches de registros de tarefa de Atualização de Patch e Correção na aplicação Vulnerability Response em sua instância Now Platform.

Antes de Iniciar

A partir da versão 16.1, você pode programar patches nos Espaços Vulnerability Response ou no ambiente clássico.

Funções necessárias:

- Função sn_vul_patch_orch.configure_patch para configurar e programar patches
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para o IT Remediation and Vulnerability Manager Workspaces

Procedimento

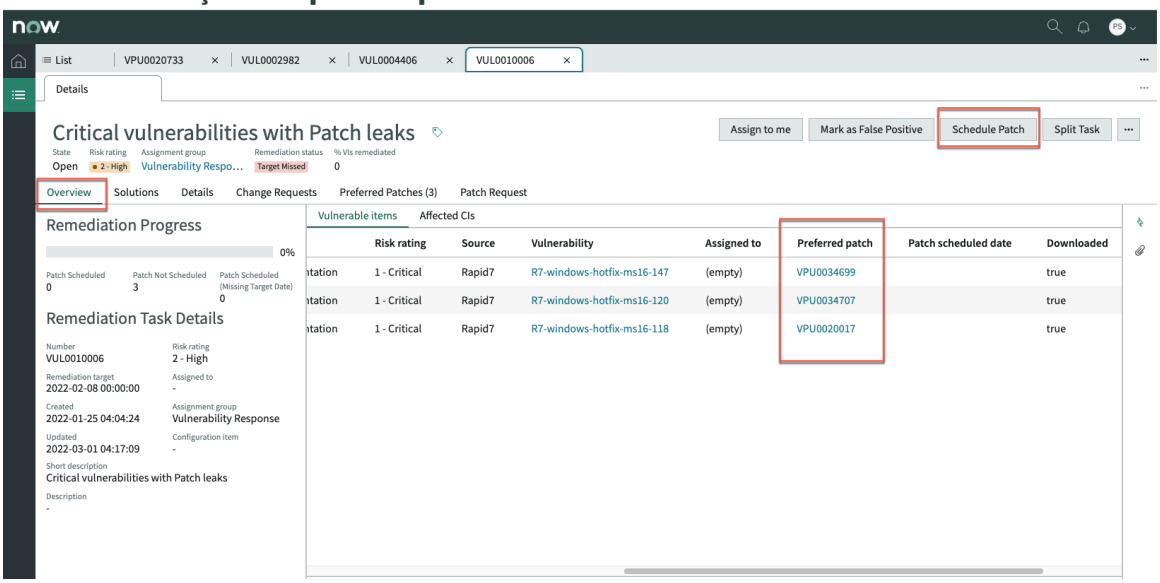
1. Nos espaços de vulnerabilidade Vulnerability Response, como um usuário com a função sn_vul.remediation_owner, navegue até **Todos** > **Vulnerability Response** > **Espaço de correção de TI**.
2. Na página inicial, clique **em Patch preferencial em IVs**.
   A lista de registros de atualização de patch para os IVs com patches preferenciais atribuídos a você é exibida.
3. Localize um registro que você deseja abrir e clique para abri-lo.
4. Como alternativa, na exibição de lista no espaço de trabalho, clique em **Patches** > **Todos** e localize um registro de atualização de patch.
   O registro de atualização de patch é exibido. Talvez você prefira revisar os dados antes de programar um patch, pois pode haver outros patches já programados.
5. Consulte a tabela a seguir sobre os dados exibidos no espaço de correção de TI e o que você pode fazer.
6. Clique **em Programar patch**.
7. Na caixa de diálogo, preencha os campos.
8. Clique em **Implantar**.
   A solicitação de patch é enviada para para revisão. Você pode exibir o status de todas as solicitações enviadas de **Solicitações de exceção** > **Minhas solicitações** na exibição de lista.
9. Como alternativa, você pode programar patches de tarefas de correção (RT) que são atribuídas a você ou ao seu grupo.

Nota:
A opção de programar um patch de um registro de tarefa de correção está disponível somente se houver patches mapeados para (associados aos) IVs na tarefa. Esses patches serão exibidos na coluna Patch preferencial se você rolar para a direita de um registro de tarefa de correção com a guia Visão geral selecionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa de correção com patches preferenciais



10. Clique em **Programar patch** no registro RT e siga as etapas listadas acima para programá-lo na caixa de diálogo.
11. **Opcional:** Você pode programar patches para as etapas anteriores no ambiente clássico. Para localizar esses registros, siga estas etapas.

    a. No ambiente clássico, navegue até **Todos** > **Vulnerability Response** > **Patches** > **Todos**.

    b. Na lista exibida, localize um registro de atualização de patch.

    c. Para tarefas de correção, navegue até **Vulnerability Response** > **Tarefas de correção** e localize um registro.
    O rastreia o status da correção na guia Status da correção. Na parte inferior do registro, os dados do patch são exibidos nos Links relacionados.

    d. Clique em **Programar patch** e preencha os campos.

Campo	Descrição
Nome da implantação	Insira um nome para esta implantação de patch. Este nome ajuda a rastrear suas atualizações.
Descrição	Adicione mais texto para sobre o patch. Essas informações são exibidas no campo Descrição do registro de Atualização de Patch.
Tipo de implantação	Escolha uma opção na lista. ▪ Obrigatório: este patch é uma atualização necessária. ▪ Disponível - este patch não é necessário, mas está disponível para implantação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Coleção	Escolha uma coleção (grupo de ativos) na lista para continuar. Esses grupos são as coleções de ativos importadas do SCCM.
Tempo de implantação com base em	Selecione um fuso horário na lista para basear sua janela de tempo de implantação.
Tempo disponível	Defina o valor para a hora em que o patch se torna disponível para implantação.
Vencimento	Defina o prazo. Este valor indica o último dia em que o patch pode ser instalado.

e. Clique em **Implantar**.

Mensagens REST para a Orquestração de patches [Vulnerability Response com Microsoft SCCM

O Vulnerability Response Patch Orchestration com Microsoft SCCM usa as classes SCCM Windows Management Instrumentation (WMI) para fazer chamadas para a API do SCCM Server.

Visão geral

O Provedor de SMS fornece à API um acesso de interoperabilidade por HTTPS, chamado de serviço de administração. O serviço de administração é uma API de transferência de estado representacional (REST) baseada no protocolo Open Data (OData) v4.

Consulte O que é o serviço de administração no Configuration Manager para obter mais informações sobre o uso do serviço de administração com esta integração.

Como a autenticação necessária usa o protocolo Windows New Technology LAN Manager NTLM, as chamadas para as APIs são feitas por meio do MID Server usando scripts do PowerShell.

Microsoft Integração SCCM

Você pode usar a mensagem REST para a integração do Microsoft SCCM para recuperar informações do Microsoft SCCM. As mudanças no método de registro da mensagem REST afetam as solicitações feitas ao Microsoft SCCM para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Nomes de classe WMI:

- Coleção_SMS
- Resumo_de_implantação de SMS

Nome do parâmetro	Valor	Descrição
url	Valores dinâmicos com base no usuário	Indica o endpoint do Console do SCCM

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Microsoft Patch de implantação do SCCM

Você pode usar a mensagem REST para a integração do Microsoft SCCM para programar patches do seu Now Platform® para o Microsoft SCCM. As mudanças no método de registro da mensagem REST afetam as solicitações feitas ao SCCM para recuperar informações. As mensagens REST contêm os seguintes métodos REST.

Método REST	Descrição
Patch de implantação POST	Programa o patch para o console do SCCM em um ou vários computadores.

Nome do parâmetro	Valor	Descrição
url	Valores dinâmicos com base no usuário	Indica o endpoint do Console do SCCM.
título	Valores dinâmicos com base no usuário	Título da implantação.
configurações_tag	Configurações de nome de marcador XML com valores	Indica configurações que têm parâmetros diferentes e são enviadas para o SCCM ao programar o patch.
computer_tag	Computadores nomeados com marcador XML com valores	Indica a lista de computadores nos quais o patch será programado.
site_name	Valor da atualização do patch	Nome do site onde o Patch está presente.
Patch_id	Valor da atualização do patch	ID do patch.

Transformação de dados para a Orquestração de patches com a integração do SCCM Microsoft

Os dados são recuperados da Orquestração de patches com integração do Microsoft SCCM, processados por meio de um conjunto de fontes de dados e transformados em sua instância Now Platform®.

Importação de coleção do SCCM

Os dados das coleções importadas são carregados na tabela Importação de coleção do SCCM [sn_vul_sccm_collection_import]. As Coleções SCCM (mapa de transformação) são usadas para transformar as informações importadas.

Nota:
As mudanças neste mapa de transformação alteram a forma como os dados da importação da Coleção SCCM são processados.

Para acessar este mapa de transformação, navegue até **Todos** > **Conjuntos de importação do sistema** > **Mapas de transformação** e localize Transformação de coleção do SCCM. A tabela a seguir lista os campos do mapa de transformação por integração.

Campo de origem	Campo de destino	Descrição
u_collectionid	source_id	ID exclusivo da coleção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_name	nome	Nome da coleção.
u_membercount	device_count	Número de dispositivos nesta coleção.
[script]	integration_instance	Nome da instância da qual o patch é importado.

Tempo do script do mapa de transformação de importação da coleção do SCCM

Script	Descrição
OnStart (quando um conjunto de importação criou uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto de importação concluir a transformação).	O script usado para atualizar os valores na variável de escopo [sn_vul_sccm]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de atualização de patch do SCCM

Os dados dos patches importados são carregados na tabela Importação de atualização de patch do SCCM [sn_vul_sccm_patch_update_import].

A transformação de atualização do patch do SCCM é usada para transformar as informações importadas.

Nota:
As mudanças neste mapa de transformação alteram como os dados da importação de atualização do patch do SCCM são processados.

Para acessar este mapa de transformação, navegue até **Todos** > **Conjuntos de importação do sistema** > **Mapas de transformação** e localize a transformação de atualização do patch do SCCM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Campos do mapa de transformação de importação de atualização de patch do SCCM

Campo de origem	Campo de destino	Descrição
[Script]	urls	URLs do Patch.
u_numfalta	num_missing	Número de dispositivos sem este patch.
[Script]	data_versão	Data de lançamento do patch.
u_bulletinid	ID_do_boletim	ID do boletim para o patch.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de importação de atualização de patch do SCCM

Campo de origem	Campo de destino	Descrição
u_numtotal	num_total	Número total de dispositivos.
u_localizeddescription	descrição	Descrição do patch.
[Script]	is_highest_supersedence	É o Patch com a maior substituição.
u_numnãoaplicável	num_not_applicable	Número de dispositivos não aplicáveis a este Patch.
u_iscontentprovisioned	is_downloaded	Se o Patch for baixado para o SCCM Server.
u_num desconhecido	número_desconhecido	Número total de dispositivos desconhecidos.
u_articleid	artigo_id	ID do artigo do patch.
u_localizeddisplayname	título	Título do patch.
u_ci_id	source_id	ID exclusivo do patch no SCCM.
u_numpresent	num_present	Número de dispositivos em que o Patch está instalado.
[Script]	integration_instance	Nome da instância da qual o patch é importado.
[Script]	sn_vul_solution	Solução baseada no ID de origem.
[Script]	last_modified	Data da última modificação do patch.
u_severidade	source_severity	Severidade do Patch.

Tempo do script do mapa de transformação de importação de patch do SCCM

Script	Descrição
OnStart (quando um conjunto de importação criou uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto de importação concluir a transformação).	O script usado para atualizar os valores na variável de escopo [sn_vul_sccm]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importação de atualização de patch do dispositivo SCCM

Os dados dos patches relevantes importados nos dispositivos são carregados na tabela Importação de atualização de patch do dispositivo SCCM [sn_vul_sccm_device_patch_import].

A transformação de atualização de patch do dispositivo SCCM é usada para transformar as informações importadas.

Nota:
As mudanças neste mapa de transformação alteram como os dados da importação de atualização de patch do dispositivo SCCM são processados.

Para acessar este mapa de transformação, navegue até **Todos** > **Conjuntos de importação do sistema** > **Mapas de transformação** e localize a transformação de atualização de patch do dispositivo SCCM.

A tabela a seguir lista os campos do mapa de transformação por integração.

Tempo do script do mapa de transformação da atualização do patch do dispositivo SCCM

Script	Descrição
OnStart (quando um conjunto de importação criou uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto de importação concluir a transformação).	Script usado para criar e atualizar ICs com base em regras de pesquisa de IC e patches, bem como o relacionamento entre eles. Com base nos resultados, este script modifica os valores na variável de escopo [sn_vul_sccm]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Importação de coleção de dispositivos do SCCM

Os dados das coleções de dispositivos importados são carregados na tabela Importação de coleção de dispositivos SCCM [sn_vul_sccm_device_collection_import].

A transformação de importação da coleção de dispositivos SCCM é usada para transformar as informações importadas.

Nota:
As mudanças neste mapa de transformação alteram como os dados da importação de coleção de dispositivos SCCM são processados.

Para acessar este mapa de transformação, navegue até **Todos** > **Conjuntos de importação do sistema** > **Mapas de transformação** e localize a transformação da coleção de dispositivos SCCM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A tabela a seguir lista os campos do mapa de transformação por integração.

Tempo do script do mapa de transformação de importação da coleção de dispositivos

Script	Descrição
OnStart (quando um conjunto de importação criou uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.
onBefore (antes de um conjunto de importação concluir a transformação).	O script usado para criar e atualizar ICs com base nas Regras de pesquisa de IC e nas coleções, bem como no relacionamento entre elas. Com base nos resultados, este script modifica valores na variável de escopo [sn_vul_sccm]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Campos do mapa de transformação de importação da coleção de dispositivos do SCCM

Campo de origem	Campo de destino	Descrição
u_id	source_id	ID exclusivo de uma ação.
U_name	nome	Nome da ação
[Script]	Sn_vul_sccm_discovered_item	Referência do item descoberto no qual o patch está implantado
U_status	status	Status da ação
[Script]	Sn_vul_patch_orch_update	Referência do patch
U_apply_count	Contagem_success	Contagem de sucesso da ação.
U_retry_count	tentar novamente	Contagem de novas tentativas da ação.
[Script]	Deployment_time	Hora de início da ação.
[Script]	prazo	Hora de término da ação.
[Script]	Origem_criada	Hora de criação da ação.
[Script]	Integration_instance	Nome da instância da qual a ação é importada.

Importação de implantação do SCCM

Os dados das implantações importadas são carregados na tabela Importação de implantação do SCCM [sn_vul_sccm_deployment_import].

A transformação de importação de implantação do SCCM é usada para transformar as informações importadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
As mudanças neste mapa de transformação alteram como os dados da importação de implantação do SCCM são processados.

Para acessar este mapa de transformação, navegue até **Todos** > **Conjuntos de importação do sistema** > **Mapas de transformação** e localize a Transformação de implantação do SCCM.

Campos do mapa de transformação de implantação do SCCM

Campo de origem	Campo de destino	Descrição
u_id	source_id	ID exclusivo de uma implantação.
u_name	nome	Nome da implantação.
[Script]	prazo	Hora do prazo para a implantação.
u_numberem andamento	count_progress	Contagem de dispositivos em andamento para a implantação.
[Script]	deployment_time	Hora de início da implantação.
[Script]	integration_instance	Nome da instância da qual a implantação é importada.
[Script]	source_created	Hora de criação da implantação.
[Script]	sn_vul_patch_orch_update	Referência do Patch
[Script]	sn_vul_patch_orch_collection	Referência do item descoberto em que o patch está implantado.
u_softwarename	nome	Nome da implantação.
u_numberoutro	contagem_outros	Outra contagem de dispositivos para a implantação.
u_numberunknown	contagem_desconhecida	Contagem de estados desconhecidos de dispositivos para a implantação.
u_deploymentid	source_id	Identificador exclusivo da implantação.
u_numbersuccess	count_success	Contagem de sucesso de dispositivos para a implantação.
u_numbererrors	erro_contagem	Contagem de erros de dispositivos para a implantação.
u_numbertargeted	contagem_total	Contagem total de dispositivos para a implantação.

Tempo do script do mapa de transformação de importação da implantação do SCCM

Script	Descrição
OnStart (quando um conjunto de importação criou uma transformação).	Script usado para inicializar os valores na variável de escopo [sn_vul_sccm] para o processo de integração. Este script é para uso interno e não deve ser modificado ou excluído.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tempo do script do mapa de transformação de importação da implantação do SCCM

Script	Descrição
onBefore (antes de um conjunto de importação concluir a transformação).	O script usado para atualizar os valores na variável de escopo [sn_vul_sccm]. Este script é para uso interno e não deve ser modificado ou excluído.
onComplete (quando um conjunto de importação concluiu a transformação).	Script usado para definir o número de itens criados, atualizados e ignorados. Este script é para uso interno e não deve ser modificado ou excluído.

Exemplo de fluxo de trabalho para a integração do Patch Orchestration [Vulnerability Response com o Microsoft SCCM

Um exemplo de como a orquestração de patches funciona com o Microsoft SCCM.

Antes de Iniciar

Digamos, por exemplo, que todo o seu ambiente seja corrigido uma vez a cada três semanas. A janela de patch mais recente foi concluída há uma semana, mas você deseja aplicar um patch para corrigir uma vulnerabilidade crítica que se tornou conhecida recentemente. Devido à natureza crítica desta vulnerabilidade, você não pode esperar mais duas semanas pelo próximo patch programado.

Funções necessárias:

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin para o Vulnerability Manager Workspace.
- sn_vul.remediation_owner para exibir o espaço do proprietário de correção de TI.
- Função sn_vul_patch_orch.configure_patch para configurar e programar patches.
- sn_vul_patch_orch.read_patch para exibir (somente leitura) informações de patch nos registros. Esta função é herdada com as funções sn_vul.remediation_owner e sn_vuln.vulnerability_analyst que são necessárias para o IT Remediation e Vulnerability Manager Workspaces.

Por Que e Quando Desempenhar Esta Tarefa

Como gerente de vulnerabilidade ou analista que trabalha no Vulnerability Manager Workspace, você pode considerar a criação de tópicos de observação ou a edição de tópicos de observação existentes para ajudá-lo a capturar IVs importados com vulnerabilidades críticas. Com a integração de orquestração de patches, você também pode ver os patches que deseja usar para corrigir e rastrear essas vulnerabilidades. A tabela a seguir lista alguns exemplos com as condições que você pode definir para tópicos de observação para orquestração de patches. Use esses exemplos para ajudá-lo a determinar as configurações que funcionam melhor para o seu ambiente. Consulte Criar um tópico de observação no Vulnerability Manager Workspace para obter mais informações sobre como configurar o tópico de observação.

Amostra de tópicos de observação para orquestração de patches no Vulnerability Manager Workspace

Nome do tópico de observação	Descrição
Vulnerabilidades críticas com vazamentos de patch	A classificação de risco é 1 - crítico E

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Amostra de tópicos de observação para orquestração de patches no Vulnerability Manager Workspace

Nome do tópico de observação	Descrição
	O motivo é o patch não programado
Vulnerabilidades críticas com patches programados (ANS ausente)	O motivo é patch programado (data de destino ausente)
Vulnerabilidades críticas com patches programados	A classificação de risco é 1 - crítico E A data programada do patch não está vazia E O motivo é Patch programado

- Como gerente ou analista de vulnerabilidade, depois de criar os tópicos de observação e os esforços de correção, você gera tarefas de correção. Em registros de IV e tarefas de correção, você pode fazer uma busca detalhada na guia Detecções e localizar registros de itens descobertos que têm a vulnerabilidade que você está rastreando, junto com os ativos importados pelo produto SCCM.
- Como analista de vulnerabilidade ou administrador, você pode monitorar os dados de patch associados à vulnerabilidade. Você também pode implantar um patch ou vários patches em um ativo específico (item de configuração) de um registro de item descoberto.

Como especialista em correção de TI, você tem opções de como lidar com a vulnerabilidade com uma implantação de patch.

- Você pode programar o patch a partir de um registro de atualização de patch (VPU#).
- Se os itens vulneráveis (IV) tiverem soluções preferenciais mapeadas para eles e forem atribuídos a você ou aos seus grupos, você poderá programar os patches de uma tarefa de correção que tenha esses itens vulneráveis.

Procedimento

1. Como Especialista em correção de TI, no Espaço de correção de TI, clique na exibição inicial.
2. Na exibição inicial, clique no cartão de pontuação **Tarefas de correção atribuídas** para exibir os registros.

   Para fins deste exemplo, você pode verificar o campo Descrição resumida na tarefa de correção (VUL#) para qualquer texto relacionado à sua vulnerabilidade crítica. Digamos, por exemplo, que você saiba que seu gerenciador de vulnerabilidades criou um tópico de observação chamado Vulnerabilidades críticas com vazamentos de patch para capturar IVs (VIT#) com esta vulnerabilidade crítica.

   Com o registro aberto, você também pode revisar os IVs, os patches preferenciais e ver se você ou alguém do seu grupo já enviou solicitações de patch para aprovação.
3. Se você tiver informações suficientes, talvez prefira enviar uma solicitação de patch agora a partir desta tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Se os IVs associados ao registro não tiverem patches mapeados para eles, o botão **Programar patch** não estará disponível no registro.

4. Clique em **Programar patch** e preencha os campos na caixa de diálogo.
   Para obter mais informações sobre como programar um patch, consulte Programar patches com a integração do SCCM [Microsoft com Vulnerability Response.
5. Como alternativa, na exibição de lista no Espaço de correção de TI, você pode clicar nos links Tarefas de correção, Itens vulneráveis, Soluções e Patches para exibir esses registros.
   No caso deste exemplo, em vez de um nome de tópico de observação, você pode saber o ID do artigo ou o ID do boletim e o título do patch. Em caso afirmativo, convém verificar se algum dos IVs com esta vulnerabilidade está atribuído a você ou aos seus grupos. Em registros de atualização de patch, você pode enviar solicitações de patch. Em registros de IV, você pode verificar possíveis patches e abrir a tarefa de correção associada se quiser enviar uma solicitação de patch.
6. Se você não tiver acesso aos espaços ou se preferir exibir dados e programar patches no ambiente clássico, siga estas etapas.

   a. Navegar até **Vulnerability Response** > **Patches** > **Todos**.

   b. Localize o registro de atualização de patch desejado.
   Você pode preferir filtrar os registros com pontuações de risco crítico.

   c. Revise os campos de IVs associados e % de IVs corrigidos na guia Status de correção.
   Se os IVs tiverem patches disponíveis, o botão **Programar patch** será exibido no canto superior direito do registro.

   d. Se você decidir enviar uma solicitação, clique em **Programar patch**.
   Para obter mais informações sobre como programar um patch, consulte Programar patches com a integração do SCCM [Microsoft com Vulnerability Response.

   e. Como alternativa, digamos que você não tenha as informações do ID do patch, mas verifique o campo Descrição resumida nas tarefas de correção atribuídas ao seu grupo para qualquer texto relacionado à sua vulnerabilidade crítica.

   f. Navegar até **Vulnerability Response** > **Tarefas de correção** > **Atribuído aos Meus grupos**.

   g. Localize o registro desejado e clique nele para abri-lo.
   No registro aberto, revise a guia Status de correção para IVs e % de IVs corrigidos. Clique nos Links relacionados para registros IV, Soluções preferenciais, Patches preferenciais e Solicitações de patch.

   Nota:
   Se os IVs associados ao registro não tiverem patches mapeados para eles, o botão **Programar patch** não estará disponível no registro.

   h. Clique em **Programar patch** no registro se quiser enviar uma solicitação de patch.

Noções básicas sobre o Qualys Vulnerability Integration

Os sensores do produto Qualys coletam os dados e os enviam automaticamente para a aplicação Qualys, que analisa e correlaciona continuamente as informações. Ele se integra facilmente com Vulnerability Response como o Qualys Vulnerability Integration para mapear

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidades para ICs e serviços de negócios para determinar o impacto e a prioridade de ameaças potencialmente mal-intencionadas.

Configure seu Qualys Vulnerability Integration usando **Vulnerabilidade** > **Administração** > **Assistente de configuração** para tornar a recuperação de dados mais flexível e escalonável.

Se você tiver várias implantações da aplicação Qualys Cloud Platform, poderá adicionar uma integração para cada implantação. Os ativos, identificados por várias implantações de terceiros e suas vulnerabilidades, são consolidados e reconciliados com o seu CMDB. Essa consolidação acontece mesmo quando os processos de verificação se sobrepõem entre as várias implantações. Os dados provenientes de cada implantação são identificados e disponíveis em uma única instância de Vulnerability Response. Qualys Vulnerability Integration Os registros da Base de conhecimento são normalizados entre implantações, garantindo que as instâncias da mesma vulnerabilidade em implantações sejam tratadas como a mesma vulnerabilidade.

Nota:
Você não pode excluir a integração de vulnerabilidade original, mas pode desabilitá-la. As integrações criadas a partir de modelos desabilitados são desabilitadas por padrão.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Nota:
Embora o Qualys Vulnerability Integration crie integrações para Lista de dispositivos, Grupo de ativos, Lista de pesquisa dinâmica e Lista de pesquisa estática, eles não são necessários para a operação normal.

Versões disponíveis

Versão de lançamento para Washington DC	Notas de versão
Qualys Vulnerability Integration v12.7, v12.8	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Componentes instalados

Para obter uma lista atual das funções, trabalhos de integração e tabelas instaladas com a integração, bem como um link para instruções sobre como exibir o que está instalado na sua instância, consulte Componentes instalados com o Qualys Vulnerability Integration.

Integrações primárias e de suporte

Qualys As integrações primárias e de suporte enriquecem os dados de vulnerabilidade em sua instância recuperando dados da integração de vulnerabilidade da Qualys. Uma série de trabalhos programados invoca as integrações automaticamente. Você também pode executá-los manualmente. Os trabalhos programados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades. As integrações primárias e de suporte podem ser modificadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As Qualys integrações são executadas como trabalhos programados. Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Este valor não deve ser alterado.

Nota:
Falha ao definir um usuário executar como válido resulta em vários anexos de recuperação de dados, geralmente duplicados, nos registros de fonte de dados, sempre que a integração é executada. Vários anexos na fonte de dados aumentam o tempo de processamento, resultando em resultados de transformação inconsistentes.

Durante a importação, os registros CVE, ainda não presentes, são criados como registros NVD e referenciados em entradas de terceiros para Qualys por padrão.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Integrações primárias

Uma integração primária é um ponto de entrada para o Qualys Cloud Platform interagindo com a API Qualys invocada em uma programação.

Exiba as integrações primárias navegando até **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.

Integrações de suporte

Uma integração de suporte é um processo que não deve ser executado em uma programação nem sem invocação por uma integração primária.

Exiba as integrações de suporte navegando até **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações de Suporte**.

Conector do Service Graph para Qualys

A partir da versão 2.2, o Conector do Service Graph para Qualys está disponível no ServiceNow® Store. Para obter mais informações, consulte Service Graph Connector for Qualys .

Os dados dos campos de fonte de dados da Qualys são importados com a API Ativo global e a API Gestão e marcação de ativos.

API de ativos globais:

- É necessária uma licença do CSAM.
- As informações de ativos incluem detalhes como Categoria de hardware e Categoria de SO.

API de marcação e gestão de ativos:

- Não é necessária uma licença de CSAM
- As informações de ativos não incluem detalhes sobre Categoria de hardware e Categoria de SO.

Para obter mais informações, consulte Service Graph Connector for Qualys APIs

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

.

Criar ICs usando o Mecanismo de Identificação e Reconciliação (IRE)

Você pode usar o Mecanismo de Identificação e Reconciliação para criar novos ICs quando um IC existente não puder ser correspondido com um host importado de um scanner de terceiros. Habilite o plug-in CMDB CI Class Models para criar ICs usando as novas classes, caso contrário, ICs incompatíveis serão criados nas classes de IC incompatíveis. Para obter mais informações, consulte Criando ICs para Vulnerability Response usando o mecanismo de Identificação e Reconciliação. Para obter mais informações sobre como configurar a categorização de recursos de nuvem incompatíveis em sua classe de IC preferencial, consulte Atualizando classe de IC para ativos de nuvem incompatíveis.

Listas de pesquisa

As listas de pesquisa são usadas em Qualys para criar grupos personalizados de vulnerabilidades. Você pode salvá-los e usá-los para criação de tíquetes e para personalizar verificações e relatórios de vulnerabilidades. O módulo Listas de pesquisa permite que você baixe os dados da lista de pesquisa do Qualys para sua instância de forma programada.

As listas de pesquisa são extraídas de Qualys usando os mapas de transformação de dados Importação de lista de pesquisa dinâmica e/ou Importação de lista de pesquisa estática. Em cada uma dessas transformações, você pode definir programações para executar a importação.

Perfis de opção

Perfis de opção estão disponíveis com Qualys configurações de verificação. Um perfil de opção é necessário ao iniciar uma verificação do Now Platform.

Os perfis de opção são importados do produto Qualys pela Integração da lista de perfis de opção. Você pode preferir executar a integração da lista de perfis de opção após uma importação das integrações de listas de pesquisa, Qualys lista de pesquisa dinâmica e Qualys integrações de lista de pesquisa estática para que você possa ver quais listas de pesquisa estão associadas aos perfis de opção.

Grupos de ativos

Os grupos de ativos são configurados na plataforma Qualys. Os grupos de ativos identificam quais dispositivos de scanner são usados para verificar endereços IP correspondentes quando uma verificação é iniciada do Now Platform.

Os grupos de ativos que têm dispositivos associados são extraídos de Qualys pela Integração da lista de grupos de ativos.

Inicie a integração da lista de dispositivos depois de importar grupos de ativos para preencher os campos Nome do dispositivo e Status do dispositivo nos registros de Aplicações padrão Qualys na Now Platform.

Marcadores de host

Todos os marcadores de host são importados como parte da integração da lista de hosts Qualys. Os marcadores de host são usados principalmente para filtragem em Vulnerability Response Regras de Grupo de Atribuição e Vulnerabilidade. Eles são exibidos no formulário Item descoberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A integração da lista de hosts Qualys deve ser executada antes de criar Regras de atribuição ou de tarefa de correção em Vulnerability Response para que todos os marcadores possam estar presentes nas regras e antes que os itens vulneráveis sejam importados e agrupados.

- O armazenamento de marcador não faz distinção entre maiúsculas e minúsculas. Se um marcador **San Diego** for criado, um marcador **SAN DIEGO** não poderá ser armazenado na tabela de marcadores do host. "San Diego" e "SAN DIEGO" são considerados o mesmo marcador de host. Qualquer marcador que tenha sido importado primeiro vencerá.
- Usar marcadores de host como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. Os marcadores de host devem ser usados somente no Construtor de condição.
- Os marcadores de host são controlados pela propriedade do sistema global **sn_vul.import_host_tags**. Esta propriedade é definida como verdadeira por padrão. Desativar os marcadores os desativa em todas as instâncias.

Marcadores de host (também chamados de marcadores de ativo) são usados para organizar e rastrear os ativos em sua organização. Você pode atribuir marcadores aos ativos de host. Em seguida, ao iniciar as verificações, você pode selecionar marcadores associados aos hosts que deseja verificar. O módulo Marcadores de host permite que você baixe dados de marcador de host de Qualys para sua instância de forma programada.

Reabrir itens vulneráveis resolvidos não encerrados por verificações

Itens vulneráveis definidos como "Resolvidos" em sua instância Now Platform, mas não transicionados para "Encerrado/Corrigido" pelas execuções de integração de terceiros serão reabertos se forem detectados durante novas verificações.

Para Qualys detecções, se o scanner continuar a encontrar IVs que foram definidos como "Resolvido", mas não transicionados para "Encerrado/Corrigido" pelas verificações subsequentes, esses IVs retornam para "Aberto" quando a última data encontrada for posterior a Data de resolução.

Limitações de recuperação de dados

Por padrão, não há restrições sobre como os dados são recuperados de Qualys. Muitos registros podem estar relacionados a vulnerabilidades de baixa severidade que um cliente não está disposto a corrigir usando seu processo de resposta de vulnerabilidade. Atualizar os parâmetros de mensagem/método REST correspondentes pode modificar esse comportamento.

A mensagem/método REST responsável por esta atualização é **Qualys Host Detection – Standard/post**. Para atualizar os valores, adicione um novo parâmetro de consulta HTTP ao método post com os seguintes valores:

- Nome: severities
- Valor: 3-5 (ou quaisquer gravidades apropriadas desejadas)

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Mensagens REST da Qualys

Preparando para o Qualys Vulnerability Integration

Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração. É essencial que você se prepare para a integração executando estes procedimentos. O Qualys Vulnerability Integration pressupõe que você esteja familiarizado com e execute verificações da plataforma de nuvem Qualys em seu ambiente.

Nota:
Faça as mudanças de configuração necessárias com base em seus requisitos antes de executar as integrações.

Pré-requisitos importantes

Valide o dimensionamento da instância com base no número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a longos tempos de carregamento. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente.

Use a filtragem para limitar o número de itens para importação inicial e fasear sua implantação ajustando os filtros nas importações subsequentes.

Os scanners Qualys são desativados por padrão na aplicação Vulnerability Response. Se você tentar executar uma nova verificação a partir dos itens vulneráveis ou das tarefas de correção que têm essas aplicações como origem, o botão **Verificar novamente** não estará disponível.

Ações a serem tomadas

- Determine uma data de início para integrações de **importação de lista de detecção de host**.

  Considere definir o campo **Hora** de início como algumas horas ou dias no passado. O ideal é escolher a data da última verificação do Qualys. A data de início pode incluir vulnerabilidades descobertas antes de usar a solução de gestão de vulnerabilidades. Defina a hora de início mais antiga usada para o início do ciclo de verificação. Portanto, se demorar uma semana até que todos os hosts sejam verificados, defina este valor como uma semana antes dessa hora.

- Adicione usuários às funções de administrador, sn_vuln.admin e sn_vul_qualys.admin. Para obter mais informações, consulte Atribuir uma função a um usuário .

- Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

- Se você não usar calculadoras de vulnerabilidade, Desabilitar a calculadora de vulnerabilidade padrão se não for usada, além de quaisquer outras que você tenha definido. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é criado ou atualizado e podem afetar o desempenho da importação inicial.
- Durante a importação inicial de registros, determinadas regras de negócios relacionadas à notificação podem fazer com que muitas notificações sejam geradas, afetando o desempenho. Antes da importação inicial, desabilite as regras de negócio.
- Se você quiser usar um scanner diferente do padrão da Qualys, consulte configurar dispositivos scanner.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Tenha o URL do servidor Qualys e as credenciais de autenticação prontos. As credenciais devem fornecer permissões adequadas para recuperar informações de conhecimento, verificação e detecção para uma assinatura da Qualys.
- Se você planeja usar marcadores de host em Vulnerability Response Regras de grupo de atribuição ou vulnerabilidade, certifique-se de que a integração da Lista de hosts Qualys tenha sido executada antes de criar regras.

Instalar o Qualys Vulnerability Integration

Antes de executar o Qualys Vulnerability Integration em sua instância, você deve instalar e configurar a aplicação Qualys Vulnerability Integration. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Função necessária: administrador para baixar e instalar a aplicação

Tarefas de configuração	Descrição
Verifique se a aplicação Vulnerability Response está instalada e ativada.	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Vulnerability Response.
Obtenha direitos para a aplicação Qualys Vulnerability Integration e baixe-os para sua instância Now Platform®.	Se a aplicação ainda não tiver sido baixada em sua instância, consulte .
Prepare-se para a integração.	Consulte Preparando para o Qualys Vulnerability Integration.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração**.

   Após alguns momentos, as aplicações disponíveis para instalação em sua instância serão exibidas.

2. Localize o bloco Qualys Vulnerability Integration e clique em **Instalar**.
3. Siga as instruções do Assistente de configuração.
   Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Vulnerability Response aplicações de terceiros usando o Assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Navegue até **Configuração de integração>Integrações de scanner** no Assistente de configuração para continuar com a configuração.
   Para obter mais informações sobre como complementar os prompts fornecidos no Assistente de configuração, consulte Configurar o Qualys Vulnerability Integration usando o Assistente de configuração.

O que Fazer Depois
Ative os scanners, já que eles estão inativos por padrão na aplicação Vulnerability Response. Para obter mais informações sobre como ativar os scanners Qualys, consulte Ativar os scanners Qualys.

Ativar os scanners Qualys

Você deve ativar os scanners depois de instalar o Qualys Vulnerability Integration porque os scanners são desativados por padrão na aplicação Vulnerability Response.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Se você tentar executar uma nova verificação dos itens vulneráveis ou das tarefas de correção que têm essas aplicações como origem, o botão **Verificar novamente** não estará disponível.

Procedimento
1. Navegar até **Todos** > **Vulnerability Response** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o scanner que você deseja ativar e selecione o registro para abri-lo.
3. Marque a caixa de seleção **Ativo**.
4. Selecione **Atualizar**.
5. O produto que você ativou é exibido no campo **Origem** em um item vulnerável e nos registros de tarefa de correção após a próxima importação, e a **opção Nova verificação** está disponível como uma ação de IU.

Componentes instalados com o Qualys Vulnerability Integration

As funções, os trabalhos de integração e as tabelas a seguir são instalados com o Qualys Vulnerability Integration.

Nota:
A tabela Arquivos da Aplicação lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Exibir listas filtradas de componentes instalados com uma aplicação

Filtre a tabela Arquivos de aplicações para que somente as funções, os trabalhos programados e as tabelas que são instaladas com uma aplicação sejam exibidos. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.
2. Selecione o construtor de condição (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação. Por exemplo, **Aplicação** > **é** > **Vulnerability Response**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No construtor de condição, para adicionar um segundo filtro, selecione **E e**, em seguida, selecione, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função**, **Trabalho programado**ou **Tabela**.
4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
sn_vul_qualys.read	Tem acesso de leitura aos registros Qualys Vulnerability Integration.	
sn_vul_qualys.usuário	Usuário para Qualys Vulnerability Integration. Pode ler e gravar registros	sn_vul_qualys.read
sn_vul_qualys.admin	Administrador paraQualys Vulnerability Integration. Por exemplo, você pode modificar as datas de início da integração e executar algumas definições de configuração avançadas.	• sn_vul_qualys.usuário • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	Pode configurar o Qualys Vulnerability Integration	sn_vul_qualys.admin

Trabalhos de integração instalados

Trabalho de integração	Descrição
Qualys Integração da lista de pesquisa estática	Sincroniza Qualys listas de pesquisa para encontrar entradas vulneráveis. Recupera somente registros do tipo lista estática.
Qualys Integração de detecção de host abrangente	Recupera dados de host e vulnerabilidade de Qualys e os processa em sua instância. Ele coordena as chamadas de mensagem REST para a API de detecção de host. A saída desta integração são itens vulneráveis. Esta integração importa todos os estados da vulnerabilidade: Novo, Corrigido, Ativo e Reaberto. Por padrão, esta integração está inativa e é executada semanalmente. **Nota:** Depois que essa integração é ativada, o trabalho abrangente diário importa somente os estados Novo, Corrigido e Reaberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho de integração	Descrição
Qualys Integração da lista de hosts	Recupera dados de verificação de host autenticados e não autenticados e marcadores de host de Qualys uma vez por semana e os armazena no módulo Itens descobertos em sua instância. Ajuda a identificar ativos que não foram verificados recentemente.
Qualys Integração de detecção de host	Recupera dados de host e vulnerabilidade de Qualys e os processa em sua instância. Ele coordena as chamadas de mensagem REST para a API de detecção da lista de hosts. As saídas desta integração são itens vulneráveis. Qualys marcadores de host são importados nesta integração.
Qualys Integração de tíquete	Recupera Qualys tíquetes e os adiciona à sua instância. Ele coordena as chamadas de mensagem REST para a API da lista de tíquetes. Frequentemente, há menos tíquetes do que Detecções de host, já que as configurações Qualys podem restringir as detecções que resultam em um tíquete.
Qualys Integração da lista de perfis de opção	Recupera perfis de opção do produto Qualys. Os perfis de opção incluem configurações de verificação que são necessárias quando você inicia verificações da sua instância Now Platform.
Qualys Integração da lista de dispositivos	Recupera informações do dispositivo scanner de Qualys.
Qualys Integração de grupo de ativos	Recupera informações do grupo de ativos de Qualys. Os grupos de ativos são usados para identificar quais dispositivos scanner usar para verificar itens de configuração correspondentes.
Qualys Base de conhecimento (preenchimento)	Recupera Qualys entradas da base de conhecimento. Programado para ser executado após a Qualys Integração de detecção de host. Atualiza sua instância com todos os QIDs que foram referenciados na integração de detecção de host, mas não existiam no sistema.
Qualys Base de Conhecimento	Recupera Qualys entradas da base de conhecimento. Os dados recuperados são baseados na data em que as vulnerabilidades foram atualizadas por Qualys e desde a última vez em que a integração foi executada. Esses dados são úteis para preencher dados históricos em sua instância, bem como garantir que os Qualys Identificadores (QIDs) estejam atualizados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho de integração	Descrição
Qualys Integração da lista de pesquisa dinâmica	Sincroniza Qualys listas de pesquisa para encontrar entradas vulneráveis e recupera registros do tipo de lista dinâmica.
Corrigindo as detecções da chave atualizada para Qualys	Uma combinação de hash de campos que fornecia uma maneira de identificar e vincular uma detecção a um Qualys item vulnerável.
Qualys Atualizar itens descobertos existentes com identificador de partição de rede	Atualiza os itens descobertos existentes. Os ICs dos dados de integração de vulnerabilidade Qualys existentes são criados ou atualizados para incluir a granularidade do identificador de partição de rede.

Tabelas instaladas

Tabela	Descrição
Vulnerabilidade da Lista de Pesquisa sn_vul_qualys_m2m_search_list_vul	Armazena o mapeamento entre a lista de pesquisa Qualys e uma vulnerabilidade.
Qualys Scanner de vulnerabilidade sn_vul_qualys_scanner	Tabela que estende os scanners de vulnerabilidade para armazenar informações do scanner para o recurso de nova verificação Qualys.
Qualys Pesquisar Listas sn_vul_qualys_search_list	Armazena listas de pesquisa recuperadas pela integração da lista de pesquisa Qualys.
Qualys Importação de dispositivo sn_vul_qualys_appliance_imp	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo da resposta é processado diretamente com o script onComplete.
Qualys IC sn_vul_qualys_ci	A tabela não é mais usada.
Paginação de Detecção de Host sn_vul_qualys_host_detection_pagination	A tabela não é mais usada.
Qualys Execução de Integração sn_vul_qualys_integration_run	A tabela não é mais usada.
Qualys Integração sn_vul_qualys_integration	Tabela que estende a integração de vulnerabilidade e armazena todas as integrações que correspondem a Qualys.
Qualys Importação de lista de pesquisa estática sn_vul_qualys_static_search_list_imp	Tabela que estende a linha do conjunto de importação. Os mapas de campo são usados para transformar dados na tabela de destino, Qualys Listas de pesquisa.
Qualys Base de Conhecimento sn_vul_qualys_knowledge_base	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
	anexo da resposta é processado diretamente com o script onComplete.
Qualys Lista de tíquetes sn_vul_qualys_ticket_list_imp	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo da resposta é processado diretamente com o script onComplete.
Qualys Perfil de opção sn_vul_qualys_option_profile	Tabela que armazena os perfis de opção recuperados de Qualys. Esta tabela usada com a nova verificação.
Qualys Importação de lista de pesquisa dinâmica sn_vul_qualys_dynamic_search_list_imp	Tabela que estende a linha do conjunto de importação. Os mapas de campo são usados para transformar dados na tabela de destino, Qualys Listas de pesquisa.
Qualys Reexecutar conjunto de importação sn_vul_qualys_import_rerun	A tabela não é mais usada.
Qualys Importação de perfil de opção sn_vul_qualys_option_profile_import	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo da resposta é processado diretamente com o script onComplete.

Atualizar itens de configuração com o identificador de partição de rede para Qualys Vulnerability Integration

Crie itens de configuração (ICs) exclusivos para ativos em seu ambiente que compartilham endereços IP. Identifique os ativos distintos em seu ambiente e atualize automaticamente os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Por padrão, na aplicação Vulnerability Response, uma maneira de identificar seus ativos é por endereço IP. Em determinados casos, os ativos podem compartilhar endereços IP, mas eles são armazenados como um IC no seu CMDB.

Por exemplo, conforme mostrado nas tabelas a seguir, vários ativos (IC) em seu ambiente podem compartilhar endereços IP, mas têm IDs de rede e repositório exclusivos. No entanto, por padrão, esses ativos são normalmente identificados e armazenados como um único IC (IC 1) durante a pesquisa de endereço IP.

Pesquisa de IP padrão e criação de IC

Origem	Endereço IP	NETWORK_Identificador	Item de configuração
Qualys Vulnerability Integration: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1
	123.12.12.141	03713	IC 1

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Origem	Endereço IP	REPOSITÓRIO_ID	Item de configuração
Qualys Vulnerability Integration: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1
	123.12.12.141	13	IC 1

Você pode criar ICs individuais para ativos que têm o mesmo endereço IP para que possa identificá-los como ativos distintos. Iniciando de uma importação de dados recente, você pode atualizar seus ICs existentes com mais granularidade que inclua o identificador de partição de rede [network_partition_identifier] executando o trabalho programado, *`Update existing discovered items with network partition identifier`*.

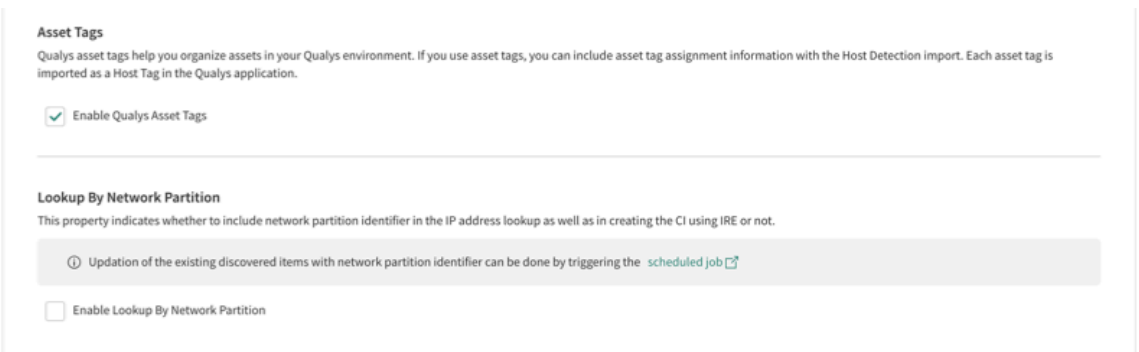
Este trabalho programado está desabilitado por padrão. Ative este recurso para as integrações de ativos e vulnerabilidades fixas e abertas para Qualys Vulnerability Integration no Assistente de configuração para exibir este identificador em seus registros.

Quando ativado, este trabalho programado adiciona o identificador de partição de rede [network_partition_identifier] aos registros de IC existentes a partir de dados importados. Os ICs existentes criados pelo IRE também são atualizados. O trabalho programado também cria ICs que incluem o identificador da partição de rede que começa com a próxima importação. Como alternativa, você pode iniciar o trabalho sob demanda para atualizar os dados existentes.

A partir da v14.0 de Vulnerability Response e v12.1 da Qualys Vulnerability Integration Integração de vulnerabilidade, os CMDB CI Class Models (1.0.21.) são compatíveis. Os modelos de classe têm o identificador de partição de rede [network_partition_identifier] nas regras de identificação de Identificação e Reconciliação (IRE).

Procedimento

1. Navegar até **Vulnerability Response** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
2. Escolha Qualys Vulnerability Integration.
3. **Edite** a integração necessária.
4. Escolher **Configuração de Detecção de Host**.
5. Escolher **Habilitar pesquisa por partição de rede** caixa de seleção do **Pesquisa por partição de rede**



seção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Concluir**.

Identificadores de partição de rede NETWORK_ID e REPOSITORY _ID incluídos na pesquisa de IP e na criação de IC

Origem	Endereço IP	NETWORK_Identifi	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Qualys Vulnerability Integration: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1	IC 1
	123.12.12.141	03713	IC 1	IC 2

Origem	Endereço IP	REPOSITÓRIO_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Qualys: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1	IC 1
	123.12.12.141	13	IC 1	IC 2

As regras de pesquisa de identificação de IC de endereço IP e endereço IP incompleto incluem o atributo do identificador de partição de rede automaticamente para uma importação de dados das integrações de ativos e vulnerabilidades fixas e abertas para Qualys Vulnerability Integration.

Depois de ativar o trabalho programado e salvar os registros, você pode atualizar os itens descobertos existentes com ICs que incluem o identificador de partição de rede iniciando trabalhos programados sob demanda. Os ICs no item descoberto existente, no item vulnerável e nos registros de detecção são atualizados automaticamente.

Tradução automática

Modificações opcionais do Qualys

Configure modificações opcionais e simplifique alguns dos dados especificamente para a integração do Qualys.

Você pode redefinir essa data de início no Assistente de configuração ou na integração primária ou modificar as regras de negócios para desativá-las durante uma importação inicial.

Desabilitar regras de negócio relacionadas a notificação antes da importação de registro inicial

Durante a importação inicial de registros, determinadas regras de negócios relacionadas à notificação podem gerar muitas notificações, afetando o desempenho. Essas regras de negócios devem ser modificadas para desativá-las durante a importação.

Antes de Iniciar

Função necessária: administrador

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Regras de negócios**.
2. Pesquise **notificações de IC afetado**.
3. Abra a regra de negócios e insira esta condição: `current.sys_class_name != “sn_vul_vulnerable_item”`.
4. Clique em **Atualizar**.
5. Repita este procedimento para as seguintes regras de negócios:
   - Notificações de centro de custos afetado
   - Notificações do grupo afetado
   - Notificações de local afetado

Nota:
Após a conclusão da importação do registro inicial, você terá a opção de reativar essas regras de negócio. No entanto, considere deixá-los desabilitados. Eles podem gerar um grande número de notificações e afetar o desempenho da sua instância.

Modificar uma data de início inicial

Durante a instalação usando o Assistente de configuração, você define uma data de início inicial para as integrações do Qualys. Você pode redefinir essa data de início no Assistente de configuração ou na integração primária, conforme mostrado abaixo.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa
Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
2. Clique **em Qualys Host Detection Integration**.
3. Clique **em Detalhes da integração**.
4. Defina o campo **Hora** de início com um valor no passado, para que todas as vulnerabilidades verificadas e detectadas desde essa hora sejam detectadas.

   Se você configurou Qualys usando o Assistente de configuração, o campo **Hora** de início será preenchido previamente, inicialmente para três meses antes da data de hoje e, subsequentemente, para a data de hoje.

   Nota:
   Considere definir o valor como no máximo um mês no passado. Isso evita que uma grande quantidade de dados exceda as limitações de taxa da API da Qualys, bem como aciona os tempos limites de execução.

5. Clique em **Enviar** ou **Atualizar**.
6. **Opcional:** Clique **em Executar agora** para executar imediatamente.

Configurações e modificações avançadas do Qualys

Configure modificações opcionais avançadas e simplifique alguns dos dados especificamente para a integração do Qualys. A maioria dessas modificações requer codificação ou conhecimento avançado ServiceNow ou Qualys Cloud Platform.

Modificar os valores de mapeamento de estado e prioridade da Qualys para a ServiceNow

Modifique os valores de mapeamento de prioridade e estado dos seus requisitos.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Esta é uma opção de personalização avançada.

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Regras de negócios**.
2. Pesquise por **Mapear valores do Qualys** e abra-o.
3. Clique na guia **Avançado**.
4. Modifique de acordo com seus requisitos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As modificações mais comuns incluem a adição de novos valores de estado ou a revisão da criticidade ou da prioridade.

5. Clique em **Atualizar**.

Restringir a capacidade de gravar em um registro com base em um grupo de atribuição

Você pode restringir os direitos de gravação/leitura em registros com base na associação a um grupo atribuído. Modifique as condições e o script com base em requisitos específicos.

Antes de Iniciar

Função necessária: security_admin (função elevada de administrador)

Nota:
Esta ação é realizada no escopo de vulnerabilidade.

Procedimento

1. Navegar até **Todos** > **Segurança do sistema** > **Controle de Acesso (ACL)**.
2. Pesquise ACLs que começam com `sn_vul`.
3. Escolha um registro de controle de acesso, por exemplo, sn_vul_vulnerable_item, **Operation write**.
4. Marque a caixa **Avançado** no registro, se necessário, para exibir as entradas da **Função**.
5. Modifique o script de **função** para seus requisitos.
   Exemplo de script de modificação do acesso por grupo.

```
answer = (current.assigned_to == gs.getUserID() ||
 isMemberOfForScopedApp(current.assignment_group));
// Note: standard 'isMemberOf' does not work within Scoped App
// gs.getUser().isMemberOf(current.assignment_group);
function isMemberOfForScopedApp(groupID){
var result = false;
if (groupID != ''){
var userID = gs.getUserID();
var now_GR = new GlideRecord("sys_user_grmember");
gr.addQuery("group", groupID);
gr.addQuery("user", userID);
gr.query();
if (gr.next()){
result = true;
}
}
return result;
}
```

6. Clique em **Atualizar**.

Configurar dispositivos scanner

Se você estiver iniciando as verificações do seu Now Platform® em vez de diretamente do Qualys, poderá configurar verificações para intervalos de endereços IP.

Antes de Iniciar

Os dados vêm da integração Qualys com base em Qualys grupos de ativos e seus dispositivos padrão relacionados (scanners).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se nenhum dispositivo estiver configurado para os intervalos de endereços IP de destino, o dispositivo definido como padrão para a instância de integração será usado para a verificação.

Função necessária: sn_vul_qualys.admin

Procedimento

1. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Dispositivos de Scanner**.
2. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Nome do dispositivo	Você será solicitado a preencher este campo ao criar um registro manualmente. Insira o nome do dispositivo scanner Qualys a ser usado para invocar verificações para itens de configuração correspondentes. Use o valor `Externo` quando quiser que a verificação seja iniciada com um scanner externo.
ID de dispositivo	Insira o identificador do dispositivo do scanner Qualys a ser usado para invocar verificações para itens de configuração correspondentes. Você será solicitado a preencher este campo ao criar um registro manualmente. Use o valor `0` quando quiser que a verificação seja iniciada com um scanner externo.
Status do dispositivo	Exibe o último status do dispositivo scanner nos dados retornados pela integração Qualys. Para registros criados manualmente, o status será atualizado somente se um **ID de dispositivo** válido for especificado.
ID de grupo de ativos	Exibe o identificador do grupo de ativos Qualys que criou este registro. Este campo exibe um valor somente para registros criados pela integração Qualys.
Nome do grupo de ativos	Exibe o nome do grupo de ativos Qualys que criou este registro. Este campo exibe um valor somente para registros criados pela integração Qualys.
Ordem	Insira um valor a ser usado para determinar a prioridade de verificação. Para dispositivos com critérios conflitantes, um dispositivo com um valor de pedido menor recebe uma prioridade mais alta.
Criado manualmente	Indica se este registro foi criado manualmente pelo usuário.
Usar grupo de filtros	Marque esta caixa de seleção para especificar um grupo de filtros para localizar itens de configuração correspondentes para verificação.
Grupo de filtros	Selecione o grupo de filtros que você deseja usar para encontrar itens de configuração correspondentes para verificação. Este campo será exibido somente se você tiver selecionado **Usar grupo de filtros**.
IPs	Uma lista separada por vírgulas de endereços IP ou intervalos de endereços IP a serem usados por este dispositivo ao invocar verificações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Instância de integração	A instância de integração Qualys associada a este dispositivo.
Perfil de opção	Selecione o perfil de opção que você deseja usar para verificações de itens de configuração correspondentes.

3. Clique em **Atualizar**.

Configurar e gerenciar scanners e verificações de vulnerabilidade Qualys

Qualys verificações de vulnerabilidade podem ser realizadas para encontrar vulnerabilidades de software que afetam seus ICs. Você pode iniciar verificações a partir de um registro de item vulnerável ou criando um registro de verificação diretamente para itens de configuração (ICs) e endereços IP.

Se você verificar Qualys itens vulneráveis diretamente na tela Itens vulneráveis, também terá a opção de verificar vários itens vulneráveis ao mesmo tempo.

Se Security Incident Response estiver ativado, você também poderá iniciar uma verificação a partir do catálogo de incidentes de segurança, de um registro de incidente de segurança ou de uma solicitação de verificação de segurança.

As verificações enviadas de Qualys itens vulneráveis, Catálogo de incidentes de segurança, incidentes de segurança ou solicitações de verificação de segurança são realizadas pelo scanner Qualys padrão.

Você pode selecionar o perfil de opção que deseja usar para verificações de itens de configuração correspondentes.

- Os perfis de opção contêm Qualys configurações de verificação.
- Um perfil de opção é necessário ao iniciar uma verificação de [Qualys de seu Now Platform®.

Configurar a verificação de IP iniciada pela ServiceNow Qualys

O scanner Qualys incluído com o sistema de base fornece uma integração de linha de base para iniciar verificações com base em endereços IP.

Antes de Iniciar

Você pode selecionar o perfil de opção que deseja usar para verificações de itens de configuração correspondentes.

- Os perfis de opção contêm Qualys configurações de verificação.
- Um perfil de opção é necessário ao iniciar uma verificação do Qualys a partir do Now Platform®.

Função necessária: sn_vul_qualys.admin

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Abra o registro Qualys.
3. Marque as caixas de seleção**Ativo** e **Padrão**.

   Selecionar **Ativo** é necessário para usar o scanner Qualys para verificar Qualys IVs automaticamente. Você também não precisa selecionar **Padrão** para que ele seja executado automaticamente.

   Antes da v12.0, **o ativo** é necessário para usar o scanner. Se **Padrão** também for selecionado, o scanner será usado automaticamente sem precisar ser selecionado durante a digitalização.
4. Para o campo Integração de origem, clique no ícone de pesquisa e selecione a opção para **Qualys**, por exemplo, **Qualys Cloud Platform**.
5. Clique em **Atualizar**.
6. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
7. Abra a **Integração da lista de grupos de ativos da Qualys**.
   a. Marque a caixa de seleção **Ativo**.
   b. Clique em **Executar agora**.
8. Siga estas etapas para preencher seus dispositivos scanner.

   Nota:
   Você pode preferir executar a integração da lista de perfis de opções após uma importação das integrações de listas de pesquisa, da lista de pesquisa dinâmica da Qualys e das integrações da lista de pesquisa estática da Qualys, para que você possa ver quais listas de pesquisa estão associadas aos perfis de opção.

   a. Abra a **integração da lista de perfis de opção da Qualys**.
   b. Marque a caixa de seleção **Ativo**.
   c. Clique em **Executar agora**.
   d. Siga as etapas listadas em Configurar dispositivos scanner para configurar seus dispositivos scanner. Retorne aqui depois de concluir essas etapas para continuar com a configuração.
   e. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
   f. Abra a **integração da lista de dispositivos da Qualys**.
   g. Marque a caixa de seleção **Ativo**.
   h. Clique em **Executar agora**.
   Seus dispositivos scanner Qualys agora estão preenchidos corretamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Noções básicas sobre o Qualys Vulnerability Integration

Verificar várias Qualys vulnerabilidades ou itens vulneráveis

Você pode verificar simultaneamente várias Qualys vulnerabilidades ou itens vulneráveis que contenham pelo menos um item de configuração (IC) afetado ou um endereço IP preenchido no formulário.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Procedimento

1. Siga um destes procedimentos:
   - Navegar até **Todos** > **Vulnerability Response** > **Tarefas de correção**.
   - Navegar até **Todos** > **Vulnerability Response** > **Todos os Itens vulneráveis**.
2. Marque as caixas de seleção dos registros que você deseja verificar.
3. Clique na lista **Ações nas linhas selecionadas** e clique em **Verificar novamente se há itens vulneráveis**.
   Uma mensagem aparece com um link para a verificação e as anotações de trabalho são atualizadas.
4. Clique no link para ver o andamento ou os resultados da verificação.

Configurar a verificação automática Qualys para tarefas de correção resolvidas

Você pode programar a verificação que é executada automaticamente para atualizar seus Qualys itens vulneráveis.

Antes de Iniciar

Depois que uma tarefa de correção é transicionada para **Resolvida**, uma verificação é iniciada automaticamente para atualizar o estado dos itens vulneráveis associados.

- A verificação está desabilitada por padrão.
- Habilite a verificação com o parâmetro de instância de integração **scan_on_resolved** no registro **Qualys** localizado em **Todos** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração** > **Qualys**. Consulte as etapas a seguir para obter mais informações.
- Esta verificação é específica da instância. Se você tiver várias instâncias e quiser habilitar ou desabilitar esta verificação, deverá desabilitar o parâmetro **scan_on_resolved** nos parâmetros de instância de integração em cada instância que deseja alterar.
- Quando a verificação está habilitada, você pode iniciar a verificação sob demanda ou pode programar a verificação para ser executada somente dentro de uma janela de tempo especificada. Consulte Configure Qualys novas verificações para serem executadas somente em intervalos programados para saber como definir as horas de início e de término da janela de tempo.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_vul_qualys.admin

Procedimento

1. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Instâncias de Integração**.
2. Selecione **Qualys** para abrir o registro.
   Os parâmetros de instância de integração para Qualys são exibidos em uma guia.
3. Para habilitar a verificação automática, localize o parâmetro *scan_on_resolved*.
4. Na coluna Valor da propriedade, insira verdadeiro.
5. Clique em **Atualizar**.

Configure Qualys novas verificações para serem executadas somente em intervalos programados

Para a Integração de vulnerabilidade Qualys, defina os parâmetros de hora de início e término da verificação para que as novas verificações sejam executadas ou estejam disponíveis somente durante as horas desejadas.

Antes de Iniciar

Esta configuração se aplica a verificações programadas e a verificações iniciadas manualmente no produto Qualys da sua instância Now Platform®.

Definir os parâmetros de hora de início e término da verificação para instâncias de integração permite especificar janelas de tempo quando novas verificações no produto Qualys estão disponíveis. Por exemplo, você pode preferir especificar que as novas verificações só estejam disponíveis fora do horário de expediente, por exemplo, da meia-noite às 10h.

Esta configuração é específica da instância. Se você tiver várias instâncias, deverá configurar os valores scan_start_time e scan_end_time nos parâmetros da instância de integração em cada instância que deseja mudar.

Função necessária: sn_vul_qualys.admin

Procedimento

1. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração** > **Qualys**.
2. Clique em **Qualys** para abrir o registro.
   Os parâmetros da instância de integração para Qualys são exibidos.
3. Para o parâmetro scan_start_time, na coluna Valor, insira a hora no fuso horário UTC no formato de 24 horas (00:00 a 24:00) para a hora de início da janela para a qual você deseja novas verificações disponíveis.
4. Para scan_end_time, na coluna Valor, insira horas no mesmo formato (00:00 a 24:00) para a hora de término da janela disponível.
   Por exemplo, se você inserir uma hora de início de 00:00 para o parâmetro scan_start_time e um scan_end_time de 10h nessa mesma manhã, as verificações programadas ou iniciadas manualmente fora da janela de tempo da meia-noite às 10h serão enfileiradas e iniciadas no hora de início da janela de tempo do dia seguinte, 00:00.

   No mesmo exemplo, se um proprietário de correção iniciar manualmente uma nova verificação às 11h, a nova verificação não será iniciada imediatamente, pois está fora dos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

horários de verificação configurados disponíveis. A solicitação de verificação permanece na fila até o início da janela de tempo do dia seguinte, neste exemplo, (00:00).

5. Clique em **Atualizar** para salvar suas configurações.

Qualys limites de taxa de verificação de vulnerabilidades

Você pode definir a taxa em que diferentes tipos de verificações são realizadas para limitar o número de solicitações enviadas para um scanner externo. Depois de definir os limites de taxa, você pode aplicá-los aos scanners Qualys.

Definir Qualys limites de taxa de verificação

Você pode definir a taxa em que diferentes tipos de verificações são realizadas para equilibrar a carga na fila de verificação. As condições definidas no limite de taxa determinam se os limites de taxa são aplicados às entradas enfileiradas.

Antes de Iniciar

Função necessária: sn_vul.admin

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Verificação de Vulnerabilidades** > **Definições de Limite de Taxa**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Definição de limite de taxa

Campo	Descrição
Nome	Forneça um nome descritivo que identifique as condições que a entrada da fila deve atender. Por exemplo, varreduras por minuto
Condições de fila	Insira as condições usadas para determinar se uma entrada de verificação enfileirada está sujeita a este limite de taxa. As condições não devem ser específicas de um scanner específico.
Script de avaliação	Grave um script com a lógica para avaliar a entrada enfileirada. É importante que o script retorne verdadeiro/falso para definir se a entrada será processada. Além disso, baseie o script de avaliação na entrada enfileirada que está sendo avaliada.

4. Clique em **Enviar**.

Aplicar limites de taxa de verificação a scanners Qualys

Depois de definir os limites de taxa de verificação usando **Definições de limite de taxa**, você pode aplicar limites de taxa a scanners Qualys específicos.

Antes de Iniciar

Função necessária: sn.vul_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Verificação de Vulnerabilidades** > **Limites de Taxa do Scanner**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Limite de taxa do scanner

Campo	Descrição
Scanner	Selecione o scanner ao qual você deseja aplicar um limite de taxa.
Limite de taxa	Selecione o limite de taxa que você deseja aplicar a este scanner.
Limite	Insira o limite ao qual você deseja sujeitar o scanner selecionado para o limite de taxa selecionado. Por exemplo, se o scanner permitir quatro varreduras por minuto e o limite de taxa for definido como solicitações por minuto, o limite será 4.

4. Clique em **Enviar**.

Exibir a Qualys fila de verificação de vulnerabilidade

As solicitações de verificação de vulnerabilidade enviadas para Qualys integração de verificação de vulnerabilidade são enfileiradas para não sobrecarregar os recursos do sistema. Você pode exibir o status das solicitações enfileiradas, conforme necessário.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa

Na lista de verificações enfileiradas, cada verificação inclui um nome de verificação gerado automaticamente que identifica o IC que foi verificado.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Verificação de Vulnerabilidades** > **Fila de Verificação**.
   Todas as Qualys solicitações de verificação que foram enviadas são mostradas em uma lista. A coluna **Estado** mostra o estado atual de cada entrada na fila. Um estado **Concluído** indica que a verificação saiu da fila. Isso não indica necessariamente que a verificação concluiu o processamento. Quando as verificações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

forem concluídas ou houver falha, a coluna **Processamento** mostrará o texto de anotações de trabalho apropriado.

Nota:
Se um valor de hash tiver sido enviado para verificação e o scanner não encontrar um resultado, o **Estado** mostrará **Concluído** e a anotação de trabalho na coluna **Processamento** indicará **Desconhecido**.

2. Depois que uma verificação terminar o processamento, clique em um registro enfileirado para exibir detalhes da solicitação de verificação.

Habilitar filtro do sistema de base para importações de detecção confirmada

Habilite um filtro padrão usando parâmetros de integração para importar somente detecções confirmadas de Qualys Cloud Platform.

Antes de Iniciar
Função necessária: sn_vul_qualys.admin, sn_vul.vr_import_admin

Por Que e Quando Desempenhar Esta Tarefa
Um parâmetro de instância de integração do sistema básico "include_only_confirmed" está disponível para importar uma lista filtrada de detecções de Qualys Cloud Platform. Por padrão, este parâmetro é definido como `FALSO`e todas as detecções, sejam potenciais, confirmadas ou informativas, são importadas.

Procedimento

1. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Instâncias de Integração**.
2. Abra a integração da plataforma Qualys Cloud na lista de instâncias de integração.
3. Na lista Parâmetros de instância de integração, abra o parâmetro '`include_only_confirmed`'.
4. Atualize o valor padrão para `Verdadeiro`.
5. Clique em **Atualizar**.
   Você habilitou o filtro para importar detecções confirmadas da integração Qualys Cloud Platform.

Resultado
Por padrão, somente as detecções confirmadas da integração Qualys Cloud Platform são importadas quando a próxima importação de vulnerabilidade da Qualys é executada. Todas as outras detecções, como informativas e possíveis, são ignoradas e não importadas. Para obter mais informações, consulte Exibir dados de detecção de item vulnerável do Vulnerability Response.

Iniciar nova verificação para Qualys Vulnerability Integration

Verifique se seus itens vulneráveis foram corrigidos entre os ciclos de verificação programados iniciando novas verificações no produto Qualys de seu Now Platform sob demanda.

Antes de Iniciar
Você pode iniciar novas verificações nos espaços do Vulnerability Response. Para obter mais informações, consulte Verificar novamente registros e tarefas de correção no Vulnerability Manager Workspace e Verifique novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para novas verificações no ambiente clássico, consulte as seções a seguir para saber como iniciar novas verificações.

Configuração necessária para novas verificações no produto Qualys iniciadas de seu Now Platform:

Você pode iniciar uma nova verificação sob demanda de itens vulneráveis para o produto Qualys da sua instância Now Platform®.

Para ajudar a reduzir a sobrecarga e o volume envolvidos nas verificações completas programadas, os proprietários de correção, especialistas em TI, analistas de vulnerabilidade ou gerentes de vulnerabilidade podem iniciar novas verificações direcionadas sob demanda para vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas verificações no produto Qualys de item vulnerável (IV), tarefas de correção (RT), entrada de terceiros (TPE) ou registros de item descoberto de sua instância Now Platform.

As novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

Caso de uso

Por exemplo, digamos que todo o seu ambiente seja verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada de seus Now Platform para Qualys itens vulneráveis.

Você pode iniciar novas verificações para IVs que tenham Qualys como origem em estados diferentes de encerrado. Consulte Verificar novamente registros e tarefas de correção no Vulnerability Manager Workspace e Verifique novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI.

Verifique se você concluiu a configuração a seguir, necessária para novas verificações. Consulte as etapas que começam com Configurar e gerenciar Qualys verificações e verificações de vulnerabilidade listadas nas seções anteriores para obter mais informações.

Função necessária: sn_vul_manually_initiate_rescan

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Itens vulneráveis**.
2. Localize o registro do item vulnerável do qual você deseja acionar uma nova verificação e abra-o.

> **Nota:**
> Você só pode iniciar novas verificações de IVs com Qualys como origem. Verifique se Qualys é exibido na coluna **Origem** nas exibições de Lista de IV ou nos campos **Origem** em registros individuais. Você pode usar o construtor de condição para agrupar IVs por origem. Ou, se a coluna Origem não for exibida na exibição da lista de IVs, no canto superior esquerdo da lista, clique no ícone**Personalizar lista** (ícone de engrenagem) e use o Slushbucket para mover a **origem** de **Disponível** para **Selecionado**.

3. Como alternativa, navegue até **Todos** > **Vulnerability Response** > **Tarefas de correção**, **Vulnerability Response** > **Bibliotecas** > **Terceiros**ou para **Itens descobertos** para a tarefa de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

correção, entrada de terceiros ou registros de itens descobertos, respectivamente, que você deseja usar para a nova verificação.

Dependendo da sua escolha, o botão **Verificar novamente** está disponível nos seguintes registros:

- Em um único registro de IV, o IV deve ser do produto Qualys e em qualquer estado diferente de **Encerrado**. Para vários registros de IV, todos os IVs devem ter Qualys como origem e em qualquer estado diferente de **Encerrado**.
- Em um registro RT, a tarefa de correção pode estar em qualquer estado diferente de **Encerrado**e todos os IVs associados devem ter Qualys como origem.
- Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro de IV associado em qualquer estado diferente de **Encerrado** com Qualys como origem.
- Em um registro de item descoberto, o item de configuração tem pelo menos um IV associado a Qualys como origem em qualquer estado diferente de **Encerrado**.

4. No canto superior direito do registro escolhido, clique em **Verificar novamente**.
Na caixa de diálogo exibida, escolha um para continuar.

Opção	Descrição
Marque a caixa de seleção **Especificar perfis de opção**.	Na lista, escolha o perfil de opção para o scanner Qualys que você deseja usar para a nova verificação. Estes são os dispositivos (scanners) que você configurou e listou em **Integração de Vulnerabilidade da Qualys** > **Dispositivos de Scanner**.
Desmarque a caixa de seleção **Especificar perfis de opção** (não selecionada).	O perfil de opção Qualys do scanner que você definiu como padrão na lista Dispositivos scanner é usado para a verificação. Para obter mais informações sobre como definir os scanners padrão que você inicia a partir do seu Now Platform, configure os dispositivos de scanner listados na seção anterior para obter mais informações.

5. Clique **em Solicitar verificação**.

Uma mensagem será exibida indicando que a verificação está sendo processada. O status de todas as novas verificações pode ser encontrado a qualquer momento nas listas relacionadas à verificação no IV, RT, TPE e nos registros de item descoberto que você usou para iniciar as novas verificações. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e todas as outras verificações iniciadas a partir de um determinado registro.

Sua instância rastreia o status de nova verificação até que seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando Now Platform parou de acompanhar seu status de nova verificação, não quando a nova verificação real parou.

Depois que a nova verificação for concluída com sucesso, a Integração de detecção de host Qualys será iniciada automaticamente para atualizar seus itens vulneráveis. Dependendo de quantos IVs você tiver, suas detecções, IVs e RTs serão atualizados após

Tradução automática

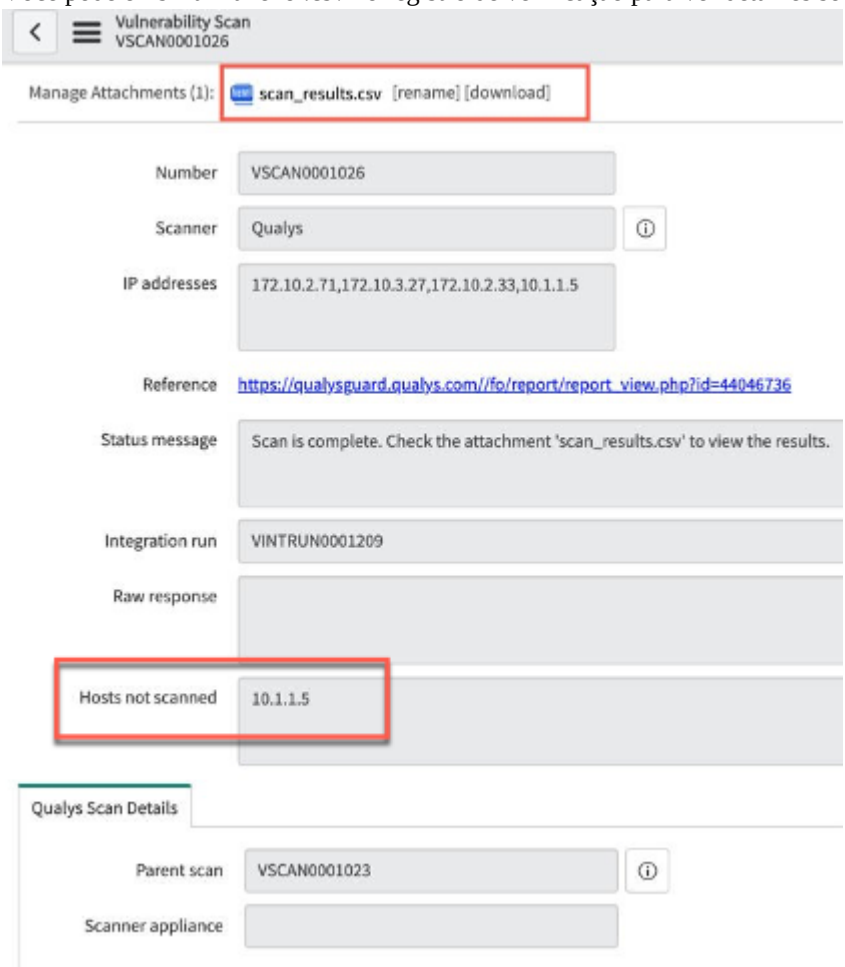
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a conclusão da Qualys verificação de integração de detecção de host. Navegue até esses registros para exibir as atualizações após a conclusão da integração de detecção de host.

Esta verificação é específica da instância e pode ser desabilitada. Para obter mais informações sobre as integrações Qualys e como exibir as integrações, consulte Noções básicas sobre o Qualys Vulnerability Integration.

O que Fazer Depois

Você pode exibir um anexo .csv no registro de verificação para ver detalhes sobre as novas verificações.



Conforme mostrado na imagem anterior, durante a nova verificação, se os hosts (itens de configuração) em seu ambiente não estiverem acessíveis, todas as detecções e IVs associados a esses ativos não serão atualizados quando a nova verificação for concluída. Para ajudar você a entender por que eles não estão incluídos, depois que a nova verificação for concluída, os endereços IP do ativo para esses ICs serão listados em Registros de vulnerabilidade no campo Hosts não verificados.

Qualys metadados para vulnerabilidades

A Integração de detecção de host Qualys foi aprimorada para incluir mais campos de Qualys. Esses campos ajudam a filtrar as vulnerabilidades não exploráveis Linux. Este aprimoramento melhora a integração no nível de detecção e no nível de item vulnerável (IV).

Importar metadados adicionais de Qualys

Importe metadados adicionais para itens de vulnerabilidade (IV) para filtrar vulnerabilidades com base no impacto em um kernel ou serviço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Procedimento
1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração**.
2. Em Configuração de integração, clique em **Integrações de scanner**.
3. Em Aplicação instalada, clique em **Editar** para a aplicação Qualys.
4. Clique **em Configuração de detecção de host**.
5. Navegar até **Importar metadados adicionais para detecções**.
6. Para importar metadados adicionais de Qualys, marque manualmente qualquer uma das caixas de seleção a seguir.
   - **Metadados do Kernel**: identifica vulnerabilidades encontradas em kernels do Linux em execução ou não em execução.

     Se o valor dos metadados retornados for **Não**, isso significa que a vulnerabilidade não pode ser explorada devido a um kernel que não está em execução. Para obter informações sobre os valores recuperados, consulte Qualys valores de metadados para vulnerabilidades.
   - **Metadados de serviço**: identifica vulnerabilidades encontradas em portas ou serviços em execução ou não em execução.
   - **Metadados de configuração**exploráveis: identifica vulnerabilidades que podem ou não ser exploráveis devido à configuração do host atual.

   Nota:
   Por padrão, essas caixas de seleção não estão marcadas.
7. Execute a Qualys Integração de detecção de host com uma data anterior.
   Para obter mais informações sobre como definir a data de início, consulte Modificações opcionais do Qualys.

Resultado
Os metadados foram importados.

O que Fazer Depois
Para exibir os metadados importados, insira `sn_vul_detection.list` na Navegação do filtro. A lista de Detecções de item vulnerável é exibida. Para obter mais informações sobre os valores exibidos nas colunas recém-adicionadas, consulte Qualys valores de metadados para vulnerabilidades.

Qualys valores de metadados para vulnerabilidades

Quando os metadados do kernel, os metadados de serviço e os metadados de configuração são importados, alguns valores também são recuperados. Os valores **0**, **1** e **Não disponível** são processados no back-end e convertidos em **Não**, **Sim** e **Vazio**, respectivamente.

Esses valores são preenchidos nas seguintes colunas na lista Detecções de item de vulnerabilidade e Itens de vulnerabilidade:

- Afeta a coluna de serviço em execução
- Afeta a coluna de configuração explorável
- Afeta as colunas do kernel em execução

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- Essas colunas não estão visíveis por padrão. Para obter mais informações sobre como configurar o layout do formulário, consulte Configurar o layout do formulário
- Para detecções mais antigas, os valores dessas colunas podem estar vazios. Para atualizar os dados, execute uma integração de detecção de host Qualys datada. Para obter mais informações sobre como definir a data de início, consulte Modificações opcionais do Qualys.

A tabela a seguir mostra os valores recuperados e sua significância.

Valores de campo recuperados e sua significância

Campo	Valor	Significância
AFFECT_RUNNING_KERNEL	0	A vulnerabilidade foi encontrada em um kernel que não está em execução. A vulnerabilidade não é explorável.
AFFECT_RUNNING_KERNEL	1	A vulnerabilidade foi encontrada em um kernel em execução. A vulnerabilidade é explorável.
AFFECT_RUNNING_KERNEL	Não disponível	A vulnerabilidade não é uma vulnerabilidade relacionada ao kernel.
AFFECT_RUNNING_SERVICE	1	A vulnerabilidade é encontrada em portas ou serviços que não estão em execução. A vulnerabilidade não é explorável.
AFFECT_RUNNING_SERVICE	0	A vulnerabilidade é encontrada nas portas ou serviços em execução. A vulnerabilidade é explorável.
AFFECT_RUNNING_SERVICE	Não disponível	A vulnerabilidade não é uma vulnerabilidade relacionada.
AFFECT_EXPLOITÁVEL_CONFIG	1	A vulnerabilidade não pode ser explorada devido à configuração do host.
AFFECT_EXPLOITÁVEL_CONFIG	0	A vulnerabilidade é explorável devido à configuração do host.
AFFECT_EXPLOITÁVEL_CONFIG	Não disponível	A vulnerabilidade não é uma vulnerabilidade relacionada.

Tradução automática

Definir parâmetros de filtro adicionais para importações de Qualys

Personalize os parâmetros de filtragem das suas consultas programadas com Qualys Vulnerability Integration para ajudar a refinar ainda mais os dados de vulnerabilidade importados com as integrações Qualys compatíveis.

Antes de Iniciar

Casos de uso: como gerente ou analista de vulnerabilidade, convém filtrar os dados de suas consultas para que você possa revisar somente os detalhes específicos da vulnerabilidade. Por exemplo, digamos que você queira exibir vulnerabilidades importadas que são filtradas por IPs ou intervalos de IP específicos. Ou você deseja importar somente máquinas que estão no seu escopo, por exemplo, somente máquinas em sua rede corporativa que não sejam dispositivos externos.

Para ajudá-lo a coletar esses dados, você pode adicionar parâmetros Qualys para ajudá-lo a importar os detalhes da vulnerabilidade específica de que precisa.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

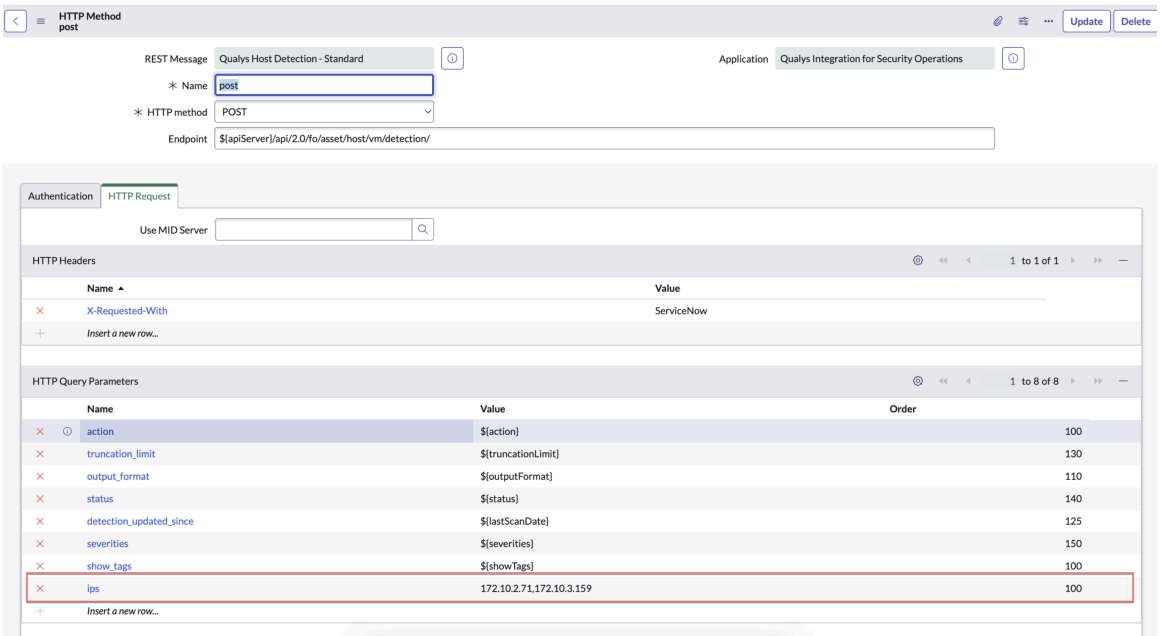
Sem adicionar chamadas de API ou codificação adicionais, este recurso permite que você personalize suas informações de solicitação HTTP com parâmetros Qualys em seu Now Platform. Você modifica ou adiciona esses valores ao registro do método HTTP no método REST para as integrações Qualys compatíveis do Qualys Vulnerability Integration.

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Localize os parâmetros compatíveis com o produto Qualys no site do desenvolvedor que você deseja usar para sua filtragem.
   Os parâmetros e valores inseridos no produto Qualys são compatíveis somente no nível da instância de integração em seu Now Platform. Todas as integrações Qualys são compatíveis com filtragem usando parâmetros de consulta.
2. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
3. Na página da lista de integrações Qualys, clique no registro da integração que você deseja abrir.
4. Com a guia Qualys Detalhes REST selecionada, localize e clique no ícone de informações (I) do método REST, seguido por **Abrir registro** para abrir o registro do método HTTP.
5. Selecione a guia **Solicitação HTTP**.
6. Nos Parâmetros de consulta HTTP do corpo da solicitação, adicione os valores obtidos do site do desenvolvedor Qualys.

   Na imagem a seguir, como exemplo, o parâmetro que ingere somente determinados endereços IP/intervalos, `ips={value}` foi adicionado. Nesse caso, o **valor** é um ou mais IPs/intervalos que você especificar. Várias entradas são separadas por vírgulas, 172.10.2.71, 172.10.3.159e um intervalo é especificado com um hífen, 10.10.10.1-10.10.10.100. Consulte o site do desenvolvedor Qualys para obter mais informações.



   Se você quiser inserir mais de um parâmetro, consulte a documentação Qualys para obter mais informações sobre como separar cada valor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Você deve estar ciente de seus requisitos de API. Talvez você precise adicionar essas propriedades de API aos Parâmetros de consulta ou ao conteúdo do corpo.

Alguns outros parâmetros que você pode achar úteis no site do desenvolvedor Qualys :

- `ag_ids` - IDs da lista do grupo de ativos a serem recuperados. Este parâmetro garante que somente máquinas no seu escopo sejam trazidas.
- `qids` - Este parâmetro limita os resultados a somente determinadas vulnerabilidades (QID na tabela de entrada de terceiros). Esta configuração evita a sobrecarga do sistema com registros informativos.

7. Clique em **Atualizar**.

Resolver problemas de integração de vulnerabilidade da Qualys

Alguns problemas comumente encontrados, junto com soluções alternativas, são discutidos.

Anexos não exibidos após a importação

Se os anexos não estiverem aparecendo conforme o esperado para as fontes de dados ou em um incidente de segurança após as importações de integração de terceiros, verifique as restrições de IP.

As restrições de acesso IP podem impedir que os anexos sejam vistos, a menos que você esteja conectado a partir de um IP seguro. Como um novo anexo é adicionado a cada importação, isso pode resultar em duplicatas que você precisa remover.

Por exemplo, ao executar uma integração de importação de host de terceiros, se você não vir nenhum anexo em suas fontes de dados, verifique as restrições de IP e adicione usuários à lista segura antes da importação.

Modificar mapas de transformação

Os mapas de transformação são fornecidos com configurações de base e geralmente são suficientes. Você pode modificar os mapeamentos de transformação, dependendo das necessidades da sua organização.

Antes de Iniciar
Função necessária: sn_vul_qualys.admin + import_admin

Procedimento

1. Navegar até **Todos** > **Conjuntos de importação do sistema** > **Administração** > **Mapas de transformação** para exibir as mensagens REST.
2. Filtre a lista resultante por aplicação e limite a lista à aplicação **Qualys Vulnerability Integration**.
3. Modifique os mapas de transformação de acordo com os requisitos do cliente.

Para obter detalhes sobre os dados fornecidos pela API Qualys, consulte a documentação da API Qualys .

Verificar o tamanho da propriedade do anexo XML

Verifica se a propriedade de anexo XML é suficiente para arquivos grandes.

Antes de Iniciar
Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Propriedades do sistema** > **Importação/Exportação**.
2. Rolar para baixo até **Propriedades de importação** > **Formato XML** na parte inferior da página.

3. Se necessário, altere o valor para 250 e clique em **Salvar**.

Tópicos relacionados

Propriedades do sistema disponíveis

Limitações de recuperação de dados

Por padrão, não há restrições sobre como os dados são recuperados do Qualys. Muitos registros podem estar relacionados a vulnerabilidades de baixa severidade que um cliente não está disposto a corrigir usando seu processo de resposta de vulnerabilidade. Atualizar os parâmetros de mensagem/método REST correspondentes pode modificar esse comportamento.

A mensagem/método REST responsável por esta atualização é **Qualys Host Detection – Standard/post**. Para atualizar os valores, adicione um novo parâmetro de consulta HTTP ao método post com os seguintes valores:

- Nome: severities
- Valor: 3-5 (ou quaisquer gravidades apropriadas desejadas)

Resolver falha de integração da base de conhecimento da Qualys

Resolver Qualys falha de integração da base de conhecimento reduzindo o tamanho do anexo da carga recebida de Qualys para o limite especificado.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Certifique-se de que o tamanho do anexo da carga esteja dentro do limite especificado.
   a. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração**.
   b. Selecione a guia **Parâmetros de instância de integração**.
   c. Selecione **max_delta_days** e modifique o valor padrão para 3.
2. Se a integração ainda falhar, execute as seguintes etapas:
   a. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias**.
   b. Selecione **Base de conhecimento da Qualys**.
   c. Selecione a guia **Detalhes da integração**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

d. No campo **Hora** de início, selecione a data atual para ignorar a execução da execução desse dia.

e. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração**.

f. Selecione a guia **Parâmetros de instância de integração**.

g. Selecione **kb_backfill_full_import** e modifique o valor padrão para verdadeiro.

Resultado
Executar a integração do Qualys Knowledge Base Backfill atualiza todas as entradas de terceiros (TPEs) no sistema. Enquanto a integração de detecção de host da Qualys cria uma entrada de espaço reservado, a integração de preenchimento da base de conhecimento da Qualys a atualiza.

Qualys Vulnerability Integration relatório

A visão geral Qualys Cloud Platform é uma exibição executiva da atividade de vulnerabilidade. Ao fornecer tendências, relatórios e detalhamentos em dados específicos, um administrador ou analista pode identificar rapidamente as áreas de preocupação. Os gráficos são preenchidos com dados depois que os itens vulneráveis e os dados da base de conhecimento Qualys foram recuperados.

Visualizações de dados nos espaços Vulnerability Response

Os espaços Vulnerability Response incluem visualizações de dados que podem ajudar a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a severidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizadas conforme os dados de vulnerabilidade mudam. Consulte Vulnerability Response Espaços, Espaço para gerentes de vulnerabilidades e Explorando o Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos que estão disponíveis.

Versões anteriores de Vulnerability Response

Os analistas de vulnerabilidade também podem usar os painéis padrão no ambiente clássico para monitorar os dados de vulnerabilidade. Para obter mais informações, consulte Usando os painéis padrão Vulnerability Response.

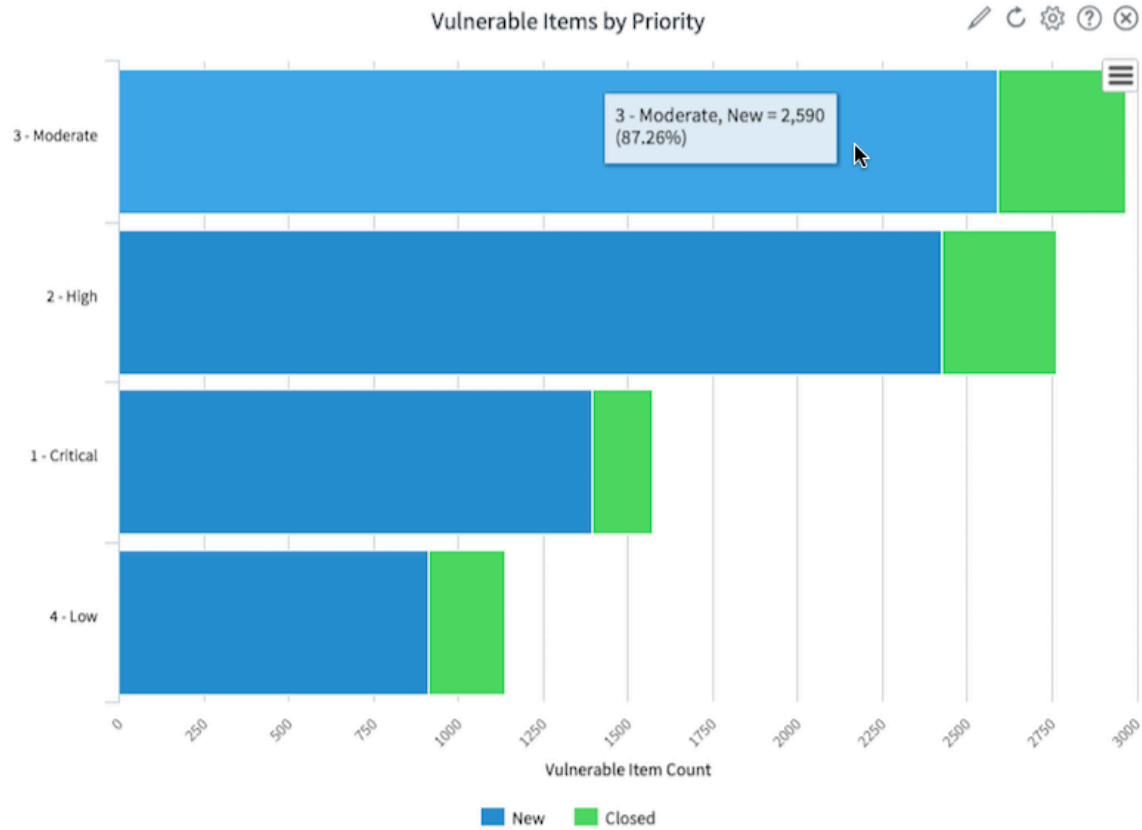
Nota:
O uso da integração de vulnerabilidade Qualys Cloud Platform pressupõe que o ajuste, o teste e a implantação tenham ocorrido em sua instância. Essas funções estão fora do escopo da documentação do produto. Para obter assistência, entre em contato com Suporte e atendimento ao cliente.

Em cada gráfico, você pode apontar para qualquer parte de um gráfico (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gráfico de amostra Qualys Vulnerability Integration



Os relatórios a seguir estão disponíveis na página inicial do Qualys Cloud Platform.

Qualys Vulnerability Integration Relatórios de visão geral

Nome	Visual	Descrição
ICs sincronizados com o Qualys	Barra	Exibe o número de itens vulneráveis em aberto registrados para cada IC, do maior para o menor.
Itens vulneráveis do Qualys em aberto	Barra	Exibe o número de itens vulneráveis em aberto associados a vulnerabilidades (registros CVE), do maior para o menor.
Total de itens vulneráveis da Qualys	Barra	Exibe o número de itens vulneráveis ignorados programados para expirar em 7 dias.
Itens vulneráveis por prioridade	Tendência	Exibe o número de entradas de vulnerabilidade registradas a cada semana.
Prevalência de QID	Barra	Exibe o número de itens vulneráveis registrados para cada modelo, do mais para o menos.
Itens vulneráveis do Qualys em aberto	Lista de	Exibe o número de itens vulneráveis registrados para cada fornecedor, do mais para o menos.

Qualys gráfico de status de execução de integração

O módulo Qualys Status de execução de integração é uma exibição gráfica do status de Qualys execuções de integração.

Para exibir o status das execuções de integração, navegue até **Integração de Vulnerabilidade da Qualys** > **Status da Execução da Integração**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A partir da versão 19.0 do Vulnerability Response, este painel está disponível na IU da nova experiência.

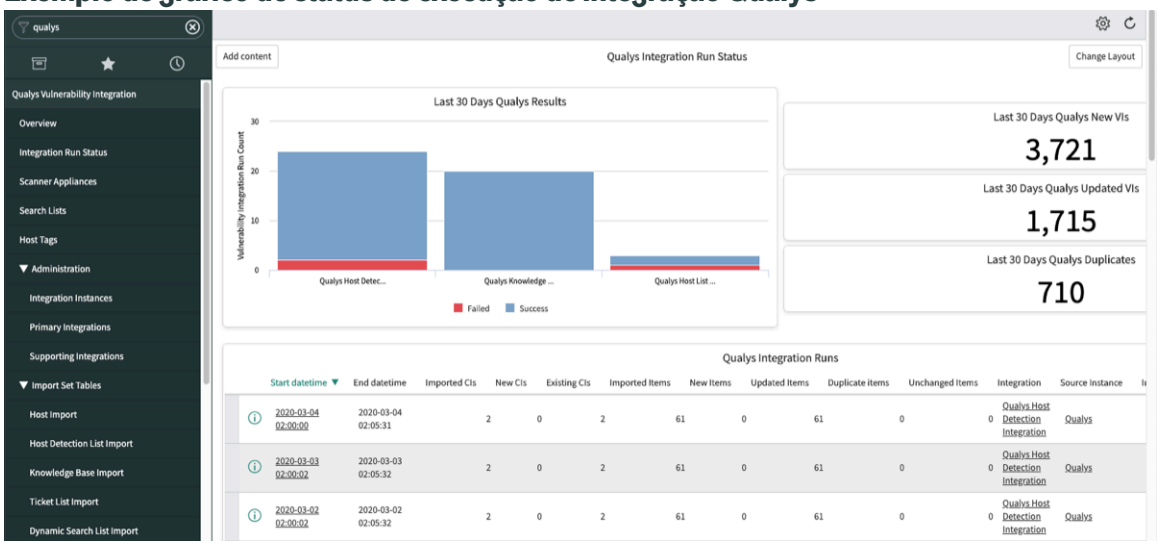
Nota:
Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

No gráfico, aponte para qualquer parte (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

O Qualys Status de execução de integração exibe o status de execução da integração de vulnerabilidade nos últimos 30 dias. A contagem de IVs atualizados da Qualys[qualys] indica a contagem de detecções exclusivas no mesmo ativo. O IV é atualizado com a nova detecção.

Nota:
A contagem de execuções de integração de vulnerabilidade é exibida somente para as integrações, que estão definidas para o estado ativo. Navegar até **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias** e defina o estado como ativo.

Exemplo de gráfico de status de execução de integração Qualys



- Os valores na coluna Itens importados representam o número total de registros que são criados a partir de uma execução de integração.
- A coluna Novos itens exibe o número de registros que são criados a partir de uma execução de integração.
- A coluna Itens duplicados não está mais preenchida. Você pode preferir remover esta coluna da exibição.
- A coluna Itens atualizados exibe o número de vezes que os registros são atualizados durante uma execução de integração. Este valor não é o número de registros exclusivos que são atualizados. Se, por exemplo, um registro for atualizado duas vezes durante a execução da integração, ele será contado duas vezes e exibido como dois itens atualizados.
- A coluna Itens inalterados exibe registros encontrados durante a execução da integração que já existem no banco de dados, mas não foram atualizados, porque nenhum dos valores de campo relevantes foi alterado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A integração é executada com resultados zero para todos os quatro valores a seguir: **Novos ICs**, **ICs existentes**, **Novos itens**e **Itens atualizados** são filtrados da lista de execuções de **integração da Qualys**.

Qualys relatórios de gráfico de status de execução de integração

Nome	Descrição
Resultados dos últimos 30 dias Qualys	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Executar em um visual de barra.
Últimos 30 dias Qualys Novos IVs	O número de novos registros importados nos últimos 30 dias. Mostrado como um número inteiro.
IVs atualizados nos últimos 30 dias Qualys	O número de registros atualizados importados nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Qualys Duplicatas	O número de registros duplicados importados nos últimos 30 dias. Mostrado como um número inteiro.
Qualys Execuções de integração	Os registros de execução de integração em uma lista. **Nota:** **V16.1:** para verificar as detecções para esta integração, compare as detecções ou descobertas com os dados de detecção ServiceNow`sn_vul_detection`] na tabela . Enquanto a integração está em andamento, pode haver uma mudança na detecção ou na contagem de descobertas. Este relatório exibe a contagem de detecções na coluna "Contagem até a data" na instância, após a conclusão da execução da integração.
Últimos 30 dias Qualys Métricas de desempenho de ingestão de item vulnerável	Métricas de desempenho diárias para itens vulneráveis comparadas nos últimos 30 dias.
Últimos 30 dias Qualys Rendimento do desempenho de ingestão de item vulnerável	Rendimento diário de ingestão de item vulnerável medido para a integração de detecção de host Qualys nos últimos 30 dias.

Vários fatores podem afetar o desempenho da execução da integração, como a quantidade de dados e o tempo necessário para processar esses dados. Dois gráficos comparam as métricas de desempenho:

- Qualys Métricas de desempenho de ingestão de item vulnerável: compare as métricas de desempenho diárias para regras de atribuição, regras de grupo, regras de risco, tempo de espera da fila, tempo de processamento da fila e outras estatísticas de itens vulneráveis nos últimos 30 dias para identificar a causa de quaisquer desvios no desempenho. O desempenho é calculado com base no tempo gasto em cada atividade. Esses parâmetros são calculados e associados no nível de execução da integração. Cada parâmetro é codificado por cor para facilitar a identificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Qualys Rendimento de desempenho de ingestão de item vulnerável: compare o rendimento de ingestão de item vulnerável diário para a integração de detecção de host Qualys. O rendimento é medido em itens por hora. Este relatório mostra o desempenho geral em um dia específico e não no nível de parâmetro individual.

Transformação de dados da Qualys

Os dados recuperados do Qualys são processados por meio de um conjunto de fontes de dados e transformações.

A maioria das transformações para Qualys Vulnerability Integration é realizada usando scripts de transformação. Esses scripts são para uso interno e a exclusão não é recomendada. As modificações exigem codificação ou conhecimento avançado ServiceNow ou Qualys Vulnerability Integration. Os mapas restantes estão listados nesta seção e usam mapas de campo.

Nota:
Durante a instalação, os mapas de severidade normalizados, que transformam os níveis de severidade Qualys Cloud Platform importados em níveis de severidade ServiceNow padrão, são instalados no módulo Mapeamento de severidade normalizado Vulnerability Response. Para obter mais informações, consulte Criar um mapa de severidade Vulnerability Response.

Importação de Lista de Pesquisa Dinâmica

O mapa de transformação da lista de pesquisa dinâmica da Qualys é usado para transformar e importar listas de pesquisa dinâmica da Qualys. As mudanças nesta transformação alteram como as listas de pesquisa dinâmica são processadas e inseridas no sistema.

Para acessar este mapa de transformação, navegue até **Integração de Vulnerabilidade da Qualys** > **Tabelas do conjunto de importação** > **Importação de lista de pesquisa dinâmica**.

A tabela mostra os campos que estão sendo transformados no momento.

Campos do mapa de transformação da lista de pesquisa dinâmica da Qualys

Campo de origem	Campo de destino	Descrição
u_id	id	Usado como o identificador da lista de pesquisa dinâmica do Qualys.
[Script]	lista_tipo	O tipo de lista de pesquisa. Dinâmico é o padrão para a transformação Lista de pesquisa dinâmica.
u_title	título	O nome no Qualys para esta lista de pesquisa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Além dos mapeamentos de campo, também há um script de transformação que é executado durante o processo de transformação.

A tabela a seguir mostra quando este script é executado e para que ele é usado.

Tempo e finalidade do script do mapa de transformação da lista de pesquisa dinâmica da Qualys

Quando o script é executado	Finalidade do script
onAfter (depois que um conjunto de importação concluiu a transformação).	Cria os relacionamentos entre as Listas de pesquisa e suas vulnerabilidades relacionadas. Para uso interno. Modificar ou excluir não é recomendado.

Importação de Lista de Pesquisa Estática

O mapa de transformação da lista de pesquisa estática da Qualys é usado para transformar e importar listas de pesquisa estática da Qualys. As mudanças nesta transformação alteram como as listas de pesquisa estática são processadas e inseridas no sistema.

Para acessar este mapa de transformação, navegue até **Integração de Vulnerabilidade da Qualys** > **Tabelas do conjunto de importação** > **Importação de Lista de Pesquisa Estática**.

A tabela mostra os campos que estão sendo transformados no momento.

Campos do mapa de transformação da lista de pesquisa estática da Qualys

Campo de origem	Campo de destino	Descrição
u_id	id	Usado como o identificador da lista de pesquisa estática da Qualys.
u_title	título	O nome no Qualys para esta lista de pesquisa.
[Script]	lista_tipo	O tipo de lista de pesquisa. Estático é o padrão para a transformação Lista de pesquisa estática.

Além dos mapeamentos de campo, também há um script de transformação que é executado durante o processo de transformação.

A tabela a seguir mostra quando este script é executado e para que ele é usado.

Tempo e finalidade do script do mapa de transformação da lista de pesquisa estática da Qualys

Quando o script é executado	Finalidade do script
onAfter (depois que um conjunto de importação concluiu a transformação).	Cria os relacionamentos entre as Listas de pesquisa e suas vulnerabilidades relacionadas. Para uso interno. Modificar ou excluir não é recomendado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importação de Grupo de Ativos

O mapa de transformação de dispositivo do Qualys Asset Group é usado para transformar dados do Qualys Asset Group para criar registros de dispositivo scanner. Mudanças nesta transformação alteram como os dispositivos scanner são criados e modificados.

Para acessar este mapa de transformação, navegue até **Integração de Vulnerabilidade da Qualys** > **Tabelas do conjunto de importação** > **Importação de Grupo de Ativos**.

A tabela mostra os campos que estão sendo transformados no momento.

Campos do mapa de transformação do grupo de ativos da Qualys

Campo de origem	Campo de destino	Descrição
u_id	id	Usado como identificador do grupo de ativos da Qualys.
[Script]	manual	Valor de script para determinar como o registro de destino foi criado. Quando criado por meio de transformações, este campo é sempre falso.
[Script]	ips	Os endereços IP associados ao grupo de ativos que está sendo transformado.
u_default_appliance_id	dispositivo_id	O identificador do dispositivo Qualys para o dispositivo padrão neste grupo de ativos.
u_title	asset_group_name	O nome do grupo de ativos da Qualys.

Além dos mapeamentos de campo, também há um script de transformação que é executado durante o processo de transformação.

A tabela a seguir mostra quando este script é executado e para que ele é usado.

Tempo e finalidade do script do mapa de transformação do grupo de ativos da Qualys

Quando o script é executado	Finalidade do script
onBefore (antes de um conjunto de importação concluir a transformação).	O script que restringe as importações de grupo de ativos somente a grupos de ativos com um dispositivo padrão e um conjunto de endereços IP mapeados. Para uso interno. Modificar ou excluir não é recomendado.

Importação de Dispositivo

O mapa de transformação de dispositivo Qualys é usado para transformar dados de dispositivo Qualys em registros de dispositivo. Isso é usado para atualizar os registros do dispositivo que seriam criados inicialmente a partir da importação de grupo de ativos. As mudanças nesta transformação alteram como os registros do dispositivo são atualizados com os detalhes do dispositivo.

Para acessar este mapa de transformação, navegue até **Integração de Vulnerabilidade da Qualys** > **Tabelas do conjunto de importação** > **Importação de Dispositivo**.

A tabela mostra os campos que estão sendo transformados no momento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação do dispositivo Qualys

Campo de origem	Campo de destino	Descrição
u_name	dispositivo_name	O nome do dispositivo scanner da Qualys.
u_status	dispositivo_status	O último status relatado do dispositivo scanner da Qualys.
u_id	dispositivo_id	O identificador do dispositivo Qualys.

Além dos mapeamentos de campo, também há um script de transformação que é executado durante o processo de transformação.

A tabela a seguir mostra quando este script é executado e para que ele é usado.

Tempo e finalidade do script do mapa de transformação do dispositivo Qualys

Quando o script é executado	Finalidade do script
onBefore (antes de um conjunto de importação concluir a transformação).	Usado para atualizar nomes e status de dispositivo para o ID fornecido. Para uso interno. Modificar ou excluir não é recomendado.

Mensagens REST da Qualys

As mensagens REST da Qualys são usadas para fazer chamadas para a API da Qualys.

A partir da versão 12.9.2 do Qualys, você tem a opção de escolher entre Autenticação básica ou OAuth. O parâmetro de instância do método Qualys Cloud Authentication é pré-configurado para Basic Auth. Se você preferir usar o OAuth, deverá modificar o parâmetro de instância de integração e configurar a mensagem REST diretamente para o OAuth.

Mensagem REST de detecção de host da Qualys

A mensagem REST de detecção de host da Qualys faz a chamada inicial para a API de detecção da lista de hosts para a integração de detecção de host da Qualys.

Parâmetros de mensagem REST de detecção de host da Qualys

Nome do parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório. As mudanças não são necessárias.
output_format	XML	Define o formato do relatório retornado pelo Qualys. Os vários scripts e transformações assumem XML, portanto, as mudanças no valor não são recomendadas.
detecção_processada_após	${lastScanDate}	Mostra somente detecções cujo status de detecção foi alterado após uma determinada data e hora. Para detecções que nunca foram alteradas, a data é aplicada à data da última detecção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de mensagem REST de detecção de host da Qualys

Nome do parâmetro	Valor	Descrição
truncation_limit	500	O número de hosts dos quais recuperar dados, de acordo com a solicitação. Este parâmetro é usado para fins de paginação. O valor padrão é 500, mas valores maiores ou menores podem ser usados. Não defina menos de 100, pois isso aumenta significativamente a carga do sistema. Valores menores exigem mais chamadas para a API do Qualys e valores maiores resultam em conjuntos de resultados maiores para processar e possíveis tempos limites de recuperação/processamento de dados.
status	Novo, Corrigido, Ativo, Reaberto	Status de detecção a serem recuperados do Qualys. O padrão é recuperar todos os status. Para extrações de dados grandes (geralmente a extração inicial de dados), pode ser útil excluir os status Fixo desta lista. É importante incluir o status Corrigido ao atualizar vulnerabilidades que já existem no sistema.

Mensagem REST de paginação de detecção de host da Qualys

A mensagem REST de paginação de detecção de host lida com solicitações de paginação para a API de detecção de host.

Quando a detecção do host primário é executada, se a API do Qualys fornece um URL para buscar a próxima página de dados, essa mensagem REST recupera esses dados adicionais. Esses dados são usados pelo Manipulador de Paginação de Detecção de Host.

REST de paginação de detecção de host é uma mensagem REST especializada e não deve ser modificada.

Mensagem REST da base de conhecimento da Qualys (preenchimento)

A mensagem REST da Base de conhecimento da Qualys (preenchimento) recupera os dados da base de conhecimento da Qualys com base no carimbo de data/hora da última modificação dos dados de vulnerabilidade para a integração da Base de conhecimento da Qualys.

As mudanças no registro do método de mensagem REST afetam a solicitação feita à Qualys para recuperar informações da base de conhecimento.

A tabela a seguir mostra os parâmetros de solicitação enviados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de mensagem REST da base de conhecimento da Qualys (preenchimento)

Parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação que está sendo solicitada. Parâmetro obrigatório. Mudanças não são recomendadas.
detalhes	Todos	Indica o nível de detalhe mostrado para as vulnerabilidades recuperadas. Seguro para modificar conforme necessário.
IDs	${qids}	Especifica quais QIDs serão recuperados do Qualys. Referenciado em código. Modificações não são recomendadas.

Mensagem REST da base de conhecimento da Qualys (baseada em data)

A mensagem REST da Base de conhecimento da Qualys (baseada em data) é usada para recuperar dados da base de conhecimento da Qualys com base no carimbo de data/hora da última modificação dos dados da vulnerabilidade. Esta mensagem é usada pela integração da Base de conhecimento da Qualys.

As mudanças no registro do método de mensagem REST afetam a solicitação feita à Qualys para recuperar informações da base de conhecimento.

A tabela a seguir mostra os parâmetros de solicitação enviados.

Parâmetros de mensagem REST da base de conhecimento da Qualys (baseada em data)

Campo de origem	Campo de destino	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório. Mudanças não são recomendadas.
detalhes	Todos	Indica o nível de detalhe mostrado para as vulnerabilidades recuperadas. Seguro para modificar conforme necessário.
last_modified_after	${dateStart}	Indica quando iniciar a recuperação de dados históricos. Usado pelo código para determinar a hora de início e para ajudar na paginação. Modificações ou remoção não são recomendadas.
last_modifiedbefore	${dateEnd}	Indica quando terminar a recuperação de dados históricos. Usado pelo código para determinar a hora de término e para ajudar na paginação. Modificações ou remoção não são recomendadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagem REST de tíquetes da Qualys

A mensagem REST de tíquetes da Qualys recupera informações do tíquete da Qualys para a integração do tíquete da Qualys. As mudanças no registro do método de mensagem REST afetam as solicitações feitas à Qualys para recuperar informações do tíquete.

A tabela mostra os parâmetros de solicitação enviados.

Parâmetros de mensagem REST de tíquetes da Qualys

Nome do parâmetro	Valor	Descrição
modificado_desde_data/hora	${lastRunDatetime}	Indica a data da última execução da integração e a data após a qual os dados serão extraídos. Usado por código. Mudanças não são recomendadas.
desde_ticket_number	${lastTicketNumber}	Indica qual tíquete foi recuperado pela última vez do Qualys. Usado para paginação. Mudanças não são recomendadas.
show_vuln_details	1	Indica se os detalhes da vulnerabilidade são recuperados.

Noções básicas sobre o Rapid7 Vulnerability Integration

O ServiceNow® Rapid7 Vulnerability Integration usa dados importados do data warehouse [Rapid7 ou dos produtos Rapid7 InsightVM para ajudar a determinar o impacto e a prioridade de ameaças potencialmente mal-intencionadas.

Os sensoresRapid7 Nexpose coletam dados e os enviam automaticamente para os produtos de data warehouse Rapid7 (no local) ou Rapid7 InsightVM (baseados em nuvem), que analisam e correlacionam continuamente as informações. Ele se integra facilmente com ServiceNow® Vulnerability Response para mapear vulnerabilidades para ICs e serviços. O Rapid7 Vulnerability Integration enriquece os dados de vulnerabilidade em sua instância.

Rapid7 integrações são pontos de entrada que interagem com o data warehouse [Rapid7 ou produtos Rapid7 InsightVM, invocados como trabalhos programados. Os trabalhos programados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades. Os trabalhos programados são executados automaticamente e na ordem especificada. Você também pode executar trabalhos programados individuais manualmente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Se você usar Rapid7 data warehouse e Rapid7 InsightVM como fontes para seus dados, você corre o risco de duplicar registros de vulnerabilidade.

Nota:
Ao migrar do tipo de integração de **Data Warehouse** para o tipo **InsightVM**, você pode desduplicar seus registros de data warehouse existentes. Para obter mais informações, consulte Desduplicar Rapid7 Vulnerability Integration registros de data warehouse.

Se você tiver várias implantações da integração de vulnerabilidade Rapid7 InsightVM, poderá adicionar uma integração para cada implantação. Os ativos, identificados por várias implantações de terceiros e suas vulnerabilidades, são consolidados e reconciliados com o seu CMDB. Essa consolidação acontece mesmo quando os processos de verificação se sobrepõem entre as várias implantações. Os dados provenientes de cada implantação são identificados e disponíveis em uma única instância de Vulnerability Response.

Nota:
Você não pode excluir a integração de vulnerabilidade original, mas pode desabilitá-la. As integrações criadas a partir de modelos desabilitados são desabilitadas por padrão.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Versões disponíveis

Versão de lançamento para Washington DC	Notas de versão
Rapid7 Vulnerability Integration v13.6, 13.7	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Funções

Rapid7 tarefas de integração de vulnerabilidade envolvem as funções a seguir.

- sn_vul_r7.admin: pode ler, gravar e excluir registros.
- sn_vul_r7.user: pode ler e gravar registros.
- sn_vul_r7.read: pode ler registros.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Rapid7 Vulnerability Integration

Para exibir o Rapid7 Vulnerability Integration, navegue até **Rapid7** > **Administração** > **Integrações**.

As integrações a seguir estão incluídas no sistema de base.

Rapid7 integrações de data warehouse

Integração	Descrição
Rapid7 Vulnerability Integration	Recupera dados de vulnerabilidade de Rapid7 Nexpose e os processa em sua instância.
Rapid7 Integração da lista de ativos	Recupera dados de verificação uma vez por semana do Rapid7 Nexpose data warehouse e os armazena no módulo Itens descobertos em sua instância. Ajuda a identificar ativos que não foram verificados recentemente usando a data **da última verificação**. Exiba a hora da **última verificação** na lista de itens descobertos em Vulnerability Response.
Rapid7 Integração de categoria	Recupera informações de categoria de Rapid7 Nexpose. As categorias fornecem classificação de alto nível para vulnerabilidades.
Rapid7 Explorar integração	Recupera informações de exploração de Rapid7 Nexpose.
Rapid7 Integração do kit de malware	Recupera informações do kit de malware de Rapid7 Nexpose.
Rapid7 Integração de referência	Recupera referências a documentos de autoridade externa, como CVEs ou referências de vulnerabilidade específicas do fornecedor.
Rapid7 Integração da Solução	Recupera dados da solução de Rapid7 Nexpose, que fornece soluções recomendadas para vulnerabilidades específicas.
Rapid7 Integração da solução de substituição	Recupera informações sobre quais soluções são substituídas por outras soluções.
Rapid7 Integração da solução de pré-requisito	Recupera informações sobre as soluções que são pré-requisitos para outras soluções. Quando esta integração é executada, ela busca o mapeamento de soluções e soluções de pré-requisito do data warehouse Rapid7. **Nota:** Esta integração funciona somente se o plug-in Solução de gerenciamento de vulnerabilidade estiver ativado.
Rapid7 Integração do mapa de solução de vulnerabilidade	Recupera o mapeamento para associar soluções a vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rapid7 integrações de data warehouse

Integração	Descrição
Rapid7 Integração de item vulnerável	Recupera dados de item vulnerável de Rapid7 Nexpose e os processa em sua instância. As saídas desta integração são itens vulneráveis.
Rapid7 Integração de resolução de item vulnerável	Recupera informações sobre quais itens vulneráveis estão marcados como encerrados em Rapid7 Nexpose e fecha os itens vulneráveis correspondentes em Vulnerability Response.
Rapid7 Integração de Site	Recupera dados do site de Rapid7 Nexpose. Um site é uma coleção de ativos direcionados para uma verificação.
Rapid7 Integração da lista de ativos	Recupera marcadores de host e dados de verificação uma vez por semana do data warehouse Rapid7 e os armazena no módulo Itens descobertos em sua instância. Ajuda a identificar ativos que não foram verificados recentemente usando a data **da última verificação**. Exibir a hora da **última verificação** na lista de itens descobertos em Vulnerability Response
Rapid7 Integração abrangente de item vulnerável	Importa todas as detecções do Rapid7 para todos os itens de configuração verificados desde a última execução de integração bem-sucedida. Com base nos dados importados mais atuais, os itens vulneráveis encontrados não recentemente durante as verificações são transferidos automaticamente para "Encerrado" quando o módulo Fechar automaticamente itens vulneráveis obsoletos está habilitado.

Integrações do Rapid7 InsightVM

Integração	Descrição
Rapid7 Integração de item vulnerável - API	Recupera dados de item vulnerável do Rapid7 InsightVM e os processa em sua instância.
Rapid7 Vulnerability Integration — API	Recupera dados de referência, categoria, exploração, kit de malware e vulnerabilidade do Rapid7 InsightVM e os processa em sua instância.
Rapid7 Integração da lista de ativos - API	Recupera marcadores de host e dados de verificação uma vez por semana de Rapid7 InsightVM e os armazena no módulo Itens descobertos em sua instância. Ajuda a identificar ativos que não foram verificados recentemente usando a data **da última verificação**. Exiba a hora da **última verificação** na lista de itens descobertos em Vulnerability Response.
Rapid7 Integração de item vulnerável abrangente - API	Importa todas as detecções do Rapid7 para todos os itens de configuração verificados desde a última execução de integração bem-sucedida. Com base nos dados importados mais atuais, os itens vulneráveis encontrados não recentemente durante as verificações são transferidos automaticamente para "Encerrado" quando o módulo Fechar automaticamente itens vulneráveis obsoletos está habilitado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Rapid7 InsightVM

Integração	Descrição
Rapid7 Integração de Site	Recupera dados do site do produto Rapid7 InsightVM. Esta integração está definida para ser executada semanalmente às 00:00:00.

Durante a importação, os registros CVE que ainda não estão presentes são criados como registros NVD e referenciados em entradas de terceiros para Rapid7 por padrão. A integração do modelo para Rapid7 não pode ser excluída. Em vez disso, desabilite-o.

O Conector do Service Graph para Rapid7

A partir da versão 2.0, o Conector do Service Graph para Rapid7 está disponível na ServiceNow® Store. Para obter mais informações, consulte Service Graph Connector for Rapid7 .

Regras de Pesquisa de IC

As Regras de Pesquisa de IC determinam como preencher o campo **Item de configuração** em um registro de item vulnerável.

Para obter mais informações sobre como funcionam as regras de pesquisa de IC, consulte Regras de pesquisa de IC para identificar itens de configuração de Vulnerability Response integrações de vulnerabilidade de terceiros.

Para criar ou editar regras de pesquisa, consulte Criar uma regra de pesquisa de IC do Vulnerability Response.

Nota:
As regras, depois de removidas, não podem ser recuperadas. Em vez de remover as regras existentes, desative-as ao criar novas.

Itens Descobertos

Este módulo lista os itens de configuração detectados durante a importação das Rapid7 Integrações de item vulnerável (armazém de dados ou API InsightVM) e a Rapid7 Integração da lista de ativos - API. A Rapid7 Integração da lista de ativos - API importa todos os ativos Rapid7 verificados quanto a vulnerabilidades desde a última execução da integração. A integração da lista de ativos do data warehouse Rapid7 está incluída.

Nota:
O filtro padrão desta lista é definido como **Incompatível**. Você pode exibir todos os itens descobertos de uma importação removendo o filtro.

Consulte Itens Descobertos em Vulnerability Response para obter mais informações sobre o módulo Itens descobertos.

Marcadores de host

Os marcadores de host são importados como parte da Rapid7 Integração da lista de ativos - integração de API para Rapid7 InsightVM. Eles são usados principalmente para filtragem em Vulnerability Response Regras de tarefa de atribuição e correção em Rapid7 InsightVM. Eles são exibidos no formulário Item descoberto.

Marcadores de host

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A integração Rapid7 Lista de ativos - integração de API deve ser executada antes da criação de Regras de atribuição ou de tarefa de correção em Vulnerability Response para que todos os marcadores possam estar presentes nas regras e antes que os itens vulneráveis sejam importados e agrupados.

- O armazenamento de marcador não faz distinção entre maiúsculas e minúsculas. Se um marcador **San Diego** for criado, um marcador **SAN DIEGO** não poderá ser armazenado na tabela de marcadores do host. "San Diego" e "SAN DIEGO" são considerados o mesmo marcador de host. Qualquer marcador que tenha sido importado primeiro vencerá.
- Usar marcadores de host como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. Os marcadores de host devem ser usados somente no Construtor de condição.
- Os marcadores de host são controlados pela propriedade do sistema global **sn_vul.import_host_tags**. Esta propriedade é definida como verdadeira por padrão. Desativar os marcadores os desativa em todas as instâncias.

Sites

Um site é uma coleção de ativos direcionados para uma verificação. Um site consiste em ativos de destino, um modelo de verificação, um ou mais mecanismos de verificação e outras configurações relacionadas à verificação, como programações ou alertas. Os sites são gerenciados por aplicações Rapid7.

Rapid7 Vulnerability Integration A filtragem de site durante a configuração permite categorizar e solicitar ativos por site durante a importação. Consulte Filtrar por Rapid7 sites para obter mais informações sobre como filtrar importações.

O data warehouse Rapid7 InsightVMRapid7 e as integrações de sites [] importam sites como um trabalho programado semanalmente.

Para exibir os sites importados em uma lista, navegue até **Rapid7** > **Sites**.

Reabrir itens vulneráveis resolvidos não encerrados por verificações

Itens vulneráveis definidos como "Resolvidos" em sua instância Now Platform, mas não transicionados para "Encerrado/Corrigido" pelas execuções de integração subsequentes, serão reabertos se forem detectados durante novas verificações.

Para Rapid7 detecções, agora está disponível uma opção na página de configuração do Rapid7 em sua instância para reabrir IVs resolvidos por idade. Se habilitado, os IVs definidos como "Resolvido", mas não transicionados para "Encerrado/Corrigido" pelas verificações subsequentes, retornam para "Aberto" após o número de dias inserido.

Criar ICs usando o Mecanismo de Identificação e Reconciliação (IRE)

Você pode usar o Mecanismo de Identificação e Reconciliação para criar novos ICs quando um IC existente não puder ser correspondido com um host importado de um scanner de terceiros. Habilite o plug-in CMDB CI Class Models para criar ICs usando as novas classes, caso contrário, ICs incompatíveis serão criados nas classes de IC incompatíveis. Para obter mais informações, consulte Criando ICs para Vulnerability Response usando o mecanismo de Identificação e Reconciliação. Para obter mais informações sobre como configurar a categorização de recursos de nuvem incompatíveis em sua classe de IC preferencial, consulte Atualizando classe de IC para ativos de nuvem incompatíveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verificar novamente itens vulneráveis

Inicie novas verificações na plataforma Rapid7 para verificar se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Consulte Iniciar nova verificação para a integração de vulnerabilidade Rapid7.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Rapid7 gestão de soluções

Se você ativou o plug-in Solução de gerenciamento de vulnerabilidade, as soluções Rapid7Rapid7 para o data warehouse [] e Rapid7 InsightVM] serão preenchidas na tabela Soluções de vulnerabilidade [sn_vul_solution]. No entanto, se você não ativou o plug-in Solução de gerenciamento de vulnerabilidade, o Rapid7 Vulnerability Integration funcionará como está e importará as soluções na tabela [sn_vul_r7_solution] personalizada. Para obter mais informações, consulte Rapid7 gestão de soluções.

Preparando para o Rapid7 Vulnerability Integration

Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. O Rapid7 Vulnerability Integration pressupõe que você esteja familiarizado com e execute Rapid7 data warehouse ou Rapid7 InsightVM verificações de produto em seu ambiente.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Os scanners Rapid7 são desativados por padrão na aplicação Vulnerability Response. Se você tentar executar uma nova verificação a partir dos itens vulneráveis ou das tarefas de correção que têm essas aplicações como origem, o botão **Verificar novamente** não estará disponível.

Antes de baixar a aplicação Rapid7 Vulnerability Integration do ServiceNow® Store e instalá-lo em sua instância, revise as seguintes informações sobre os tipos de integração e as informações de configuração:

Existem dois tipos de integrações incluídas com o Rapid7 Vulnerability Integration que está disponível no ServiceNow® Store:

- Rapid7 InsightVM
- Rapid7 data warehouse

O tipo de data warehouse Rapid7 :

- Requer sua Rapid7 URL do servidor de data warehouse e credenciais de autenticação
- Requer um MID Server
- Usa um driver PostgresSQL para executar consultas no data warehouse
- Não oferece suporte a várias instâncias

O tipo de integração Rapid7 InsightVM :

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- É baseado em nuvem e usa uma REST API. Esta integração requer uma chave de API de dentro da sua conta do Insight Rapid7.
- Oferece suporte a várias instâncias.

Consulte Configurar para a integração de data warehouse Rapid7 (data warehouse) e Configurar para a integração Rapid7 InsightVM para obter mais informações sobre os requisitos de configuração para esses tipos de integração.

Configurar para a integração de data warehouse Rapid7

A integração Rapid7 de data warehouse é um dos tipos de integração incluídos com o Rapid7 Vulnerability Integration Rapid7 Vulnerability Integration.

Antes de Iniciar

Antes de executar a integração de data warehouse Rapid7, conclua as seguintes tarefas de configuração:

- Obtenha o complemento de data warehouse Rapid7. Consulte o Rapid7 site e a documentação para adquirir e instalar este complemento.
- Obtenha o driver PostgresSQL mais atual. Vá para https://jdbc.postgresql.org/ e baixe o driver mais recente.
- Um MID Server para executar consultas ao data warehouse. Consulte MID Server para obter mais informações sobre como configurar um MID Server.

  Anote o nome do data warehouse. O tipo de integração de data warehouse Rapid7 oferece suporte somente a MID Servers autônomos. MID Servers em cluster não são compatíveis.

- Obtenha suas credenciais de autenticação e URL do servidor de data warehouse Rapid7 e deixe-as acessíveis.

Função necessária: o administrador do sistema [admin] baixa e instala o app. O sn_vul.vulnerability_admin ou sn_vul.admin supervisiona a configuração e verifica os resultados esperados.

Procedimento

1. Faça login na instância Now Platform na qual você deseja instalar a aplicação Rapid7 Vulnerability Integration.
2. Instale o arquivo JAR do PostgreSQL que você baixou nas tarefas de configuração listadas anteriormente.

   a. Em sua instância Now Platform, navegue até **Todos** > **MID Server** > **Arquivos JAR**.

   b. Clique em **Nova**.

   c. Insira o nome do driver PostgresSQL que você baixou anteriormente.

   Opcionalmente, insira as informações de **Versão**, **Origem**e **Descrição**. Deixe a caixa de seleção **Ativa** marcada.

   d. Anexe o arquivo JAR baixado usando o ícone de clipe de de papel no cabeçalho.

   e. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você concluiu a configuração da integração de data warehouse Rapid7. Se você não revisou os requisitos para a integração Rapid7 InsightVM, antes de instalar o Rapid7 Vulnerability Integration, consulte Configurar para a integração Rapid7 InsightVM e Preparando para o Rapid7 Vulnerability Integration.

Para obter as etapas para obter direitos, baixar e instalar o Rapid7 Vulnerability Integration, consulte Instalar o Rapid7 Vulnerability Integration.

Configurar para a integração Rapid7 InsightVM

A integração Rapid7 InsightVM é um dos tipos de integração incluídos com o Rapid7 Vulnerability Integration Rapid7 Vulnerability Integration.

Antes de Iniciar

Antes de executar a integração Rapid7 InsightVM, conclua as tarefas de configuração a seguir.

Função necessária: o administrador do sistema [admin] baixa e instala o app. O sn_vul.vulnerability_admin ou sn_vul.admin supervisiona a configuração e verifica os resultados esperados.

Procedimento

1. Para o tipo de integração Rapid7 InsightVM, tenha sua região e chave de API prontas.
   Entre em contato com Rapid7 para obter a região e a chave de API apropriadas.
   Você concluiu a configuração da integração Rapid7 InsightVM. Se você não revisou os requisitos para a integração de data warehouse Rapid7, antes de instalar o Rapid7 Vulnerability Integration, consulte Configurar para a integração de data warehouse Rapid7 e Preparando para o Rapid7 Vulnerability Integration.
2. Para obter as etapas para obter direitos, baixar e instalar o Rapid7 Vulnerability Integration, consulte Instalar o Rapid7 Vulnerability Integration.

Instalar o Rapid7 Vulnerability Integration

Depois de concluir as etapas de configuração da integração para que ela se integre corretamente a Vulnerability Response, obtenha direitos, baixe e instale a aplicação na sua instância Now Platform®.

Antes de Iniciar

Funções necessárias: administrador para download e instalação, sn_vuln.admin supervisiona a configuração e verifica os resultados esperados.

1. Consulte Preparando para o Rapid7 Vulnerability Integration, Configurar para a integração de data warehouse Rapid7 e Configurar para a integração Rapid7 InsightVM para obter mais informações sobre os tipos de integração e os requisitos de configuração para o Rapid7 Vulnerability Integration.
2. Conclua a check-list de configuração a seguir antes de baixar e instalar. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.
3. Depois que a aplicação for ativada, siga as etapas listadas abaixo para configurar o Rapid7 Vulnerability Integration.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
Verifique se a aplicação Vulnerability Response está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Vulnerability Response.
Verifique se você tem as funções Now Platform necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados. Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response. • O administrador do sistema [admin] instala o app. Se ainda não estiver atribuído, o administrador atribuirá a função de Administrador de vulnerabilidade [sn_vul.vulnerability_admin ou sn_vul.admin]. • O administrador de vulnerabilidades supervisiona a configuração e verifica os resultados esperados. A função de administrador Rapid7 é herdada quando você recebe uma função administrativa na aplicação Vulnerability Response (VR).
Valide o dimensionamento da instância com base no número de itens vulneráveis que você espera importar.	Uma instância subdimensionada pode levar a longos tempos de carregamento. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente.
Configurar filtragem	Use a filtragem para limitar o número de itens para importação inicial e fasear sua implantação ajustando os filtros nas importações subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
Desabilitar calculadoras de vulnerabilidade	Se você não usar calculadoras de vulnerabilidade, Desabilitar a calculadora de vulnerabilidade padrão se não for usada, além de quaisquer outras que você tenha definido. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é criado ou atualizado e podem afetar o desempenho da importação inicial.
Manter o valor padrão para executar como usuário	Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.
Usando marcadores de host	Se você planeja usar marcadores de host em Vulnerability Response Regras de atribuição ou de tarefa de correção, execute a integração da Lista de ativos Rapid7 antes de criar regras.
Desduplicar registros de dados existentes	Ao migrar do tipo de integração de **Data Warehouse** para o tipo **InsightVM**, você pode desduplicar seus registros de data warehouse existentes. Para obter mais informações, consulte Desduplicar Rapid7 Vulnerability Integration registros de data warehouse.

Procedimento

1. Faça login na instância na qual você deseja instalar a aplicação Rapid7 Vulnerability Integration.
2. Navegue até ServiceNow Store e faça login.
3. No ServiceNow Store, pesquise a aplicação Rapid7 Vulnerability Integration.

   Nota:
   No ServiceNow Store, a aplicação é chamada, Rapid7 Integration for Security Operations. Esta aplicação requer uma assinatura.

4. Clique no bloco da aplicação.
   Informações detalhadas sobre a aplicação que você está instalando são exibidas.

   Nota:
   Considere ler as seções **Outros requisitos** e **Dependências**, conforme aplicável.

5. Clique em **Solicitar app** e insira suas Now Support credenciais de login.
6. Clique **em Obter**.
7. Insira o **Nome da instância** e **o Motivo da instância**e clique em **Validar instância**.
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Em sua instância Now Platform, navegue até **Aplicações do sistema** > **Todas as aplicações** > **Todos**.
10. Localize a aplicação, selecione-a e clique em **Instalar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na caixa de diálogo Instalar, seu status de dependência é exibido. Se você precisar de uma aplicação de dependência, a aplicação necessária será exibida. Siga as instruções na caixa de diálogo para instalar a aplicação Rapid7 Vulnerability Integration em sua instância.

Nota:
O administrador de vulnerabilidades agora pode concluir a configuração da aplicação. Consulte Configurar o Rapid7 Vulnerability Integration.

Configurar o Rapid7 Vulnerability Integration

Configure o Rapid7 Vulnerability Integration depois que a aplicação for instalada e ativada em seu Now Platform®.

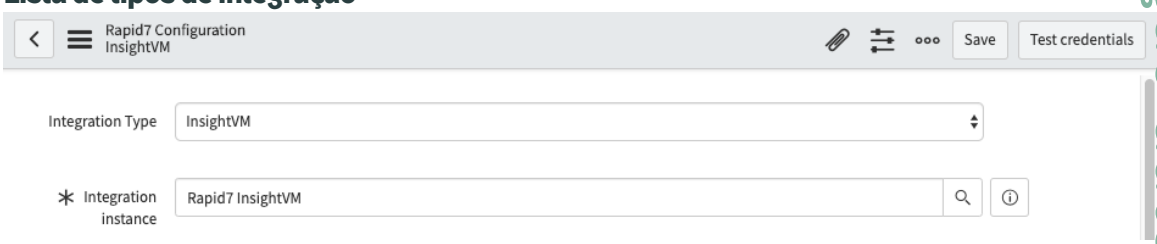
Antes de Iniciar

Função necessária: o administrador [admin] baixa e instala o app. O sn_vul.vulnerability_admin ou sn_vul.admin supervisiona a configuração e verifica os resultados esperados.

Procedimento

1. Depois que a aplicação for ativada (instalada), navegue até **Rapid7 Vulnerability Integration** > **Administração** > **Configuração**.
2. Selecione um tipo de integração na lista.

Lista de tipos de integração



3. Selecione uma instância de integração.
   A instância de integração padrão Rapid7 InsightVM é selecionada por padrão. Se esse for o tipo de integração desejado, siga estas etapas. Se você quiser configurar o tipo de integração de data warehouse Rapid7, prossiga para a etapa 4.

   a. Com a guia **Configuração de integração** selecionada no formulário exibido, preencha os campos:

Guia Configuração de integração para o tipo de integração do InsightVM

Campo	Descrição
Região do InsightVM	O URL do servidor que você adquiriu no site Rapid7.
Chave de API	A chave de API que você adquiriu da sua conta do Insight Rapid7.
Status de Validação	Somente leitura: status do processo de validação de credencial.

   b. Verifique a configuração bem-sucedida clicando em **Testar credenciais**.
   Se uma mensagem de erro for exibida durante a configuração, insira novamente seus dados.

   c. Após um teste bem-sucedido, clique em **Salvar**.

   d. Clique na guia **Importar configuração**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

No formulário exibido, preencha os campos.

Guia Importar configuração para InsightVM

Campo	Descrição
Pontuação mín. do CVSS	Pontuação mínima de CVSS de item vulnerável usada para filtrar itens vulneráveis durante a importação.
Pontuação máx. de CVSS	Pontuação máxima de CVSS de item vulnerável usada para filtrar itens vulneráveis durante a importação.
Filtro do site	Limita os dados aos Rapid7 InsightVM locais escolhidos na lista de locais. Consulte Filtrar por Rapid7 sites. Você pode escolher mais de um site. O padrão (vazio) traz todos os sites. Para preencher previamente a lista de sites, execute a API Rapid7 Site Integration - antes de definir este campo. Para obter informações sobre como usar a filtragem de site, consulte Filtrar por Rapid7 sites.
Criar entrada de CVE automaticamente	A propriedade do sistema para criar uma entrada CVE está ativa (verdadeiro) por padrão. Os espaços reservados do CVE serão criados automaticamente com a ingestão de conhecimento do Rapid7 se o ID do CVE não existir. Se você quiser que este recurso fique inativo, desative a propriedade [sn_vul_r7.create_cve_for_vulnerabilities] na lista Propriedades do sistema.
Reabrir resolvido por idade	Quando selecionados, os itens vulneráveis são reabertos automaticamente quando o número de dias em que eles foram resolvidos, mas não encerrados, corresponde ao valor exibido no campo **Reabrir resolvido após**.

e. Clique em **Salvar**.

Para várias implantações do tipo de integração Rapid7 InsightVM :

f. No campo **Instância de integração**, abra o de pesquisa da lista de pesquisa e selecione uma instância de integração existente ou clique em **Novo** no menu pop-up.

g. Em **Novo**, insira um **Nome** para a instância de integração e clique em **Enviar**.
O tipo de integração aparece no formulário de configuração Rapid7.

Nota:
Você pode excluir qualquer instância de integração, exceto a padrão. A exclusão de uma instância exclui o seguinte (exceto IVs):

- Integrações
- Parâmetros de instância
- Execuções de Integração
- Processos de integração
- A coluna de instância no IV está marcada como vazia

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

h. Verifique a configuração bem-sucedida clicando em **Testar credenciais**.

i. Após um teste bem-sucedido, clique em **Salvar**.

4. No campo Tipo de integração, expanda a lista e clique em **Data Warehouse**.

a. Selecione a guia **Configuração de integração**.

No formulário exibido, preencha os campos.

Guia Configuração de integração para o tipo de integração de data warehouse

Campo	Descrição
Nome da credencial JDBC	Nome das credenciais do seu data warehouse.
Nome de usuário	Nome de usuário do data warehouse Rapid7.
Senha	Senha do data warehouse da Rapid7.
Status de Validação	Somente leitura: status do processo de validação de credencial.
Detalhe da Validação	Somente leitura: somente data warehouse. Mostra informações adicionais sobre a verificação de validação depois que você clica em Testar credenciais pelo menos uma vez. Isso pode ser útil na depuração da sua configuração (por exemplo, validar se o seu MID Server está configurado incorretamente ou se você apenas tem as credenciais incorretas.
DNS/IP do servidor de banco de dados	DNS ou endereço IP do seu data warehouse.
Porta do banco de dados	Porta a ser usada para sua integração de data warehouse.
Nome do banco de dados	Nome do seu data warehouse.
Deslocamento de atraso de dados (Dias)	Os fatores de compensação de atraso de dados no atraso entre os dados em tempo real no scanner Rapid7 Nexpose e os dados no data warehouse.
MID Server	MID Server a ser usado. Somente servidores MID autônomos são compatíveis. MID Servers em cluster não são compatíveis.
Tempo limite do MID Server (mín.)	Número de minutos de espera para o MID Server responder antes de expirar a execução da integração.

b. Verifique a configuração bem-sucedida clicando em **Testar credenciais**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Após um teste bem-sucedido, clique em **Salvar**.

d. Clique na guia **Importar configuração**.

No formulário exibido, preencha os campos.

Guia Importar configuração para data warehouse

Campo	Descrição
Antes da v12.0: caixa de seleção Criar entrada de CVE	Quando marcados, os espaços reservados para CVEs, ainda não presentes, são criados como registros NVD e referenciados na entrada de terceiros para Rapid7. Quando desmarcados, esses CVEs são ignorados.
Pontuação mín. do CVSS	Pontuação mínima de CVSS de item vulnerável usada para filtrar itens vulneráveis durante a importação.
Pontuação máx. de CVSS	Pontuação máxima de CVSS de item vulnerável usada para filtrar itens vulneráveis durante a importação.
Filtro do site	Limita os dados de integração de sites importados aos sites escolhidos. Você pode escolher mais de um. **Nota:** Como a configuração padrão é importar dados de todos os sites, você não precisa usar o filtro se quiser todos os sites. Isso torna a solicitação mais lenta.
Reabrir resolvido por idade	Quando selecionados, os itens vulneráveis são reabertos automaticamente quando o número de dias em que eles foram resolvidos, mas não encerrados, corresponde ao valor exibido no campo **Reabrir resolvido após**.

5. Clique em **Salvar**.

6. Opcional: Se você quiser definir uma data de início na Rapid7 Integração de vulnerabilidade - API e Integração de item vulnerável Rapid7 - registros de integração de API para recuperar dados históricos durante a importação inicial da verificação Rapid7, siga estas etapas.
Você pode usar esses dados para ajudá-lo com Fechando detecções obsoletas em Vulnerability Response.

a. Navegar até **Rapid7 Vulnerability Integration** > **Administração** > **Integrações**.
A lista de integrações Rapid7 é exibida.

b. Clique em um dos registros de integração para abri-lo.

(Optional) Próximo à parte superior do formulário, clique no link **aqui** para editar o registro.

O campo **Importar desde** a data nas integrações Rapid7 está em branco, por padrão, exceto para a Integração de vulnerabilidade Rapid7 - API e a Integração de item vulnerável Rapid7 - API. Para essas integrações, esses campos são definidos como 31/12/1998 ou 01/01/1999.

Para recuperar dados históricos durante a importação inicial da verificação Rapid7, defina uma data de início nos registros de integração apropriados. Este processo funciona para qualquer integração Rapid7 com as seguintes exceções:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- As integrações de Exploit e Malware Kit Rapid7 não mostram o campo **Importar desde** porque elas não fazem atualizações delta e, portanto, não usam esse campo.
- A integração Rapid7 Lista de ativos ignora o campo, já que sua intenção é recuperar todos os dados.
- Para a execução inicial da Rapid7 InsightVM Integração de item vulnerável abrangente - API quando o módulo Fechar automaticamente itens vulneráveis obsoletos estiver habilitado e o campo **Importar desde** estiver em branco.

  Ao habilitar o recurso de fechamento automático, é necessária uma execução bem-sucedida da Integração de item vulnerável abrangente do Rapid7 ou da Integração de item vulnerável do Rapid7 - API. Essas integrações estão desabilitadas por padrão.

  Ao habilitar a Rapid7 InsightVM Integração de item vulnerável abrangente - API, se você deixar o campo **Importar desde** em branco na página de configuração da integração, o valor no campo **dias atrás** do formulário Fechar automaticamente itens vulneráveis obsoletos também será usado para a **Importação desde** data na primeira execução de integração. O valor padrão para itens vulneráveis obsoletos de fechamento automático é (90 dias).

  Por exemplo, se o campo **dias atrás** no formulário Fechar automaticamente itens vulneráveis obsoletos for 90 e o campo **Importar desde** na página Integração abrangente de item vulnerável do Rapid7 - Configuração da API estiver em branco, a primeira execução de integração importará os dados dos últimos 90 dias.

  Esse relacionamento entre os campos **Importar desde** e **dias atrás** se aplica somente à primeira execução de integração. Depois disso, alterar o campo **dias atrás** no formulário Fechar automaticamente itens vulneráveis obsoletos não afeta o campo **Importar desde** na página de configuração da API Integração abrangente de item vulnerável da Rapid7. O campo é alterado para a hora de início da primeira execução para que as execuções de integração subsequentes importem somente as informações delta

  O campo **Importar desde** é editável e você pode inserir os valores desejados para cada uma das integrações.

7. Navegar até **Todos** > **sn_sec_int_impl.list** > **Rapid7 InsightVM**.

a. O parâmetro de instância de integração **import_startime_buffer_compreensivo** define um tempo de buffer de 24 horas antes da hora especificada no campo **Importar desde** para que os ativos que são verificados a partir desse tempo de buffer sejam obtidos durante a execução da **Integração de item vulnerável abrangente Rapid7 - integração de API**.
Você pode modificar este tempo de buffer de acordo com seus requisitos.

b. **Opcional:** Defina o parâmetro **close_stale_detections** como *verdadeiro* para fechar as detecções obsoletas que não estão mais chegando por meio da API Rapid7 para os ativos que são verificados e recuperados por meio da API Rapid7 por meio da API **Rapid7 Integração de item vulnerável abrangente**.

Você concluiu com sucesso as etapas de instalação e configuração do Rapid7 Vulnerability Integration. Agora você está pronto para revisar e verificar os dados importados.

O que Fazer Depois

Os scanners Rapid7 e Qualys são desativados por padrão na aplicação Vulnerability Response. Se você tentar executar uma nova verificação a partir dos itens vulneráveis ou das tarefas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de correção que têm essas aplicações como origem, o botão **Verificar novamente** não estará disponível.

Para ativar esses scanners, como um usuário com a função sn_vul.vulnerability_admin:

1. Navegar até **Todos** > **Vulnerability Response** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o scanner que você deseja ativar e clique no registro para abri-lo.
3. Marque a caixa de seleção Ativo.
4. Clique em **Atualizar**.

   O produto que você ativou é exibido no campo Origem no item vulnerável e nos registros de tarefa de correção após a próxima importação, e a **opção Nova verificação** está disponível como uma ação de IU.

Se o seu ambiente requer importações separadas por domínio, consulte Criar importações separadas por domínio para uma integração.

Para criar ou refinar suas regras de pesquisa antes da importação, consulte Criar uma regra de pesquisa de IC do Vulnerability Response.

Filtrar por Rapid7 sites

Filtre por site para tipos de integração Rapid7 InsightVM bem como Rapid7 Nexpose tipos de integração de data warehouse.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Nota:
O uso de filtragem de site pode afetar o desempenho. Para obter informações sobre desempenho e outras considerações antes de usar a filtragem de site, consulte KB0789221 .

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Navegar até **Todos** > **Rapid7 Vulnerability Integration** > **Configuração**.
2. Selecione uma instância de integração.
3. Clique na guia **Importar configuração**.

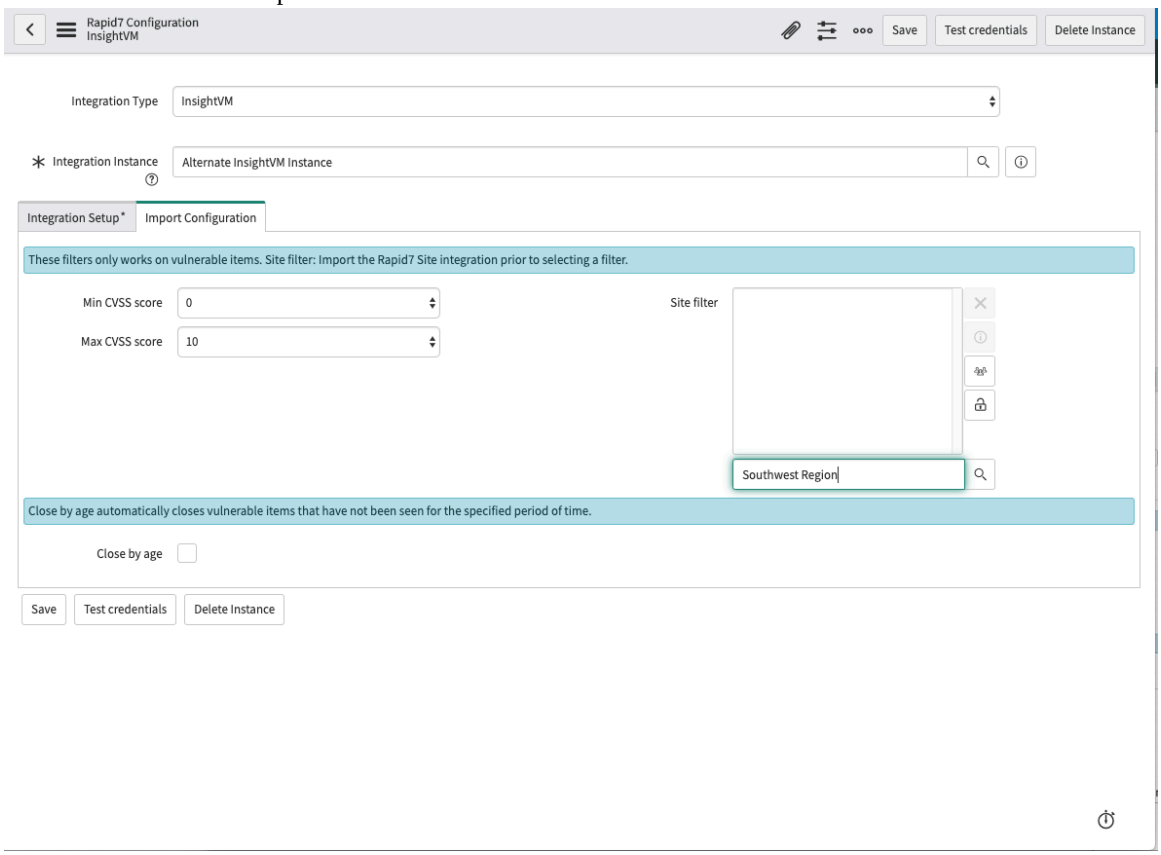
Nota:
Se você quiser todos os sites, deixe o campo de filtro de site em branco. Nenhum filtro de site é equivalente à adição de todos os sites.

Os sites são específicos da instância de integração. A lista de pesquisa para filtragem de site exibe sites de instância de integração de data warehouse Rapid7 InsightVM e Rapid7 Nexpose. Verifique se o site escolhido corresponde à instância de integração selecionada. Por exemplo, se você escolher um site de data warehouse, por engano, esse site não funcionará para filtragem de site por Rapid7 InsightVM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique na lista de pesquisa para exibir os registros do site da instância de integração atual.
5. Adicione um site da lista para adicionar ao filtro de site.



6. Repita a seleção para adicionar locais adicionais.
7. Clique em **Salvar**.
   Esses sites são usados para filtrar por site durante a próxima importação. Consulte Acrescentar SITE aos marcadores do site Rapid7 InsightVM para obter informações sobre como adicionar o prefixo SITE aos dados do seu site.

Acrescentar SITE aos marcadores do site Rapid7 InsightVM

Adicione o prefixo SITE aos marcadores do site Rapid7 InsightVM para destacá-los na lista de marcadores.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Nota:
Se necessário, alterne seu escopo para a Integração Rapid7 para Security Operations.

Procedimento

1. Na caixa de navegação à esquerda, digite: `sys_properties.list`.
2. Em **Nome**, pesquise por: `sn_vul_r7.prefix_site_to_rapid7_tags`.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Abra o *sn_vul_r7.prefix_site_to_rapid7_tags*.
4. Altere o **valor** para **verdadeiro**.
5. Clique em **Atualizar**.
   Marcadores de site novos e existentes serão prefixados durante a próxima importação de Rapid7 InsightVM.

Desduplicar Rapid7 Vulnerability Integration registros de data warehouse

Ao migrar para o tipo de integração **InsightVM** do tipo de integração de **Data Warehouse**, você pode desduplicar itens vulneráveis de data warehouse existentes, desde que eles pertençam à mesma origem de dados que seus dados Rapid7 InsightVM.

Antes de Iniciar

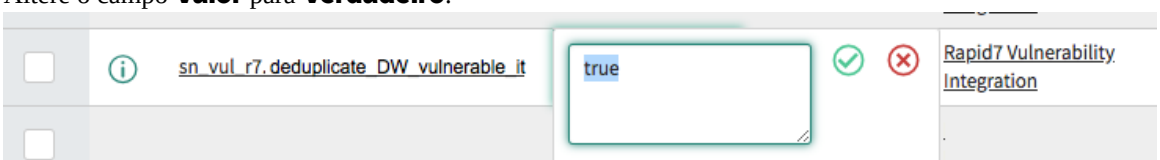
Função necessária: sn_vul_r7.admin ou, sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)
Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa

Esta desduplicação funciona somente ao migrar do data warehouse [Rapid7 Nexpose para a integração de item vulnerável Rapid7 InsightVM.

Procedimento

1. Navegar até **Todos** > **Rápido 7** > **Integrações**.
2. Defina todas as Rapid7 Nexpose configurações de coluna **ativas** de integrações de data warehouse como **Falso**, desabilitando as integrações.
3. Insira sys_properties.list no painel de navegação esquerdo.
4. Pesquise o **Nome**: sn_vul_r7.deduplicate_DW_vulnerable_item.
5. Altere o campo **Valor** para **Verdadeiro**.



6. Clique no ícone de marca de seleção .
   Durante a próxima Rapid7 InsightVM importação de integração de item vulnerável, qualquer correspondência com registros de data warehouse existentes impede a criação de um item vulnerável duplicado.

Rapid7 Vulnerability Integration gráfico de status de execução

Os sensoresRapid7 Nexpose coletam os dados e os enviam automaticamente para os produtos Rapid7 Nexpose ou Rapid7 InsightVM, que analisam e correlacionam continuamente as informações.

Visualizações de dados nos espaços Vulnerability Response

Os espaços Vulnerability Response incluem visualizações de dados que podem ajudar a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a severidade das vulnerabilidades ativas que são

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

importantes para sua organização em visualizações de dados dinâmicos que são atualizadas conforme os dados de vulnerabilidade mudam. Consulte Vulnerability Response Espaços, Espaço para gerentes de vulnerabilidades e Explorando o Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos que estão disponíveis.

Rapid7 Vulnerability Integration funciona facilmente com Vulnerability Response para mapear vulnerabilidades para ICs e serviços de negócios para determinar o impacto e a prioridade de ameaças potencialmente mal-intencionadas. O módulo Status de execução Rapid7 Vulnerability Integration é uma exibição gráfica do status de Rapid7 Vulnerability Integration execuções.

Para exibir esses dados na exibição legada, navegue até **Todos** > **Todas as integrações de vulnerabilidade da Rapid7** > **Status da Execução da Integração**.

A partir da versão 19.0 do Vulnerability Response, este painel está disponível na IU da nova experiência.

Nota:
Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Versões anteriores de Vulnerability Response

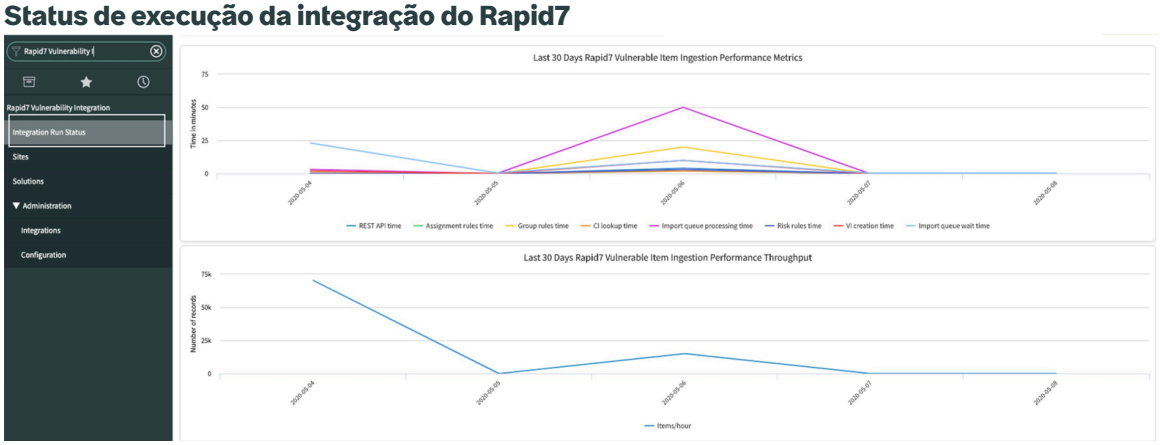
No gráfico, aponte para qualquer parte (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Vários fatores podem afetar o desempenho da execução da integração, como a quantidade de dados e o tempo necessário para processar esses dados. Dois novos gráficos foram adicionados para comparar as métricas de desempenho:

- Rapid7 Métricas de desempenho de ingestão de item vulnerável: compare as métricas de desempenho diárias para regras de atribuição, regras de grupo, regras de risco, tempo de espera da fila, tempo de processamento da fila e outras estatísticas de itens vulneráveis nos últimos 30 dias para identificar a causa de quaisquer desvios no desempenho.
- Rapid7 Rendimento de desempenho de ingestão de item vulnerável: compare o rendimento de ingestão de item vulnerável diário para a Rapid7 Integração de item vulnerável - API. O rendimento é medido em itens por hora.

Nota:
Em Rapid7, esses gráficos são compatíveis somente com a integração do Insight VM.

Status de execução da integração do Rapid7



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Gráfico de status de execução de amostra Rapid7 Vulnerability Integration

- O valor na coluna Itens importados representa o número total de itens vulneráveis que são criados a partir de uma execução de integração.
- A coluna Novos itens exibe o número de itens vulneráveis criados a partir de uma execução de integração.
- A coluna Itens duplicados não está mais preenchida. Você pode preferir remover esta coluna da exibição.
- A coluna Itens atualizados exibe o número de vezes que os itens vulneráveis são atualizados durante uma execução de integração. Este valor não é o número de itens vulneráveis exclusivos que são atualizados. Se, por exemplo, um item vulnerável for atualizado duas vezes durante a execução da integração, ele será contado duas vezes e exibido como dois itens atualizados.
- A coluna Itens inalterados exibe itens vulneráveis encontrados durante a execução da integração que já existem no banco de dados, mas não foram atualizados porque nenhum dos valores de campo relevantes foi alterado.

Nota:
A integração é executada com resultados zero para todos os quatro valores a seguir: **Novos ICs**, **ICs existentes**, **Novos itens**e **Itens atualizados** são filtrados da lista de execuções de **integração do Rapid7**.

Rapid7 Vulnerability Integration executar relatórios de gráfico de status

Nome	Descrição
Resultados dos últimos 30 dias Rapid7	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Executar em um visual de barra.
Últimos 30 dias Rapid7 Novos IVs	O número de novos itens vulneráveis importados nos últimos 30 dias. Mostrado como um número inteiro.
IVs atualizados nos últimos 30 dias Rapid7	O número de itens vulneráveis atualizados importados nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Rapid7 Duplicatas	O número de itens vulneráveis duplicados importados nos últimos 30 dias. Mostrado como um número inteiro.
Rapid7 Execuções de integração	Os registros de execução de integração em uma lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rapid7 Vulnerability Integration executar relatórios de gráfico de status

Nome	Descrição
	Nota: **V16.1:** para verificar as detecções para esta integração, compare as detecções ou descobertas com os dados de detecção ServiceNow`sn_vul_detection`] na tabela . Enquanto a integração está em andamento, pode haver uma mudança na detecção ou na contagem de descobertas. Este relatório exibe a contagem de detecções na coluna "Contagem até a data" na instância, após a conclusão da execução da integração.
Últimos 30 dias Rapid7 Métricas de desempenho de ingestão de item vulnerável	Métricas de desempenho diárias para itens vulneráveis comparadas nos últimos 30 dias.
Últimos 30 dias Rapid7 Rendimento do desempenho de ingestão de item vulnerável	Rendimento diário de ingestão de item vulnerável para a Rapid7 Integração de item vulnerável - API medido nos últimos 30 dias.

Exibir o painel de status de execuções de importação Rapid7 Vulnerability Integration

Use o painel de status de execução de importação de vulnerabilidade Rapid7 para verificar o sucesso de suas execuções de integração, localizar problemas e informar suas decisões de correção.

Antes de Iniciar

Funções necessárias: sn_vuln.admin

Por Que e Quando Desempenhar Esta Tarefa

Este procedimento faz as seguintes suposições.

- Você tem Vulnerability Response e o Rapid7 Vulnerability Integration instalados e configurados.
- Rapid7 Vulnerability Integration importações estão programadas e em execução.
- Rapid7 gráficos de status de execução de integração estão em uso.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 19.0 do Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Rapid7** > **Status da Execução da Integração**.

   A partir da versão 19.0 do Vulnerability Response, este painel está disponível na IU da nova experiência.

   Nota:
   Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

2. Se você não estiver usando o gráfico de status de execução de integração Rapid7, navegue até **Rapid7** > **Integrações**.
   a. Escolha uma integração.
   b. Clique na lista relacionada **Execuções de integração de vulnerabilidade**.
3. Verifique se todas as importações foram bem-sucedidas.

   Trouble?

   As causas mais comuns para uma execução com falha:

   - Interrupção de rede
   - Deterioração de bits na transferência de dados, resultando em dados corrompidos durante a transformação

   Para todas essas condições, clique em **Executar agora** e execute novamente a integração.

Iniciar nova verificação para a integração de vulnerabilidade Rapid7

Inicie novas verificações na plataforma Rapid7 para verificar se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados.

Antes de Iniciar

Nota:
Não há suporte para novas verificações de Rapid7 itens vulneráveis de data warehouse.

Você pode iniciar novas verificações nos espaços do Vulnerability Response. Para obter mais informações, consulte Verificar novamente registros e tarefas de correção no Vulnerability Manager Workspace e Verifique novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI.

Funções necessárias: Funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Para novas verificações no ambiente clássico, consulte as seções a seguir.

Novas verificações são compatíveis. Você pode iniciar uma nova verificação sob demanda para itens vulneráveis importados de Rapid7 InsightVM integrações de sua instância Now Platform®.

Nota:
O scanner Rapid7 está desabilitado por padrão na aplicação Vulnerability Response. Se você tentar executar uma nova verificação dos itens vulneráveis ou das tarefas de correção que têm a aplicação Rapid7 como origem, o botão Verificar novamente não estará disponível.

Para ajudar a reduzir a sobrecarga e o volume envolvidos nas verificações completas programadas, os proprietários de correção, especialistas em TI, analistas de vulnerabilidade ou gerentes de vulnerabilidade podem iniciar novas verificações direcionadas sob demanda para vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas verificações de item vulnerável (IV), tarefas de correção (RT), entrada de terceiros (TPE) ou registros de item descoberto da sua instância Now Platform®.

As novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

Por exemplo, todo o ambiente é verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada de seus Now Platform para Rapid7 itens vulneráveis. Você pode exibir resultados atualizados em seus itens vulneráveis com a próxima importação programada de Rapid7 InsightVM Integrações de vulnerabilidade e item vulnerável.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Itens vulneráveis**.
2. Localize o registro do item vulnerável do qual você deseja acionar uma nova verificação e abra-o.

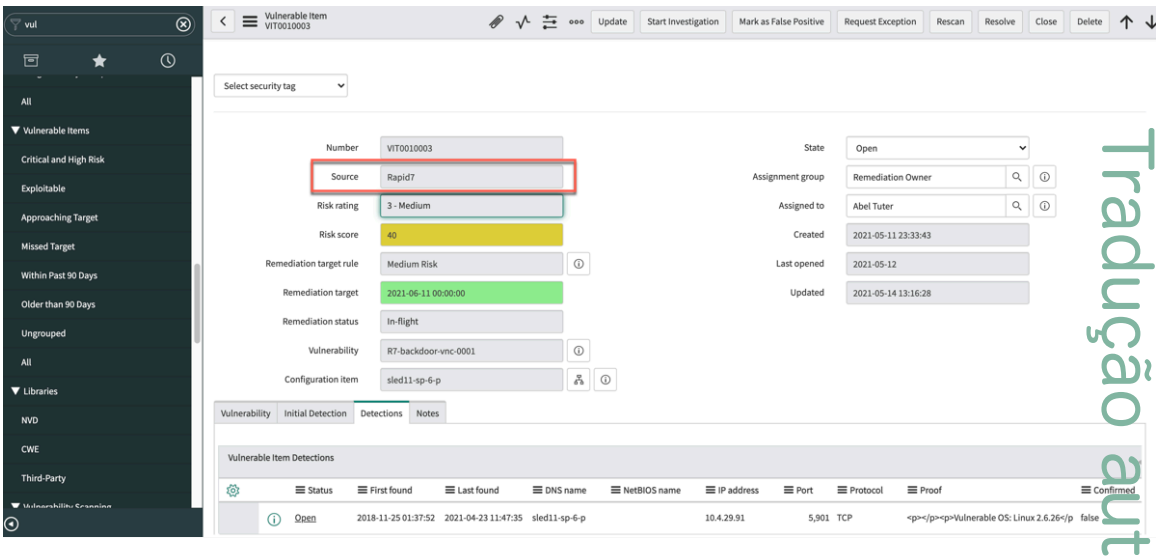
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Inicie novas verificações de IVs com Rapid7 como origem. Verifique se Rapid7 é exibido na coluna **Origem** nas exibições de Lista de IV ou nos campos **Origem** em registros individuais. Você pode usar o construtor de condição para agrupar IVs por origem. Ou, se a coluna **Origem** não for exibida na exibição Lista de IVs, no canto superior esquerdo da lista, clique no ícone de engrenagem e mova a **Origem** de **Disponível** para **Selecionado**.

Ao iniciar novas verificações, evite acionar simultaneamente verificações para um ID de origem de várias origens. A solicitação de verificação mais recente apresentará erro.

Por exemplo, se você iniciar uma nova verificação para um IV de um registro de IV e também solicitar outra nova verificação de um registro de tarefa de correção que contém esse mesmo IV, é provável que a segunda solicitação falhe.



3. Como alternativa, navegue até **Vulnerability Response** > **Tarefas de correção** ou **Vulnerability Response** > **Bibliotecas** > **terceiro** para a tarefa de correção ou registros de entrada de terceiros, respectivamente, que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o botão **Verificar novamente** está disponível nos seguintes registros:

   - Em um único registro de IV, o IV deve ser do produto Rapid7 e em qualquer estado diferente de Encerrado. Para vários registros de IV, todos os IVs selecionados na exibição de lista devem ser do produto Rapid7 e em qualquer estado diferente de Encerrado.
   - Em um registro de tarefa de correção, a tarefa de correção pode estar em qualquer estado diferente de Encerrado e todos os IVs associados devem ser do produto Rapid7.
   - Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro IV associado do produto Rapid7 em qualquer estado diferente de Encerrado.
   - Em um registro de item descoberto, o IV deve ser do produto Rapid7 e em qualquer estado diferente de **Encerrado**.

4. No canto superior direito do registro, clique em **Verificar novamente**.
   Para exibições de lista, selecione os IVs na lista que você deseja verificar novamente e, na lista **Ação nas linhas selecionadas**, selecione **Verificar novamente**.

5. No pop-up exibido, confirme a nova verificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

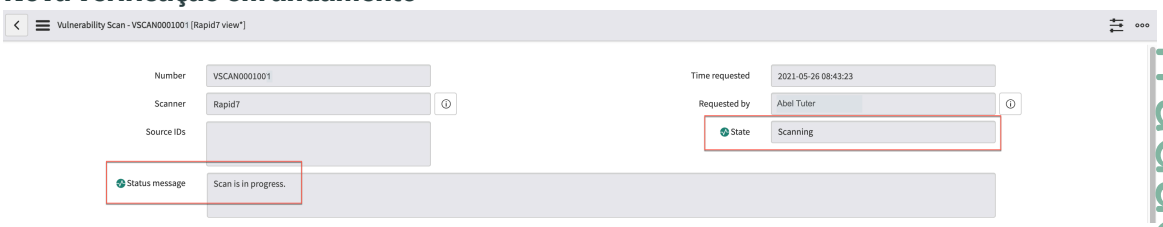
Uma mensagem será exibida indicando que a verificação está sendo processada (**Em fila**). Na mensagem, clique no link **Exibir detalhes** para verificar o status da nova verificação (verificação secundária) e exibir outras verificações iniciadas a partir do registro. O status de todas as novas verificações pode ser encontrado a qualquer momento na lista relacionada Verificações na parte inferior do IV, da tarefa de correção, do TPE e dos registros de item descoberto que você usa para iniciar as novas verificações.

Quando a verificação está em andamento, o campo Estado muda para **Verificando**e o campo Mensagem de status exibe **A verificação está em andamento**.

Nota:
Cada nova verificação oferece suporte a 500 ativos por verificação. Se sua solicitação tiver mais de 500 ativos, mais verificações secundárias serão solicitadas.

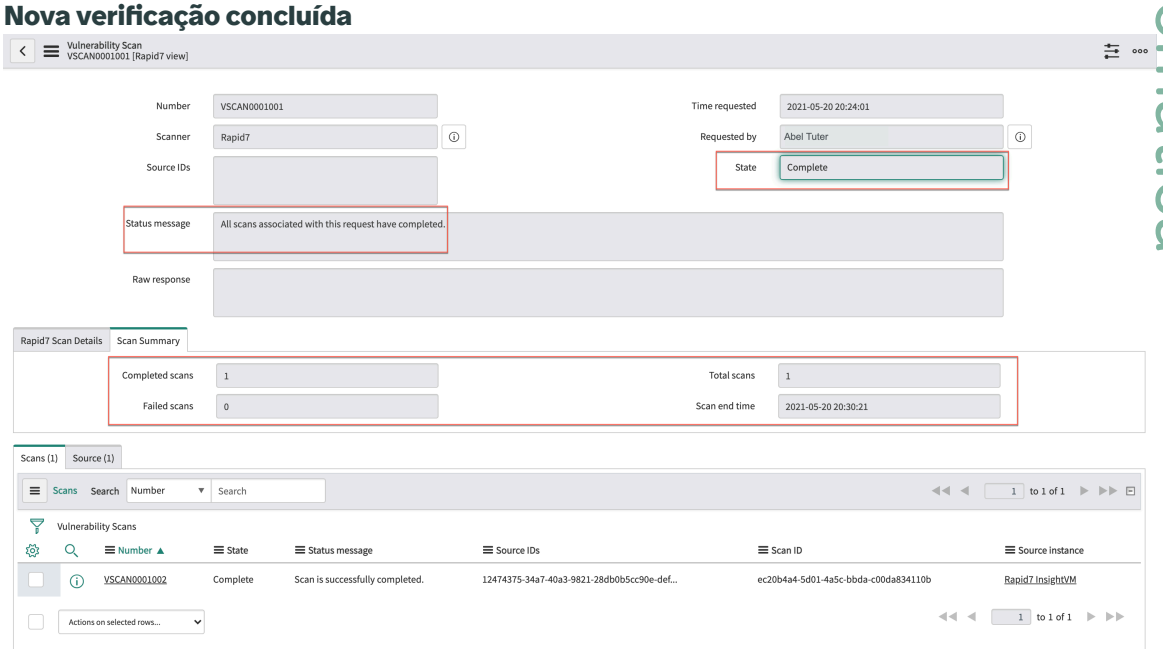
Sua instância Now Platform® rastreia o status de nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro.

Nova verificação em andamento



O tempo limite não interrompe a verificação. O tempo limite se refere a quando Now Platform® parou de acompanhar seu status de nova verificação, não quando a nova verificação real parou. Todos os IVs que fizeram a transição ou farão a transição para Encerrado/Corrigido são importados com a próxima importação programada das integrações Rapid7.

Nova verificação concluída



Como alternativa, você pode iniciar uma nova verificação sob demanda para uma vulnerabilidade específica em um ativo específico. Você pode exibir os resultados dessas verificações depois que a verificação for concluída no IV atualizado, na tarefa de correção, no TPE e nos registros de item descobertos a partir dos quais você iniciou a verificação.

Tradução automática

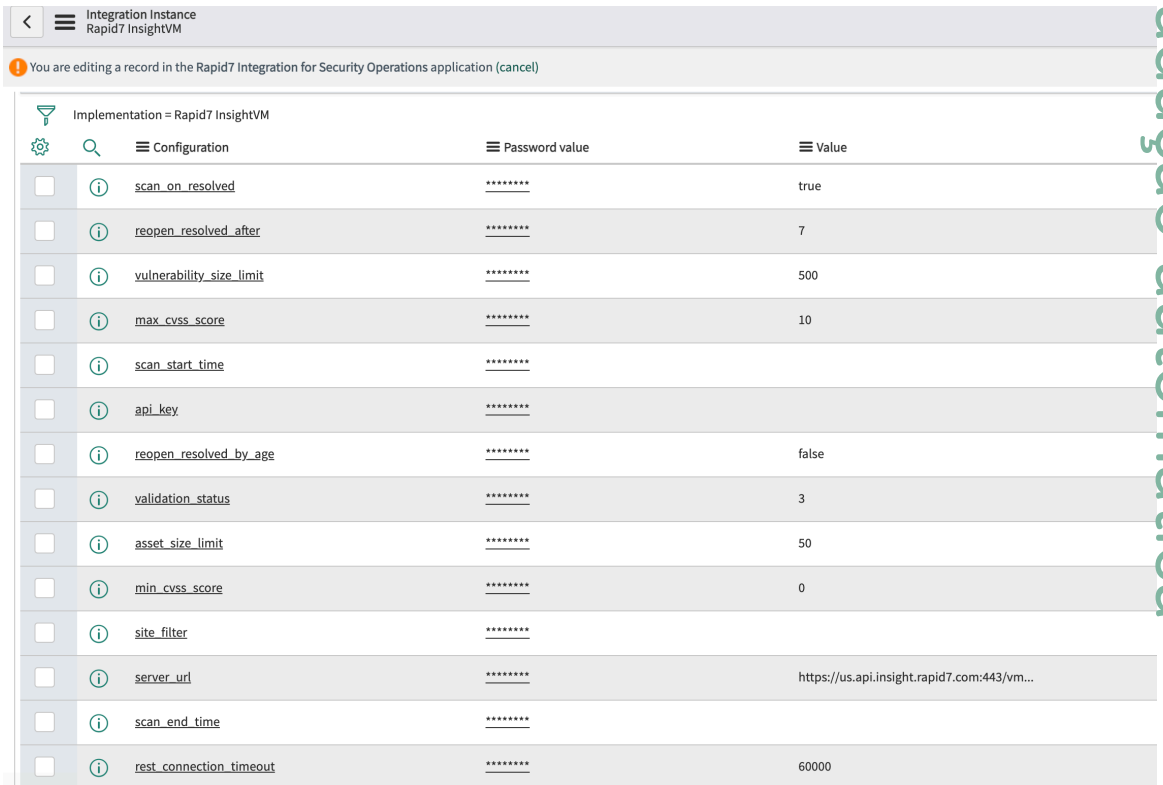
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O valor do campo Estado nos registros de verificação de vulnerabilidade é importado de Rapid7. Quando a verificação é concluída com sucesso, o estado é definido como Concluído. Se a verificação não for concluída com sucesso, um valor de erro será exibido.

Verificações automáticas e programadas

Como gerente ou analista de vulnerabilidade, você pode especificar e programar quando as novas verificações são iniciadas para IVs e RTs. Você também pode habilitar verificações automáticas para IVs e tarefas de correção que estão definidas para resolver.

6. Para modificar os parâmetros de integração na instância de integração, navegue até **Rapid7 Vulnerability Integration** > **Administração** > **Configuração**.
7. No registro de Configuração do Rapid7, se não estiver selecionado, na lista **Tipo de integração**, selecione **Rapid7 InsightVM**.
8. À direita do campo **Instância de integração**, clique no ícone de informações e em **Abrir registro**.
9. No registro Integration Instance Rapid7 InsightVM, localize os parâmetros para programar verificações e edite conforme necessário.



scan_on_resolved indica se a verificação é iniciada quando uma vulnerabilidade é resolvida. O padrão é **falso** (desabilitado).

Se este parâmetro for definido como `verdadeiro`, sempre que um IV ou RT for definido como Resolvido, o fluxo de trabalho para verificar novamente o respectivo IV e a tarefa de correção será acionado automaticamente.

scan_start_time

Defina a hora de início da verificação em **HH:mm** (formato de 24 horas) no fuso horário UTC para a hora de início da janela em que você deseja novas verificações disponíveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O valor padrão é 00:00.

scan_end_time

Defina a hora de término da verificação em **HH:mm** (formato de 24 horas) no fuso horário UTC para a hora de término da janela de verificação disponível.

O valor padrão é 23:59.

Se uma verificação for iniciada dentro da janela de tempo programada, ela será iniciada instantaneamente. Se a verificação for iniciada fora da janela, ela será enfileirada para a próxima janela programada.

Por exemplo, se você inserir uma hora de início de 00:00 para o parâmetro *scan_start_time* e um *scan_end_time* de 10:00 da mesma manhã, as verificações programadas ou iniciadas manualmente fora da janela de tempo da meia-noite às 10h serão enfileiradas e iniciadas na hora de início da janela de tempo do dia seguinte 00:00.

No mesmo exemplo, se você iniciar manualmente uma nova verificação às 11h, a nova verificação não será iniciada imediatamente, pois está fora dos horários de verificação configurados disponíveis. A solicitação de verificação permanece na fila até o início da janela de tempo do dia seguinte, neste exemplo 00:00.

Definir parâmetros de filtro adicionais para importações de Rapid7 InsightVM

Personalize os parâmetros de filtragem das consultas programadas com Integração Rapid7 para Security Operations para ajudar a refinar ainda mais os dados de vulnerabilidade importados com o produto Rapid7 InsightVM.

Antes de Iniciar

Casos de uso: como gerente ou analista de vulnerabilidade, convém filtrar os dados de suas consultas para que você possa revisar somente os detalhes específicos da vulnerabilidade. Por exemplo, talvez você queira exibir somente vulnerabilidades importadas que sejam Críticas e Graves.

Para ajudá-lo a coletar esses dados, adicione parâmetros Rapid7 para ajudá-lo a importar os detalhes da vulnerabilidade específica de que precisa.

Sem adicionar chamadas de API ou codificação adicionais, a partir da v13.4, o recurso permite que você personalize suas informações de solicitação HTTP com parâmetros Rapid7 InsightVM em seu Now Platform. As seguintes integrações Rapid7 InsightVM oferecem suporte à filtragem adicionando conteúdo JSON ao corpo da solicitação:

- Rapid7 InsightVM API de integração de item vulnerável
- Rapid7 InsightVM API de integração de vulnerabilidade
- Rapid7 InsightVM

Você deve saber como usar cadeias de caracteres JSON para este recurso.

Função necessária: sn_vul.vulnerability_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

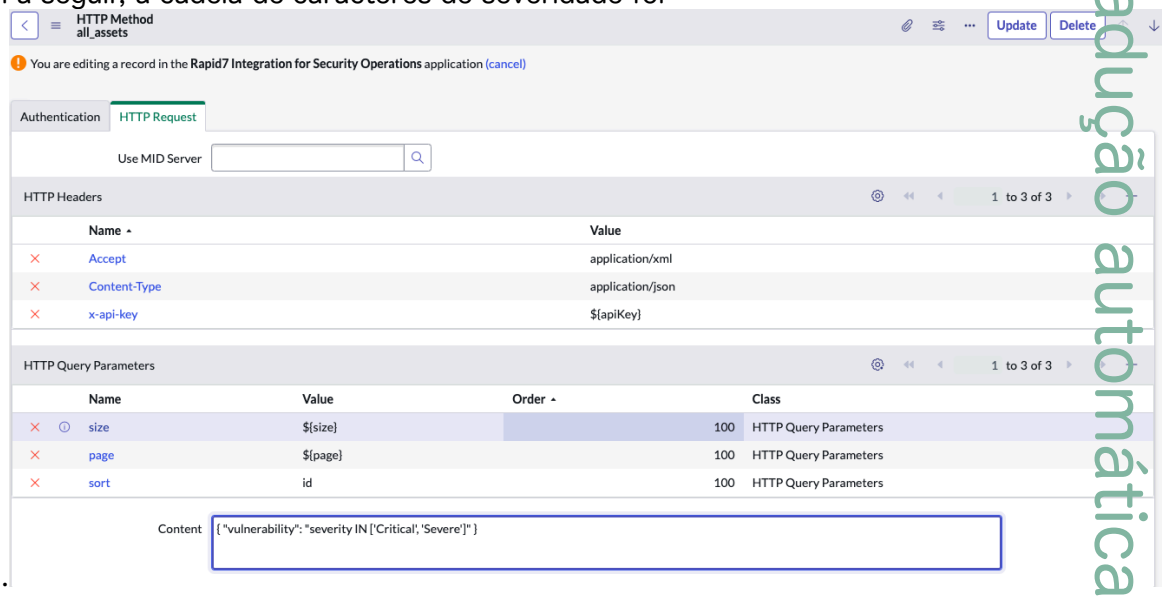
Procedimento

1. Localize os parâmetros compatíveis com o produto [Rapid7 InsightVM no site do desenvolvedor Rapid7 que você deseja usar para sua filtragem.

   Você pode criar os parâmetros para o corpo da solicitação consultando a documentação Rapid7. Os parâmetros e valores inseridos no produto Rapid7 InsightVM são compatíveis somente no nível da instância de integração.

2. Navegar até **Todos** > **Rapid7 Vulnerability Integration** > **Administração** > **Integrações**.
3. Na página da lista de integrações do Rapid7, clique no registro da integração Rapid7 InsightVM que você deseja abrir.
4. À direita da página, clique no ícone de informações (I) da mensagem REST, seguido por **Abrir registro**.
5. Com a guia Solicitação HTTP selecionada, em Métodos HTTP, na coluna Nome, clique em um item para abrir seus parâmetros de Consulta HTTP.
6. No registro do método HTTP, em Parâmetros de consulta HTTP, no campo Conteúdo, insira os valores de parâmetro que você encontrou no site do desenvolvedor Rapid7.

   Na imagem a seguir, a cadeia de caracteres de severidade foi adicionada.



   Se você quiser inserir mais de um parâmetro, consulte a documentação Rapid7 para obter mais informações sobre como separar cada valor.

7. Clique em **Atualizar**.

Noções básicas sobre a integração de exploração do Shodan

A aplicação Exploit Integration ServiceNow® Shodan usa dados importados do mecanismo de pesquisa Shodan para ajudar a determinar o impacto e a prioridade de explorações potencialmente mal-intencionadas.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Shodan Exploit Integration

O mecanismo de pesquisa Shodan coleta dados de exploração e a API do Shodan disponibiliza esse banco de dados para o Now Platform®. Ele se integra facilmente à aplicação ServiceNow® Vulnerability Response para mapear explorações para vulnerabilidades de terceiros, enriquecendo os dados de exploração em sua instância.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Todos os dias, os trabalhos programados invocam as integrações automaticamente na ordem em que estão listadas. Você também pode executar trabalhos programados individuais manualmente. Os trabalhos programados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Versões disponíveis

Versão de lançamento para Washington DC	Notas de versão
Shodan Exploit Integration v10.6, 10.7	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Funções

Shodan As tarefas de integração de exploração envolvem as funções a seguir.

- sn_vul_shodan.admin: usuários com esta função podem ler, gravar e excluir registros.
- sn_vul_shodan.user: usuários com esta função podem ler e gravar registros.
- sn_vul_shodan.read: usuários com esta função podem ler registros.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Integrações de exploração do Shodan

Para exibir as integrações de exploração Shodan, navegue até **Todos** > **Shodan Exploit Integration** > **Integrações**.

As integrações a seguir estão incluídas no sistema de base. Essas integrações estão ativas por padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações de exploração do Shodan

Integração	Descrição
Shodan ExploitDB Integration	Recupera dados do ExploitDB de Shodan e aprimora seus dados de vulnerabilidade de terceiros. Esta integração está definida para ser executada diariamente às 03:15:00.
Shodan Metasploit Integration	Recupera informações do Metasploit de Shodan e enriquece seus dados de vulnerabilidade de terceiros. Esta integração está definida para ser executada diariamente às 01:15:00.

Para mudar a hora de início padrão das importações de integração programadas, consulte Definir Shodan Hora de importação da integração de exploração.

Para exibir dados de exploração em vulnerabilidades de terceiros, consulte Exibir Vulnerability Response bibliotecas de vulnerabilidade.

Alterar outras configurações de integração de exploração de Shodan requer conhecimento avançado de ServiceNow e Vulnerability Response e está além do escopo da documentação do produto.

Preparando para a integração de exploração Shodan

Uma integração de exploração Shodan bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. A integração de exploração Shodan pressupõe que você esteja familiarizado com o mecanismo de pesquisa Shodan e a API.

Antes de Iniciar

A integração de exploração Shodan requer uma chave de API. Registre-se no Shodan site para obter uma assinatura gratuita para adquirir esta chave.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Nota:
Antes de executar a integração, faça as mudanças de configuração necessárias com base em seus requisitos.

- Se você não importou os dados do NIST Vulnerability Database (NVD) para o Vulnerability Response, faça-o antes de instalar a Shodan Exploit Integration. Importar os dados do NVD garante que os dados de vulnerabilidade e exposição comuns (CVE) preencham automaticamente os registros de exploração.

  Sem dados do NVD, um espaço reservado é criado no registro de exploração e não é inserido até a próxima atualização do NVD. Para obter mais informações sobre NVD, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

- Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Instalar e configurar o Shodan Exploit Integration para Security Operations

Antes de executar o Shodan Exploit Integration em sua instância, baixe-o e instale-o do ServiceNow Store. Esta aplicação está disponível como uma assinatura separada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Tarefas de configuração	Descrição
Verifique se você tem direitos ServiceNow válidos para a aplicação Vulnerability Response e a aplicação Shodan Exploit Integration para Security Operations.	Para verificar direitos, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Para obter mais informações sobre como obter direitos para uma aplicação Security Operations do ServiceNow Store, consulte Obter direito para um produto ou aplicação Security Operations.
(Opcional) Se ainda não estiver instalado e ativado, talvez você prefira instalar a aplicação Vulnerability Response antes de instalar a aplicação de terceiros.	Para obter mais informações sobre como instalar e ativar a aplicação Vulnerability Response, consulte Como instalar Vulnerability Response.
Tenha a chave de API de integração de exploração Shodan à mão.	Consulte Preparando para a integração de exploração Shodan.

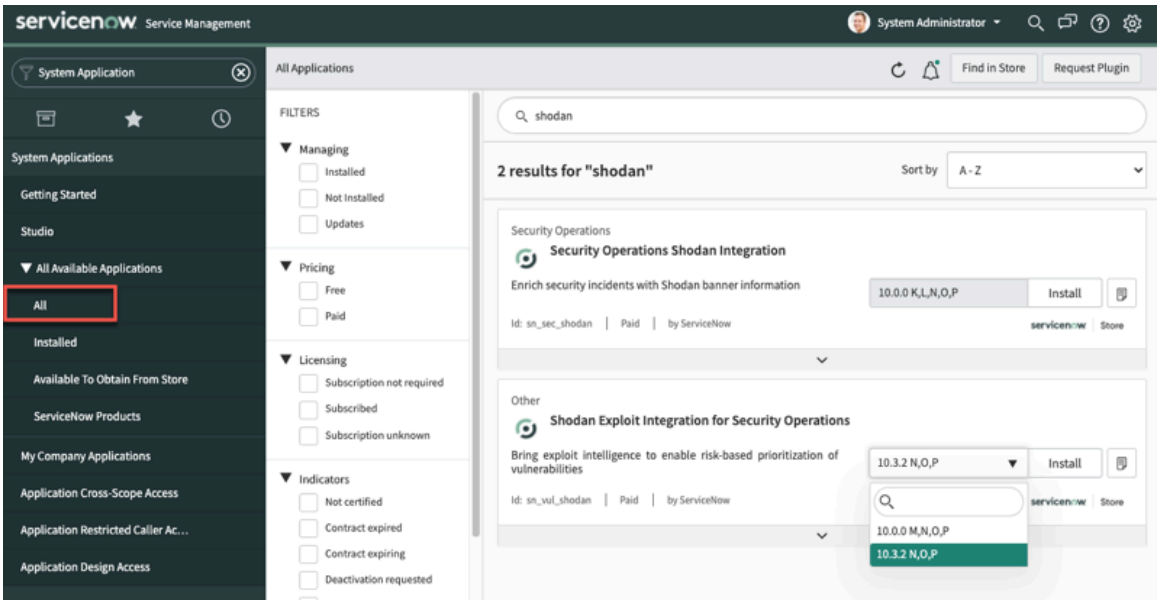
Função necessária: administrador

Procedimento

1. Faça login na instância Now Platform na qual você deseja instalar a aplicação Shodan Exploit Integration.
2. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
3. Localize a aplicação Shodan Exploit Integration para Security Operations, selecione a versão desejada e clique em **Instalar**.

Tradução automática

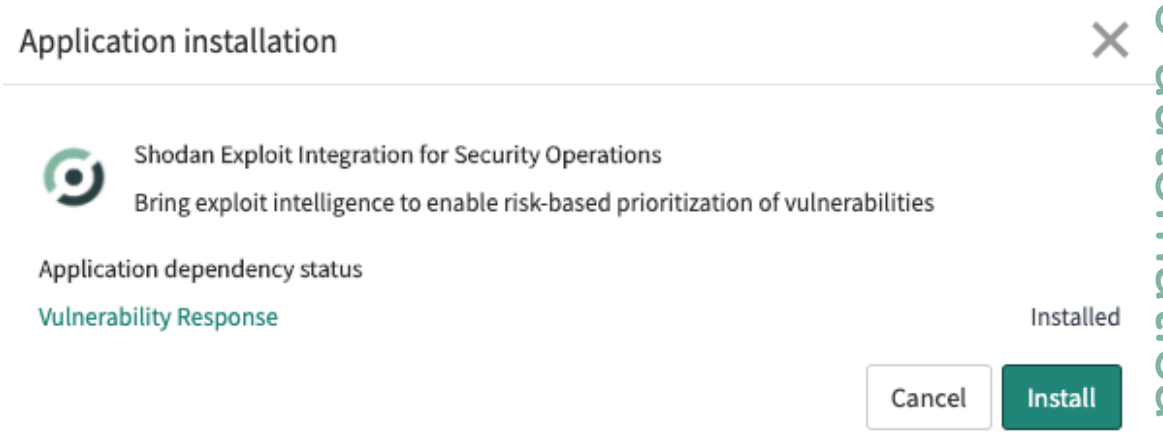
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:
Se você tiver direito a uma atualização para esta aplicação, o botão **Atualizar** será exibido.

A caixa de diálogo de instalação da aplicação exibe o status de dependência da aplicação. Todas as dependências necessárias ainda não instaladas são instaladas automaticamente junto com a aplicação.

4. Na caixa de diálogo, clique em **Instalar**.

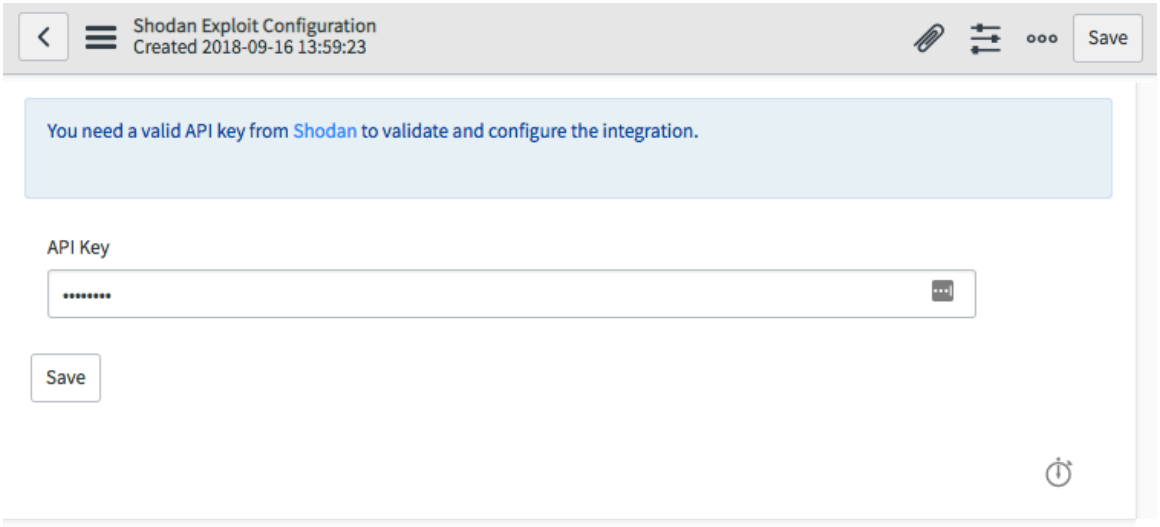


A caixa de diálogo Instalar indica quando a instalação foi concluída com sucesso.

5. Feche a caixa de diálogo Instalar.
6. Navegar até **Shodan Exploit Integration** > **Configuração**.
7. Insira sua chave de API Shodan.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. Clique em **Salvar**.
   Sua configuração Shodan Exploit Integration está concluída.

Definir Shodan Hora de importação da integração de exploração

Para sua conveniência, você pode redefinir a hora de início das integrações de exploração Shodan.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Após a importação inicial, as integrações de exploração Shodan trarão dados delta, a menos que uma importação completa seja solicitada. Consulte Executar uma importação de exploração manual Shodan para obter mais informações sobre importações completas.

Procedimento

1. Navegar até **Todos** > **Shodan Exploit Integration** > **Integrações**.
2. Escolha uma integração.
3. Clique no link para editar o registro.
4. Defina as novas opções **Executar** e **Hora**.
   O tempo é calculado como Horas no horário local. O tempo padrão para as importações de exploração Shodan é 03:15:00.
5. Clique em **Atualizar**.
   A nova hora é usada para a próxima importação programada.

Executar uma importação de exploração manual Shodan

Se a importação inicial falhar ou você não quiser aguardar a importação inicial programada, poderá executar uma importação de dados completa independentemente do trabalho programado diariamente.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)
Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Shodan Exploit Integration** > **Integrações**.
2. Escolha uma integração.
3. Marque a caixa de seleção **Importação de dados completa**.
4. Clique em **Executar agora**.
   Quando a importação estiver concluída, a caixa de seleção será desmarcada e as importações delta serão retomadas.

Exibir o status de execução de importação da integração de exploração Shodan

Use a lista relacionada Execuções de integração de vulnerabilidade para verificar o sucesso de suas execuções de integração, localizar quaisquer problemas, e informar suas decisões de correção.

Antes de Iniciar

Para exibir o status da execução de importação do Shodan:

- A aplicação Vulnerability Response e a integração de exploração Shodan devem ser instaladas e configuradas.
- As importações de integração de exploração Shodan devem ser programadas e em execução.

Função necessária: sn_vuln.admin

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- `sn_sec_cmn.record_threshold_heartbeat`: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- `sn_sec_cmn.maximum_heartbeat_delay`: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Shodan Exploit Integration** > **Integrações**.
2. Selecione uma integração.
3. Clique na lista relacionada **Execuções de integração de vulnerabilidade**.
4. Verifique se todas as importações foram bem-sucedidas.

Trouble?

As causas mais comuns para uma execução com falha incluem:

- Interrupção de rede
- Deterioração de bits na transferência de dados, resultando em dados corrompidos durante a transformação

Se você encontrar qualquer uma dessas condições, marque a caixa de seleção **Importação de dados completa**, clique em **Executar agora**e execute novamente a integração.

Noções básicas sobre a integração de vulnerabilidade da Tenable

A aplicação Integração do Vulnerability Response com Tenable desenvolvida pela engenharia ServiceNow para o Tenable Vulnerability Integration usa dados importados dos produtos Tenable.io e Tenable.sc para ajudar você a priorizar e corrigir vulnerabilidades de seus ativos. A aplicação está disponível com uma assinatura separada do ServiceNow® Store.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

A integração de vulnerabilidade da Tenable emprega duas integrações da Tenable, Tenable.io e Tenable.sc, para importar dados do scanner de terceiros sobre seus ativos e vulnerabilidades. A aplicação Integração do Vulnerability Response com Tenable oferece suporte ao produto Tenable.sc a partir da versão 5.13.

- Tenable.io é uma integração empresarial baseada em nuvem.
- Tenable.sc é uma integração no local que oferece a opção de usar um MID Server se o produto Tenable.sc e sua instância Now Platform estiverem no mesmo ambiente.
- Se o produto Tenable.sc e sua instância Now Platform não estiverem no mesmo ambiente, você precisará usar um MID Server.

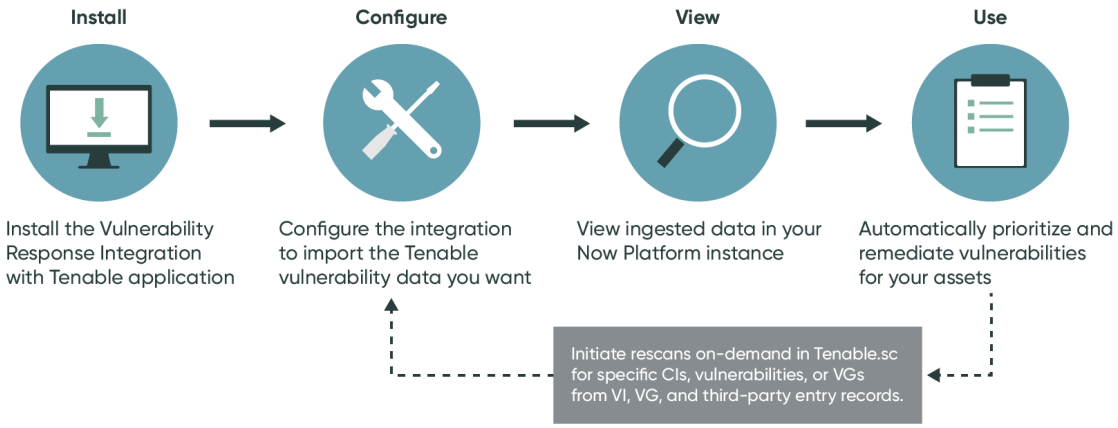
A aplicação Integração do Vulnerability Response com Tenable está disponível no ServiceNow Store com uma assinatura separada.

Para obter listas e descrições das integrações no Tenable Vulnerability Integration, consulte Tenable.io integrações com as aplicações Vulnerability Response e Configuration Compliance e Tenable.sc integrações com a aplicação Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de vulnerabilidade Tenable



Versões disponíveis para Washington DC

Versão de lançamento	Notas de versão
Integração do Vulnerability Response com Tenable v3.5, v3.6	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Termos e principais recursos das integrações

Itens vulneráveis e vulnerabilidades

Um item vulnerável é criado na sua instância Now Platform quando:

- Uma vulnerabilidade importada de um scanner de terceiros é correspondida a um ativo existente (um item de configuração em CMDB). O produto Tenable se refere a essas correspondências como **vulnerabilidades**.
- Uma vulnerabilidade importada de um scanner de terceiros não corresponde a um ativo existente no seu CMDB. Nesse caso, um IC incompatível também é criado junto com um item vulnerável.

  Para ICs incompatíveis, você também pode usar o Mecanismo de Identificação e Reconciliação (IRE) para criar ICs em duas novas classes quando um IC existente não puder ser correspondido com um host. Caso contrário, ICs incompatíveis serão criados nas classes de IC incompatíveis. Para obter mais informações, consulte Criando ICs para Vulnerability Response usando o mecanismo de Identificação e Reconciliação.

Entradas de vulnerabilidade de terceiros e plug-ins

As entradas de vulnerabilidade de terceiros são importadas de scanners de terceiros e listadas na tabela Entradas de vulnerabilidade de terceiros na sua instância Now Platform. As entradas de vulnerabilidade de terceiros da Tenable são ingeridas em Vulnerability Response e correspondidas aos ativos existentes listados em CMDB. A Tenable se refere às entradas de vulnerabilidade de terceiros como plug- **ins**.

IC (Configuration Item, item de configuração)

Itens de configuração são os ativos existentes listados em seu CMDB.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item descoberto

Os ativos ingeridos da importação de ativos da Tenable são correspondidos aos itens de configuração existentes em seu CMDB. Os ativos importados são atualizados.

Se uma correspondência não for encontrada, um IC será criado na classe de IC incompatível do CMDB. Se o plug-in CMDB CI Class Models estiver habilitado, o Mecanismo de Identificação e Reconciliação (IRE) criará novos ICs usando novas classes. Para obter mais informações, consulte Criando ICs para Vulnerability Response usando o mecanismo de Identificação e Reconciliação. Se o IC original incompatível for reclassificado, os registros de item descoberto serão atualizados para refletir o estado. Os itens descobertos fornecem visibilidade de como os ativos são identificados e mapeados para ICs no CMDB.

Regras de pesquisa de IC

Quando os dados são importados de uma integração de terceiros, o Vulnerability Response usa automaticamente os dados do host (ativo) para pesquisar correspondências no Configuration Management Database (CMDB). As regras de pesquisa de IC são usadas para identificar ICs e adicioná-los aos registros de IV quando os IVs são criados para ajudá-lo na correção.

Nova verificação e verificação de correção

Você pode iniciar um comando de nova verificação direcionado em um item de configuração específico, grupo de vulnerabilidade ou entrada de terceiros diretamente do item vulnerável, tarefa de correção e registros de entrada de vulnerabilidade de terceiros em sua instância Now Platform. A Tenable se refere a esta nova verificação como uma **verificação de correção**.

Fechar automaticamente IVs mais antigos

Com o módulo Fechar automaticamente itens vulneráveis obsoletos no seu Now Platform, você pode limpar itens vulneráveis (IV) obsoletos que não foram encontrados recentemente por suas integrações de terceiros. Mover esses IVs para **Encerrado** ajuda a reduzir o número de itens vulneráveis ativos e tarefas de correção e reconciliar ativos em seu CMDB. Você pode usar todas as integrações com Integração do Vulnerability Response com Tenable para fechar automaticamente IVs obsoletos.

Instância

Este termo se refere a uma ocorrência distinta da sua aplicação Now Platform®.

Integração

Uma integração é uma referência específica de produto para uma integração, como a Tenable.io Integração de ativos ou a Tenable.sc Integração de plug-in. Essas são as integrações separadas que pertencem a produtos específicos da Tenable na integração de vulnerabilidade da Tenable em sua instância.

Instância de integração

Este termo se refere às integrações separadas da Tenable listadas por seus produtos Tenable.io e Tenable.sc.

Implantação

Quando uma integração oferece suporte a várias origens, uma existência de integração única e distinta é chamada de implantação da sua integração. O termo é usado para se referir às integrações e produtos em seu ambiente. Por exemplo, você pode ter várias implantações de várias integrações dos produtos Tenable.io e Tenable.sc em seu ambiente.

As integrações Tenable.io e Tenable.sc também incluem os seguintes recursos principais:

- As descobertas da avaliação de configuração, ou seja, resultados de testes junto com políticas, testes de configuração (controles) e citações com fontes autorizadas podem ser importados para a aplicação Configuration Compliance com o produto Tenable.io. Consulte Tenable.io integrações com as aplicações Vulnerability Response e Configuration Compliance e Explorar o

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuration Compliance para obter mais informações sobre como esta integração funciona com a aplicação Configuration Compliance.

- A partir da v2.1 do Tenable Vulnerability Integration, crie itens de configuração (ICs) exclusivos que incluem diferentes identificadores de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. Identifique os ativos distintos em seu ambiente e atualize os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.
- Você pode programar quando deseja que os trabalhos sejam executados para todas as integrações Tenable.io e Tenable.sc. Você também pode executar trabalhos programados manualmente sob demanda.
- Para importações de ativo com Tenable.io, você pode habilitar etiquetas do ativo para organizar e rastrear os ativos listados em CMDB no ambiente Tenable.io.
- As integrações Tenable.io e Tenable.sc permitem que você configure Regras de pesquisa de IC para definir como os dados de ativo de fontes de terceiros são usados para identificar itens de configuração (ICs) em seu Now Platform CMDB.
- As integrações Tenable.io e Tenable.sc permitem que você defina filtros de importação na importação de vulnerabilidades para que você importe somente as vulnerabilidades desejadas da Tenable. Para Tenable.io, você tem a opção de importar vulnerabilidades **fixas** da Tenable com a importação de vulnerabilidades.
- Para Tenable.sc, você tem a opção de iniciar novas verificações sob demanda diretamente do item vulnerável, da tarefa de correção e dos registros de entrada de terceiros na sua instância Now Platform. Se os IVs tiverem sido transicionados para **Encerrado/Corrigido**, mas ainda não estiverem atualizados em sua instância, você poderá verificar se as vulnerabilidades em itens de configuração específicos foram corrigidas. Consulte Iniciar nova verificação para a integração Tenable.sc.

As seções a seguir listam mais detalhes sobre as integrações da Tenable.

Funções necessárias de Now Platform

As tarefas de integração exigem as seguintes funções na sua instância Now Platform.

admin

O administrador do sistema usa o Assistente de configuração para instalar a aplicação Integração do Vulnerability Response com Tenable. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração.

sn_vul.vulnerability_admin

Depois de atribuído, o administrador de vulnerabilidade conclui a configuração das integrações da Tenable no Assistente de configuração. Esta função tem acesso completo à aplicação Vulnerability Response (VR) e seus registros. O administrador de vulnerabilidades configura todas as aplicações de VR e regras para integrações de terceiros instaladas.

sn_vul_tenable.configure_integration

Esta função contém a função granular sn_vul_tenable.read_integration e os usuários com esta função podem configurar a aplicação Integração do Vulnerability Response com Tenable.

sn_vul_tenable.read_integration

Usuários com essas funções podem exibir (ler), mas não editar registros da aplicação Integração do Vulnerability Response com Tenable.

Grupo do Vulnerability Response

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por padrão, o grupo do Vulnerability Response está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Vulnerability Response herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente.

Itens vulneráveis

Os itens vulneráveis são agrupados em tarefas de correção de acordo com as regras do grupo e atribuídos para correção com base nas regras de atribuição. Para obter mais informações, consulte Vulnerability Response tarefas de correção e regras de tarefa visão geral e Vulnerability Response visão geral de regras de atribuição.

Regras de pesquisa de item de configuração (IC)

As Regras de Pesquisa de IC identificam ICs e determinam quando adicioná-los a um item vulnerável. Para obter mais informações sobre como funcionam as regras de pesquisa de IC, consulte Regras de pesquisa de IC para identificar itens de configuração de Vulnerability Response integrações de vulnerabilidade de terceiros.

Nota:
As regras, depois de removidas, não podem ser recuperadas. Em vez de remover as regras existentes, desabilite-as ao criar novas.

As regras de pesquisa Tenable.io a seguir são enviadas com o sistema de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- Nome do host
- DNS
- IP

As regras de pesquisa Tenable.sc a seguir são enviadas com o sistema de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Nota:
Vários valores para ip_address, mac_address, fqdns e network_interfaces são usados para um ativo. Todos os valores são considerados nas regras de pesquisa de IC para correspondência. Todos os valores são usados para criar vários adaptadores de rede usando IRE.

Para obter mais informações sobre como configurar a categorização de recursos de nuvem incompatíveis em sua classe de IC preferencial, consulte Atualizando classe de IC para ativos de nuvem incompatíveis.

Novas propriedades para ignorar endereços IP

Em Tenable.io, há duas propriedades disponíveis se você quiser ignorar vários endereços IP ou vários endereços Mac como parte de suas regras de pesquisa de IC:

ignoreIPAddress

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma lista de endereços IP a serem ignorados para pesquisa de IC e criação de IC.

ignoreMacAddress

Uma lista de endereços MAC a serem ignorados para pesquisa de IC ou criação de IC.

Itens descobertos

Este módulo lista os itens de configuração detectados durante a importação das integrações de item vulnerável da Tenable e das integrações de ativo da Tenable.

Nota:
O filtro padrão desta lista é definido como Incompatível. Você pode exibir todos os itens descobertos de uma importação removendo o filtro.

Para obter mais informações sobre o módulo Itens descobertos, consulte Itens Descobertos.

Etiquetas do ativo

As etiquetas do ativo (também conhecidas como etiquetas do host) são usadas para organizar e rastrear os ativos em sua organização. Você pode atribuir marcadores aos seus ativos. Em seguida, ao iniciar as verificações, você pode selecionar marcadores associados aos ativos que deseja verificar. O módulo Etiquetas do ativo permite que você baixe dados de etiqueta do ativo de Tenable.io para sua instância de forma programada. Os dados de ativo que incluem marcadores de ativo são extraídos de Tenable.io e transformados usando os mapas de transformação de integração Tenable.io Asset Transform.

Todas as etiquetas do ativo são importadas como parte da integração do ativo Tenable.io. As etiquetas do ativo geralmente são usadas para filtragem em regras de atribuição Vulnerability Response e regras de tarefa de correção. Os marcadores são exibidos no formulário Item descoberto.

Nota:
Execute a integração de ativo Tenable.io antes de criar regras de atribuição Vulnerability Response ou regras de tarefa de correção na aplicação Vulnerability Response para que todos os marcadores estejam disponíveis para essas regras antes que os itens vulneráveis sejam importados e agrupados. Observe também os seguintes pontos sobre marcadores:

- O armazenamento de marcador não faz distinção entre maiúsculas e minúsculas. Por exemplo, se você criar um marcador para descrever ativos em seu local de San Diego e criar o marcador San Diego, também não poderá criar um marcador SAN DIEGO e armazená-lo na tabela Etiqueta do ativo. San Diego e SAN DIEGO são considerados a mesma etiqueta do ativo pelo sistema. O marcador que for importado primeiro será o marcador armazenado e reconhecido daqui em diante.
- Usar etiquetas do ativo como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. As etiquetas do ativo devem ser usadas somente no Construtor de condição.
- As etiquetas do ativo são controladas pela propriedade do sistema global sn_vul.import_asset_tags. Esta propriedade é definida como verdadeira por padrão. Desabilitar os marcadores os desabilita em todas as Now Platform® instâncias.

Filtros de recuperação de dados

As configurações de recuperação de dados ajudam a determinar especificamente o tipo e o escopo dos dados que você deseja importar da aplicação Tenable para sua instância Now Platform®. Para obter uma lista das configurações usadas com mais frequência, consulte Configurações de recuperação de dados para a integração de vulnerabilidade da Tenable.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Classificação de prioridade de vulnerabilidade (VPR)

A classificação de prioridade de vulnerabilidade (VPR) é um atributo do produto Tenable que é importado e usado com uma nova calculadora de risco padrão em Vulnerability Response. A Regra de risco da Tenable é instalada com a aplicação Integração do Vulnerability Response com Tenable como parte da Calculadora de risco padrão nas Calculadoras de vulnerabilidade da Vulnerability Response.

Esta regra de risco está desabilitada por padrão.

Ao habilitar a regra da calculadora de risco da Tenable, os valores de VPR importados são usados para calcular a pontuação de risco dos itens vulneráveis. A distribuição de peso padrão para esta calculadora de risco: VPR = 70%, Ativo = 15% e Criticalidade dos negócios = 15%. Habilitar esta regra da Calculadora de risco da Tenable pode afetar o desempenho da ingestão de dados. Para obter mais informações sobre calculadoras Vulnerability Response e a regra da calculadora de risco da Tenable, consulte Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade.

Instalação e configuração

Depois de baixar o Integração do Vulnerability Response com Tenable do ServiceNow® Store, a instalação e a configuração serão compatíveis com o Assistente de configuração em Vulnerability Response. Para obter mais informações, consulte Configuração de Vulnerability Response usando o Assistente de configuração.

Tenable.io integrações com as aplicações Vulnerability Response e Configuration Compliance

As integrações Integração do Vulnerability Response com TenableTenable.io na aplicação [] estão disponíveis nas aplicações Vulnerability Response e Configuration Compliance.

Lista de Tenable.io integrações

Várias origens são compatíveis com todas as integrações Tenable.io e Tenable.sc. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente do Assistente de configuração em Vulnerability Response. Você também instala e configura a aplicação Integração do Vulnerability Response com Tenable no Assistente de configuração.

Tenable.io é uma integração empresarial baseada em nuvem. Consulte a tabela a seguir para obter os nomes e as descrições das integrações compatíveis com o produto Tenable.io.

A integração de resultados de conformidade Tenable.io e a integração de backfill de resultados de conformidade Tenable.io estão inativas por padrão.

Para ativá-los:

1. Navegar até **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
2. Na lista Integrações da Tenable, clique em um nome de integração para abrir o registro e marque a caixa de seleção **Ativo** para habilitá-lo. Você pode preferir deixar as configurações de programação em seus valores padrão para que essas integrações sejam iniciadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
Tenable.io Integração de ativos	• Recupera todos os dados do ativo, incluindo etiquetas do ativo, do produto Tenable.io e os processa em sua instância. • A partir da v3.0, se a integração de resultados de conformidade Tenable.io estiver ativada, você poderá importar dados de avaliação de configuração segura junto com os dados de ativos importados. Esses dados podem ajudar a identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API do ativo. • A saída desta integração são itens descobertos. • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. • A partir da v2.2, `Last Scan Time` é importado e atualizado somente para ativos que têm vulnerabilidades.
Tenable.io Integração de resultados de conformidade	• A partir da v3.0, os dados de avaliação de configuração segura importados da Integração de resultados de conformidade junto com os dados importados da Integração de ativos podem ajudar a identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos. • Se habilitado, recupera dados de avaliação de configuração segura de alto nível e os processa em sua instância Now Platform. Os dados importados incluem resultados de testes junto com políticas, testes de configuração (controles) e citações com fontes autorizadas. • Os dados de avaliação para ativos ausentes ou ativos sem IDs de ativo não são importados. • Se um resultado de teste for importado e o ativo correspondente não puder ser correspondido em sua instância, o resultado do teste será ignorado e o ID

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	do ativo ausente será armazenado em um registro temporário na tabela [sn_vul_tenable_missing_asset]. • O valor total de ativos ignorados (ausentes) está listado no campo **ICs ignorados** na guia **Configuração** no registro de execução da integração para esta integração.
Tenable.io Compliance Results Backfill Integration	• Quando ativada, essa integração é executada automaticamente depois que a integração de ativos é concluída com sucesso como parte de uma execução de integração encadeada. Esta integração corresponde aos dados de avaliação de configuração com os ativos ausentes listados na tabela [sn_vul_tenable_missing_asset]. • Importa até 200 IDs de ativo para todos os ativos ausentes descobertos ou presentes na instância após a conclusão bem-sucedida da importação de integração de ativos. • Remove os registros temporários da tabela [sn_vul_tenable_missing_asset] quando os ativos podem ser correspondidos com os dados de avaliação de configuração correspondentes.
Tenable.io Integração de credencial de verificação	• Esta integração recupera as credenciais de verificação configuradas em Tenable.io. • Coordena as chamadas de mensagem REST para a API de credenciais. • A saída desta integração são as credenciais de verificação preenchidas na tabela [sn_vul_tenable_scan_credential],. • As credenciais importadas são usadas para acessar o scanner quando as solicitações de verificação são iniciadas a partir do Now Platform. • Esta integração está programada para ser executada semanalmente.
Tenable.io Integração de modelo	Um registro de modelo é enviado para Tenable.io durante a nova verificação. Esta integração recupera credenciais Tenable.io disponíveis para usar em novas verificações. As credenciais são específicas da instância e um único registro de modelo é importado e armazenado com segurança temporariamente na tabela [sn_vul_tenable_io_template].

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
Tenable.io Integração de plug-in	• Recupera os dados do plug-in do produto Tenable.io. Os dados recuperados são baseados na data em que os plug-ins foram atualizados pela última vez por uma Tenable.io execução de integração. • Esta importação garante que os identificadores Tenable.io (Dez IDs) sejam atuais. • Coordena as chamadas de mensagem REST para a API do plug-in. • A saída desta integração são as vulnerabilidades de terceiros.
Tenable.io Integração de vulnerabilidades corrigidas	• Recupera dados de vulnerabilidade com base em filtros de severidade do produto Tenable.io e os processa em sua instância. Itens vulneráveis são criados para registros de detecção que estão nos estados **Aberto** e **Reaberto**, porque esses registros exigem correção. Os itens vulneráveis existentes serão atualizados pelo Vulnerability Response se as detecções forem **Corrigidas**, mas os itens vulneráveis não serão criados para detecções **Corrigidas** por padrão, porque a Tenable considera as vulnerabilidades **CorrigidasMitigadas**. • Quando o sinalizador **Criar horários vulneráveis para detecções de vulnerabilidade fixa** é ativado no Assistente de configuração, novos IVs são criados no estado **Fixo** para que você tenha visibilidade das detecções que os criaram. Como os IVs são criados para detecções **fixas** que ainda não existem em sua instância, isso pode afetar negativamente o desempenho da importação. Você pode preferir deixar este recurso desativado para que as detecções **fixas** atualizem somente os estados dos itens vulneráveis existentes. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração é Itens vulneráveis (IVs) **encerrados/corrigidos**. Ele também cria ativos e entradas de terceiros se eles não existirem. • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	Esta execução de integração está programada. É uma integração encadeada, o que significa que, após a conclusão bem-sucedida de uma execução, a integração de vulnerabilidades em aberto descrita abaixo é acionada. A partir do Tenable v3.3, você pode exibir as seguintes informações das execuções de integração de vulnerabilidade: • **Total de partes:** número total de partes geradas pela Tenable • **Blocos disponíveis:** número de blocos disponíveis para download para ServiceNow
Tenable.io Abrir integração de vulnerabilidades	• Esta integração é acionada após a conclusão bem-sucedida da Tenable.io Integração de vulnerabilidades fixas. • Recupera dados de vulnerabilidade com base nos filtros de severidade do produto Tenable.io e os processa em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração são itens vulneráveis (IVs) **novos/reabertos**. Ele também cria itens de configuração e entradas de terceiros se eles não existirem. A Tenable considera as vulnerabilidades ativas como **cumulativas** (atuais). • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. A partir do Tenable v3.3, você pode exibir as seguintes informações das execuções de integração de vulnerabilidade: • **Total de partes:** número total de partes geradas pela Tenable • **Blocos disponíveis:** número de blocos disponíveis para download para ServiceNow

Tenable.sc integrações com a aplicação Vulnerability Response

As integrações Integração do Vulnerability Response com TenableTenable.sc na aplicação [].

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Começando com Vulnerability Response v20.0, se um ativo for verificado por um agente, a coluna Agente existente exibirá o valor, verdadeiro na lista de itens descobertos, o que indica que é uma verificação autentica.

Lista de Tenable.sc integrações

Várias origens são compatíveis com todas as integrações Tenable.io e Tenable.sc. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente do Assistente de configuração em Vulnerability Response. Você também instala e configura a aplicação Integração do Vulnerability Response com Tenable no Assistente de configuração.

- Tenable.sc é uma integração no local que oferece a opção de usar um MID Server se o produto Tenable.sc e sua instância Now Platform estiverem no mesmo ambiente.
- Se o produto Tenable.sc e sua instância Now Platform não estiverem no mesmo ambiente, você precisará usar um MID Server.

Integrações do Tenable.sc

Integração	Descrição
Tenable.sc Integração de ativos	Para evitar a criação de itens descobertos duplicados com dados de ativo importados, a integração de ativo do produto Tenable.sc é composta por duas integrações. **A Tenable.sc Open Assets Integration** Esta integração importa dados de vulnerabilidade sobre seus ativos que a Tenable considera **Cumulativos** (atuais) ou **Abertos**. Os itens vulneráveis (IVs) criados em sua instância com esses dados de ativo importados são considerados abertos, ou seja, no estado **Aberto**. Esses itens vulneráveis requerem investigação e podem precisar de correção. **A Tenable.sc Integração de ativos fixos** Esta integração importa dados de vulnerabilidade sobre seus ativos que a Tenable considera **Atenuados** (não mais vulneráveis) ou **Corrigidos**. Os itens vulneráveis desses ativos passam do estado **Aberto** para o estado **Encerrado/Corrigido** em sua instância, pois os resultados das verificações mostram que eles não estão mais vulneráveis. • Recupera todos os dados de ativo do produto Tenable.sc e os processa em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de ativos. • A saída desta integração são itens descobertos. • O filtro de consulta da Tenable selecionado no Assistente de configuração também se aplica à Integração de ativos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	Tenable.sc. Somente os ativos com as vulnerabilidades que correspondem às condições do filtro de consulta são importados.
Tenable.sc Integração de plug-in	• Recupera os dados do plug-in do produto Tenable.sc. Os dados recuperados são baseados na data em que os plug-ins foram atualizados pela última vez por uma Tenable.sc execução de integração. • Essa importação garante que os Tenable.sc Identificadores (Dez IDs) sejam atuais e que somente as vulnerabilidades ativas sejam importadas. • Coordena as chamadas de mensagem REST para a API de plug-ins. • A saída desta integração são as vulnerabilidades de terceiros.
Tenable.sc Integração de vulnerabilidades corrigidas	• Recupera dados de vulnerabilidade com base em filtros de severidade do produto Tenable.sc e os processa em sua instância. Itens vulneráveis são criados para registros de detecção que estão nos estados **Aberto** e **Reaberto**, porque esses registros exigem correção. Os itens vulneráveis existentes serão atualizados pelo Vulnerability Response se as detecções forem **Corrigidas**, mas os itens vulneráveis não serão criados para detecções **Corrigidas** por padrão, porque a Tenable considera as vulnerabilidades **CorrigidasMitigadas**. • Quando o sinalizador **Criar horários vulneráveis para detecções de vulnerabilidade fixa** é ativado no Assistente de configuração, ele cria novos IVs no estado **Fixo** para que você tenha visibilidade das detecções que os criaram. Como os IVs são criados para detecções **fixas** que ainda não existem em sua instância, isso pode afetar negativamente o desempenho da importação. Você pode preferir deixar este recurso desativado para que as detecções **fixas** atualizem somente os estados dos itens vulneráveis existentes. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração é Itens vulneráveis (IVs) **encerrados/corrigidos**. Ele também cria ativos e entradas de terceiros se eles não existirem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	Esta execução de integração é uma execução programada. É uma integração encadeada, o que significa que, após a conclusão bem-sucedida de uma execução, a Tenable.sc Integração de vulnerabilidades em aberto descrita abaixo é acionada. **Nota:** Por padrão, os IDs de família 0 e 39 são excluídos desta integração.
Tenable.sc Abrir integração de vulnerabilidades	• Esta integração é acionada após a conclusão bem-sucedida da Tenable.sc Integração de vulnerabilidades fixas. • Recupera dados de vulnerabilidade com base nos filtros de consulta selecionados do produto Tenable.sc e os processa em sua instância. • Cria itens vulneráveis correspondentes para vulnerabilidades ativas. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração é **Atualizar/criar novos** itens vulneráveis (IVs) se eles ainda não existirem. Ele também cria itens de configuração e entradas de terceiros se eles não existirem. **Nota:** Por padrão, os IDs de família 0 e 39 são excluídos desta integração.
Tenable.sc Integração de credencial de verificação	• Esta integração recupera as credenciais de verificação configuradas em Tenable.sc. • Coordena as chamadas de mensagem REST para a API de credenciais. • A saída desta integração são as credenciais de verificação preenchidas na tabela [sn_vul_tenable_scan_credential]. • As credenciais importadas são usadas para acessar o scanner quando as solicitações de verificação são iniciadas a partir do Now Platform. • Esta integração está programada para ser executada semanalmente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
Tenable.sc Integração de vulnerabilidades de preenchimento	• Esta integração de preenchimento importa todas as vulnerabilidades abertas e corrigidas que podem ter sido perdidas durante uma importação. • Esta integração importa vulnerabilidades abertas e corrigidas dos últimos sete dias para atualizar suas detecções e itens vulneráveis. • Esta integração pode afetar seu desempenho. • Esta integração está desabilitada por padrão. • Para atualizar seus dados de vulnerabilidade e evitar possíveis problemas de desempenho, talvez você prefira programar as Vulnerabilidades corrigidas e as Integrações de vulnerabilidades abertas da Tenable.sc para serem executadas quando nenhuma outra verificação estiver em execução. • A saída desta integração é: ○ Itens vulneráveis (IVs)**encerrados/corrigidos**. Ele também cria ativos e entradas de terceiros se eles não existirem. ○ para **atualizar/criar novos** itens vulneráveis (IVs) se eles ainda não existirem. Ele também cria itens de configuração e entradas de terceiros se eles não existirem.

Autenticação de usuário e Tenable.sc

A autenticação do usuário é compatível com sua instância Now Platform® e a versão 5.13 do produto Tenable.sc. A autenticação do usuário será necessária se você estiver usando a versão 5.12 e anterior do produto Tenable.sc.

Quando você seleciona a autenticação de usuário para as Tenable.sc integrações, os tokens podem expirar e ser substituídos durante as execuções de integração. Na coluna Anotações no registro de execução de integração de vulnerabilidade (VIN), a seguinte mensagem é exibida para um processo quando um token expira, Erro: falha na validação de token. Nenhuma ação será necessária se esta mensagem for exibida. Os tokens expirados são atualizados automaticamente em segundo plano e a mensagem não indica uma pausa ou erro com o processo de integração.

Preparando para a integração de vulnerabilidade da Tenable

Prepare-se para a integração de vulnerabilidade da Tenable ServiceNow® executando as tarefas de configuração a seguir.

Antes de começar

Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração. Para uma instalação e configuração sem problemas da aplicação Integração do Vulnerability Response com Tenable, convém imprimir a check-list a seguir e verificar

Tradução automática

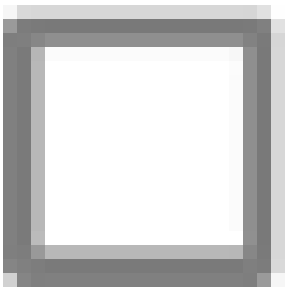
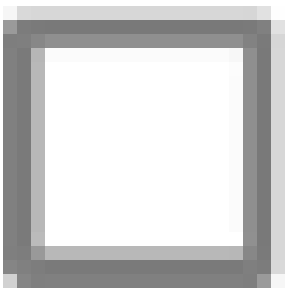
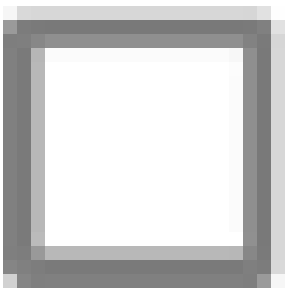
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

se os itens listados foram concluídos antes de instalar a aplicação e importar dados de vulnerabilidade para sua instância Now Platform®.

Nota:
Se você estiver importando dados com a integração criada pela Tenable e quiser começar a usar a ServiceNow® Integração do Vulnerability Response com a Tenable, consulte a

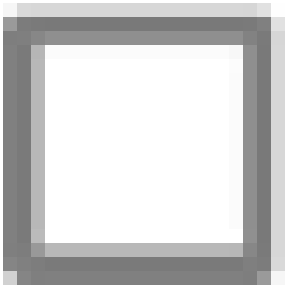
Para obter informações atuais de limpeza e migração de dados da integração criada pela Tenable para a integração criada por ServiceNow, consulte o artigo Diretrizes para migrar da integração do Vulnerability Response da Tenable para a integração do Vulnerability Response da ServiceNow com a Tenable [KB0960667] .

Função necessária: administrador para baixar e instalar a aplicação.

Tarefa	Descrição
	(Opcional) Se ainda não estiver instalado e ativado, talvez você prefira instalar a aplicação Vulnerability Response antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar a aplicação Vulnerability Response, consulte Como instalar Vulnerability Response. Esta integração requer a versão 12.1 de Vulnerability Response ou posterior.
	Se você ainda não o tiver em sua instância, obtenha direitos e baixe a aplicação Integração do Vulnerability Response com Tenable para sua instância Now Platform®. A aplicação Integração do Vulnerability Response com Tenable oferece suporte ao produto Tenable.sc a partir da versão 5.13. Consulte .
	Estime o número de itens vulneráveis que você espera importar. Verifique se sua instância pode aceitar o número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a longos tempos de carregamento. Se você não souber o tamanho da sua instância ou se precisar de assistência, entre em contato com o ServiceNow® Suporte técnico.

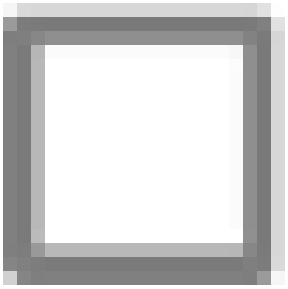
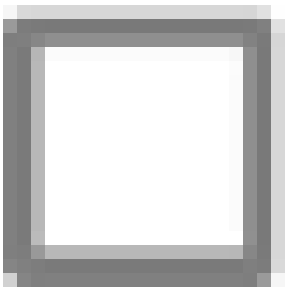
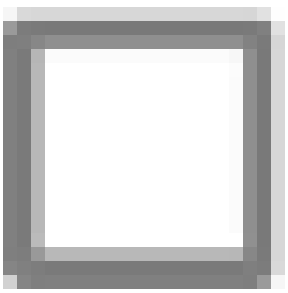
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Verifique se você tem grupos ou usuários para gerenciar as integrações e corrigir itens vulneráveis. **admin** O administrador do sistema usa o Assistente de configuração para instalar a aplicação Integração do Vulnerability Response com Tenable. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração. **sn_vul.vulnerability_admin** Depois de atribuído, o administrador de vulnerabilidade conclui a configuração das integrações da Tenable. Esta função tem acesso completo à aplicação Vulnerability Response (VR) e seus registros. Configura todas as aplicações e regras de VR e configura integrações de terceiros. **sn_vul_tenable.configure_integration** Pode configurar a integração de vulnerabilidade da Tenable. Esta função contém a função granular sn_vul_tenable.read_integration. **sn_vul_tenable.read_integration** Pode exibir (ler) registros da integração de vulnerabilidade da Tenable. **Grupo do Vulnerability Response** Por padrão, o grupo do Vulnerability Response está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Vulnerability Response herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente. O administrador do sistema executa a atribuição inicial de funções a usuários e grupos no Assistente de configuração para a integração. Por padrão, o grupo Vulnerability Response está disponível. Se ainda não tiver sido criado, talvez você prefira criar grupos adicionais e adicionar usuários com o módulo Administração de usuários em sua instância antes de usar o Assistente de configuração. Consulte Criação de um grupo de usuários . Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que os usuários podem fazer e ver na aplicação Vulnerability Response. Para obter a atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Para promover um desempenho aprimorado para sua primeira importação, convém desabilitar determinados recursos, regras ou trabalhos em sua instância. • Desabilite as calculadoras de vulnerabilidade se você não as usar. Essas calculadoras, além de qualquer outra que você tenha definido, são executadas sempre que um registro de item vulnerável é criado ou atualizado. Consulte Desabilitar calculadoras de vulnerabilidade. • Durante a importação inicial de registros, determinadas regras de negócios relacionadas à notificação podem fazer com que muitas notificações sejam geradas, afetando o desempenho. Antes da importação inicial, talvez você prefira Desabilitar as regras de negócios relacionadas à notificação, conforme descrito em Importar modificações para a integração de vulnerabilidade da Tenable.
	Verifique se você habilitou todos os recursos, regras, plug-ins de dependência ou trabalhos em sua instância necessários para a integração. • Tenable.sc é uma integração no local que oferece a opção de usar um MID Server se o produto Integração do Vulnerability Response com Tenable e sua instância Now Platform estiverem no mesmo ambiente. Se o produto Tenable.sc e sua instância Now Platform não estiverem no mesmo ambiente, você precisará usar um MID Server. Para obter mais informações sobre MID Servers em sua instância, consulte MID Server . • Verifique se o plug-in IntegrationHub está instalado e ativado. Este plug-in permite que os componentes do sistema de base chamem sistemas externos usando APIs de integração e ative etapas de protocolo como REST. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e localize o plug-in. Se não estiver instalado em sua instância, instale-o e ative-o.
	Obter credenciais da Tenable. Verifique se você tem nomes de conta, senhas e outras informações de serviço exigidas pelos seus produtos Tenable para que você tenha acesso a eles. Tenable.io requer acesso de Administrador com um atributo de permissão maior ou igual a 64. Tenable.sc requer acesso de Analista de Segurança ou Gerente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Nota: A partir da v3.8 de Integração do Vulnerability Response com Tenable, o acesso a Tenable.io não precisa mais de privilégios de administrador. Um usuário básico com um atributo de permissão igual a 16 também pode acessar o produto.

Você está pronto para Instalar a aplicação Integração do Vulnerability Response com Tenable usando o Assistente de configuração.

Instalar a aplicação Integração do Vulnerability Response com Tenable usando o Assistente de configuração

Antes de executar o ServiceNow® Tenable Vulnerability Integration, você precisa baixar a aplicação Integração do Vulnerability Response com Tenable do ServiceNow Store e instalá-lo e configurá-lo usando o Assistente de configuração no aplicativo Vulnerability Response.

Antes de Iniciar

Antes de instalar a aplicação Tenable, verifique se você concluiu todos os itens da check-list em Preparando para a integração de vulnerabilidade da Tenable.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Funções necessárias: administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação Tenable no Assistente de configuração. Administrador de vulnerabilidade (sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) para configurar a aplicação no Assistente de configuração depois que ele for instalado.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Instalação da aplicação de integração**.

   Após alguns momentos, as aplicações disponíveis para instalação em sua instância serão exibidas.

2. Localize o bloco **Tenable (Plataforma Tenable)** e clique em **Instalar**.

   Esta ação instala a aplicação Integração do Vulnerability Response com Tenable que você baixou do ServiceNow Store.

3. Siga os prompts fornecidos no Assistente de configuração para continuar com a instalação.
4. Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Vulnerability Response aplicações de terceiros usando o Assistente de configuração.

O que Fazer Depois

Depois de concluir a instalação no Assistente de configuração, navegue até **Configuração de integração>Integrações do scanner** no Assistente de configuração para continuar com a configuração. Se você quiser mais informações para complementar os prompts fornecidos no Assistente de configuração, consulte Configurar a integração de vulnerabilidade da Tenable usando o assistente de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de recuperação de dados para a integração de vulnerabilidade da Tenable

As configurações de recuperação de dados a seguir ajudam a determinar especificamente o tipo e o escopo dos dados que você deseja importar da ServiceNow® Tenable Vulnerability Integration para sua instância Now Platform®.

As configurações descritas nas seções a seguir ajudam a controlar os dados que você deseja importar. Além disso, você pode definir os valores desses filtros em Instâncias de integração. Para exibir instâncias de integração, navegue até **Integração de vulnerabilidade Tenable** > **Instâncias de Integração** e clique na sua integração, Tenable.io ou Tenable.sc.

Na página Instância de integração exibida, clique nos Parâmetros de instância de integração para exibir uma lista de parâmetros ou nas guias Integrações de vulnerabilidade para uma programação, Detalhes de REST, Detalhes de integração, Fontes de dados e informações de execução de integração.

Configurações e filtros comuns de severidade e recuperação para Tenable.io e Tenable.sc na sua instância Now Platform

As configurações a seguir estão disponíveis para as integrações Tenable.io e Tenable.sc na sua instância Now Platform. Essas e outras definições de configuração são exibidas na página Instância de integração da sua instância Now Platform. Você pode preferir deixar essas configurações em seus padrões para as primeiras execuções de integração.

Tenable.io

inserir_fixo

Se você habilitar o sinalizador **insert_fixed** no Assistente de configuração para a integração de importação de vulnerabilidades, novos IVs serão criados para detecções no estado **Fixo** que ainda não existem na sua instância.

severidade_crítica

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de severidade crítica das Tenable.io Integrações de vulnerabilidades abertas e Tenable.io Vulnerabilidades fixas.

severidade_alta

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de severidade de alto nível das Tenable.io Integrações de vulnerabilidades abertas e Tenable.io Vulnerabilidades fixas.

severidade_média

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de severidade de nível médio das Tenable.io Integrações de vulnerabilidades abertas e Tenable.io Vulnerabilidades fixas.

severidade_info

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de severidade de nível de informação das Tenable.io Integrações de vulnerabilidades abertas e Tenable.io Vulnerabilidades fixas.

severidade_baixa

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de severidade de baixo nível das Tenable.io Integrações de vulnerabilidades abertas e Tenable.io Vulnerabilidades fixas.

tamanho

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta configuração define o número de registros de plug-in a serem incluídos no conjunto de resultados da Tenable.io Integração de plug-ins. Deve estar no formato int32. O valor padrão é 1.000. O tamanho máximo é 10.000.

num_assets

O número máximo de vulnerabilidades por bloco exportado das Tenable.io Integrações de vulnerabilidades fixas e Tenable.io Vulnerabilidades abertas. O valor padrão é 50.

chunk_size

Especifica o número de ativos por bloco exportado pela Tenable.io integração de ativos. O padrão é 1.000.

Tenable.sc

assíncrono_request

Este parâmetro está inativo por padrão (falso). Habilite ou desabilite este parâmetro para fazer chamadas de API assíncronas ou síncronas com Tenable.sc respectivamente. Para chamadas síncronas, se houver um tempo limite de 30 segundos, entre em contato com o suporte do produto Tenable para ajustar a caixa. Este parâmetro, uma vez habilitado, é aplicável a todas as integrações de Tenable.sc. Para clientes existentes que usam chamadas assíncronas, um script de correção está disponível, o que adiciona um novo parâmetro async_request às instâncias de integração Tenable.sc existentes. Para exibir os scripts de correção, navegue até **Definição do Sistema** > **Corrigir Scripts**.

inserir_fixo

Se você habilitar o sinalizador **insert_fixed** no Assistente de configuração para a integração de importação de vulnerabilidades, novos IVs serão criados para detecções no estado **Fixo** que ainda não existem na sua instância.

deslocamento

Especifica o número de ativos, plug-ins e vulnerabilidades importados em uma execução de integração.

Filtros de consulta

Os filtros de consulta são configurados no console da Tenable. Esses filtros de consulta têm IDs que podem ser selecionados no Assistente de configuração ou na página Instâncias de integração na sua instância Now Platform. Esses filtros são aplicados ao recuperar os dados das integrações Tenable.sc.

Mensagens REST para a integração de vulnerabilidade da Tenable

As ServiceNow® mensagens REST de integração de vulnerabilidade da Tenable são usadas para fazer chamadas para a API da Tenable.

Tenable.io Mensagem REST de ativos

A mensagem REST de Tenable.io ativos recupera informações de ativos para a Tenable.io integração de ativos. As mudanças no registro do método de mensagem REST afetam as solicitações feitas a Tenable.io para recuperar informações de ativos. O trabalho de exportação de ativos é enviado com os seguintes filtros:

- "is_deleted": falso
- "is_licensed": verdadeiro

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tenable.io Mensagem REST de plug-ins

A mensagem REST de plug-ins Tenable.io recupera informações de plug-in para a integração de plug-in Tenable.io. As mudanças no registro do método de mensagem REST afetam as solicitações feitas a Tenable.io para recuperar informações de plug-ins.

Tenable.io Mensagem REST de vulnerabilidades

A mensagem REST de vulnerabilidades Tenable.io recupera informações de vulnerabilidades abertas e encerradas da Tenable.io Integração de vulnerabilidade. As mudanças no registro do método de mensagem REST afetam as solicitações feitas a Tenable.io para recuperar informações de vulnerabilidades.

Mensagem REST de consultas Tenable.sc

A mensagem REST de consultas da Tenable.sc recupera as informações do filtro de consulta da integração de ativos da Tenable.sc e da integração de vulnerabilidades da Tenable.sc em que o filtro de consulta está configurado.

Tenable.sc Mensagem REST de plug-ins

A mensagem REST de plug-in Tenable.sc recupera informações de plug-in para a integração de plug-ins Tenable.sc. As mudanças no registro do método Obter plug-ins da mensagem REST afetam as solicitações feitas a Tenable.sc para recuperar informações de plug-ins.

Nome do parâmetro	Valor	Descrição
tipo	ativo	Indica a origem da qual a Tenable extrai dados. Usado por código. Mudanças não são recomendadas.
campos	id, descrição, cvssVector,cvssV3Vector, cvssV3TemporalVector, sinopse, cvssVector, baseScore, temporalScore, cvssV3Vector, cvssV3BaseScore, cvssV3TemporalVector, name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, família, cvssV3TemporalScore, explore tipo, direitos autorais, versão, sourceFile, dependências, necessáriosPorts, necessáriosUDPPorts, srcPort, dstPort,protocol, checkType, cvssVectorBF, sigSeverity, patchPubDate, patchModDate, vulnPubDate, modificadoTempo, md5	Indica a lista de campos importados da Tenable.

Tenable.sc Mensagem REST de vulnerabilidades

A mensagem REST de vulnerabilidades Tenable.sc recupera informações de vulnerabilidade da integração Tenable.sc. As mudanças no método Buscar vulnerabilidades da mensagem

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

REST ou Buscar vulnerabilidades corrigidas ou, a partir da v14.0 Vulnerability Response e v2.2 da Integração de vulnerabilidade da Tenable, Buscar registro de vulnerabilidades de preenchimento afetam as solicitações feitas a Tenable.sc para recuperar informações de vulnerabilidades.

Tenable.sc Mensagem REST de credenciais de verificação

Tenable.sc Mensagem REST de política

A mensagem POST REST de política Tenable.sc adiciona uma política para os plug-ins solicitados. A política gerada será usada em Tenable.sc solicitações de verificação.

Tenable.sc Verificar mensagem REST

A mensagem POST REST de verificação da Tenable.sc adiciona uma verificação que depende do acesso e da permissão definidos no corpo da solicitação da mensagem REST. Ele usa política, ID de plug-in e IP(s) no corpo da solicitação para a solicitação de verificação.

Tenable.sc Mensagem REST do resultado da verificação

A mensagem Tenable.sc Scan Result GET REST fornece detalhes da verificação gerada usando a mensagem Scan REST. Ele usa o scanResultId na resposta das mensagens REST de verificação e recupera os detalhes da verificação acionada.

Tenable.sc Credenciais de verificação

A mensagem REST de credenciais de verificação Tenable.sc recupera as informações de credenciais de Tenable.sc. As mudanças no registro do método "Importar" da mensagem REST afetam as solicitações feitas a Tenable.sc para recuperar as informações de credenciais.

Nome do parâmetro	Valor	Descrição
campos	id, nome, descrição, tipo	Indica a lista de campos importados de Tenable.sc
filtros	utilizável	Indica que a integração extrai somente credenciais utilizáveis de Tenable.sc Mudanças em qualquer um dos parâmetros não são recomendadas.

Transformação de dados para a integração de vulnerabilidade da Tenable

Depois de identificar os dados a serem importados, eles são recuperados do produto Tenable e processados por meio de um conjunto de fontes de dados e transformações em sua instância.

Durante a instalação, os mapas de severidade normalizados são instalados no módulo Mapeamento de severidade normalizado. Esses mapas transformam os níveis de severidade da Tenable importados em níveis de severidade padrão para processamento em sua instância. Para obter informações sobre como criar mapas de severidade, consulte Criar um mapa de severidade do Vulnerability Response na documentação do Vulnerability Response.

Importação de ativo da Tenable.io

Os dados do ativo importado são carregados primeiro na tabela Importação de ativo Tenable.io [sn_vul_tenable_io_asset_import].

O mapa de transformação de integração de ativos da Tenable.io é usado para transformar as informações de ativos importados. As mudanças nesta transformação alteram

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

como os dados da importação do ativo da Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação**. Pesquise Transformação de ativo Tenable.io.

As tabelas a seguir listam os campos do mapa de transformação por integração.

Campos do mapa de transformação de ativo da Tenable.io

Campo de origem	Campo de destino	Descrição
u_id	source_id	A Tenable fornece um ID exclusivo para ativos e mapas para o registro do item descoberto e é usado para pesquisa de IC.
u_ipv4s	ip_address	Mapeia o primeiro valor de IP para o campo ip_address no registro do item descoberto.
u_mac_addresses	mac_address	Mapeia o primeiro valor de mac_address para o campo de endereço mac no registro do item descoberto.
u_fqdns	fqdn	Mapeia o primeiro valor fqdn para o campo fqdn no registro do item descoberto.
u_netbios_names	netbios	Mapeia o primeiro valor netbios para o campo netbios no registro do item descoberto.
u_operating_systems	os	Mapeia o primeiro valor de SO para o campo de SO no registro do item descoberto.
(Antes da v 14.0 Vulnerability Response e v2.2 da integração de vulnerabilidade da Tenable)u_last_scan_time	data_última_verificação	Mapeia para o campo last_scan_date no registro do item descoberto.
u_last_authenticated_scan_date	last_auth_scan_date	Mapeia para o campo last_auth_scan_date no registro do item descoberto.
[script]	nome	Mapeia o nome do host usando a lógica do script.
u_tags		Os marcadores são salvos em sn_sec_cmn_host_tag. O mapeamento de marcadores para ativos é salvo em sn_sec_cmn_m2m_src_ci_tag.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tempo e finalidade do script do mapa de transformação de ativo da Tenable.io

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Modificar ou excluir não é recomendado.
onBefore (antes de um conjunto de importação concluir a transformação).	Uma função usada para atualizar valores no host e verificar se o host já existe. Com base nos resultados, modifica os valores em um import_set. Para uso interno. Modificar ou excluir não é recomendado.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos ICs criados e ICs que foram atualizados e ignorados. Para uso interno. Modificar ou excluir não é recomendado.

Integração de plug-ins Tenable.io

O mapa de transformação de plug-ins Tenable.io é usado para transformar plug-ins importados do Tenable.io.

Nota:
As mudanças neste mapa de transformação alteram como os dados recebidos dos plug-ins da Tenable são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação**. Pesquise a transformação do plug-in Tenable.io.

A carga dos plug-ins da Tenable.io contém todos os campos na coluna u_attributes da tabela sn_vul_tenable_io_plugin_import. O campo de atributos é analisado e mapeado para os registros da tabela de entrada de terceiros, conforme listado na tabela a seguir.

Campo de origem	Campo de destino	Descrição
id	id	Mapeia o ID da origem e adiciona o prefixo TEN- a ele. Por exemplo, se o ID recebido for 12345, o ID na tabela de destino será TEN-12345.
Descrição	resumo	Mapeia a descrição do plug-in para a coluna de resumo.
[script]	fonte	A origem do TPE importado é Tenable.io.
[script]	source_instance	Referência à implantação da Tenable que importa este registro.
família	categoria	Mapeia a família do plug-in para a coluna da categoria
plug-in_modification_date	last_modified	Mapeia o plugin_modification_date para o último campo modificado.
data_publicação_plug-in	date_published	Mapeia o plugin_publication_date para a data de publicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
tem_patch	correção_tipo	Mapeia o tipo de correção do valor has_patch.
synopsis	ameaça	Mapeia as informações de ameaça sobre esta vulnerabilidade.
cvss_base__score	pontuação	Mapeia a pontuação base de cvss para a coluna de pontuação na tabela de entrada de terceiros.
solução	solução	Mapeia a solução fornecida pelo scanner para a coluna de solução na tabela de entrada de terceiros.
explore_available	exploração	Mapeia o explore_available fornecido pelo scanner para a coluna de exploração na tabela de entrada de terceiros
vpr.pontuação	source_risk_score	Mapeia a pontuação vpr fornecida pelo scanner para source_risk_score na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 - Crítico • 7 – 9 – Alto • 4 – 7 – Médio • 0-4 - Baixo
vpr.drivers.age_of_vuln	age_of_vuln	Mapeia a idade da vulnerabilidade do scanner para a coluna age_of_vuln na tabela de entrada de terceiros.
vpr.drivers.exploit_code_maturity	explore_code_maturity	Mapeia a maturidade do código de exploração do scanner para explore_code_maturity na tabela de entrada de terceiros.
vpr.drivers.product_coverage	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
vpr.drivers.threat_sources_last28	ameaça_fontes	Mapeia as origens de ameaça nos últimos 28 dias do scanner para o Threat_sources na tabela de terceiros.
vpr.drivers.threat_intensity_last28	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para o Threat_intensity na tabela de entrada de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
vpr.drivers.threat_recency	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para Threat_recency na tabela de entrada de terceiros.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mapeia a pontuação de impacto do cvss3 para a coluna v3_impact_subscore na tabela de entrada de terceiros.
cvss_pontuação_temporais	cvss_pontuação_temporais	Mapeia a pontuação temporal para CVSS v2.
cvss_v3_tempo_pontuação	v3_tempo_pontuação	Mapeia a pontuação temporal para CVSS v3.
risk_factor	source_severity	Mapeia para a severidade de origem na tabela de entrada de terceiros.
nome	nome	Mapeia o nome do plug-in para o nome na tabela de entrada de terceiros.
stíg_severidade	stíg_severidade	Mapeia a pontuação vpr fornecida pelo scanner para source_risk_score na tabela de entrada de terceiros.
plug-in_type	check_type	Mapeia o tipo de plug-in para check_type na tabela de entrada de terceiros.
unsupported_by_vendor	unsupported_by_vendor	Mapeia o campo unsupported_by_vendor para a coluna unsupported_by_vendor.
[script]	explore_attack_vector	A coluna explore_attack_vector na tabela de entrada de terceiros é preenchida com base em explore_available e v3_attack_vector das colunas.

Além dos campos diretos, outras informações são adicionadas como listas relacionadas às entradas de terceiros.

Campo de origem	Descrição
cve	Insere dados relacionados a CVE na tabela de referência (sn_vul_nvd_entry). Se o mesmo CVE na tabela de entrada do NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada do NVD. O mapeamento pode ser encontrado em sn_vul_m2m_entry_cve.
bid	A lista de traqs de erros é adicionada como uma referência.
ver_também	A lista de URLs é adicionada como uma referência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Descrição
xrefs	A lista de X-REF é adicionada como referência.
[script]	A lista de explorações para esse plug-in e insere mapeamento para estrutura de exploração aplicável e plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Modificar ou excluir não é recomendado.
onBefore (antes de um conjunto de importação concluir a transformação).	Uma função usada para atualizar os valores na entrada do terceiro e verificar se a entrada do terceiro já existe. Com base nos resultados, modifica os valores em uma entrada de terceiros. Para uso interno. Modificar ou excluir não é recomendado.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos ICs criados e ICs que foram atualizados e ignorados. Para uso interno. Modificar ou excluir não é recomendado.

A inclusão de script TenableIOPluginsImportProcessor é chamada a partir do script de transformação onBefore. Ele obtém a saída da integração de plug-ins Tenable.io e a transforma em Now Platform entradas de vulnerabilidade de terceiros. Quaisquer mudanças nesta inclusão de script podem alterar a transformação dos dados dos plug-ins Tenable.io na tabela de entrada de terceiros.

Importação de vulnerabilidades da Tenable.io

O mapa de transformação de item vulnerável da Tenable.io é usado para transformar informações de vulnerabilidades abertas e fixas importadas da Tenable.io.

Nota:
As mudanças neste mapa de transformação alteram como os dados da importação de vulnerabilidades da Tenable são processados.

O mesmo mapa de transformação é usado para a integração de vulnerabilidades fixas da Tenable.io e a integração de vulnerabilidades abertas da Tenable.io. Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação**. Pesquise o mapa de transformação do item vulnerável Tenable.io.

Campo de origem	Campo de destino	Descrição
u_asset.uuid	id	O Uuid é mapeado para o campo id do registro cmdb_ci.
u_asset.ipv4	ip_address	O campo ipv4 é mapeado para o campo de endereço IP do registro cmdb_ci.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_asset .last_authenticated_results	last_auth_scan_date	A data da última verificação autenticada é mapeada para a data da última verificação de autenticação do registro cmdb_ci.
u_asset.mac_address	mac_address	O endereço Mac é mapeado para o campo de endereço MAC do host do registro cmdb_ci.
u_asset.netbios_name	netbios	O NetBIOS é mapeado para o campo netBIOS do registro cmdb_ci.
u._plugin.cvss3_base_score	v3_base_score	A pontuação base do CVSS v3 é mapeada para a pontuação base v3 do registro de entrada do terceiro.
u._plugin.cvss3_tempo_score	v3_tempo_pontuação	A pontuação temporal do CVSS v3 é mapeada para a pontuação temporal do v3 no registro de entrada de terceiros.
u._plugin.cvss_base_score	pontuação	A pontuação base do CVSS é mapeada para o campo de pontuação do registro de entrada de terceiros.
u._plugin.cvss_tempo_score	temporal_score	A pontuação temporal é mapeada para a pontuação temporal no registro de entrada do terceiro.
u_plugin.description	resumo	A descrição é mapeada para o campo de resumo no registro de entrada do terceiro.
u_plugin.family	categoria	Mapeia a família de plug-ins para a coluna de categoria do registro de entrada de terceiros.
u_plugin.modification_date	last_modified	A data da última modificação é mapeada para a data da última modificação do plug-in no registro de entrada do terceiro.
u_plugin.publication_date	date_published	A data de publicação é mapeada para o campo de data de publicação do registro de entrada do terceiro.
u_plugin.risk_factor	source_severity	O fator de risco é mapeado para o campo source_severity

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		do registro de entrada do terceiro.
u_plugin.solução	solução	A solução é mapeada para o campo de solução do registro de entrada do terceiro.
u_plugin.sinopse	ameaça	A sinopse é mapeada para o campo de ameaça do registro de entrada do terceiro.
u_id_severidade	prioridade	A prioridade é mapeada para o ID de severidade da carga útil. O valor padrão é 5.
u_plugin.exploit_available	exploração	Mapeia o explore_available fornecido pelo scanner para a coluna de exploração na tabela de entrada de terceiros.
vpr.pontuação	source_risk_score	Mapeia a pontuação vpr fornecida pelo scanner para source_risk_score na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 - Crítico • 7 – 9 – Alto • 4 – 7 – Médio • 0-4 - Baixo
u_plugin.vpr.drivers.age_of_vuln	age_of_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_plugin.vpr.drivers.exploit_code_maturity	explore_code_maturity	Mapeia a maturidade do código de exploração do scanner para explore_code_maturity na tabela de entrada de terceiros.
u_plugin.vpr.drivers.product_coverage	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_plugin.vpr.drivers.threat_sources_last28	ameaça_fontes	Mapeia as origens de ameaça nos últimos 28 dias do scanner para Threat_sources na tabela de entrada de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_plugin.vpr.drivers.threat_intensity_last28	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para o Threat_intensity na tabela de entrada de terceiros.
u_plugin.vpr.drivers.threat_recency	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para Threat_recency na tabela de entrada de terceiros.
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS3 v3 para a coluna v3_impact_subscore na tabela de entrada de terceiros.
u_plugin.type	check_type	Mapeia o tipo de plug-in para check_type na tabela de entrada de terceiros.
u_plugin.unsupported_by_vendor	unsupported_by_vendor	Mapeia o campo unsupported_by_vendor no plug-in para a coluna unsupported_by_vendor.
[script]	explore_attack_vector	A coluna explore_attack_vector na tabela de entrada de terceiros é preenchida com base em explore_available e v3_attack_vector das colunas.
u_plugin.family_id	Family_id	Mapeia o ID da família do plug-in para a coluna family_id na tabela de entrada de terceiros.
port	port	A porta é mapeada para o campo de porta do registro do item vulnerável.
protocolo	protocolo	O protocolo é mapeado para o campo de protocolo do registro do item vulnerável.
u_first_found	first_found	O primeiro encontrado é mapeado para o primeiro campo encontrado do registro do item vulnerável.
u_last_found	last_found	O último encontrado é mapeado para o último campo encontrado do registro do item vulnerável.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_state	state	O estado é mapeado para o campo Estado no registro do item vulnerável
[script]	fonte	A origem da integração é preenchida. Os itens vulneráveis criados a partir desta integração têm o Tenable.io como origem.
[script]	integration_instance	integration_instance é o nome da instância da qual o item vulnerável é importado.
u_plugin.name	nome	Mapeia o nome do plug-in para o nome na tabela de entrada de terceiros.
u_plugin.sting_severity	stíg_severidade	Mapeia a severidade padrão do plug-in para a coluna de severidade padrão na tabela de entrada de terceiros

Além dos campos diretos, outras informações são adicionadas como listas relacionadas às entradas de terceiros.

Campo de origem	Descrição
cve	Insere dados relacionados a CVE na tabela de referência (sn_vul_nvd_entry). Se o mesmo CVE na tabela de entrada do NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada do NVD. O mapeamento pode ser encontrado em sn_vul_m2m_entry_cve.
bid	A lista de traqs de erros é adicionada como uma referência.
ver_também	A lista de URLs é adicionada como uma referência.
xrefs	A lista de X-REF é adicionada como referência.
[script]	A lista de explorações para esse plug-in e o mapeamento de inserções para a estrutura de exploração aplicável e o plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação aciona o TenableIOVulnerabilitiesProcessor, que importa dados do Tenable.io usando o conjunto de importação e carrega cada registro na tabela de IC do CMDB, na tabela de itens vulneráveis e na tabela de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando o script é executado	Finalidade
	vulnerabilidade de terceiros.Para uso interno. Modificar ou excluir não é recomendado.
onBefore (antes de um conjunto de importação concluir a transformação).	Uma função para verificar se a entrada e as detecções de terceiros já existem. Caso contrário, esses registros serão criados em suas respectivas tabelas. Para uso interno. Modificar ou excluir não é recomendado.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para atualizar a contagem de ICs, IVs e Detecções conforme importados do Tenable.io. Para uso interno. Modificar ou excluir não é recomendado.

Importação de ativo da Tenable.sc

Os dados de ativo importados do Tenable.sc são carregados primeiro na tabela de importação de ativo do Tenable.sc (sn_vul_tenable_sc_asset_import). O mapa de transformação de integração de ativos da Tenable.sc é usado para transformar as informações de ativos importados. As mudanças nesta transformação alteram como os dados da importação de ativos da Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação**. Pesquise a Transformação do ativo Tenable.sc.

Campo de origem	Campo de destino	Descrição
u_uuid	id	O uuid não é preenchido a partir da API da Tenable, portanto, o atributo "u_uniqueness" é usado para criar um campo uuid exclusivo para ativos e mapeá-lo para o registro cmdb_ci.
u_ip	ip_address	Mapeia o campo ip da API para o campo ip_address em um registro cmdb_ci.
u_macaddress	mac_address	Mapeia o campo de endereço eletrônico da API para o campo de endereço no registro cmdb_ci.
u_dnsname	fqdn	Mapeia o campo dnsname da API para o campo fqdn no registro cmdb_ci.
u_netbiosname	netbios	Mapeia o campo netbios da API para o campo netbios no registro cmdb_ci.
u_oscpe	os	As informações do SO são extraídas do atributo oscpe na carga útil e as mapeiam para o campo os no registro cmdb_ci.
u_lastauthrun	last_auth_scan_date	Mapeia o campo lastauthrun da API para o campo last_auth_scan_date no registro do item descoberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_lastauthrun e u_lastunauthrun	data_última_verificação	O lastauthrun é extraído da API da Tenable ou lastunauthrun. Com base no valor que aparece na carga útil, o campo last_scan_date no registro do item descoberto é preenchido.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Modificar ou excluir não é recomendado.
onBefore (antes de um conjunto de importação concluir a transformação).	Função usada para atualizar os valores no host e verificar se o host já existe. Com base nos resultados, modifica os valores em um import_set. Para uso interno. Modificar ou excluir não é recomendado.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos ICs criados e ICs que foram atualizados e ignorados. Para uso interno. Modificar ou excluir não é recomendado.

Importação de plug-ins Tenable.sc

Os dados de plug-ins importados do Tenable.sc são carregados primeiro na tabela de importação de plug-ins do Tenable.sc (sn_vul_tenable_sc_plugin_import). O mapa de transformação de plug-in Tenable.sc é usado para transformar as informações de plug-in que foram importadas. As mudanças nesta transformação alteram como os dados da importação do plug-in da Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação**. Pesquise o mapa de transformação do plug-in Tenable.sc.

Campo de origem	Campo de destino	Descrição
u_id	id	Mapeia o ID da origem e adiciona o prefixo TEN-. Por exemplo, se o ID recebido for 12345, o ID na tabela de destino será TEN-12345.
u_description	resumo	Mapeia a descrição do plug-in para a coluna de resumo.
[script]	fonte	O TPE importado desta integração tem Tenable.sc como origem.
[script]	source_instance	Referência à implantação da Tenable que importa este registro.
u_family	categoria	Mapeia o campo de nome no objeto de família do plug-in para a coluna de categoria.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_plugin_modification_date	last_modified	Mapeia o plugin_modification_date para o último campo modificado.
u_plugin_publication_date	date_published	Mapeia o plugin_publication_date para a data de publicação.
u_has_patch	Remediation_type	Mapeia o tipo de correção do valor has_patch.
u_sinopse	ameaça	Mapeia as informações de ameaça sobre esta vulnerabilidade.
u_cvss_base_score	pontuação	Mapeia a pontuação base do CVSS para a coluna de pontuação na tabela de entrada de terceiros.
u_solution	solução	Mapeia a solução fornecida pelo scanner para a coluna de solução na tabela de entrada de terceiros.
u_cvss_tempo_pontuação	cvss_pontuação_temporais	Mapeia a pontuação temporal para CVSS v2.
u_cvss_v3_tempo_pontuação	v3_tempo_pontuação	Mapeia a pontuação temporal para CVSS v3.
u_risk_factor	severidade de origem	Mapeia para a severidade de origem na tabela de entrada de terceiros.
u_cvss_v3_base_score	v3_base_score	Mapeia a pontuação base do CVSS na tabela de entrada de terceiros.
u_exploit_available	exploração	Mapeia a exploraçãoDisponível fornecida pelo scanner para a coluna de exploração na tabela de entrada de terceiros.
u_vpr_score	source_risk_score	Mapeia a pontuação VPR do scanner para a pontuação de risco de origem na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 - Crítico • 7 – 9 – Alto • 4 – 7 – Médio • 0-4 - Baixo
u_vpr_context[id=age_of_vuln]	age_of_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_vpr_context[id=exploit_code_maturity]	explore_code_maturity	Mapeia a maturidade do código de exploração do scanner para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		explore_code_maturity na tabela de entrada de terceiros.
u_vpr_context[id=product_coverage]	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_vpr_context[id="threat_sources_last_28"]	ameaça_fontes	Mapeia origens de ameaça nos últimos 28 dias do scanner para Threat_sources na tabela de terceiros.
u_vpr_context[id="threat_intensity_last_28"]	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para o Threat_intensity na tabela de entrada de terceiros.
u_vpr_context[id="threat_recency"]	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para Threat_recency na tabela de entrada de terceiros.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS v3 do scanner para v3_impact_subscore na tabela de entrada de terceiros.
u_name	nome	Mapeia o nome do plug-in para a coluna de nome na tabela de entrada de terceiros.
u_sting_severity	stíg_severidade	Mapeia o campo stíg_severity no plug-in para stíg_severidade na tabela de entrada de terceiros.
u_check_type	check_type	Mapeia o tipo de verificação para check_type na tabela de entrada de terceiros.
u_family.id	id_da_família	Mapeia o plug-in family_id para family_id na tabela de entrada de terceiros.
[script]	explore_attack_vector	A coluna explore_attack_vector na tabela de entrada de terceiros é preenchida com base em explore_available e v3_attack_vector das colunas.

Além dos campos diretos, outras informações são adicionadas como listas relacionadas às entradas de terceiros.

Campo de origem	Descrição
u_cpe	A lista de CPEs é adicionada como referência.
u_see_also	A lista de URLs é adicionada como uma referência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Descrição
u_exploit_frameworks	A lista de explorações para esse plug-in e insere mapeamento para estrutura de exploração aplicável e plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Modificar ou excluir não é recomendado.
onBefore (antes de um conjunto de importação concluir a transformação).	Função usada para atualizar os valores na entrada do terceiro e verificar se a entrada do terceiro já existe. Com base nos resultados, modifica os valores em uma entrada de terceiros. Para uso interno. Modificar ou excluir não é recomendado.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de plug-ins criados e ignorados. Para uso interno. Modificar ou excluir não é recomendado.

A inclusão de script TenableSCPluginsImportProcessor é chamada a partir do script de transformação onBefore. Ele obtém a saída da integração de plug-ins Tenable.sc e a transforma em entradas de vulnerabilidade de terceiros da Servicenow. Quaisquer mudanças nesta inclusão de script podem alterar a transformação dos dados dos plug-ins Tenable.sc na tabela de entrada de terceiros.

Importação de vulnerabilidades da Tenable.sc

O mapa de transformação Tenable.sc Open Vulnerabilities é usado para transformar dados importados da integração de vulnerabilidades abertas Tenable.sc, e o mapa de transformação Tenable.sc e Vulnerabilidades fixas é usado para transformar dados importados da integração de vulnerabilidades fixas Tenable.sc.

Nota:
As mudanças nesses mapas de transformação alteram como os dados da importação de vulnerabilidades fixas/em aberto da Tenable são processados.

Para acessar os mapas de transformação de vulnerabilidades abertas e fixas da Tenable.sc, navegue até **Integração de vulnerabilidade Tenable** > **Administração** > **Instâncias de Integração** > **Integração de vulnerabilidades fixas/em aberto da Tenable.sc** > **Fontes de dados** > **Vulnerabilidades em aberto/corrigidas da Tenable.sc** > **Transformações**.

Campo de origem	Campo de destino	Descrição
u_pluginID	Id	Usado como o identificador do plug-in. Este campo é mapeado para o ID do plug-in no registro de entrada do terceiro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_riskfactor	source_severity	Este campo é mapeado para source_severity no registro de entrada de terceiros.
u_severidade	prioridade	O campo de prioridade é mapeado com a severidade. O valor padrão é 5.
u_hasbeenmitigado	state	Hasbeenmitigado é mapeado para o campo de estado do registro de vulnerabilidade. Para a integração de vulnerabilidades corrigidas, todos os IVs estão no estado "Encerrado".
u_ip	ip_address	O endereço IP é mapeado para o campo de ip do host da tabela cmdb_ci.
u_port	port	A porta é mapeada para o campo de porta do registro do item vulnerável.
u_protocol	protocolo	O protocolo é mapeado para o campo de porta do registro do item vulnerável.
u_firstVen	first_found	O primeiro valor visto é mapeado para o primeiro campo encontrado do registro IV.
u_lastVen	last_found	O último valor visto é mapeado para o último campo encontrado do registro IV.
u_exploitDisponível	exploração	ExploitAvailable é mapeado para o campo de exploração no registro de entrada do terceiro.
u_sinopse	ameaça	A sinopse é mapeada para o campo de ameaça no registro de entrada do terceiro.
u_description	resumo	A descrição é mapeada para o campo de resumo no registro de entrada do terceiro.
u_solution	solução	A solução é mapeada para o campo de solução no registro de entrada do terceiro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_basescore	pontuação	BaseScore é mapeado para o campo de pontuação no registro de entrada do terceiro.
Pontuação_temporais	temporal_score	A pontuação temporal é mapeada para a pontuação temporal no registro de entrada do terceiro.
u_cvssv3basescore	v3_base_score	O cvssv3basescore é mapeado para a pontuação base v3 no registro de entrada do terceiro.
u_cvsspontuação temporal	v3_tempo_pontuação	A pontuação cvssv3 temporal é mapeada para a pontuação temporal v3 no registro de entrada do terceiro.
u_pluginpublicar data	date_published	A data de publicação do plug-in é mapeada para a data de publicação do plug-in no registro de entrada de terceiros.
u_pluginmoddate	last_modified	A data da última modificação é mapeada para a data da última modificação do plug-in no registro de entrada do terceiro.
u_dnsname	fqdn	DnsName é mapeado para o campo FQDN do registro cmdb_ci.
u_macaddress	mac_address	MacAddress é mapeado para o campo mac_address do registro cmdb_ci.
u_netbiosName	netbios	NetBIOSName é mapeado para o campo NETBIOS do registro cmdb_ci.
u_ip	ip	O IP é mapeado para o campo IP do registro cmdb_ci.
hostUniqueness	uuid	A exclusividade do host não é mapeada para nenhum campo, mas é usada para determinar o UUID do host.
u_family	categoria	Mapeia o campo de nome no objeto de família do plug-in para a coluna de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		categoria do registro de entrada do terceiro.
u_plugintext	prova	O texto do plug-in é mapeado para a prova no registro.
[script]	fonte	A origem da integração é preenchida. Os itens vulneráveis criados a partir desta integração têm Tenable.sc como origem.
[script}	integration_instance	integration_instance é o nome da instância da qual o item vulnerável é importado.
u_vpr_score	source_risk_score	Mapeia a pontuação VPR do scanner para a pontuação de risco de origem na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 - Crítico • 7 – 9 – Alto • 4 – 7 – Médio • 0-4 - Baixo
u_vpr_context[id=age_of_vuln]	age_of_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_vpr_context[id=exploit_code_maturity]	explore_code_maturity	Mapeia a maturidade do código de exploração do scanner para explore_code_maturity na tabela de entrada de terceiros.
u_vpr_context[id=product_coverage]	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_vpr_context[id=”threat_sources_last_28]	ameaça_fontes	Mapeia as origens de ameaça nos últimos 28 dias do scanner para Threat_sources na tabela de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_vpr_context[id=”threat_intensity_last_28]	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para o Threat_intensity na tabela de entrada de terceiros.
u_vpr_context[id=”threat_recency”]	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para Threat_recency na tabela de entrada de terceiros.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS v3 do scanner para v3_impact_subscore na tabela de entrada de terceiros.
u_pluginname	nome	Mapeia o nome do plug-in para a coluna de nome na tabela de entrada de terceiros.
u_stiqueseveridade	stíg_severidade	Mapeia o campo stíg_severity no plug-in para stíg_severidade na tabela de entrada de terceiros.
u_checktype	check_type	Mapeia o tipo de verificação para check_type na tabela de entrada de terceiros.
u_family.id	id_da_família	Mapeia o plug-in family.id para family_id na tabela de entrada de terceiros.
[script]	explore_attack_vector	A coluna explore_attack_vector na tabela third_party_entry é preenchida com base em explore_available e v3_attack_vector das colunas.

Campo de origem	Descrição
u_cve	Insere dados relacionados a CVE na tabela de referência (sn_vul_nvd_entry). Se o mesmo CVE na tabela de entrada do NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada do NVD. O mapeamento é encontrado em sn_vul_m2m_entry_cve.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Descrição
u_id	A lista de traqs de erros é adicionada como uma referência.
u_cpe	A lista de CPEs é adicionada como referência.
u_seealso	A lista de URLs é adicionada como uma referência.
u_xrefs	A lista de X-REFs é adicionada como referência.
u_exploitframeworks	A lista de explorações para esse plug-in e o mapeamento de inserções para a estrutura de exploração aplicável e o plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Modificar ou excluir não é recomendado.
onBefore (antes de um conjunto de importação concluir a transformação).	Função usada para atualizar os valores na vulnerabilidade e verificar se a vulnerabilidade já existe. Com base nos resultados, modifica os valores em uma tabela de itens vulneráveis. Para uso interno. Modificar ou excluir não é recomendado.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos IVs criados e IVs que foram atualizados e ignorados. Para uso interno. Modificar ou excluir não é recomendado.

Definir parâmetros de filtro adicionais para importações de Tenable.io

Personalize os parâmetros de filtragem das consultas programadas com Tenable Vulnerability Integration para ajudar a refinar ainda mais os dados de vulnerabilidade importados com o produto Tenable.io.

Antes de Iniciar

Casos de uso: como gerente ou analista de vulnerabilidade, convém filtrar os dados de suas consultas para que você possa revisar somente os detalhes específicos da vulnerabilidade. Por exemplo, digamos que você queira exibir vulnerabilidades importadas que são filtradas por `cidr_range`, `num_assets`, `indexed_ate` `plugin_family`. Ou digamos que você queira executar uma integração Tenable.io de modo que uma execução importe somente vulnerabilidades críticas a cada quatro horas e outra seja executada a cada 24 horas para buscar todas as outras vulnerabilidades não críticas.

Para ajudá-lo a coletar esses dados, você pode adicionar parâmetros compatíveis com a Tenable para ajudá-lo a importar os detalhes da vulnerabilidade específica de que precisa.

Sem adicionar chamadas de API ou codificação adicionais, este recurso permite que você personalize suas informações de solicitação HTTP com parâmetros da Tenable em seu Now Platform. As seguintes integrações Tenable.io oferecem suporte à filtragem, fornecendo conteúdo JSON no corpo da solicitação:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Integração de ativos
- Integração de vulnerabilidade fixa
- Abrir integração de vulnerabilidades

Você deve saber como usar cadeias de caracteres JSON para este recurso.

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Localize os parâmetros compatíveis com o produto Tenable.io no site do desenvolvedor que você deseja usar para sua filtragem.

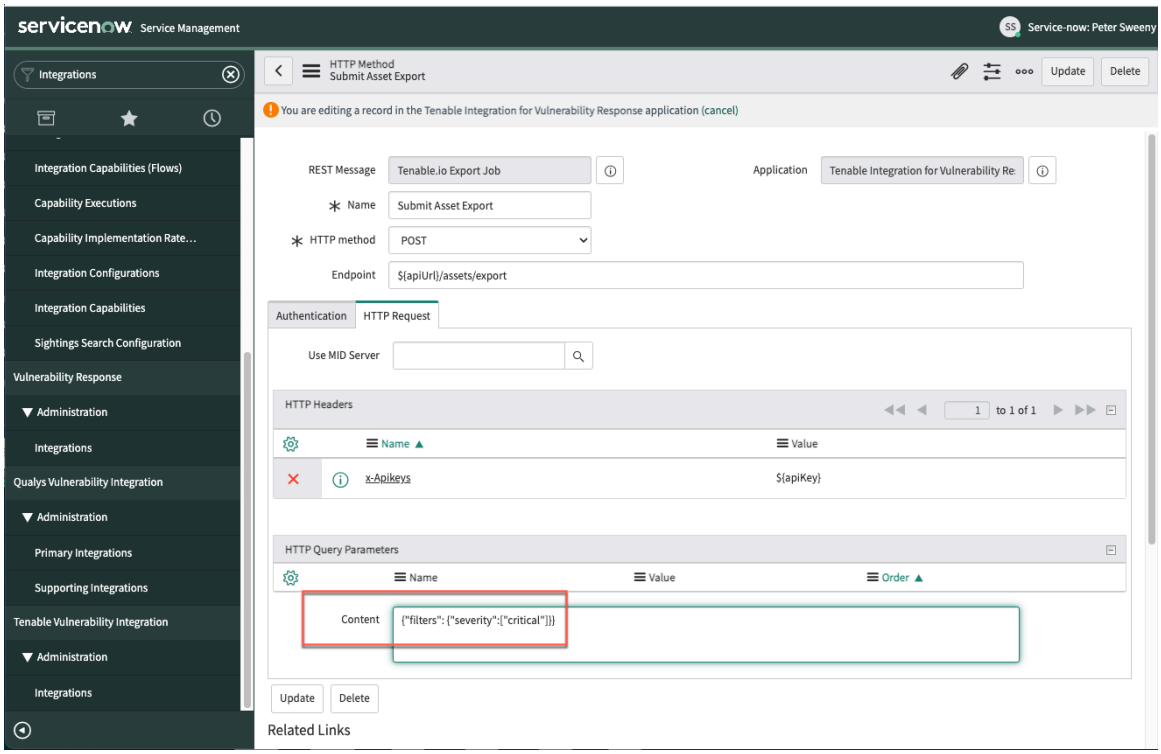
   Os parâmetros e valores inseridos no produto Tenable.io são compatíveis somente no nível da instância de integração.

2. Navegar até **Todos** > **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
3. Na página da lista de integrações da Tenable, clique no registro da integração Tenable.io que você deseja abrir.
4. Com a guia Métodos REST da Tenable selecionada, clique no ícone de informações (I) do método REST seguido por **Abrir registro**.
5. Selecione a guia **Solicitação HTTP**.
6. Para editar o registro, na parte superior da página, clique no link em. Para editar o registro, clique **aqui**.
7. No registro Método REST no campo Conteúdo, insira o conteúdo JSON que você deseja como parte do corpo da solicitação.

   Na imagem a seguir, como exemplo, o parâmetro de severidade das vulnerabilidades importadas, `{"filters": {"severity": ["critical"]}}` foi personalizado para a integração de ativos Tenable.io. Este valor importa somente vulnerabilidades críticas (pontuação de CVSS de 10,0).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se você quiser inserir mais de um parâmetro, consulte a documentação Tenable.io para obter mais informações sobre como separar cada valor.

8. Clique em **Atualizar**.

Relatório de integração de vulnerabilidade da Tenable

Exiba relatórios sobre vulnerabilidades e itens vulneráveis nos painéis Vulnerability Response.

Visualizações de dados nos espaços Vulnerability Response

Os espaços Vulnerability Response incluem visualizações de dados que podem ajudar a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a severidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizadas conforme os dados de vulnerabilidade mudam. Consulte Vulnerability Response Espaços, Explorando o Vulnerability Manager Workspace e Explorando o Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos que estão disponíveis.

Versões anteriores de Vulnerability Response

O painel de visão geral do Vulnerability Response (Vulnerability Management) fornece uma visão executiva de vulnerabilidades e itens vulneráveis, ajudando o Administrador de Vulnerabilidades a identificar rapidamente as áreas de preocupação. O painel de correção do Vulnerability Response (Correção de vulnerabilidade) permite que um especialista em correção se concentre nas tarefas de correção e nos itens vulneráveis que possui.

Para obter mais informações, consulte Usando os painéis padrão Vulnerability Response.

Função necessária: responsável pela correção.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que os usuários podem fazer e ver na aplicação Vulnerability Response. Para obter a atribuição inicial das

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração.

Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

para exibir o painel, navegue até **Vulnerability Response** > **Visão Geral da Correção**.

Gráfico de status de execução da integração para a integração de vulnerabilidade da Tenable

O módulo Status de execução de integração da Tenable fornece uma exibição gráfica do status das execuções de integração da Tenable.

No gráfico, aponte para qualquer parte do gráfico para exibir um resumo dos dados específicos dessa parte. Se você clicar em qualquer parte do gráfico de barras, uma lista será aberta para fornecer informações mais detalhadas.

Função necessária: administrador de vulnerabilidade.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que os usuários podem fazer e ver na aplicação Vulnerability Response. Para obter a atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração.

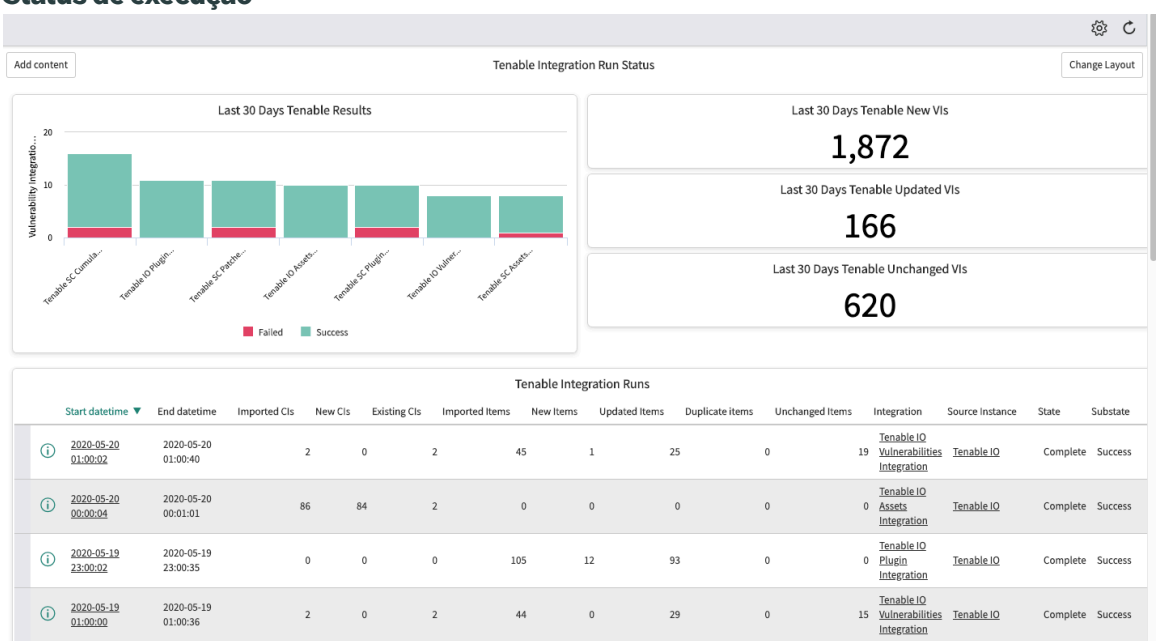
Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Para exibir os dados, navegue até **Todos** > **Integração de vulnerabilidade Tenable** > **Status da Execução da Integração**.

A partir da versão 19.0 do Vulnerability Response, este painel está disponível na IU da nova experiência.

Nota:
Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Status de execução



Start datetime	End datetime	Imported CIs	New CIs	Existing CIs	Imported Items	New Items	Updated Items	Duplicate items	Unchanged Items	Integration	Source Instance	State	Substate
2020-05-20 01:00:02	2020-05-20 01:00:40	2	0	2	45	1	25	0	19	Tenable IO Vulnerabilities Integration	Tenable IO	Complete	Success
2020-05-20 00:00:04	2020-05-20 00:01:01	86	84	2	0	0	0	0	0	Tenable IO Assets Integration	Tenable IO	Complete	Success
2020-05-19 23:00:02	2020-05-19 23:00:35	0	0	0	105	12	93	0	0	Tenable IO Plugin Integration	Tenable IO	Complete	Success
2020-05-19 01:00:00	2020-05-19 01:00:36	2	0	2	44	0	29	0	15	Tenable IO Vulnerabilities Integration	Tenable IO	Complete	Success

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

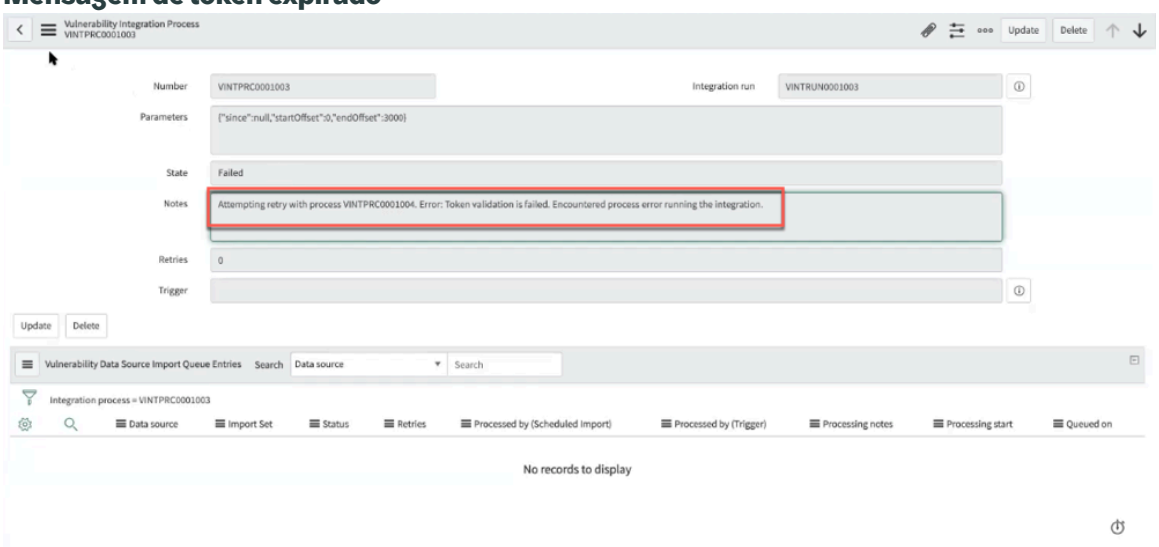
Relatórios do gráfico de status de execução da integração da Tenable

Nome	Descrição
Resultados do Tenable nos últimos 30 dias	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Cada execução exibida como uma barra no gráfico.
VIs novos do Tenable nos últimos 30 dias	O número de novos itens vulneráveis importados nos últimos 30 dias. Mostrado como um número inteiro.
VIs atualizados do Tenable nos últimos 30 dias	O número de itens vulneráveis atualizados importados nos últimos 30 dias. Mostrado como um número inteiro.
VIs inalterados do Tenable nos últimos 30 dias	O número de itens vulneráveis duplicados importados nos últimos 30 dias. Mostrado como um número inteiro.
Execuções de integrações do Tenable	Os registros de execução de integração em uma lista. **Nota:** **V16.1:** para verificar as detecções para esta integração, compare as detecções ou descobertas com os dados de detecção ServiceNow`sn_vul_detection`] na tabela . Enquanto a integração está em andamento, pode haver uma mudança na detecção ou na contagem de descobertas. Este relatório exibe a contagem de detecções na coluna "Contagem até a data" na instância, após a conclusão da execução da integração.

Expiração da validação do token

Se uma execução de integração do Tenable.sc falhar por qualquer motivo, o token de autenticação do Tenable.sc expirará automaticamente e uma mensagem será exibida no registro do Processo de integração de vulnerabilidade.

Mensagem de token expirado



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um novo token é gerado automaticamente para o próximo processo de integração. Todos os processos de integração, com falha e bem-sucedidos, são exibidos na guia Processo de integração de vulnerabilidade no registro do Processo de integração de vulnerabilidade.

Iniciar nova verificação para a integração Tenable.sc

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados iniciando novas verificações na plataforma Tenable. Você pode iniciar uma nova verificação sob demanda de itens vulneráveis para o produto Tenable.sc da sua instância Now Platform®.

Antes de Iniciar

Funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Nota:
Tenable.sc não é compatível com a inicialização de uma nova verificação em máquinas baseadas em agente.

Verifique se o scanner está ativado antes de começar. Navegar até **Vulnerability Response** > **Verificação de Vulnerabilidades** > **Scanners**.

Por Que e Quando Desempenhar Esta Tarefa

Para iniciar a nova verificação nos espaços, consulte Verificar novamente Tenable.io e Tenable.sc itens vulneráveis dos espaços Vulnerability Response.

Siga as etapas listadas abaixo para iniciar uma nova verificação no ambiente clássico.

Para ajudar a reduzir a sobrecarga e o volume envolvidos nas verificações completas programadas, os proprietários de correção, especialistas em TI, analistas de vulnerabilidade ou gerentes de vulnerabilidade podem iniciar novas verificações direcionadas sob demanda para vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas verificações de item vulnerável (IV), tarefas de correção (RT), entrada de terceiros (TPE) ou registros de item descoberto da sua instância Now Platform.

As novas verificações permitem que os proprietários de correção e os analistas de vulnerabilidade verifiquem se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

Por exemplo, todo o ambiente é verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada de seus Now Platform para Tenable.sc itens vulneráveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Ao solicitar uma nova verificação da sua instância Now Platform®, a seleção das credenciais Integração do Vulnerability Response com Tenable é opcional. O ServiceNow® Tenable.sc Scan Credential Integration importa e atualiza as credenciais do scanner do produto Tenable.sc em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais da Tenable.

Observe que esses dados importados não incluem senhas da Tenable ou outras informações confidenciais da conta da Tenable. A ServiceNow® Tenable.sc Integração de credencial de verificação é habilitada (Ativo) automaticamente no Assistente de configuração em sua instância quando você configura as Tenable.sc Integrações de vulnerabilidades (Tenable.sc Integrações de vulnerabilidades abertas e corrigidas).

Observe as seguintes informações sobre as credenciais importadas para que os usuários possam vê-las conforme necessário na instância Now Platform :

- As credenciais criadas com a função de usuário administrador Tenable.sc estão disponíveis para usuários em todas as suas organizações.
- As credenciais criadas com a função de usuários organizacionais Tenable.sc estão disponíveis somente para usuários dessa organização. Essas credenciais não são importadas para o Now Platform para usuários fora da organização do criador, a menos que sejam compartilhadas com a conta do usuário que está sendo usada para se conectar à instância.

Consulte o site de documentação Tenable.sc para obter mais informações.

Consulte Configurar a integração de vulnerabilidade da Tenable usando o assistente de configuração para obter mais informações sobre como configurar a aplicação Tenable.sc. Para exibir mais informações sobre o Scan Credential Integration, navegue até **Todos** > **Integração de vulnerabilidade Tenable** > **Integrações** > **Integração de credencial de verificação da Tenable.sc**.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- `sn_sec_cmn.record_threshold_heartbeat`: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- `sn_sec_cmn.maximum_heartbeat_delay`: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Itens vulneráveis**.
2. Localize o registro do item vulnerável do qual você deseja acionar uma nova verificação e abra-o.

   Nota:
   Você só pode iniciar novas verificações de IVs com Tenable.sc como origem. Verifique se Tenable.sc é exibido na coluna **Origem** nas exibições de Lista de IV ou nos campos **Origem** em registros individuais. Você pode usar o construtor de condição para agrupar IVs por origem. Ou, se a coluna Origem não for exibida na exibição da lista de IVs, no canto superior esquerdo da lista, clique no ícone **Personalizar lista** (ícone de engrenagem) e use o Slushbucket para mover a **origem** de **Disponível** para **Selecionado**.

3. Como alternativa, navegue até **Todos** > **Vulnerability Response** > **Tarefas de correção** ou **Vulnerability Response** > **Bibliotecas** > **Terceiros** para a tarefa de correção ou registros de entrada de terceiros, respectivamente, que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o botão **Verificar novamente** está disponível nos seguintes registros:

   - Em um único registro de IV, o IV deve ser do produto Tenable.sc e em qualquer estado diferente de **Encerrado**. Para vários registros de IV, todos os IVs devem ser do produto Tenable.sc e em qualquer estado diferente de **Encerrado**.
   - Em um registro RT, a tarefa de correção pode estar em qualquer estado diferente de **Encerrado**e todos os IVs associados devem ser do produto Tenable.sc.
   - Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro IV associado do produto Tenable.sc em qualquer estado diferente de **Encerrado**.

4. No canto superior direito do registro, clique em **Verificar novamente**.
   Você será solicitado a escolher as credenciais do scanner para acessar o scanner. Essas são as credenciais importadas pela Tenable.sc Scan Credential Integration.
5. Na caixa de diálogo, selecione os filtros e os tipos de credencial desejados.
6. Clique **em Solicitar verificação**.

   Uma mensagem será exibida indicando que a verificação está sendo processada. O status de todas as novas verificações pode ser encontrado a qualquer momento nas listas relacionadas à verificação nos registros IV, RT e TPE usados para iniciar as novas verificações. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e todas as outras verificações iniciadas a partir de um determinado registro.

   O campo Estado no registro de verificação primário é marcado como concluído depois que todas as verificações secundárias são concluídas com sucesso. O secundário verifica os dados de importação. O registro de verificação primário é um contêiner para as verificações secundárias.

   Sua instância Now Platform® rastreia o status de nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando Now Platform® parou de acompanhar seu status de nova verificação, não quando a nova verificação real parou. Todos os IVs que fizeram a transição ou farão a transição para **Encerrado/Corrigido** são importados com a próxima importação programada da integração de vulnerabilidades corrigidas da Tenable.sc.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Iniciar nova verificação para a integração Tenable.io

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados iniciando novas verificações na plataforma Tenable. Você pode iniciar uma nova verificação sob demanda de itens vulneráveis para o produto Tenable.io da sua instância Now Platform®.

Antes de Iniciar

Funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Verifique se o scanner está ativado antes de começar. Navegar até **Vulnerability Response** > **Verificação de Vulnerabilidades** > **Scanners**.

Por Que e Quando Desempenhar Esta Tarefa

- Consulte e Verificar novamente registros e tarefas de correção no Vulnerability Manager Workspace e Verifique novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI para iniciar uma nova verificação nos espaços do Vulnerability Response.
- Siga as etapas listadas abaixo para iniciar uma nova verificação no ambiente clássico.

Nota:
Tenable.io não é compatível com a inicialização de uma nova verificação em máquinas baseadas em agente.

Para ajudar a reduzir a sobrecarga e o volume envolvidos com verificações completas programadas, como proprietário de correção, especialista de TI, analista de vulnerabilidade ou gerente de vulnerabilidade, você pode iniciar novas verificações direcionadas sob demanda. você pode verificar vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas verificações a partir de item vulnerável (IV), tarefas de correção (VUL), entrada de terceiros (TPE) ou registros de item descoberto (SDI) da sua instância Now Platform. As novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Ao solicitar uma nova verificação da sua instância Now Platform®, a seleção das credenciais Integração do Vulnerability Response com Tenable é opcional. O ServiceNow® Tenable.io Scan Credential Integration importa e atualiza as credenciais do scanner do produto Tenable.io em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais da Tenable.

Observe que esses dados importados não incluem senhas da Tenable ou outras informações confidenciais da conta da Tenable.

As informações a seguir descrevem as credenciais que você importa para que os usuários possam vê-las conforme necessário na sua instância Now Platform :

- As credenciais criadas com a função de usuário administrador Tenable.io estão disponíveis para usuários em todas as suas organizações.
- As credenciais criadas com a função de usuários organizacionais Tenable.io estão disponíveis somente para usuários dessa organização. Essas credenciais não são importadas para o Now Platform para usuários fora da organização do criador, a menos que sejam compartilhadas com a conta do usuário que está sendo usada para se conectar à instância.

  Consulte o site de documentação Tenable.io para obter mais informações.

- A integração de modelo Tenable.io e a integração de credencial de verificação Tenable.io devem ser ativadas antes de iniciar novas verificações. Para exibir mais informações sobre o Scan Credential Integration, navegue até **Integração de vulnerabilidade Tenable** > **Integrações** > **Integração de credencial de verificação da Tenable.io**.

  Por padrão, as integrações de modelo e credencial de verificação são desativadas. Quando você insere suas credenciais para Tenable.io, todas as integrações Tenable.io são ativadas automaticamente. Para ativar ou desativar manualmente essas integrações:

  1. Navegar até **Todos** > **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
  2. Na lista exibida, localize os registros de integração Tenable.io desejados.
  3. Abra cada registro e marque a caixa de seleção **Ativo** para ativar a integração.
  4. Clique em **Atualizar** para salvar suas mudanças.
  5. Retorne ao Assistente de configuração para continuar com sua configuração para Tenable Vulnerability Integration com Vulnerability Response.

Consulte Configurar a integração de vulnerabilidade da Tenable usando o assistente de configuração para obter mais informações sobre como configurar os produtos Tenable.io e Tenable.sc.

Digamos que todo o seu ambiente seja verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada de seus Now Platform para Tenable.io itens vulneráveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode exibir resultados atualizados nos registros a partir dos quais iniciou as verificações após a próxima importação programada da integração de vulnerabilidades corrigidas.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- `sn_sec_cmn.record_threshold_heartbeat`: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- `sn_sec_cmn.maximum_heartbeat_delay`: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Itens vulneráveis**.
2. Localize o registro do item vulnerável do qual você deseja acionar uma nova verificação e abra-o.

   Nota:
   Se você estiver usando o scanner Tenable.io, só poderá iniciar novas verificações de IVs com Tenable.io como origem. Verifique se Tenable.io é exibido na coluna **Origem** nas exibições de Lista de IV ou nos campos **Origem** em registros individuais. Você pode usar o construtor de condição para agrupar IVs por origem. Ou, se a coluna Origem não for exibida na exibição da lista de IVs, no canto superior esquerdo da lista, clique no ícone **Personalizar lista** (ícone de engrenagem) e use o Slushbucket para mover a **origem** de **Disponível** para **Selecionado**.

3. Como alternativa, navegue até **Todos** > **Vulnerability Response** > **Tarefas de correção** ou **Vulnerability Response** > **Bibliotecas** > **Terceiros** para os registros que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o botão **Verificar novamente** está disponível nos seguintes registros:

   - Em um único registro de IV, o IV deve estar em qualquer estado diferente de **Encerrado**. Para vários registros de IV, todos os IVs devem ser do produto Tenable.io e em qualquer estado diferente de **Encerrado**.
   - Para registros de tarefa de correção, somente tarefas de correção em qualquer estado diferente de **Encerrado** são compatíveis. Todos os IVs associados devem estar em qualquer estado diferente de **Encerrado** e usar Tenable.io como origem.

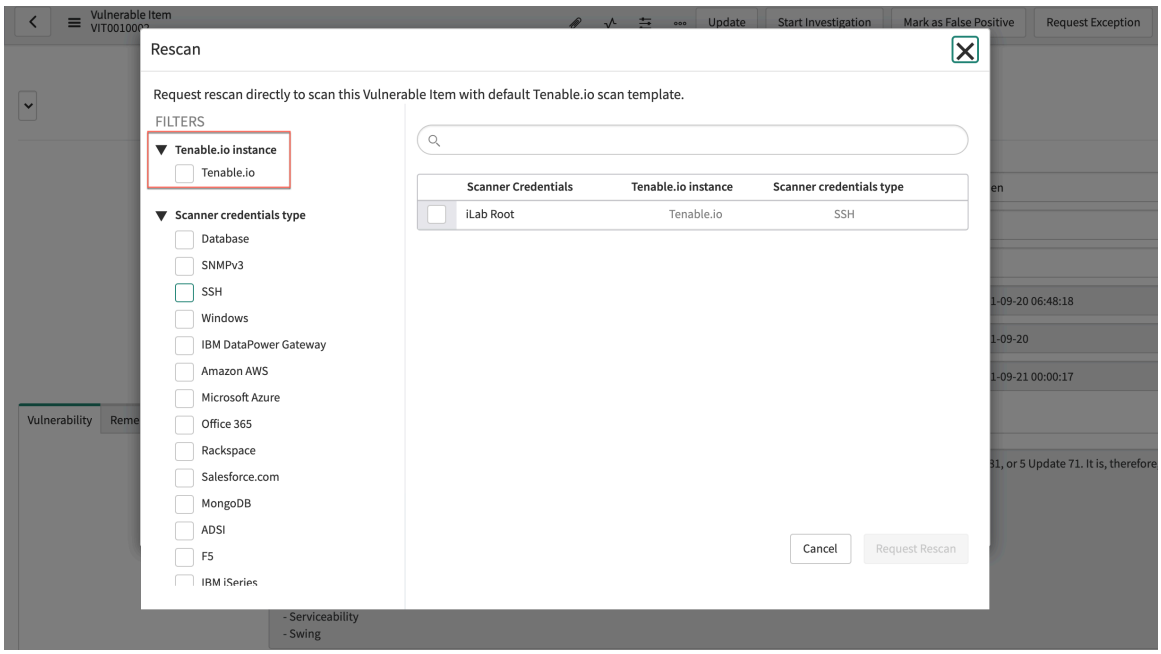
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro IV associado do produto Tenable.io em qualquer estado diferente de **Encerrado**.
- Em registros de itens descobertos, o registro deve ter pelo menos um registro IV associado do produto Tenable.io em qualquer estado diferente de **Encerrado**.
- Na lista Itens vulneráveis, você pode selecionar itens vulneráveis individuais que deseja verificar novamente. Use o menu Ações nas linhas selecionadas no canto inferior esquerdo da tela para iniciar a nova verificação. Você será solicitado a inserir suas credenciais.

4. No canto superior direito de um registro, clique em **Verificar novamente**.
   Você será solicitado a escolher a instância ou as instâncias para a nova verificação e as credenciais do scanner que deseja usar para acessar o scanner. As credenciais exibidas são aquelas importadas pela Tenable.io Scan Credential Integration.
5. Na caixa de diálogo, selecione a instância e ou as instâncias e os tipos de credencial que você deseja usar.

   Na imagem a seguir, uma instância de integração, Tenable.io, é exibida. Se você tiver mais de uma instância Tenable.io, todas elas serão exibidas na seção Tenable.io no formulário.



6. Clique **em Solicitar nova verificação**.

   Uma mensagem é exibida indicando que a verificação está sendo processada e que um registro de verificação primário foi criado. O status de todas as verificações secundárias pode ser encontrado a qualquer momento nas listas relacionadas à verificação no IV, na tarefa de correção, no TPE e nos registros de SDI usados para iniciar as novas verificações. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e todas as outras verificações iniciadas a partir de um determinado registro.

   O campo Estado no registro de verificação primário é marcado como concluído depois que todas as verificações secundárias são concluídas com sucesso. O secundário verifica os dados de importação. Cada verificação oferece suporte a uma combinação exclusiva de instância de integração, TPE, IP e ID de rede. Você pode ver várias verificações secundárias em um registro de verificação primário. Por exemplo, o número máximo de endereços IP que uma verificação secundária pode suportar é 1000. Se houver 1002 IPs para um item vulnerável, duas verificações secundárias serão criadas e listadas na lista

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

relacionada Verificações para oferecer suporte à solicitação. O registro de verificação primário é um contêiner para as verificações secundárias e seu estado de reflete o status das verificações secundárias.

Sua instância Now Platform® rastreia o status de nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando Now Platform® parou de acompanhar seu status de nova verificação, não quando a nova verificação real parou. Todos os IVs que fizeram a transição, ou farão a transição, para **Encerrado/Corrigido** são importados com a próxima importação programada da Tenable.io Integração de vulnerabilidades fixas.

Para verificações com erro, você pode verificar as verificações secundárias no registro de verificação primário. Exiba o erro na carga de resposta da verificação secundária.

Você pode exibir resultados atualizados nos registros a partir dos quais iniciou as verificações após a próxima importação programada da integração de vulnerabilidades corrigidas.

Atualizar itens de configuração com o identificador de partição de rede para Tenable Vulnerability Integration

Crie itens de configuração (ICs) exclusivos para ativos em seu ambiente que compartilham endereços IP. Identifique os ativos distintos em seu ambiente e atualize automaticamente os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Por padrão na aplicação Vulnerability Response, uma maneira de identificar seus ativos é por endereço IP. Em determinados casos, os ativos podem compartilhar endereços IP, mas eles são armazenados como um IC no seu CMDB.

Por exemplo, conforme mostrado nas tabelas a seguir, vários ativos (IC) em seu ambiente podem compartilhar endereços IP, mas têm IDs de rede e repositório exclusivos. No entanto, por padrão, esses ativos são normalmente identificados e armazenados como um único IC (IC 1) durante a pesquisa de endereço IP.

Pesquisa de IP padrão e criação de IC

Origem	Endereço IP	Network_id	Item de configuração
Tenable.io: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1
	123.12.12.141	03713	IC 1

Origem	Endereço IP	Repository_id	Item de configuração
Tenable.sc: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1
	123.12.12.141	13	IC 1

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode criar ICs individuais para ativos que têm o mesmo endereço IP para que possa identificá-los como ativos distintos. Iniciando de uma importação de dados recente, você pode atualizar seus ICs existentes com mais granularidade que inclua o identificador de partição de rede [network_partition_identifier] executando o trabalho programado, *`Update existing discovered items with network partition identifier`*.

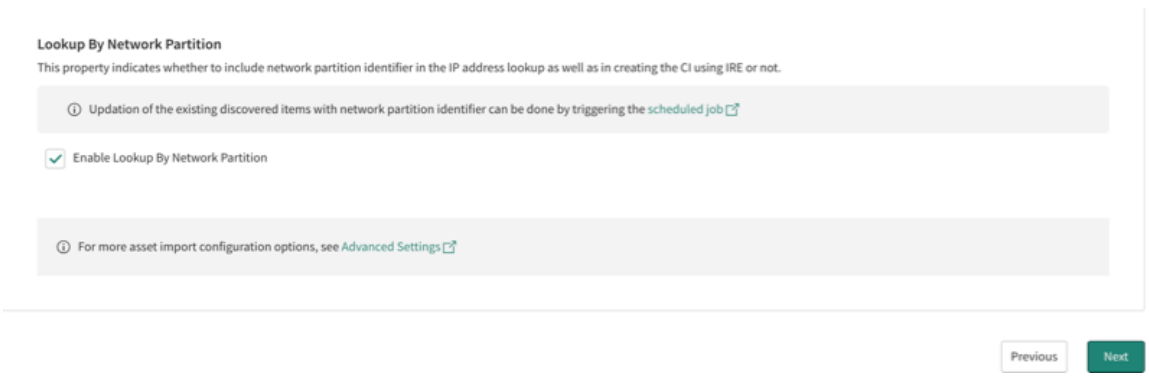
Este trabalho programado está desabilitado por padrão. Ative este recurso para os ativos e integrações de vulnerabilidades fixas e abertas para os produtos Tenable.io e Tenable.sc no Assistente de configuração para exibir este identificador em seus registros.

Quando ativado, este trabalho programado adiciona o identificador de partição de rede [network_partition_identifier] aos registros de IC existentes a partir de dados importados. Os ICs existentes criados pelo IRE também são atualizados. O trabalho programado também cria ICs que incluem o identificador da partição de rede que começa com a próxima importação. Como alternativa, você pode iniciar o trabalho sob demanda para atualizar os dados existentes.

Quando você atualiza a partir da v14.0 de Vulnerability Response e v2.2 do Tenable Vulnerability Integration, os CMDB CI Class Models (1.0.21.) são compatíveis. Os modelos de classe têm o identificador de partição de rede [network_partition_identifier] nas regras de identificação de Identificação e Reconciliação (IRE).

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
2. Selecione Tenable.io integrações ou Tenable.sc integrações.
3. **Edite** a integração necessária.
4. Selecionar **Configuração de importação de ativo**.
5. Selecionar **Habilitar pesquisa por partição de rede** caixa de seleção do **Habilitar pesquisa por partição de rede** seção.



6. Clique em **Avançar**.

   Os identificadores de partição de rede NETWORK_ID e REPOSITORY _ID estão incluídos e atualizam os ICs existentes ou criam ICs com o próximo trabalho programado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo do identificador de partição de rede incluído na pesquisa de IP e na criação de IC

Origem	Endereço IP	NETWORK_Identifi	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Tenable.io: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1	IC 1
	123.12.12.141	03713	IC 1	IC 2

Origem	Endereço IP	REPOSITÓRIO_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Tenable.sc: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1	IC 1
	123.12.12.141	13	IC 1	IC 2

Com o próximo trabalho programado, as regras de pesquisa de identificação de IC de endereço IP e endereço IP incompleto incluem o atributo do identificador de partição de rede automaticamente para uma importação de dados das integrações de ativos e vulnerabilidades fixas e abertas para os produtos Tenable.io e Tenable.sc.

Depois de habilitar a propriedade do sistema e salvar os registros, você pode atualizar os itens descobertos existentes com ICs que incluem o identificador de partição de rede iniciando os trabalhos programados sob demanda.

Importar modificações para a integração de vulnerabilidade da Tenable

Configure modificações opcionais e simplifique alguns dos dados especificamente para a integração de importação de vulnerabilidades da Tenable na ServiceNow® Integração de vulnerabilidade da Tenable.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Este conjunto de tarefas requer codificação e conhecimento avançado sobre o Now Platform.

Siga estas etapas para criar importações separadas por domínio para as integrações de vulnerabilidades da Tenable. O exemplo a seguir é para a integração Tenable.io Open Vulnerabilities, mas este conteúdo é aplicável às outras integrações da Tenable.

Procedimento

1. Crie um domínio.
2. Para cada domínio criado, crie um usuário e atribua o usuário a esse domínio.

   Pense neste usuário como um espaço reservado run_as para o domínio em Tenable.io.

Tradução automática

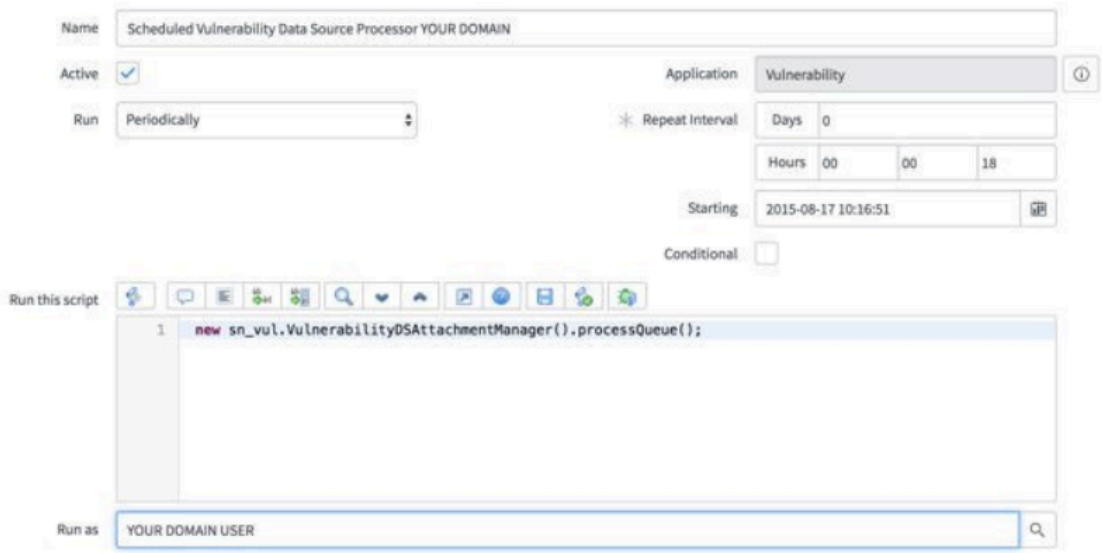
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Abra a integração de vulnerabilidades.
   O usuário é o equivalente ao usuário VR.System no domínio global e deve ter as seguintes funções: sn_vul.tenable_configure_integration, import_admin e sn_vul.vulnerability_write. Este usuário requer acesso a fontes de dados, mapas de transformação e dados de vulnerabilidade.

   Nota:
   Considere este usuário como específico para esta função. O usuário não deve ter nenhuma outra finalidade

4. Em cada domínio, crie um trabalho programado copiando o Processador de Fonte de Dados de Vulnerabilidade Programada encontrado em **Definição do Sistema** > **Trabalhos programados**.
5. Anexe o domínio ao nome para identificar o trabalho programado.
6. Altere o usuário run_as para o usuário que você criou na etapa anterior.

   Nota:
   Edite a seguinte ação de IU para que a integração seja executada no domínio do usuário run_as.



7. Edite a ação de IU Executar agora na integração de vulnerabilidades em aberto da Tenable.io para adicionar este bloco de código à parte superior do arquivo.
   ```
   //sys id below is of Tenable.io integration if(current.sys_id == "4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }
   ```

   Nota:
   Edite as inclusões de script a seguir para que a integração seja executada no domínio do usuário run_as.

8. Edite o método de inclusão de script VulnerabilityIntegrationUtils addIntegrationRun para adicionar o código realçado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. Edite o método de inclusão de script VulnerabilityIntegrationUtils addProcessRun para adicionar o código realçado.

```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Edite o método de inclusão de script DataSourceVulnReportRefreshProcessor _processFromDataSourceGroups para mudar este código original: Código _processFromDataSourcesGroups original para código _processFromDataSourcesGroups editado.

11. Edite o método de inclusão de script VulnerabilityDSAttachmentManager, queueItem, para adicionar os seguintes blocos de código realçados queueItem, _getNext, _processQueueEntry.

Você está pronto para importações de detecção de host separadas por domínio.

Desabilitar calculadoras antes da importação

Siga estas etapas para desabilitar a calculadora padrão se não for usada. Se você não usar calculadoras de vulnerabilidade, é melhor desabilitar as calculadoras padrão, além de quaisquer outras que você tenha definido. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é acessado e pode afetar o desempenho da instância.

Função necessária: sn_vul.vulnerability_admin.

12. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Calculadoras de vulnerabilidade**.

13. Abra o grupo Impacto de vulnerabilidade.

14. Abra a calculadora de pontuação e impacto baseado em serviço.

15. Desmarque o campo Ativo para desativar a calculadora.

16. Clique em Atualizar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você desativou a calculadora padrão.

Desabilitar regras de negócios baseadas em notificação antes da importação inicial

Siga estas etapas para desabilitar Desabilitar regras de negócios relacionadas à notificação antes da importação de registro inicial. Durante a importação inicial de registros, determinadas regras de negócios relacionadas à notificação podem gerar muitas notificações, afetando o desempenho. Essas regras de negócios devem ser modificadas para desativá-las durante a importação.

A função necessária é sn_vul.vulnerability_admin.

17. Navegar até **Todos** > **Definição do Sistema** > **Regras de negócios**.
18. Pesquise notificações de IC afetado.
19. Abra a regra de negócios e insira a seguinte condição: `current.sys_class_name != “sn_vul_vulnerable_item"`.
20. Clique em **Atualizar**.
21. Repita este procedimento para as seguintes regras de negócios:
    - Notificações de centro de custos afetado
    - Notificações do grupo afetado
    - Notificações de local afetado

Nota:
Após a conclusão da importação do registro inicial, você terá a opção de reativar essas regras de negócio. No entanto, considere deixá-los desabilitados. Eles podem gerar um grande número de notificações e afetar o desempenho da sua instância.

Modificar uma data de início inicial

Siga estas etapas para modificar uma data de início inicial. Durante a instalação usando o Assistente de configuração, você define uma data de início inicial para as integrações da Tenable. Você pode redefinir essa data de início no Assistente de configuração ou na integração primária, conforme mostrado nas etapas a seguir.

22. Navegar até **Todos** > **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
23. Clique em qualquer integração.
24. Clique em Detalhes da integração.
25. Defina o campo Hora de início com um valor no passado, para que todas as vulnerabilidades verificadas e detectadas desde essa hora sejam detectadas.

    Se você configurou o Tenable usando o Assistente de configuração, o campo Hora de início será preenchido previamente, inicialmente para três meses antes da data de hoje e, subsequentemente, para a data de hoje. Observação: considere definir o valor como no máximo um mês no passado. Isso evita que uma grande quantidade de dados exceda as limitações de taxa da API da Tenable, bem como aciona os tempos limites de execução.

26. Clique em **Enviar** ou **Atualizar**.
27. **Opcional:** Clique **em Executar agora** para executar imediatamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Noções básicas sobre a integração [Atlassian Jira com Vulnerability Response

A integração de [Atlassian Jira com Vulnerability Response permite que você aproveite diferentes ferramentas de acompanhamento de problemas e gestão ágil para acompanhar os esforços de correção de vulnerabilidades.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral

ServiceNow® Vulnerability Response está integrado a Atlassian Jira para criar problemas correspondentes a vulnerabilidades e sincronizou a entidade de problema em Jira e a entidade de item de vulnerabilidade em Vulnerability Response bidirecionalmente para refletir as atualizações mais recentes. Os gerenciadores de vulnerabilidade exigem que os itens de vulnerabilidade presentes em ServiceNow Vulnerability Response sejam criados e atribuídos a usuários de correção (desenvolvedores, no caso de Application Vulnerability Response) em seu sistema preferencial de registro e ferramenta de gestão de problemas, como Atlassian Jira. Qualquer andamento realizado nas vulnerabilidades na ferramenta de gestão de problemas deve ser atualizado em ServiceNow Vulnerability Response para visibilidade para os gerentes de vulnerabilidade. Além disso, todas as atualizações feitas pelos gerentes de vulnerabilidade em Vulnerability Response para itens de vulnerabilidade também devem ser passadas para a ferramenta de gestão de problemas para visibilidade aos usuários de correção.

Versões disponíveis

Versão de lançamento	Notas de versão
Vulnerability Response	Notas de versão do Vulnerability Response Integration
Vulnerability Response e Configuration Compliance para contêiner	Notas de versão do Vulnerability Response do contêiner
Spoke do Jira	Notas da versão do spoke do Jira

Jira Integrações de vulnerabilidade

Para exibir a integração de vulnerabilidade Jira, navegue até **Todos** > **Gestão do Agile para VR** > **Configurar ferramentas Agile** .

As integrações a seguir estão incluídas no sistema de base. Essas integrações não estão ativas por padrão.

Após a execução inicial, todos os dias, os trabalhos programados são encadeados para executar as integrações automaticamente na ordem. Você também pode executar trabalhos programados individuais manualmente. Os trabalhos programados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Preparando para a integração Jira Vulnerability Response

Uma integração de vulnerabilidade Jira bem-sucedida requer planejamento e execução de tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. A integração Jira Vulnerability Response pressupõe que você esteja familiarizado com o produto Jira e a API.

Componentes instalados com o Agile Integration for Vulnerability Response e Jira Integration for Vulnerability Response

Vários tipos de componentes são instalados com a ativação do plug-in Agile Integration for Vulnerability Response e Jira Integration for Vulnerability Response, incluindo tabelas e funções do usuário.

Funções instaladas

Título da função [name]	Descrição
Administrador da ferramenta Agile [sn_vul_agile.agile_tool_admin]	Permite criar uma regra de configuração para o Agile Management criar ou atualizar problemas. Crie configurações de regra para o Agile Management.
Administrador do JIRA [sn_vul_jira.admin]	Permite que você selecione a ferramenta Agile para criar problemas para a tabela de entidade selecionada.

Tabelas instaladas

Tabela	Descrição
Configuração da ferramenta Agile [sn_vul_agile_tool_rule_config]	Contém regras de configuração para criar problemas na plataforma Agile.
Mapeamento de campo da ferramenta Agile [sn_vul_agile_tool_field_mapping]	Contém o mapeamento de campo da regra de configuração.
Mapeamento de estado da ferramenta Agile [sn_vul_agile_tool_state_mapping]	Contém o mapeamento do status do problema do Jira com o estado do item vulnerável da aplicação, do item vulnerável do contêiner, da tarefa de correção da aplicação e da tarefa de correção do contêiner.
Manifesto da ferramenta Agile [sn_vul_agile_tool_manifest]	Contém carga para criação do problema.
Recurso de dados da ferramenta Agile [sn_vul_agile_tool_data_resource]	Contém as informações sobre o problema do Jira criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabelas instaladas

Tabela	Descrição
Administrador do JIRA [sn_vul_jira.admin]	Permite que você selecione a ferramenta Agile para criar problemas para a tabela de entidade selecionada.

Instalar o Vulnerability Response Integration com Jira

Antes de executar a integração na sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto Jira se integre corretamente com Application Vulnerability Response. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Função necessária: administrador

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Tarefas de configuração	Descrição
Verifique se a aplicação Vulnerability Response está instalada e ativada.	• A integração do Jira para Vulnerability Response requer a aplicação Vulnerability Response. • Para obter a versão mais atual do Jira Integration for Vulnerability Response, verifique se você tem a versão mais atual do Vulnerability Response instalada. Consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e mudanças de esquema de versão . • Se a aplicação não estiver instalada e ativada, consulte Instalar Vulnerability Response .
Verifique se o plug-in Integration Hub está instalado.	• O Jira Spoke requer o Hub de integração. • Consulte KB1112383 para obter a instalação do hub de integração. • Para obter mais informações, consulte Programações jurídicas - Visão geral do IntegrationHub .
Verifique se a versão mais recente de Jira Spoke está instalada.	Consulte KB0792632 para obter a instalação do Jira Spoke.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
Verifique se o Vulnerability Response Integration with Agile Management está instalado.	O Vulnerability Response Integration with Atlassian Jira requer essa integração.

Procedimento

1. Faça login na instância na qual você deseja instalar a integração Jira Vulnerability Response.
2. Navegue até o ServiceNow Store.
3. No ServiceNow Store, pesquise a integração [Vulnerability Response com a aplicação Jira.
4. Clique no bloco da aplicação.
   Informações detalhadas sobre a aplicação que você está instalando são exibidas.

   Nota:
   Considere ler as seções **Outros requisitos** e **Dependências**, conforme aplicável.

5. Clique em **Solicitar app** e insira suas Now Support credenciais de login.
6. Clique **em Obter**.
7. Insira o **Nome da instância** e **o Motivo da instância**e clique em **Validar instância**.
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Candidaturas**.
10. Localize a aplicação, selecione-a e clique em **Instalar**.
    Sua aplicação é instalada automaticamente na sua instância.

Configurar regras na configuração da ferramenta Agile

Jira problemas serão criados na plataforma Jira se os registros criados no item vulnerável da aplicação, no item vulnerável do contêiner, na tarefa de correção da aplicação e na tarefa de correção do contêiner corresponderem às regras criadas na configuração da ferramenta Agile.

Antes de Iniciar

Funções necessárias: sn_vul.app_read_all, sn_vul_container.read_all, sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin.

Procedimento

1. Navegar até **Todos** > **Gestão do Agile para VR** > **Configurar ferramentas Agile**.
2. Para criar uma nova regra de configuração na Configuração da ferramenta Agile, selecione **Novo**.
3. No formulário, preencha os campos.

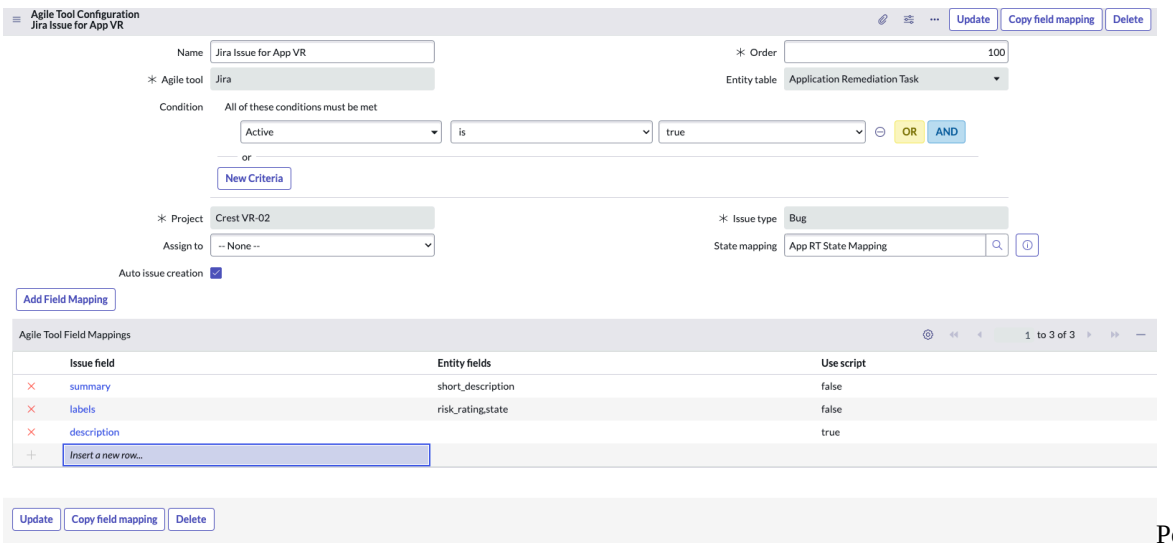
Formulário de configuração da ferramenta Agile

Campo	Descrição
Nome	Nome da configuração da ferramenta Agile.
Ordem	Ordem da configuração da ferramenta Agile.
Ferramenta Agile	A ferramenta Agile para criar problemas na plataforma Agile específica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tabela da entidade	Tabela na qual a regra de configuração será aplicada.
Condição	Filtre a condição na tabela da entidade selecionada para criar problemas na plataforma Agile.
Criação automática de problemas	A regra de configuração será consultada quando qualquer novo registro for criado na tabela da entidade selecionada, somente se a caixa de seleção estiver marcada. **Nota:** O usuário deve usar a ação de lista para criar problemas para registros de entidade existentes.
Projeto	O projeto no qual o problema do Jira será criado.
Tipo de Problema	O tipo de problema a ser criado em um projeto específico.
Atribuir a	O designado a quem o problema deve ser atribuído após a criação do problema. Para manter os problemas criados como não atribuídos, selecione "Nenhum".
Mapeamento de Estado	Os mapeamentos de estado existentes da tabela Mapeamento de estado da ferramenta Agile ou criam um novo mapeamento de estado entre o status do problema na plataforma Agile e os estados da tabela de entidade ServiceNow.



Por padrão, quando a aplicação é instalada, a Tarefa de correção da aplicação e a Tarefa de correção do contêiner são exibidas no campo Tabela de entidade no formulário Configuração da ferramenta Agile.

4. Para adicionar o item vulnerável da aplicação e o item vulnerável do contêiner na lista de seleção Tabela de entidade, navegue até **Propriedades do sistema** > **sn_vul_agile.tablesToShow** e adicione tudo no campo Valor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de propriedade do sistema

Campo	Descrição
Escolhas	Valores separados por vírgula para uma lista de seleção.
Valor	Defina o valor desejado para a propriedade. Todos os valores de propriedade são armazenados como cadeias de caracteres. Ao recuperar propriedades por meio do método gs.getProperty (), trate os resultados como cadeias de caracteres. Por exemplo, uma propriedade verdadeiro|falso retorna 'verdadeiro' ou 'falso' (cadeias de caracteres), não o equivalente booliano.

5. Selecione o registro de mapeamento de estado existente ou crie um novo mapeamento de estado no mapeamento de estado da ferramenta Agile.

Formulário Mapeamento de estado da ferramenta do Agile

Campo	Descrição
Nome	Insira o nome exclusivo do mapeamento de estado.
Ferramenta Agile	Selecione a ferramenta Agile.
Tabela da entidade	Selecione a tabela de origem na qual o mapeamento de estado será criado.
Projeto	Selecione o projeto no qual o estado será mapeado.
Estado da entidade da ServiceNow	Selecione o estado que você deseja mapear com o status da ferramenta do Agile.
Status da ferramenta Agile	Selecione o estado que você deseja mapear dos estados de item de vulnerabilidade.

6. Clique em **Salvar e buscar projetos** para buscar os projetos na regra de configuração do campo Projeto e validar as credenciais da ferramenta Agile.

Dica:
Você pode definir a propriedade do sistema **projectPageSize** para buscar um número específico de projetos por página.

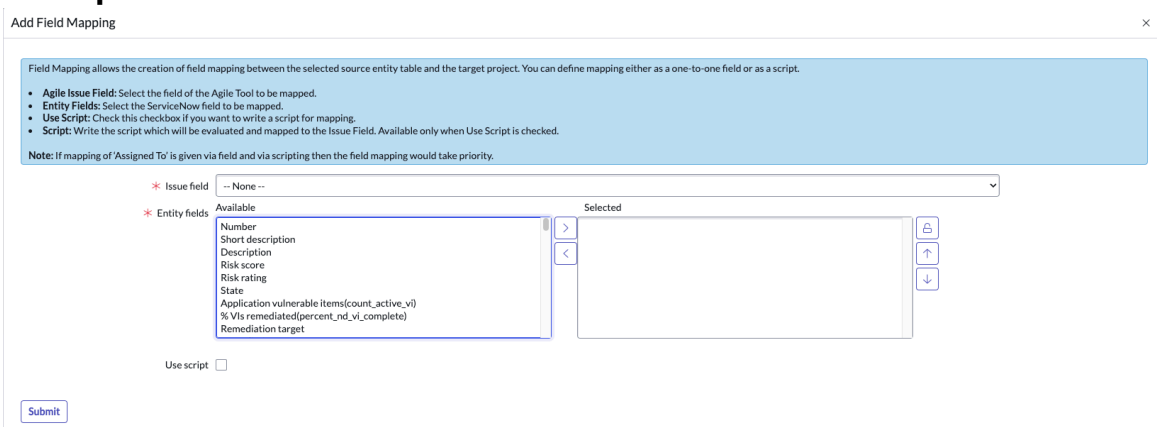
7. Navegue até **Propriedades do sistema** > **sn_vul_jira.projectsPageSize** e adicione o número de projetos a serem buscados por página no campo Valor do Jira Cloud.
8. Selecione o Projeto, o Tipo de Problema e Atribuir a na Regra de configuração depois que os projetos forem obtidos.

O mapeamento de campo padrão será preenchido na lista integrada de mapeamentos de campo da ferramenta Agile. Por padrão, os campos Resumo e Descrição dos problemas são mapeados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. Para mapear outros campos de problema com os campos ServiceNow, clique em **Adicionar mapeamento de campo**.



Nota:

- Você deve mapear somente campos do tipo Cadeia de caracteres e Opção.
- Todos os campos de problema obrigatórios da ferramenta Agile precisam estar mapeados corretamente com o campo de entidade.

Formulário Mapeamento de estado da ferramenta do Agile

Campo	Descrição
Campo do problema	Contém os campos de problema do projeto selecionado no momento e o tipo de problema na regra de configuração.
Campos da entidade	Contém os campos da tabela de entidade selecionada na Regra de configuração.
Usar o Script	Selecione para usar o script para mapear os campos de problema com campos de entidade.
Script	Script para mapear o campo do problema com campos de entidade.

10. Clique em **Enviar** no modal do glide para enviar o registro de mapeamento de campo na tabela Mapeamentos de campo da ferramenta Agile.

Nota:
Se você não mapear os campos obrigatórios, os problemas não serão criados para essa regra de configuração.

Os campos obrigatórios são exibidos na parte superior do formulário de configuração da ferramenta Agile. Todos os mapeamentos de campo para uma regra de configuração específica são exibidos na lista integrada da tabela Mapeamento de campo da ferramenta Agile na tabela Configuração da ferramenta Agile.

11. Clique com o botão direito do mouse no cabeçalho para salvar suas mudanças.
O registro salvo fica visível na tabela Configuração da ferramenta Agile. Se algum registro for criado no item vulnerável da aplicação, o item vulnerável do contêiner, a tarefa de correção da aplicação e a tarefa de correção do contêiner corresponderem a qualquer regra de configuração, o problema será criado para o registro de acordo com o mapeamento na regra de configuração.

12. Navegue até **Propriedades do sistema** > **sn_vul_jira.cloudBulkSize** e defina o número de problemas a serem criados por lote no campo Valor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
O número máximo de problemas que podem ser criados por lote na nuvem do Jira é 50.

Você pode definir o tamanho do lote para criar problemas no Jira Server.

13. Navegue até **Propriedades do sistema** > **sn_vul_jira.onPremBulkIssue** e defina o número de problemas a serem criados por lote no campo **Valor**.
Você também pode definir a contagem de erros no campo Valor na propriedade do sistema para processar os registros na tabela de manifesto para criar problemas do Jira até uma contagem de erros específica.
14. Navegue até **Propriedades do sistema** > **sn_vul_agile.ManifestErrorCount** e defina o número máximo de vezes até o qual o manifesto com erro deve ser processado.

Criar problema do Agile manualmente usando a ação de lista

Quando uma ação de lista: Criar problema do Jira é acionada, os registros que correspondem aos critérios de configuração da regra devem ser considerados para "Criar problema do Jira" e esses registros devem ser ingeridos na tabela sn_vul_agile_tool_manifest com o mapeamento selecionado na regra de configuração.

Antes de Iniciar
Função necessária: sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Procedimento

1. Navegar até **Todos** > **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista de** > **Tarefas de correção/Itens vulneráveis da aplicação/Itens vulneráveis de contêiner**.
2. Selecione vários registros para criar problemas do Jira e clique em **Criar problema do Jira**.
Os registros selecionados devem considerar o mapeamento de campo e o mapeamento de estado da ferramenta Agile associada.
Os registros selecionados que atendem à condição da regra de configuração devem estar qualificados para a criação de problemas do Jira e devem ser adicionados à tabela `sn_vul_agile_tool_manifest`.

Criar problema do Agile manualmente usando a ação de formulário

Crie um problema do Agile manualmente usando a ação de formulário. Se o registro corresponder a qualquer condição de regra de configuração, uma caixa pop-up será preenchida com os valores selecionados na regra de configuração e, se não corresponder a nenhum critério, o usuário terá permissão para selecionar valores predefinidos campos.

Antes de Iniciar
Certifique-se de que todos os campos de problema obrigatórios da ferramenta Agile estejam mapeados corretamente com o campo de entidade.

Funções necessárias: sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Procedimento

1. Navegar até **Todos** > **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista de** > **Tarefas de correção/Itens vulneráveis da aplicação/Itens vulneráveis de contêiner**.
2. Selecione qualquer registro para criar um problema do Agile manualmente.
3. Selecione **Criar problema do Agile**.
4. Insira detalhes válidos para os campos mencionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se o registro atender à condição de qualquer regra de configuração, os campos abaixo deverão ser preenchidos com o valor configurado e o usuário poderá modificar os valores do campo.

Campo	Descrição
Projeto	Selecione o projeto no qual o problema do Jira será criado.
Tipo de Problema	Selecione o tipo de problema a ser criado em um projeto específico.
Atribuir a	Selecione o designado a quem o problema deve ser atribuído após a criação do problema.
Mapeamento de Campos	Selecione os campos de tipo de problema da ferramenta Agile e insira os valores diretos para o campo selecionado.

5. Selecione **Criar problema do Agile** para enviar o registro.
   Depois de enviar o registro, a entrada de registro será criada na tabela sn_vul_agile_tool_manifest.

Sincronizar manualmente o status do problema Jira

Atualize o estado do registro único clicando no botão **Sincronizar status do Agile** do menu de contexto do formulário e atualize os estados de vários registros clicando na ação de lista **Sincronizar status do Agile** do item vulnerável da aplicação, do item vulnerável do contêiner e da tabela de tarefas de correção no o Vulnerability Manager Workspace.

Antes de Iniciar
Funções necessárias: sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Por Que e Quando Desempenhar Esta Tarefa
O estado será sincronizado de ServiceNow para a ferramenta Agile se o estado da entidade for encerrado em ServiceNow ou se qualquer entidade for reaberta (ou seja, o estado for Aberto). Todos os outros estados serão refletidos da ferramenta Agile para ServiceNow. O usuário não terá permissão para sincronizar o estado dos registros cuja regra configurada associada não tem mapeamento de estado ou os problemas que são criados diretamente a partir da ação de formulário.

Procedimento

1. Navegar até **Todos** > **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Lista de** > **Tarefas de correção/Itens vulneráveis da aplicação/Itens vulneráveis de contêiner**.
2. Selecione vários registros para criar problemas do Jira e clique em **Sincronizar status do Agile**.
   Os estados dos registros para os quais os problemas já foram criados serão atualizados se o registro não estiver no estado encerrado e o mapeamento de estado existir para os registros selecionados na regra de configuração.
3. Abra um registro e o **status da sincronização do Agile ficará** visível no menu de contexto do formulário se as seguintes condições forem atendidas.
   - O problema foi criado para o registro e o registro não está no estado Encerrado
   - O mapeamento de estado existe para o registro
4. Clique em **Sincronizar status do Agile** para sincronizar o status do Agile com o estado mapeado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode definir a propriedade do sistema para definir o tamanho do lote para buscar o status do problema do Jira.

5. Navegue até **Propriedade do sistema** > **sn_vul_jira.bulkIssueStatusSize**.
   - Para o Jira Server, o número máximo de problemas a serem retornados (o padrão é 50). O valor máximo permitido é ditado pela propriedade do Jira "jira.search.views.default.max". Se você especificar um valor maior do que este número, os resultados da pesquisa serão truncados).
   - Se o problema for criado a partir de uma ação de formulário ou se a regra configurada não tiver nenhum mapeamento de estado, esses registros não serão considerados para a sincronização de estado.

Configurar o programador para criar problemas automaticamente

Configure o programador para executar e criar automaticamente os problemas Jira para os registros que foram criados na tabela sn_vul_agile_tool_manifest.

Antes de Iniciar
Função necessária: admin ou schedule_admin.

Por Que e Quando Desempenhar Esta Tarefa
Todos os registros do item vulnerável da aplicação, do item vulnerável do contêiner, da tarefa de correção da aplicação e da correção do contêiner criados na tabela sn_vul_agile_manifest serão considerados para a criação do problema Jira.

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Trabalhos programados** > **Criar problemas do Jira**.
2. Você pode modificar os campos Executar, Fuso horário e Hora no script Programado.

Formulário Execução programada de script

Campo	Descrição
Executar	Intervalo de tempo a ser usado para executar o trabalho programado: ○ Diariamente: é executado diariamente, em um horário designado. ○ Semanalmente: é executado semanalmente, em dia e hora designados. ○ Mensalmente: é executado mensalmente, em uma hora e dia designados do mês. ○ Periodicamente: é executado em um intervalo de repetição designado. ○ Uma vez: é executado somente para uma única ocorrência. ○ Sob demanda: é executado imediatamente sob demanda. ○ Calendário comercial: início da entrada: é executado nas datas de entrada iniciais

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	do calendário comercial selecionado no campo. Um trabalho programado é executado para a data de início de cada entrada comercial definida para o calendário comercial. Por exemplo, se o calendário comercial representar um ano fiscal e a data de início de cada entrada for um mês fiscal, o trabalho programado será executado no primeiro dia de cada mês. ○ Calendário comercial: fim da entrada: é executado na data de término do calendário comercial selecionado no campo. Essa seleção é executada da mesma maneira que Calendário comercial: início da entrada, mas para as datas de término das entradas do calendário comercial associadas. **Nota:** Ao selecionar Calendário comercial: início da entrada ou Calendário comercial: fim da entrada, você pode aplicar um fator de deslocamento para programar o trabalho para ser executado antes ou depois do período do calendário comercial selecionado. Para saber mais, consulte os campos Tipo de deslocamento e Deslocamento. Para saber mais sobre como criar e usar calendários de negócios e definir entradas de calendário de negócios, consulte Create a business calendar e Define business calendar entries.
Dia	Dia em que o trabalho programado deve ser executado. ○ Se Executar estiver definido como Semanalmente, selecione o dia da semana. Por exemplo, selecione Quarta-feira. ○ Se Executar estiver definido como Mensalmente, selecione o dia do mês. Por exemplo, selecione 25 para o 25º dia do mês. Este campo aparecerá somente se você selecionar Mensalmente ou Semanalmente no campo Executar.
Intervalo de repetição	Duração do intervalo de repetição para cada execução de trabalho programada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Insira a duração em número de dias, horas ou minutos. Por exemplo: ○ Para executar o trabalho programado a cada quatro dias, insira 04 no campo Dias. ○ Para executá-lo a cada 26 horas, insira 26 no campo Horas. ○ Se ele se repetir em um intervalo de 13:30:25, insira 13 no campo Horas e insira 30 e 25 nos dois campos sem rótulo após ele.
Hora	Hora em que o trabalho programado deve ser executado, expressa em horas, minutos e segundos em um relógio de 24 horas. A seleção feita no campo Fuso horário determina o fuso horário desta entrada.
Fuso horário	Fuso horário a ser usado com a entrada do campo Hora ao especificar a hora em que o trabalho programado deve ser executado. Selecione uma entrada de fuso horário: ○ **Nenhum**: use o fuso horário padrão para o usuário conectado que está criando o trabalho programado. Por exemplo, o trabalho programado será executado às 16h45, horário dos EUA/Pacífico, se for o fuso horário atribuído ao usuário e você inserir 16:45 no campo Hora. ○ **Usar fuso horário do sistema**: use o fuso horário padrão do sistema especificado para a instância em que ele é executado. Por exemplo, o trabalho programado será executado às 22h15, horário de Londres, se Europa/Londres for o fuso horário do sistema padrão para a instância e você inserir 22:15 no campo Hora. ○ Fuso horário real. ○ Por exemplo, o trabalho programado será executado às 13h30 no fuso horário Leste dos EUA se você selecionar EUA/Leste e inserir 13h30 no campo Hora.
run_as	Por padrão, run_ como o valor do campo deve estar vazio. O usuário pode definir o valor como valor de usuário de domínio para criar um problema para um domínio específico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar programador para atualizar problemas automaticamente

Configure o programador para atualizar os problemas Jira automaticamente para os registros que foram adicionados à tabela sn_vul_agile_tool_manifest.

Antes de Iniciar
Função necessária: admin ou schedule_admin.

Por Que e Quando Desempenhar Esta Tarefa
Todos os registros do item vulnerável da aplicação, do item vulnerável do contêiner, da tarefa de correção da aplicação e da correção do contêiner criados na tabela sn_vul_agile_manifest são considerados para a atualização do problema Jira. Se o registro for encerrado e os comentários forem adicionados, esses valores também deverão ser atualizados para o problema Jira associado.

Nota:

- O trabalho programado "atualizar problemas" não atualizará o estado Jira se o fluxo de trabalho do projeto de problema do Agile escolhido impedir que qualquer usuário altere diretamente o estado de outro estado.
- Se você fechar qualquer registro de entidade com comentários adicionais, somente o último comentário será considerado no momento da atualização e, para a próxima atualização, todos os comentários serão adicionados ao Jiraassociado.

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Trabalhos programados** > **Atualizar problemas do Jira**.
2. Você pode modificar os campos **Executar**, **Fuso horário**e **Hora** no script Programado.

Formulário Execução programada de script

Campo	Descrição
Executar	Intervalo de tempo a ser usado para executar o trabalho programado: ○ Diariamente: é executado diariamente, em um horário designado. ○ Semanalmente: é executado semanalmente, em uma hora e dia designados. ○ Mensalmente: é executado mensalmente, em uma hora e dia designados do mês. ○ Periodicamente: é executado em um intervalo de repetição designado. ○ Uma vez: é executado somente para uma única ocorrência. ○ Sob demanda: é executado imediatamente sob demanda. ○ Calendário comercial: início da entrada: é executado nas datas de entrada iniciais do calendário comercial selecionado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	no campo. Um trabalho programado é executado para a data de início de cada entrada comercial definida para o calendário comercial. Por exemplo, se o calendário comercial representar um ano fiscal e a data de início de cada entrada for um mês fiscal, o trabalho programado será executado no primeiro dia de cada mês. ○ Calendário comercial: Término da entrada: executado na data final do calendário comercial selecionado no campo. Essa seleção é executada da mesma maneira que Calendário comercial: início da entrada, mas para as datas de término das entradas do calendário comercial associadas. **Nota:** Ao selecionar Calendário comercial: início da entrada ou Calendário comercial: fim da entrada, você pode aplicar um fator de deslocamento para programar o trabalho para ser executado antes ou depois do período do calendário comercial selecionado. Para saber mais, consulte os campos Tipo de deslocamento e Deslocamento. Para saber mais sobre como criar e usar calendários de negócios e definir entradas de calendário de negócios, consulte e Create a business calendar Define business calendar entries .
Dia	Dia em que o trabalho programado deve ser executado. ○ Se Executar estiver definido como Semanalmente, selecione o dia da semana. Por exemplo, selecione Quarta-feira. ○ Se Executar estiver definido como Mensalmente, selecione o dia do mês. Por exemplo, selecione 25 para o 25º dia do mês. Este campo aparecerá somente se você selecionar Mensalmente ou Semanalmente no campo Executar.
Intervalo de repetição	Duração do intervalo de repetição para cada execução de trabalho programada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Insira a duração em número de dias, horas ou minutos. Por exemplo: ○ Para executar o trabalho programado a cada quatro dias, insira 04 no campo Dias. ○ Para executá-lo a cada 26 horas, insira 26 no campo Horas. ○ Se ele se repetir em um intervalo de 13:30:25, insira 13 no campo Horas e insira 30 e 25 nos dois campos sem rótulo após ele.
Hora	Hora em que o trabalho programado deve ser executado, expressa em horas, minutos e segundos em um relógio de 24 horas. A seleção feita no campo Fuso horário determina o fuso horário desta entrada.
Fuso horário	Fuso horário a ser usado com a entrada do campo Hora ao especificar a hora em que o trabalho programado deve ser executado. Selecione uma entrada de fuso horário: ○ Nenhum: use o fuso horário padrão para o usuário conectado que está criando o trabalho programado. Por exemplo, o trabalho programado é executado às 16h45. Horário dos EUA/Pacífico se for o fuso horário atribuído ao usuário e você inserir 16:45 no campo Hora. ○ Usar Fuso horário do sistema: use o fuso horário padrão do sistema que é especificado para a instância na qual ele é executado. Por exemplo, o trabalho programado será executado às 22h15, horário de Londres, se Europa/London for o fuso horário do sistema padrão para a instância e você inserir 22:15 no campo Hora. ○ Fuso horário real. ○ Por exemplo, o trabalho programado será executado às 13h30 no fuso horário Leste dos EUA se você selecionar EUA/Leste e inserir 13h30 no campo Hora.
run_as	Por padrão, o valor do campo **run_as** está vazio. Você pode definir o valor como um usuário de domínio para criar um problema para um domínio específico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure o programador para sincronizar o status [Jira com ServiceNow® automaticamente

Configure o programador para sincronizar o estado de Jira problemas com o item de vulnerabilidade da aplicação, itens de vulnerabilidade de contêiner e tarefas na tabela sn_vul_agile_manifest.

Antes de Iniciar

Função necessária: schedule_admin ou admin

Por Que e Quando Desempenhar Esta Tarefa

O programador é executado automaticamente de acordo com a programação configurada. O estado dos registros criados no item vulnerável da aplicação, no item vulnerável do contêiner, na tarefa de correção da aplicação e na tabela de tarefas de correção do contêiner que têm problemas criados em Jira é atualizado de acordo com o status atual do problema na plataforma Jira com base no mapeamento de estado na regra de configuração.

Todos os registros de item vulnerável da aplicação, item vulnerável do contêiner, tarefa de correção da aplicação e correção de contêiner criados na tabela sn_vul_agile_manifest serão considerados para Jira criação do problema.

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Trabalhos programados** > **Status da sincronização**.
2. Você pode modificar os campos Executar, Fuso horário e Hora no script Programado.

Formulário Execução programada de script

Campo	Descrição
Executar	Intervalo de tempo a ser usado para executar o trabalho programado: ○ Diariamente: é executado diariamente, em um horário designado. ○ Semanalmente: é executado semanalmente, em uma hora e dia designados. ○ Mensalmente: é executado mensalmente, em uma hora e dia designados do mês. ○ Periodicamente: é executado em um intervalo de repetição designado. ○ Uma vez: é executado somente para uma única ocorrência. ○ Sob demanda: é executado imediatamente sob demanda. ○ Calendário comercial: início da entrada: é executado nas datas de entrada iniciais do calendário comercial selecionado no campo. Um trabalho programado é executado para a data de início de cada entrada comercial definida para o calendário comercial. Por exemplo, se o calendário comercial representar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	um ano fiscal e a data de início de cada entrada for um mês fiscal, o trabalho programado será executado no primeiro dia de cada mês. ○ Calendário comercial: Término da entrada: executado na data final do calendário comercial selecionado no campo. Essa seleção é executada da mesma maneira que Calendário comercial: início da entrada, mas para as datas de término das entradas do calendário comercial associadas. **Nota:** Ao selecionar Calendário comercial: início da entrada ou Calendário comercial: fim da entrada, você pode aplicar um fator de deslocamento para programar o trabalho para ser executado antes ou depois do período do calendário comercial selecionado. Para saber mais, consulte os campos Tipo de deslocamento e Deslocamento. Para saber mais sobre como criar e usar calendários de negócios e definir entradas de calendário de negócios, consulte Create a business calendar e Define business calendar entries.
Dia	Dia em que o trabalho programado deve ser executado. ○ Se Executar estiver definido como Semanalmente, selecione o dia da semana. Por exemplo, selecione Quarta-feira. ○ Se Executar estiver definido como Mensalmente, selecione o dia do mês. Por exemplo, selecione 25 para o 25º dia do mês. Este campo aparecerá somente se você selecionar Mensalmente ou Semanalmente no campo Executar.
Intervalo de repetição	Duração do intervalo de repetição para cada execução de trabalho programada. Insira a duração em número de dias, horas ou minutos. Por exemplo:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Para executar o trabalho programado a cada quatro dias, insira 04 no campo Dias. ○ Para executá-lo a cada 26 horas, insira 26 no campo Horas. ○ Se ele se repetir em um intervalo de 13:30:25, insira 13 no campo Horas e insira 30 e 25 nos dois campos sem rótulo após ele.
Hora	Hora em que o trabalho programado deve ser executado, expressa em horas, minutos e segundos em um relógio de 24 horas. A seleção feita no campo Fuso horário determina o fuso horário dessa entrada.
Fuso horário	Fuso horário a ser usado com a entrada do campo Hora ao especificar a hora em que o trabalho programado deve ser executado. Selecione uma entrada de fuso horário: ○ -Nenhum-: use o fuso horário padrão para o usuário conectado que está criando o trabalho programado. Por exemplo, o trabalho programado será executado às 16h45, horário dos EUA/Pacífico, se for o fuso horário atribuído ao usuário e você inserir 16:45 no campo Hora. ○ Usar Fuso horário do sistema: use o fuso horário padrão do sistema que é especificado para a instância na qual ele é executado. Por exemplo, o trabalho programado será executado às 22h15, horário de Londres, se Europa/London for o fuso horário do sistema padrão para a instância e você inserir 22:15 no campo Hora. ○ Fuso horário real. ○ Por exemplo, o trabalho programado será executado às 13h30 no fuso horário Leste dos EUA se você selecionar EUA/Leste e inserir 13h30 no campo Hora.
run_as	Por padrão, o valor do campo run_as está vazio. Você pode definir o valor como o valor do usuário do domínio necessário para criar um problema para um domínio específico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar manualmente uma integração de vulnerabilidade

As integrações de vulnerabilidade fornecem a capacidade de clientes e fornecedores de aprimorar os dados de vulnerabilidade em sua instância, recuperando dados de sistemas e fornecedores externos. Essa habilidade pode simplificar o ciclo de vida de correção de vulnerabilidade, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Para obter instruções detalhadas sobre como criar integrações, consulte Definir uma nova integração de vulnerabilidade.

Definir uma nova integração de vulnerabilidade

Uma integração de vulnerabilidade extrai dados de relatório de um sistema de terceiros, geralmente para recuperar dados de vulnerabilidade, e processa esses dados de relatório usando fontes de dados ou um processador personalizado.

Antes de Iniciar

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Integrações**.
2. Clique em **Nova**.
3. Preencha os campos, conforme necessário.

Integração da vulnerabilidade

Campo	Descrição
Nome	Um nome descritivo para a integração.
Ativo	Se a integração está ativa. Se você não quiser que ele seja executado por um período específico, poderá configurar os parâmetros que deseja usar e desativar o trabalho.
Executar	A frequência com que você deseja que a integração seja executada: Diariamente, Semanalmente, Periodicamente e assim por diante. Conforme observado, os campos subsequentes são exibidos ou não com base na sua configuração neste campo.
Dia	O dia em que você deseja que a integração seja executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Se você selecionou **Semanalmente** no campo **Executar**, este campo exibirá os dias da semana. ○ Se você selecionou **Mensalmente** no campo **Executar**, este campo exibirá os dias do mês.
Hora	A hora em que você deseja que a integração seja iniciada. Este campo aparecerá somente se você tiver selecionado **Diariamente**, **Semanalmente**ou **Mensalmente** no campo **Executar**.
Aplicação	[Somente leitura] O nome da aplicação para a qual esta integração foi criada.
Intervalo de repetição	Se você selecionou **Periodicamente** no campo **Executar**, este campo exibirá o número de dias e horas antes que a integração seja executada novamente.
Iniciando	Se você selecionou **Periodicamente** no campo **Executar**, esse campo exibirá as datas e a hora a serem usadas como ponto de partida para atualizações periódicas.
Condicional	Selecione este campo se quiser adicionar parâmetros condicionais.
Condição	Se você marcou a caixa de seleção **Condicional**, insira as condições aqui.
Detalhes de Integração	
Script de integração	Selecione a inclusão de script que estende o VulnerabilityIntegrationBase a ser executado quando a integração for executada. Este script define como recuperar dados de um sistema de terceiros.
Script de fábrica de integração	Insira um script que defina como construir o script include selecionado para o **script de integração**. Para obter mais informações, consulte Campos de script de fábrica de integração. **Nota:** Os scripts exigem experiência em ServiceNow e Vulnerability Response.
Estratégia do processador de relatórios	Selecione a estratégia que você deseja usar para lidar com os dados retornados pelo script de integração quando a integração for executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Selecione **Anexo de fonte de dados** se quiser processar dados usando uma fonte de dados. ○ Selecione **Processador de relatório personalizado** para selecionar um processador personalizado.
Processador de relatórios	Se você selecionou **Processador de relatório personalizado** no campo **Estratégia do processador** de relatório, selecione a inclusão de script que estende a inclusão de script VulnerabilityReportProcessorBase a ser executada quando a integração for executada. Este script define como processar os dados retornados pelo script de integração.
Script de fábrica do processador	Insira um script que defina como construir a inclusão de script selecionada para o **Processador de relatório**.

4. Clique em **Enviar**.

Tópicos relacionados

Script de integração de vulnerabilidade

Estratégias do processador de relatório

Campos de script de fábrica de integração

Executar manualmente uma integração de vulnerabilidade

Script de integração de vulnerabilidade

No formulário de integração de vulnerabilidade, o script de integração é uma referência a uma inclusão de script que estende a inclusão de script VulnerabilityIntegrationBase.

A funcionalidade contida neste script é chamada pelo VulnerabilityIntegrationController para gerenciar os meios pelos quais os dados são recuperados de uma fonte de dados externa. Cada subclasse de VulnerabilityIntegrationBase tem acesso a informações contextuais sobre o processo de chamada. Essas informações estão disponíveis por meio das seguintes variáveis de membro:

- integrationGr — um GlideRecord do registro de integração de vulnerabilidade que solicitou a execução da integração.
- integrationProcessGr — um GlideRecord que fornece informações contextuais para o processo atual de uma integração.

O processo de vulnerabilidade contém parâmetros especiais a serem usados em uma integração, geralmente para fins de paginação. Cada execução de uma integração de vulnerabilidade (chamada de execução de integração de vulnerabilidade) tem pelo menos um processo de integração de vulnerabilidade associado. Para integrações de várias chamadas, há um ou mais registros de processo de integração de vulnerabilidade para cada execução de integração de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A inclusão de script deve fornecer uma implementação para o método recuperaData() e retornar um objeto que é processado pelo script do processador de relatório. O objeto retornado por recuperaData é um objeto simples com propriedades para conteúdo, tipo de conteúdo e extensão.

Esta é uma captura de tela de VulnerabilityIntegrationBase.retrieveData():

VulnerabilityIntegrationBase.retrieveData()

```
/**
 * Retrieves data (generally from an external system) to be passed to a report processor.
 * Subclasses (i.e. concrete implementations of a Vulnerability Integration) should implement/override this
 * function.
 * The class should return an object structured as follows:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 * For multipage integrations (where multiple calls/integration processes must run), this function should check
 * the integrationProcessGr's parameters.
 */
retrieveData: function() {
    return {contents: "", contentType: "", extension: ""};
},
```

A lógica em recuperaData() depende da interface necessária para recuperar os dados. Por exemplo, se a origem dos dados que estão sendo extraídos tiver uma REST API, o corpo deste método poderá estar chamando o endpoint REST, provavelmente via RESTMessageV2. A resposta da chamada pode ser analisada ou colocada em um anexo, e os detalhes podem ser usados para construir o objeto de retorno.

Integrações de chamada única

Os scripts de integração de chamada única (página única) são os tipos mais simples de integrações. Eles exigem uma chamada, geralmente para uma fonte externa de dados, para recuperar dados. Somente recuperaData() precisa ser implementado para integrações de página única/chamada única.

Veja a seguir um exemplo que demonstra um script de integração de chamada única simples. Ele cria um RESTMessageV2 e o executa. Em seguida, ele retorna um objeto usando o corpo da resposta como conteúdo, junto com um contentType e uma extensão presumidos.

Script de integração de chamada única

```
var SingleRunVulnerabilityIntegration = Class.create();
SingleRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.
     */
    retrieveData: function() {
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'SingleRunVulnerabilityIntegration'
});
```

Integrações de várias chamadas

Os scripts de integração de várias chamadas (ou várias páginas) são um pouco mais complicados. Eles exigem várias chamadas para uma fonte de dados para recuperar dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como uma integração de chamada única, uma integração de várias chamadas também deve ter recuperadoData() implementado. No corpo de recuperaData(), a integração usa os métodos hasMoreData() e setNextRunParameters() fornecidos por VulnerabilityIntegrationBase.

O método hasMoreData() aceita um único booliano que instrui o VulnerabilityIntegrationController a inserir mais processos para extrair mais dados. Ao passar verdadeiro para hasMoreData(), uma chamada para setNextRunParameters() é feita para fornecer contexto para o próximo processo.

O método setNextRunParameters() aceita um único objeto que fornece informações de contexto a serem usadas pela próxima chamada para recuperaData(). Este objeto é usado para passar o estado para chamadas subsequentes para recuperadoData(). Um exemplo de caso de uso é passar um objeto que indica o número da página atual e o tamanho da página para um serviço Web.

Para várias integrações de chamada, cada chamada de recuperaData() verifica primeiro os parâmetros do processo atual. O método _getProcessParameters() é fornecido a todos os VulnerabilityIntegrationBase como uma conveniência para obter os parâmetros definidos pelo processo anterior. Se não houver parâmetros, isso indica que é o primeiro processo.

Veja a seguir uma captura de tela de um exemplo de script de integração de várias chamadas. Estendendo o exemplo de integração de chamada única, este script demonstra como fazer chamadas para um endpoint REST que tenha suporte de paginação básica. Ele mostra como você pode obter uma única página de dados, reconhecer que há mais dados a serem recuperados e informar ao próximo processo qual página recuperar.

Script de integração de várias chamadas

```
var MultiRunVulnerabilityIntegration = Class.create();
MultiRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'MultiRunVulnerabilityIntegration'
});
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Anexos como valores de retorno recuperaData()

Às vezes, é preferível retornar um anexo de recuperaData(). A lógica para criar e/ou recuperar um anexo é específica da implementação, mas depois que o anexo é conhecido, suas informações podem ser retornadas.

Para fornecer um anexo, recuperaData() retorna um objeto como:

```
{
    contents: "attachment-sys-id",
    contentType: "sys_attachment"
}
```

Um exemplo que se estende ao exemplo anterior, mas salva o corpo da resposta da Mensagem REST no registro do processo de integração. Em seguida, ele retorna esse identificador de anexo como o conteúdo do objeto de retorno.

Retornar anexo de recuperaData

```
var MultiRunAttachVulnerabilityIntegration = Class.create();
MultiRunAttachVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     *
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);

        var table = this.integrationProcessGr.getTableName();
        var sysId = this.integrationProcessGr.getUniqueValue();
        var fileName = this.integrationProcessGr.getValue("number") + ".xml";
        message.saveResponseBodyAsAttachment(table, sysId, fileName);
        var response = message.execute();
        var responsSysId = response.getResponseAttachmentSysid();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responsSysId, contentType: "sys_attachment", extension: "xml"};
    },

    type: 'MultiRunAttachVulnerabilityIntegration'
});
```

Estratégias do processador de relatório

O campo **Estratégia do processador de relatório** no formulário Integração de vulnerabilidade é usado para selecionar o método para processar os dados retornados pelo script de integração de vulnerabilidade quando o processo de integração de vulnerabilidade é executado.

O valor padrão é **Anexo da fonte de dados**. Este método é a implementação de linha de base que obtém os dados recuperados e os passa para uma fonte de dados a ser importada para o sistema. Selecionar **Processador de relatório personalizado** permite que você selecione um script de processador personalizado para processar os dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usar a estratégia do processador de relatório de anexo de fonte de dados

A estratégia do processador de relatório de anexo de fonte de dados é usada para passar os dados recuperados pelo script de integração para fontes de dados configuradas.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Integrações** e crie uma nova integração.
2. No campo **Estratégia do processador de relatório**, selecione **Anexo de fonte de dados**.
3. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**.
4. Na lista relacionada **Fontes de dados de integração de vulnerabilidade**, clique em **Novo**.
5. Defina a fonte de dados a ser usada.
6. Clique em **Enviar**.
7. Repita as etapas 4 a 6 se precisar de fontes de dados adicionais.
   Certifique-se de especificar a ordem em que as várias fontes de dados enviam informações no campo **Ordem**.
8. Clique em **Atualizar**.

Sobre scripts do processador de relatório personalizado

No formulário de integração de vulnerabilidade, o processador de relatório é uma referência a uma inclusão de script que estende a inclusão de script VulnerabilityReportProcessorBase. A funcionalidade contida neste script é chamada pelo VulnerabilityIntegrationController e define os meios pelos quais os dados retornados pelo script de integração são processados.

Cada subclasse de VulnerabilityReportProcessorBase tem acesso a informações contextuais sobre o processo de chamada. Essas informações estão disponíveis por meio das seguintes variáveis de membro:

- integrationGr — um GlideRecord do registro de integração de vulnerabilidade que solicitou a execução da integração.
- integrationProcessGr — GlideRecord do processo de vulnerabilidade que fornece informações contextuais para o processo atual de uma integração.

A inclusão de script deve fornecer uma implementação para o método `processReport()`. O objeto passado para processReport() é o objeto retornado por recuperaData e, como tal, é um objeto simples com propriedades para conteúdo, contentType e extensão. A lógica real em processReport() é específica da implementação e depende dos dados do relatório fornecidos.

Esta é uma captura de tela do VulnerabilityReportProcessorBase.processReport():

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Script do processador de relatório personalizado

```
/*
 * Processes the reportData that was pulled by a Vulnerability Integration's retrieveData().
 * The expectation is that retrieveData() will return an object that matches this function's input parameter.
 *
 * @param reportData = object with the following format:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 */
processReport: function(reportData) {
    return;
},
```

Campos de script de fábrica de integração

O formulário de integração de vulnerabilidade contém o script de fábrica de integração e, quando a estratégia do processador de relatório do processador de relatório **personalizado** é selecionada, o script de fábrica do processador. Esses campos são usados para fornecer a lógica para realmente instanciar o objeto definido pelo script, incluindo campos de referência, script de integração e processador de relatório, respectivamente.

Quando a inclusão de script é selecionada, os dois campos são preenchidos previamente com uma chamada de construtor sem argumento. Frequentemente, isso é suficiente, mas pode haver ocasiões em que mais lógica é necessária para instanciar o objeto de script.

O registro integrationProcessGr é exposto aos campos de script de fábrica para que as informações específicas do processo possam ser usadas, conforme necessário.

Executar manualmente uma integração de vulnerabilidade

Uma integração de vulnerabilidade é configurada para ser executada de forma programada. No entanto, você pode executá-los manualmente quando necessário.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- `sn_sec_cmn.record_threshold_heartbeat`: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- `sn_sec_cmn.maximum_heartbeat_delay`: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Integrações**.
2. Abra a integração que você deseja executar.
3. Clique em **Executar agora**.

Ingestão manual de vulnerabilidades

Inclua manualmente vulnerabilidades na aplicação Vulnerability Response para que você possa corrigi-las rapidamente sem precisar aguardar os resultados do scanner.

Scanners de terceiros, como Rapid7 ajudam a importar dados de vulnerabilidade para Vulnerability Response e processam os dados para relatar as descobertas. Com a integração de ingestão manual, você pode ingerir proativamente as vulnerabilidades e corrigi-las em vez de esperar que os scanners relatem os ativos que estão em risco. A ingestão manual de vulnerabilidades protege com eficácia os ativos contra ameaças desconhecidas, como explorações de dia zero.

Ingestão manual de vulnerabilidades

Você pode importar os dados de vulnerabilidade carregando um modelo nos seguintes formatos de arquivo:

- Excel
- Valor separado por vírgula (CSV)

Para acessar e baixar o modelo, navegue até **Todos** > **Vulnerability Response** > **Ingestão manual de item de vulnerabilidade** > **Carregar IU de arquivo**.

Certifique-se de seguir estes pontos-chave ao preencher os registros no modelo:

- Não cometa erros de digitação nos registros da coluna Gravidade/Estado. Se houver um erro de digitação, o registro será ignorado.
- Não mude os nomes das colunas.
- Não coloque nomes de coluna em nenhuma linha, exceto na primeira linha.
- Não altere a ordem das planilhas no modelo do Excel. Os dados de vulnerabilidades devem estar sempre presentes na segunda planilha.
- Não coloque detalhes de vulnerabilidades em nenhuma planilha, exceto a planilha de Detecções manuais de entrada.
- Não use nenhum caractere, exceto caracteres alfanuméricos e especiais, como hífen (-), ponto final (.), adição (+), sublinhado (_), espaço, colchetes '(' ')' e símbolo de arroba (@) para o nome do arquivo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter instruções sobre como preencher os dados no modelo, consulte Modelo para ingestão manual de vulnerabilidades.

Integrações de ingestão manual

A integração é acionada quando um arquivo é carregado. Com base no tipo de arquivo carregado, a integração relacionada é acionada.

Para exibir as integrações, navegue até **Todos** > **Vulnerability Response** > **Ingestão manual de item de vulnerabilidade** > **Integrações**.

As seguintes integrações de ingestão manual do sistema de base estão disponíveis por padrão.

Integrações

Tipos de integração	Descrição
Integração do Excel de ingestão manual	Recupera dados buscando o arquivo do Excel mais recente carregado da tabela Fila de push de ingestão de vulnerabilidade e copia o anexo para a respectiva execução de integração.
Integração de CSV de ingestão manual	Recupera dados buscando o arquivo CSV mais recente carregado da tabela Fila de push de ingestão de vulnerabilidade e copia o anexo para a respectiva execução de integração.

A integração de terceiros de Ingestão manual cria uma instância de integração, por padrão, com os dois parâmetros de instância de integração a seguir:

- max_input_records: define o número de registros que podem ser criados no modelo. Se você adicionar mais registros do que o especificado neste parâmetro, os registros adicionais serão ignorados. O número de registros pode ser atualizado na coluna Valor. O número recomendado de criações de registro no modelo é 1000. Qualquer coisa acima deste valor pode representar desafios de desempenho.
- insert_fixed: importa detecções de vulnerabilidades fixas.

Para exibir os parâmetros da instância de integração, navegue até **Todos** > **Vulnerability Response** > **Ingestão manual de item de vulnerabilidade** > **Integrações** e clique na instância de origem de qualquer integração. Como alternativa, você pode navegar até **Todos** > **Vulnerability Response** > **Instâncias de Integração** e clique em **Ingestão manual**.

Ingerir vulnerabilidades manualmente

Adicione manualmente vulnerabilidades carregando um modelo com dados de vulnerabilidades.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Ingestão de item vulnerável manual** > **Carregar IU de arquivo**.
2. Clique nos links Excel ou CSV e baixe o modelo no respectivo formato.
3. No modelo, insira os dados de vulnerabilidade nos registros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter instruções sobre como preencher os dados no modelo, consulte Modelo para ingestão manual de vulnerabilidades.

4. Clique **em Importar arquivo** e carregue o modelo atualizado.
5. Clique em **Enviar**.
   A página Filas de push de integração de vulnerabilidade é exibida. Você pode exibir a lista de instâncias de integração, o status das execuções de integração e as anotações de log após a conclusão da execução de integração.

O que Fazer Depois

Depois de carregar o arquivo, navegue até **Todos** > **Vulnerability Response** > **Ingestão de item vulnerável manual** > **Integrações**. Verifique se a execução da integração foi bem-sucedida.

Verificar execução de integração manual

Verifique se a execução da integração foi bem-sucedida. Exiba o número de detecções individuais e os itens vulneráveis (IVs) criados ou atualizados devido à execução da integração.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Ingestão de item vulnerável manual** > **Integrações**.
2. Clique no nome da integração com base no tipo de arquivo carregado.
3. Clique na guia **Execuções de integração de vulnerabilidade**.
4. Clique no número da execução de integração.
5. Clique na guia **Itens**.
6. Revise as informações na guia **Itens**.

Guia Itens

Guia/Campo	Descrição
Guia Itens	Exibe o número total de IVs importados. Você pode ver o total de detecções importadas adicionando os números listados na guia Detecções.
Novos itens	Exibe o número de itens vulneráveis criados a partir desta execução de integração.
Itens importados	Exibe a soma de todos os campos nesta seção.
Itens duplicados	Exibe itens duplicados. Este campo não está mais preenchido.
Itens atualizados	Exibe o número de vezes que os itens vulneráveis são atualizados durante esta execução de integração. Este valor não é o número de itens vulneráveis exclusivos que são atualizados. Se, por exemplo, um item vulnerável for atualizado duas vezes durante a execução da integração, ele será contado duas vezes e exibido como dois itens atualizados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia/Campo	Descrição
Itens inalterados	Exibe itens vulneráveis encontrados durante a execução da integração que existem no banco de dados, mas não foram atualizados porque nenhum dos valores de campo relevantes foi alterado.

O que Fazer Depois

Depois de verificar se a execução da integração foi bem-sucedida, navegue até **Todos** > **Vulnerability Response** > **Ingestão de item vulnerável manual** > **Carregar histórico de arquivos**. Verifique se há algum registro com falha das Anotações.

Configurar detecções manuais de fechamento automático

Habilite o fechamento automático de detecções manuais para fechar detecções manuais obsoletas automaticamente.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Ingestão de item vulnerável manual** > **Carregar IU de arquivo**.
2. Clique **em Mudar configuração de fechamento automático**.
3. Clique na guia **Detecções manuais**.
4. Certifique-se de que a caixa de seleção Encerrar automaticamente **as detecções manuais** esteja marcada.
5. No campo **Detecções manuais encontradas pela última vez (dias atrás)**, insira o número de dias após os quais as detecções manuais devem ser encerradas.
   O padrão é 90 dias. Você pode inserir qualquer valor positivo para o número de dias.

Verificar status do upload

Verifique se a execução da integração de vulnerabilidade foi bem-sucedida, parcialmente bem-sucedida ou uma falha.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Ingestão de item vulnerável manual** > **Carregar histórico de arquivos**.
2. Na tabela Filas de push de integração de vulnerabilidade, verifique a hora do upload e o status do upload nas colunas Criado e Estado, respectivamente.
3. **Opcional:** No campo **Anotações**, exiba o motivo da falha.

Modelo para ingestão manual de vulnerabilidades

O modelo fornece colunas que devem ser preenchidas com dados de vulnerabilidade e item de configuração (IC). Depois que o modelo é preenchido e carregado, os dados são processados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instruções para preencher o modelo

Para inserir os detalhes no modelo, siga as instruções fornecidas na tabela a seguir.

Instruções do modelo

Coluna	Obrigatório/ opcional?	Comprimento da cadeia de caracteres (máx.)/valores válidos	Descrição
ID do ativo	Opcional	255	Identificador universal exclusivo (UUID) ou ID do ativo. Pode ser o valor gerado por um scanner.
Insira informações em pelo menos uma das cinco colunas a seguir:			
Endereço MAC	Necessários	24	Informações de host ou ativo. A combinação de todos os valores fornecidos deve ser exclusiva para um ativo.
FQDN	Necessários	255	
NETBIOS	Necessários	255	
Endereço IP	Necessários	255	
Nome do host	Necessários	255	
As colunas restantes não dependem umas das outras.			
ID de vulnerabilidade	Necessários	255	Representa uma vulnerabilidade no National Vulnerability Database (NVD) ou um ID retornado de um scanner de terceiros.
Resumo de vulnerabilidade	Opcional	512	Breve descrição da vulnerabilidade. Ele é adicionado ao banco de dados somente quando o ID de vulnerabilidade está indisponível.
Gravidade	Opcional	crítico, alto, médio, baixo, nenhum	Gravidade da vulnerabilidade. Ele é adicionado ao banco de dados somente quando o ID de vulnerabilidade está indisponível. Se o registro estiver vazio, por padrão, ele será considerado crítico.
Porta	Opcional	Não aplicável	Porta da qual a vulnerabilidade é detectada. O valor deve ser um número inteiro válido. Se houver uma entrada inválida, o registro será ignorado.
Protocolo	Opcional	40	Tipo de protocolo de rede usado.
Prova	Opcional	4000	Representa o local ou o caminho do sistema da vulnerabilidade.
Estado	Opcional	aberto, fixo	Status da detecção. Se o registro estiver vazio, por padrão, ele será considerado aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerability Response Espaços

Os espaços do Vulnerability Response oferecem uma exibição consolidada dos recursos que permite realizar várias tarefas no mesmo painel, aumentando a produtividade e economizando tempo. O Vulnerability Manager e o IT Remediation Workspaces são compatíveis com Vulnerability Response, Application Vulnerability Response, Vulnerability Response contêinere Configuration Compliance.

Espaços de Vulnerability Manager, IT Remediation e Vulnerability Assessment

Espaço para gerentes de vulnerabilidades

Como analista de vulnerabilidade ou administrador, proteja os ativos da sua empresa contra malware e ataques maliciosos. Em uma única área de trabalho em seu Now Platform®, com a aplicação Vulnerability Response, junto com os dados de vulnerabilidade atuais importados para sua instância de bibliotecas de vulnerabilidades e aplicações de dados de scanner de terceiros, identifique vulnerabilidades críticas, priorize-as e envie listas de tarefas de correção por para a TI para que seus especialistas atuem.

Espaço de correção de TI

Como especialista em TI, use listas ou tarefas de correção (RT) enviadas por gerentes de vulnerabilidade para monitorar e resolver vulnerabilidades críticas atribuídas a você ou seus grupos. Corrija grupos de itens vulneráveis com patches, soluções, novas verificações de vulnerabilidade, solicitações de mudança, exceções e outras ferramentas para corrigir itens vulneráveis em um só local.

Espaço de avaliação de vulnerabilidade

Como gerenciador de eventos de vulnerabilidade, execute a avaliação de exposição e gerencie proativamente os eventos de vulnerabilidade crítica, especialmente durante os eventos de vulnerabilidade crítica, como um evento de dia zero.

Localizando os espaços Vulnerability Response

Quando você faz login inicialmente na sua instância Now Platform®, a página inicial na IU do Next Experience é exibida. Navegue até **Vulnerability Manager Workspace**, **IT Remediation Workspace** e **Vulnerability Assessment Workspace** em **Espaços**.

Funções necessárias:

- Espaço do gerenciador de vulnerabilidades: sn_vul.vulnerability_analyst, sn_vul_container.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin
- Espaço de correção de TI: sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner

Novos recursos

Os espaços Vulnerability Response incluem os seguintes recursos e aprimoramentos.

- Você pode exibir os painéis Vulnerability Management, Vulnerability Management (PA), Vulnerability Approvals, CISO, Container Vulnerability Management Overview, Application Vulnerability Management Dashboard, Unified Vulnerability Response e Integridade na IU do Next Experience na página Painéis do Espaço do gerenciador de vulnerabilidades. Para obter mais informações, consulte Visão geral dos painéis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você pode exibir o painel do Vulnerability Remediation na IU do Next Experience na página Painéis do espaço de correção de TI. Para obter mais informações, consulte Visão geral dos painéis.
- Divida as Tarefas de correção dos resultados de testes no Vulnerability Manager Workspace e no IT Remediation Workspace. Para obter mais informações, consulte Solicitar exceções para tarefas de correção e registros do Vulnerability Manager Workspace e Dividir uma tarefa de correção no Espaço de correção de problemas de TI respectivamente.
- Você pode solicitar as exceções de política para itens vulneráveis de contêiner (CVITs), grupos de resultados de testes do gerenciador de vulnerabilidades e espaços de correção de TI. Para obter mais informações, consulte Solicitar exceções para tarefas de correção e registros do Vulnerability Manager Workspace e Solicitar uma exceção usando GRC: Policy and Compliance Management no Espaço de correção de problemas de TI respectivamente.
- Você pode adicionar controles de compensação à biblioteca de controles de compensação. Para obter mais informações, consulte Adicionar um controle de compensação à biblioteca.
- Você pode solicitar a redução de risco para um item vulnerável de host e tarefa de correção do Espaço de correção de TI. Para obter mais informações, consulte Solicitar redução de risco no Espaço de correção de problemas de TI.

Para obter mais informações, consulte Explorando o Vulnerability Manager Workspace e Explorando o Espaço de correção de problemas de TI.

Para obter mais informações sobre a compatibilidade de versão com as versões da família, consulte o artigo KB0856498 Matriz de compatibilidade do Vulnerability Response e mudanças de esquema de versão na Base de conhecimento HI.

Antes de começar

Antes de usar os espaços:

- Você precisa executar algumas tarefas de configuração. Para obter mais informações, consulte Configurar os espaços Vulnerability Response.
- Revise informações importantes sobre atualizações de tarefas de correção, regras de tarefa de correção e os principais termos e conceitos sobre os espaços, em Vulnerability Response Espaços e atualizações para tarefas de correção e regras de tarefa de correção.

Orquestração de patches com os espaços Vulnerability Response

Você pode gerenciar patches e implantações de patch para vulnerabilidades críticas para grandes grupos de ativos com a Orquestração de patches com Vulnerability Response.

Orquestração de patches nos espaços

A orquestração de patches com a aplicação Vulnerability Response usa importações programadas de integrações de soluções de terceiros, fornecedores de patches e scanners de vulnerabilidade.

A orquestração de patches com a aplicação Vulnerability Response é compatível com o ambiente clássico e os espaços Vulnerability Response. Os dados correlacionados são acumulados e exibidos nos espaços e no ambiente clássico. Para obter uma visão geral dos recursos, requisitos e informações sobre orquestração de patches no ambiente clássico, consulte Orquestração de patches com Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para obter mais informações sobre as integrações compatíveis com fornecedores de patch, consulte Noções básicas sobre a integração de orquestração de patches do BigFix HCL com Vulnerability Response e Noções básicas sobre a integração de orquestração de patches [Vulnerability Response com Microsoft SCCM.
- Para obter informações sobre como programar registros de formulário de patches nos espaços de trabalho, consulte Programar patches com a integração do SCCM [Microsoft com Vulnerability Response e Programe patches com a integração de orquestração de patches Vulnerability Response HCL BigFix.

Versões disponíveis de aplicações e dependências necessárias para a integração de orquestração de patches

Para exibir dados de Orquestração de patches e atualizações disponíveis (patches) nos espaços em Vulnerability Response, os aplicativos a seguir são necessários. Todas as aplicações listadas estão disponíveis no ServiceNow® Store. Algumas aplicações exigem assinaturas separadas. Consulte Orquestração de patches com Vulnerability Response.

Funções necessárias

Além das funções sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin necessárias para os espaços Vulnerability Response, os usuários precisam de funções que sejam específicas das integrações de orquestração de patches que você está usando para exibir dados e programar patches. Consulte as seguintes integrações compatíveis para obter mais informações sobre essas funções.

Consulte Noções básicas sobre a integração de orquestração de patches do BigFix HCL com Vulnerability Response e Noções básicas sobre a integração de orquestração de patches [Vulnerability Response com Microsoft SCCM.

Dados de patch nos espaços Vulnerability Response

No IT Remediation Workspace, você pode exibir dados de patch nos espaços:

- Na exibição inicial, clique nos cartões de pontuação para exibir registros de Soluções preferenciais em IVs, ICs vulneráveis e Patches preferenciais em IVs.
- Na exibição de lista, exiba todos os registros de atualização de patch (VPUs) e os itens vulneráveis que são atribuídos a você que têm patches dos links disponíveis.

Você pode programar patches dos seguintes registros:

- Atualização de patch (VPU)
- Tarefa de correção (RT)
- Item descoberto (SDI)

No Espaço para gerentes de vulnerabilidades, você pode exibir os patches:

- Na exibição inicial dos tópicos de observação na guia Itens vulneráveis, você pode exibir os patches preferenciais e potenciais, as datas programadas dos patches e outras informações.
- Na exibição de lista em registros de esforço de correção, você pode exibir dados de patch em registros VIT na guia Itens vulneráveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerability Response Espaços e atualizações para tarefas de correção e regras de tarefa de correção

As tarefas de correção agrupam itens vulneráveis nos Vulnerability Response espaços.

Termos-chave para os Vulnerability Response Espaços

Espaços do Vulnerability Response, ou espaços

Vulnerability Response oferece suporte aos Vulnerability Response espaços. Você pode usar a experiência clássica IU principal ou os espaços.

IU Clássica (legada)

Refere-se à experiência IU principal. Você ainda executa algumas ações e exibe algumas listas no ambiente clássico.

Espaço para gerentes de vulnerabilidades

Neste espaço, os gerentes monitoram as vulnerabilidades direcionadas e selecionam os IVs e os resultados de testes com os quais mais se importam para atribuir à TI.

Espaço de correção de TI

Neste espaço, as equipes de TI podem se concentrar nas vulnerabilidades mais importantes que são atribuídas a elas pela segurança. As informações centradas em TI que incluem itens de configuração (ICs) afetados e distintos, soluções e o andamento da correção estão facilmente disponíveis para os responsáveis pela correção neste espaço.

Espaço do analista de vulnerabilidades

Neste espaço, os analistas de vulnerabilidade podem executar a avaliação de vulnerabilidade durante a análise de vulnerabilidade de dia zero. Depois que uma vulnerabilidade de dia zero é identificada, eles podem avaliar o possível impacto e o risco associado à vulnerabilidade. Os analistas podem analisar o sistema, as aplicações ou os componentes de rede afetados para entender a gravidade e os possíveis vetores de ataque na organização.

Tópico de observação

Os tópicos de observação definem um segmento dos itens vulneráveis que os gerentes e analistas de vulnerabilidade desejam monitorar no Vulnerability Manager Workspace. Os tópicos de observação mostram um conjunto de visão geral focado de relatórios que pertencem a um segmento de IVs e resultados de testes com tendências, IC e estatísticas relacionadas à vulnerabilidade. Os painéis desses tópicos podem ser usados para monitorar tendências. Os painéis também podem ajudar os gerentes a:

- Exibir o andamento da correção em itens críticos
- Determinar a existência de vulnerabilidades em sistemas críticos
- Veja quando uma nova exploração é lançada
- Gerar resposta rápida para resolver um conjunto específico de vulnerabilidades

Esforço de correção (RE)

Os esforços de correção são criados por gerentes de vulnerabilidade quando eles determinam que é hora de a TI corrigir as vulnerabilidades listadas em um tópico de observação. Os gerentes e analistas de vulnerabilidade podem escolher como desejam criar tarefas de correção, por grupo de atribuição e vulnerabilidade, por exemplo. As tarefas de correção estão contidas no esforço de correção.

Tarefa de correção (VUL)

As equipes de TI usam tarefas de correção para corrigir as vulnerabilidades atribuídas a elas pela segurança. Tarefas de correção são listas das ações necessárias para corrigir vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de correção são criadas automaticamente quando os gerentes de segurança criam esforços de correção.

Desenvolvimento dos espaços

Nas versões anteriores do Vulnerability Response, você tinha duas opções para monitorar um conjunto de itens vulneráveis (IVs) como analista de segurança e vulnerabilidade:

- O painel Visão geral, que resume todos os IVs
- Tarefas de correção

Os itens vulneráveis foram classificados em tarefas de correção automaticamente de acordo com suas regras de tarefa de correção predefinidas. As tarefas de correção foram projetadas para oferecer suporte às equipes de TI na correção de partes gerenciáveis de itens vulneráveis.

Essa automação tornou possível agrupar um número muito grande de IVs automaticamente para atribuição e correção em massa. No entanto, os gerentes e analistas de vulnerabilidade consideraram desafiador o monitoramento de todo o conjunto de itens vulneráveis das tarefas de correção. Além de problemas de desempenho com grupos grandes, pode ser difícil criar regras de tarefa de correção funcionais] que filtram somente as vulnerabilidades que você achou mais críticas.

Os Vulnerability Response Espaços:

- Ajude os gerentes de segurança a filtrar, monitorar IVs ativos e resultados de testes ao longo do tempo e orientar a correção das vulnerabilidades que eles determinam como as mais importantes.
- Forneça às equipes de TI informações centradas em TI em um local que elas possam usar para corrigir as vulnerabilidades atribuídas a elas pela segurança.

Atualizações das tarefas de correção nos espaços

No espaço do Vulnerability Manager, os analistas e gerentes de vulnerabilidade usam os *tópicos* de observação e os *esforços* de correção como dois novos métodos para monitorar e atribuir IVs para correção.

Os grupos de vulnerabilidade foram renomeados como *Tarefas de correção*. Esta mudança se aplica a rótulos em listas, registros e regras na IU legada e nos espaços. As tarefas de correção são configuradas para que as equipes de TI possam trabalhar com elas no Espaço de correção de TI. A lista a seguir ilustra como, como gerente de vulnerabilidade ou analista de vulnerabilidade, você pode monitorar vulnerabilidades e resultados de testes, filtrá-los e atribuí-los:

1. No Vulnerability Manager Workspace, os gerentes monitoram vulnerabilidades importadas em tópicos de observação. Gerentes e analistas usam tópicos de observação para monitorar um conjunto dinâmico de IVs filtrados ao longo do tempo que eles consideram os mais críticos.
2. Com os tópicos de observação, os gerentes de segurança podem determinar quando e que tipo de IVs devem ser entregues às equipes de TI nos esforços de correção (REs). Esses REs são listas estáticas dos IVs que a segurança deseja que as equipes de TI corrijam.

   Nos esforços de correção, os gerentes têm quatro opções para agrupar IVs em Tarefas de correção (VULs). As tarefas de correção são atribuídas automaticamente às equipes de TI com base nos grupos de atribuição que estão originalmente associados aos IVs.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. As equipes de TI trabalham em tarefas de correção no Espaço de correção de TI sem precisar classificar todos os IVs.

   Uma tarefa de correção passa pelos mesmos estados que a tarefa de correção nas versões anteriores do Vulnerability Response. Quando todos os IVs em uma tarefa de correção são encerrados, a tarefa de correção é encerrada e definida como **Inativa**.

   O andamento da correção é atualizado nas visualizações de dados nos tópicos de observação e na página inicial de correção de TI.

Atualizações das regras de tarefa de correção nos espaços

As Regras do grupo de vulnerabilidade são chamadas de *Regras de tarefa de correção*. Esta mudança se aplica aos rótulos em listas, registros e regras na IU legada e nos espaços.

Nomes de tabela, por exemplo, [sn_vul_m2m_vul_group_item], não são alterados.

Se você criou regras de grupos de vulnerabilidades em versões anteriores do Vulnerability Response, elas ainda estarão disponíveis para você, rotuladas como regras de tarefa de correção.

No entanto, nos espaços, as regras do grupo de vulnerabilidades não são mais usadas como o método primário de organização de um grande volume de itens vulneráveis em grupos de vulnerabilidades. Você pode preferir deixar suas regras de tarefa de correção inativas enquanto se acostuma com os espaços.

Você pode preferir começar gradativamente a usar os espaços Vulnerability Response.

1. Se você estiver atualizando de uma versão anterior do Vulnerability Response, suas regras de VG existentes serão preservadas. Eles ainda estão disponíveis para você nos espaços. A regra de grupo padrão, Vulnerabilidade, está inativa por padrão.
2. Configure regras de atribuição e, talvez se desejar, regras de risco e execute uma importação.
3. Como gerente ou analista de vulnerabilidade, você pode escolher segmentos para monitorar nos tópicos de observação no Vulnerability Manager Workspace. Você pode usar tópicos de observação como recursos autônomos. Escolha qualquer subconjunto de IVs e use o painel neles para monitorar tendências. Com eles, você pode decidir onde e quando concentrar os esforços de correção.
4. Como gerentes de vulnerabilidade ou analista, você cria esforços de correção a partir de tópicos de observação quando decide que é hora de corrigir um subconjunto de itens vulneráveis. Uma tarefa de correção também é criada automaticamente para ser entregue à TI ao criar um esforço de correção.
5. Com o tempo, como gerente ou analista de vulnerabilidade, você pode descobrir alguns padrões de rotina que podem ser tratados automaticamente com regras de tarefas de correção.

Para exibir suas regras de tarefa de correção, navegue até **Vulnerability Response** > **Administração** > **Regras de tarefa de correção**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mais informações sobre regras de atribuição, regras de tarefa de correção, esforços de correção e itens vulneráveis nos Vulnerability Response espaços

- Os registros de tarefa de correção (VUL) são exibidos em listas e registros no ambiente clássico e nos espaços.
- Uma tarefa de correção passa pelos mesmos estados que um grupo de vulnerabilidades. Quando todos os IVs em uma tarefa de correção são encerrados, a tarefa de correção muda para o estado Inativo.
- Para ajudar suas equipes na correção, um item vulnerável só pode estar em um esforço de correção. Quando estiver em um esforço de correção, um item vulnerável não será adicionado a nenhum outro esforço de correção criado.
- Se você excluir um esforço de correção, o esforço de correção se tornará inativo e todos os IVs ativos ficarão disponíveis para novos esforços de correção.
- Um item vulnerável pode estar em várias tarefas de correção.
- As tarefas de correção são atribuídas automaticamente às equipes de TI com base no grupo de atribuição associado a um item vulnerável em um esforço de correção. Se você criar uma tarefa de correção sob demanda, selecione o grupo de atribuição.
- Se você estiver atualizando de uma versão anterior do Vulnerability Response, suas regras de atribuição foram preservadas na IU legada.
- Se você estiver atualizando de uma versão anterior do Vulnerability Response, seus usuários e grupos atuais serão herdados e poderão ser acessados nos espaços.

Para obter mais informações sobre os ciclos de vida dos esforços de correção, consulte Ciclos de vida de esforços de correção, tarefas de correção e registros nos espaços do Vulnerability Response.

Configuração e configuração dos espaços Vulnerability Response

Para obter mais informações sobre regras de atribuição e regras de tarefa de correção, consulte Configurar os espaços Vulnerability Response e Vulnerability Response visão geral de regras de atribuição.

Se você é um novo cliente e ainda não os adicionou, deve configurar usuários e grupos para que os itens vulneráveis e as tarefas de correção sejam atribuídos aos grupos de correção desejados. As regras de atribuição do Vulnerability Response são usadas para atribuir trabalho a grupos.

Configurar os espaços Vulnerability Response

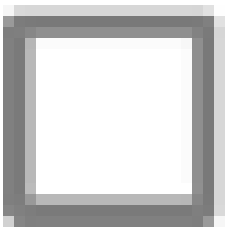
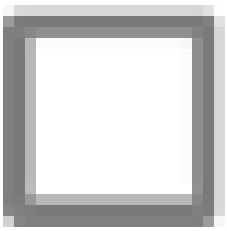
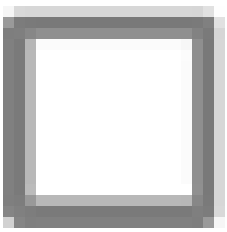
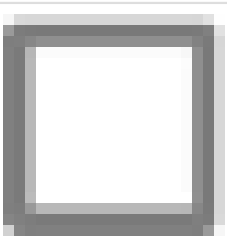
Antes de usar os espaços, confirme se você concluiu as tarefas de configuração a seguir.

Antes de Iniciar
Função necessária: administrador para atribuir funções a usuários e grupos e usuários a grupos.

sn_vul.vulnerability_admin para editar, criar regras e configurar a aplicação Vulnerability Response.

Confirme que você concluiu as tarefas de configuração a seguir. Consulte as etapas após a lista para obter mais informações sobre como executar essas tarefas.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

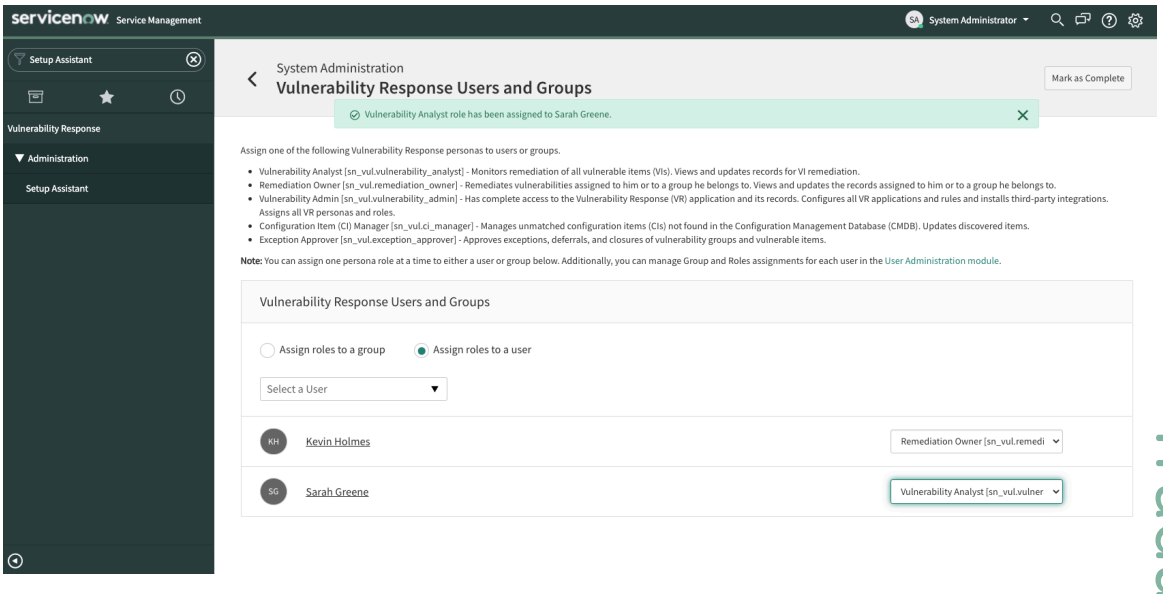
Tarefa	Descrição
	Se ainda não estiverem atribuídos, atribua usuários e grupos com as funções apropriadas para que eles tenham acesso aos espaços. Função necessária: administrador Consulte as etapas abaixo para obter mais informações.
	Configure regras de atribuição para que os itens vulneráveis sejam atribuídos aos grupos apropriados para correção. Função necessária: sn_vul.vulnerability_admin. Para obter mais informações sobre regras de atribuição, consulte Vulnerability Response visão geral de regras de atribuição. Você cria e edita regras de atribuição no ambiente clássico.
	(Opcional): edite ou crie suas regras de tarefa de correção. Função necessária: sn_vul.vulnerability_admin. **Nota:** Funcionalmente, as regras de tarefa de correção funcionam da mesma forma que as regras de tarefa de correção nas versões anteriores do Vulnerability Response. No entanto, ao contrário dos grupos de vulnerabilidade que foram criados automaticamente a partir das regras de tarefa de correção, as tarefas de correção são criadas quando você cria esforços de correção. Você tem as seguintes opções para agrupar os itens vulneráveis em um esforço de correção em tarefas de correção: • Por grupo de atribuição • Por grupo de atribuição e item de configuração • Por grupo de atribuição e vulnerabilidade • Nenhum: use esta opção se quiser adicionar IVs manualmente a uma tarefa de correção. Para obter mais informações, consulte Criar uma tarefa de correção sob demanda no Vulnerability Manager Workspace. Para obter mais informações sobre como os IVs são agrupados automaticamente e como as regras de grupo são reaplicadas no ambiente clássico, consulte Vulnerability Response tarefas de correção e regras de tarefa visão geral.
	Editar regras de destino de correção. Função necessária: sn_vul.vulnerability_admin. Adicione regras de destino de correção no ambiente clássico. Para obter mais informações sobre regras de destino de correção, consulte Criar ou editar Vulnerability Response regras de destino de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Depois de instalar e ativar a aplicação Vulnerability Response, no ambiente clássico como um usuário com a função de administrador, navegue até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração**.



2. No Assistente de configuração, atribua usuários aos grupos a seguir.

Nota:
1000 é o limite para o número de grupos de usuários aos quais um usuário pode ser atribuído nos espaços do Vulnerability Response.

Os grupos a seguir são fornecidos com a aplicação Vulnerability Response e são usados nos espaços. Você pode atribuir usuários a eles no Assistente de configuração:

- Proprietário de correção - Este grupo é para responsáveis de correção de TI no espaço de correção de TI. Usuários com esta função corrigem vulnerabilidades atribuídas a eles em tarefas de correção.

  Nota:

  Se você quiser que os responsáveis pela correção criem e exibam solicitações de mudança e exibam dados de item de configuração (IC) vulnerável no Espaço de correção de TI e no ambiente clássico, atribua a função itil a eles. Você pode preferir atribuir a função itil a usuários individuais em vez de a todos os membros de um grupo. A função cmdb_read também é uma opção para os usuários exibirem dados de IC nos espaços.

- A partir da v16.1, você pode configurar lembretes de e-mail para os responsáveis pela correção de TI. Para configurar notificações por e-mail para os espaços, consulte Configurar notificações por e-mail nos espaços Vulnerability Response.
- Administrador de vulnerabilidades - Este grupo é para gerenciadores de vulnerabilidades. Esta função configura a aplicação Vulnerability Response no Assistente de configuração. Esta função também tem permissão para processar solicitações de falso-positivo e de exceção.
- Analista de vulnerabilidade - Este grupo é para gerentes de segurança, gerentes de vulnerabilidade e analistas no Vulnerability Manager Workspace. Esta função monitora

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidades, cria tópicos de observação e esforços de correção e monitora o andamento da correção.

- Aprovador de falso-positivo - Usuários neste grupo processam solicitações de falso-positivo de itens vulneráveis ou tarefas de correção. Uma solicitação de falso-positivo requer um processo de aprovação de nível único. Você pode gerenciar a atribuição de usuários a este grupo fora do Assistente de configuração em **Administração de usuários**.
- Aprovador de exceção - uma solicitação de exceção para um item vulnerável ou tarefa de correção é aprovada usando um fluxo de trabalho de aprovação padrão de dois níveis. A solicitação de exceção requer dois níveis de aprovadores. Adicione usuários a ambos os grupos de aprovação: Aprovador de exceção - Nível 1 e Nível de aprovador de exceção - 2. Depois que a solicitação é aprovada pelo aprovador de nível 1, ela é enviada para o aprovador de segundo nível. Você gerencia a atribuição de usuários a este grupo fora do Assistente de configuração em **Administração de usuários**.

Nota:
Adicione usuários aos grupos de aprovação antes de enviar solicitações de falso-positivo e de exceção. Se você criar solicitações antes de atribuir usuários com permissão de aprovação, as solicitações podem não ficar visíveis para eles.

Como alternativa, clique no link **Administração do usuário** para gerenciar e atribuir as seguintes funções granulares aos usuários e grupos existentes. Essas funções permitem que os usuários executem ações específicas na aplicação Vulnerability Response e nos espaços.

- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vul.remediation_owner
- Para criar e exibir solicitações de mudança no Espaço de correção de TI e no ambiente clássico, atribua a função itil a elas.

Consulte Vulnerability Response personas e funções granulares e Atribua as funções de persona Vulnerability Response usando o Assistente de configuração para obter mais informações sobre como atribuir funções de persona a usuários e usuários a grupos.

3. As tarefas de correção são entregues automaticamente aos grupos de atribuição de correção de TI para processamento quando são criadas.
   - Por grupo de atribuição
   - Por grupo de atribuição e item de configuração
   - Por grupo de atribuição e vulnerabilidade
   - Nenhum: use esta opção se quiser adicionar IVs manualmente a uma tarefa de correção.

   Nota:
   Para a versão 18.0 de Vulnerability Response, a opção **Nenhum** não está disponível.

   Se você estiver atualizando de uma versão anterior do Vulnerability Response, seus grupos de atribuição serão preservados. No entanto, você pode preferir editar esses grupos para que os itens vulneráveis sejam associados a grupos de atribuição específicos até que você se acostume com o funcionamento dos tópicos de observação e dos esforços de correção. Por exemplo, você pode criar grupos de atribuição por produto ou região, mas pode usar qualquer critério que melhor se adapte à sua organização.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você também pode usar regras de atribuição para atribuir tarefas de correção a grupos. Você pode preferir executar somente regras de prioridade alta para os seguintes itens:

- Itens que precisam de tratamento especial
- Itens em que o risco é crítico ou um IV requer manipulação pela conformidade regulatória

As seguintes regras de atribuição fornecidas com a aplicação estão ativas por padrão:

- Regra de atribuição de IC descontinuada
- Atribuir ao grupo de suporte de IC
- Regra de atribuição da estação de trabalho
- Regra de atribuição de banco de dados
- Regra de atribuição da aplicação Web
- Regra de atribuição do Windows Server
- Regra de atribuição de servidor que não seja Windows
- Regra de atribuição de contato alternativo

Para obter mais informações sobre regras de atribuição, consulte Vulnerability Response visão geral de regras de atribuição. Você cria e edita regras de atribuição no ambiente clássico.

4. **Opcional:** Edite ou crie suas regras de tarefa de correção.

(Optional) Nos espaços de trabalho, as tarefas de correção são criadas quando você cria esforços de correção. Você tem as seguintes opções para agrupar os itens vulneráveis em um esforço de correção em tarefas de correção:

- Por grupo de atribuição
- Por grupo de atribuição e item de configuração
- Por grupo de atribuição e vulnerabilidade
- Nenhum: use esta opção se quiser adicionar IVs manualmente a uma tarefa de correção. Para obter mais informações, consulte Criar uma tarefa de correção sob demanda no Vulnerability Manager Workspace.

Nota:
Para a versão 18.0 de Vulnerability Response, a opção **Nenhum** não está disponível.

Para obter mais informações sobre como os IVs são agrupados automaticamente e como as regras de grupo são reaplicadas no ambiente clássico, consulte Vulnerability Response tarefas de correção e regras de tarefa visão geral.

Espaço para gerentes de vulnerabilidades

O Vulnerability Manager Workspace permite que os gerentes e analistas de vulnerabilidade monitorem as vulnerabilidades com as quais eles mais se importam e decidam estrategicamente quais vulnerabilidades eles enviam para as equipes de TI corrigir.

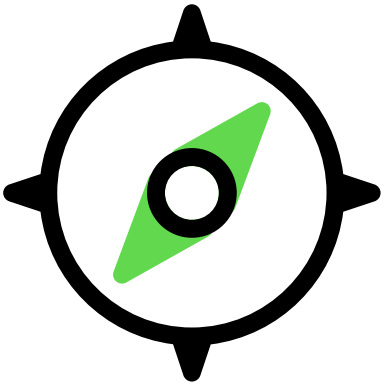
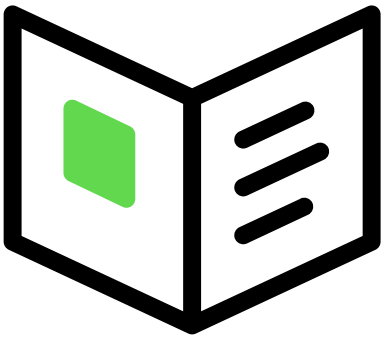
Visão geral

V18.0 Demonstração do Vulnerability Manager Workspace

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Iniciar

Explorar	Usar	Referência
		
Saiba mais sobre os recursos do Vulnerability Manager Workspace	Saiba como usar o Vulnerability Manager Workspace para monitorar, gerenciar e corrigir vulnerabilidades	Saiba mais sobre as informações adicionais necessárias para usar o Vulnerability Manager Workspace

Solucionar problemas e obter ajuda

- Security Operations na Comunidade da ServiceNow
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Explorando o Vulnerability Manager Workspace

Como gerente e analista de vulnerabilidades, obtenha uma exibição unificada de todos os tipos de vulnerabilidade no Vulnerability Manager Workspace. Você pode ver vulnerabilidades e problemas de configuração de host, aplicação e contêiner, criar tópicos de observação nessas vulnerabilidades e configurações incorretas e criar tarefas de correção.

Nota:
A partir da v19.0 de Vulnerability Response, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

Você pode exibir o Vulnerability Manager Workspace navegando até **Espaços** > **Espaço para gerentes de vulnerabilidades**.

O Vulnerability Manager Workspace consiste nas seguintes páginas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Página inicial

Consiste em filtros predefinidos que são usados para visualizar o resumo dos registros.

Para obter mais informações sobre a Página inicial, consulte Visão geral da página inicial.

Nota:
A partir da v21.0 de Vulnerability Response, os tópicos de observação aparecem na página Tópicos de observação.

Página de tópicos de observação

Consiste em uma lista de tópicos de observação, que são categorizados em quatro módulos: vulnerabilidades do host, vulnerabilidades da aplicação, vulnerabilidades do contêiner e resultados de testes de configuração.

Para obter mais informações sobre tópicos de observação, consulte Visão geral dos tópicos de observação.

Página Painéis

Consiste nos painéis Vulnerability Management, Vulnerability Management (PA), Vulnerability Approvals, CISO, Container Vulnerability Management Overview, Application Vulnerability Management, Unified Vulnerability Response e Integridade.

Para obter mais informações, consulte Visão geral dos painéis.

Nota:
A página Painéis aparece a partir da versão 19.0 do Vulnerability Response.

Página de lista

Consiste nas páginas de lista padrão e personalizadas para esforços de correção, tarefas de correção, itens vulneráveis de host, itens vulneráveis de aplicação, itens vulneráveis de contêiner, resultados de testes de configuração, exceções, aprovações e bibliotecas.

Para obter mais informações, consulte Visão geral de listas.

Principais recursos

O Vulnerability Manager Workspace fornece os seguintes recursos:

- O Vulnerability Manager Workspace é compatível com Application Vulnerability Response, Vulnerability Response contêinere Configuration Compliance.
- Obtenha um resumo de todos os itens vulneráveis (IVs) de host ativos, itens vulneráveis de aplicação (AVITs), itens vulneráveis de contêiner (CVITs) e resultados de testes de configuração na visualização do formulário na página inicial.
- Os tópicos de observação são categorizados pelo tipo de registro no painel de navegação na página de tópicos de observação. Ou seja, você pode criar um tópico de observação que contenha itens vulneráveis de host (IVs), itens vulneráveis de aplicação (AVITs), itens vulneráveis de contêiner (CVITs) ou resultados de testes de configuração.
- Você pode exibir os painéis Vulnerability Management, Vulnerability Management (PA), Vulnerability Approvals, CISO, Container Vulnerability Management Overview, Application Vulnerability Management, Unified Vulnerability Response e Integridade no Vulnerability Manager Workspace.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir um exemplo de fluxo de trabalho no Vulnerability Manager Workspace

Veja um exemplo de um fluxo de trabalho de ponta a ponta no Vulnerability Manager Workspace. Veja como um gerente ou analista de vulnerabilidade pode usar o espaço para monitorar registros críticos [e criar tarefas de correção para entregar à TI.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Procedimento

Clique no vídeo a seguir para exibir as etapas do fluxo de trabalho.
Demonstração do Vulnerability Manager Workspace

O vídeo anterior inclui as seguintes tarefas:

a. Clique em um tópico de observação na exibição **inicial** do espaço para exibir dados em um painel para diferentes categorias de registros.

b. Crie um tópico de observação usando condições de filtro e visualize os registros correspondentes. Para obter mais informações sobre como criar um tópico de observação, consulte Criar um tópico de observação no Vulnerability Manager Workspace.

c. Exiba dados sobre registros e seus itens de configuração relacionados na guia **ICs vulneráveis** em um tópico de observação. Para obter mais informações sobre as visualizações, consulte Lista de itens relacionados e visualizações em um tópico de observação.

d. Exiba dados sobre vulnerabilidades na guia **Vulnerabilidades distintas** em um tópico de observação.

e. Exiba os registros associados ao tópico de observação na guia **Itens vulneráveis** em um tópico de observação. Role para a direita para exibir quais registros já estão em um esforço de correção na coluna Esforço de correção.

f. Clique **em Criar um esforço** de correção em um tópico de observação quando estiver pronto para criar tarefas para tipos específicos de registros e atribuí-los à TI para correção. Para obter mais informações sobre como criar um esforço de correção, consulte Criar um esforço de correção no Vulnerability Manager Workspace.

g. Clique na exibição **Lista** para ver listas de seus esforços de correção, tarefas de correção, registros, exceções e aprovações. Para obter mais informações sobre a página Listas, consulte Visão geral de listas.

h. Clique na lista Esforços de correção **ativos** na exibição de lista para abrir um registro de esforço de correção para exibir o status e as informações sobre o registro. Para obter mais informações, consulte Visão geral de listas.

i. Clique na guia **Tarefa** de correção no registro do esforço de correção para exibir as tarefas de correção associadas ao registro de correção. Para obter mais informações, consulte Visão geral de listas.

j. Clique na guia **Itens vulneráveis** no registro do esforço de correção para exibir uma lista de registros associados ao esforço de correção. Para obter mais informações, consulte Visão geral de listas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

k. Se você quiser criar uma nova tarefa de correção sob demanda a partir do esforço de correção para um subconjunto de registros, selecione os registros que deseja mover e clique em **Criar tarefa de correção**.

> **Nota:**
> Na versão 18.0 do Vulnerability Response, como não é possível criar uma tarefa de correção sob demanda, o botão **Criar tarefa de correção** é removido da lista de itens relacionados a Itens vulneráveis de um esforço de correção.

Visão geral da página inicial

A partir de Vulnerability Response v21.0, a página inicial no Vulnerability Manager Workspace fornece o resumo dos registros ativos, mostrando visualizações de classificação de risco, andamento de correção, atribuições a grupos de atribuição, registros em tarefas de correção e vulnerabilidades de recursos de nuvem.

> **Dica:**
>
> Se você definir a propriedade do sistema *sn_vul_cmn_ws.navigate_to_workspace* como verdadeiro, ao selecionar os links de filtro predefinidos no painel de navegação, esses links serão abertos no Vulnerability Manager Workspace com a seleção automática do filtro salvo correspondente.
>
> Por exemplo, se você selecionar **Alto risco** navegando até **Todos** > **Vulnerability Response** > **Itens vulneráveis**, este link será redirecionado para a página inicial no Vulnerability Manager Workspace com a seleção automática do filtro de **alto risco**.

A partir da v21.0 do Vulnerability Response, os tópicos de observação aparecem na página Tópicos de observação. Para obter mais informações, consulte Visão geral dos tópicos de observação.

Na página inicial, você pode exibir as visualizações das vulnerabilidades de host pré-filtradas, vulnerabilidades de contêiner, vulnerabilidades de aplicação e resultados de testes de configuração. Você também pode exibir visualizações de um conjunto de registros desejados criando e aplicando filtros. Para obter mais informações sobre como criar, atualizar e excluir filtros, consulte Crie filtros para visualizar o resumo de registros ativos.

Vulnerabilidades do host

A guia **Vulnerabilidades do host** contém visualizações que fornecem um resumo geral das vulnerabilidades do host ativas.

Funções necessárias:

- sn_vul.vulnerability_analyst e sn_vul.vulnerability_admin para exibir as visualizações aplicando filtros e criar filtros.
- Função granular sn_vul.read_all para exibir as visualizações aplicando filtros.

A tabela a seguir descreve as visualizações na guia Vulnerabilidades do host na página inicial do. Selecione essas visualizações para obter a lista de registros correspondentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações na guia Vulnerabilidades do host na página inicial

Visualização	Descrição
Por grupo de atribuição e status de correção	Registros ativos atribuídos a vários grupos de atribuição que são agrupados por status de correção.
Por estado	Registros ativos categorizados por vários estados (Aberto, Sob investigação, Aguardando implementação, Em revisão, Resolvido e Adiado).
Por pontuação de risco	Registros ativos categorizados por classificação de risco (1 - Crítico, 2- Alto, 3 - Médio, 4 - Baixo e 5 - Nenhum)
Na tarefa de correção	Registros ativos que fazem e não fazem parte da tarefa de correção.
Com explorações existentes	Registros ativos com e sem explorações conhecidas.
Por face externa	Registros ativos de rcategorizados pela exposição do ativo à internet.
Por classe de IC	Registros ativos categorizados por classes de IC.
Por recurso de nuvem	Registros ativoscategorizados por vários recursos de nuvem.
Itens adiados por motivo	Registros adiados ativos agrupados por motivo.

Vulnerabilidades do contêiner

A guia **Vulnerabilidades do contêiner** contém visualizações que fornecem um resumo geral dos itens vulneráveis do contêiner ativos.

Funções necessárias:

- sn_vul_container.vulnerability_analyst e sn_vul_container.vulnerability_admin para exibir as visualizações aplicando filtros e criar filtros.
- Função granular sn_vul_container.read_all para exibir as visualizações aplicando filtros.

A tabela a seguir descreve as visualizações na guia Vulnerabilidades do host na página inicial do. Selecione essas visualizações para obter a lista de registros correspondentes.

Visualizações na guia Vulnerabilidades do contêiner na página inicial

Visualização	Descrição
Por grupo de atribuição e status de correção	Registros ativos atribuídos a vários grupos de atribuição que são agrupados por status de correção.
Por estado	Registros ativos categorizados por vários estados (Aberto, Sob investigação, Aguardando implementação, Em revisão, Resolvido e Adiado).
Por pontuação de risco	Registros ativos categorizados por classificação de risco (1 - Crítico, 2- Alto, 3 - Médio, 4 - Baixo e 5 - Nenhum)
Na tarefa de correção	Registros ativos que fazem e não fazem parte da tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações na guia Vulnerabilidades do contêiner na página inicial

Visualização	Descrição
Com explorações existentes	Registros ativos com e sem explorações conhecidas.
Por face externa	Registros ativos de rcategorizados pela exposição do ativo à Internet.
Imagens do Docker	Número de imagens do Docker exclusivas.
Por imagem de base	Registros ativos categorizados pelo tipo de imagem.
Itens adiados por motivo	Registros adiados ativos agrupados por motivo.

Vulnerabilidades de aplicação

A guia **Vulnerabilidades da aplicação** contém visualizações que fornecem um resumo geral das vulnerabilidades da aplicação.

Funções necessárias:

- sn_vul.app_sec_manager para exibir as visualizações aplicando filtros e criar filtros.
- Função granular sn_vul.app_read_all para exibir as visualizações aplicando filtros.

A tabela a seguir descreve as visualizações na guia Vulnerabilidades do host na página inicial do. Selecione essas visualizações para obter a lista de registros correspondentes.

Visualizações na guia Vulnerabilidades da aplicação na página inicial

Visualização	Descrição
Por grupo de atribuição e status de correção	Registros ativos atribuídos a vários grupos de atribuição que são agrupados por status de correção.
Por estado	Registros ativos categorizados por vários estados (Aberto, Sob investigação, Aguardando implementação, Em revisão, Resolvido e Adiado).
Por pontuação de risco	Registros ativos categorizados por classificação de risco (1 - Crítico, 2- Alto, 3 - Médio, 4 - Baixo e 5 - Nenhum)
Na tarefa de correção	Registros ativos que fazem e não fazem parte da tarefa de correção.
Com explorações existentes	Registros ativos com e sem explorações conhecidas.
Por face externa	Registros ativos de rcategorizados pela exposição do ativo à Internet.
Por classe de IC	Registros ativos categorizados por classes de IC.
Por recurso de nuvem	Registros ativoscategorizados por vários recursos de nuvem.
Itens adiados por motivo	Registros adiados ativos agrupados por motivo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados de testes de configuração

A guia **Resultados de testes de configuração** contém visualizações que fornecem um resumo geral das configurações incorretas ativas dos ativos em sua organização.

Funções necessárias:

- sn_vulc.admin para exibir as visualizações aplicando filtros e criar filtros.
- Função granular sn_vulc.read para exibir as visualizações aplicando filtros.

A tabela a seguir descreve as visualizações na guia Resultados de testes de configuração na página inicial. Selecione essas visualizações para obter a lista de registros correspondentes.

Visualizações na guia Resultados de testes de configuração na página inicial

Visualização	Descrição
Por grupo de atribuição e status de correção	Registros ativos atribuídos a vários grupos de atribuição que são agrupados por status de correção.
Por estado	Registros ativos categorizados por vários estados (Aberto, Sob investigação, Aguardando implementação, Em revisão, Resolvido e Adiado).
Por pontuação de risco	Registros ativos categorizados por classificação de risco (1 - Crítico, 2- Alto, 3 - Médio, 4 - Baixo e 5 - Nenhum)
Por tecnologia	Registros ativos categorizados por tecnologia.
Por teste	Registros ativos categorizados por testes.
Por face externa	Registros ativos de rcategorizados pela exposição do ativo à Internet.
Por classe de IC	Registros ativos categorizados por classes de IC.
Por recurso de nuvem	Registros ativoscategorizados por vários recursos de nuvem.
Itens adiados por motivo	Registros adiados ativos agrupados por motivo.

Você pode exibir as informações mais recentes clicando no ícone **Atualizar** no widget.

Visão geral dos tópicos de observação

Um *tópico* de observação é um conjunto de visualizações de dados que permite monitorar um conjunto filtrado de registros ao longo do tempo em um painel que pode ser de interesse particular ou prioridade para sua organização.

A partir da v21.0 do Vulnerability Response, os tópicos de observação aparecem na página Tópicos de observação.

Os dados exibidos nas visualizações de dados nos tópicos de observação são atualizados dinamicamente conforme os dados de vulnerabilidade mudam após a importação. Use os painéis para monitorar as tendências, o escopo e os tipos de vulnerabilidades e os itens de configuração para o tópico de observação selecionado. Essas informações ajudam a determinar como as vulnerabilidades em cada tópico de observação afetam seu ambiente. Para obter mais informações sobre as guias de itens relacionados e suas visualizações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

em um tópico de observação, consulte Lista de itens relacionados e visualizações em um tópico de observação.

Os tópicos de observação a seguir são fornecidos com o sistema de base no módulo Vulnerabilidades do host:

- Vulnerabilidades em ativos externos
- Vulnerabilidades com explorações disponíveis
- Vulnerabilidades em Windows Servers
- Vulnerabilidades nos servidores Linux
- Vulnerabilidades críticas atrasadas
- Vulnerabilidades críticas fora das Tarefas de correção

Nota:
Se uma visualização de dados mostrar que não há IVs para essa categoria, mas você puder ver uma lista de IVs ao clicar no ícone do gráfico, verifique a coluna com o nome do tópico de observação na lista exibida. Verifique se o valor de todos os IVs listados na coluna do tópico de observação, por exemplo, voltado para a Internet, é false. Este valor neste exemplo indica que não há IVs voltados para a Internet para este tópico de observação.

Para iniciar a correção ou quando surgir uma necessidade crítica dos registros que estão em um tópico de observação, você pode criar um *esforço* de correção a partir de um tópico de observação. Para obter mais informações, consulte Criar um esforço de correção no Vulnerability Manager Workspace.

Tópicos relacionados

Usar tópicos de observação no Vulnerability Manager Workspace

Criar um tópico de observação no Vulnerability Manager Workspace

Editar ou excluir um tópico de observação

Desativar ou ativar um tópico de observação

Lista de itens relacionados e visualizações em um tópico de observação

A partir da versão 18.0, você pode criar tópicos de observação que são categorizados em quatro módulos: Vulnerabilidades do host, Vulnerabilidades do contêiner, Vulnerabilidades da aplicação e Resultados de testes de configuração. As guias de itens relacionados em um tópico de observação diferem para cada módulo.

Nota:
A partir da v19.0 de Vulnerability Response, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

O painel de navegação na página principal contém os seguintes módulos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Vulnerabilidades do host: exibe os tópicos de observação que incluem os itens vulneráveis do host.
- Vulnerabilidades do contêiner: exibe os tópicos de observação que incluem os itens vulneráveis do contêiner.
- Vulnerabilidades da aplicação: exibe os tópicos de observação que incluem os itens vulneráveis da aplicação.
- Configuração Resultados de testes: exibe os tópicos de observação que incluem os itens de configuração.
- Inativo: exibe os tópicos de observação inativos de todos os quatro módulos.

A tabela a seguir mostra as guias de itens relacionados que estão disponíveis para diferentes módulos de tópico de observação:

Tópico de observação e itens relacionados

Tópico de observação	Guias de itens relacionados
Vulnerabilidades do host	Visão geral, ICs afetados, vulnerabilidades distintas e itens vulneráveis
Vulnerabilidades do contêiner	Visão geral, ICs afetados, vulnerabilidades distintas e itens vulneráveis
Vulnerabilidades de aplicação	Visão geral e itens vulneráveis
Resultados de testes de configuração	Visão geral, ICs afetados, testes de configuração distintos e resultados de testes de configuração

A tabela a seguir fornece uma descrição das guias de itens relacionados e das visualizações em um tópico de observação.

Guias de itens relacionados e visualização em um tópico de observação

Guia e visualização de itens relacionados	Descrição
Visão geral	
Itens vulneráveis ativos ao longo do tempo	Número de itens vulneráveis (IVs) ativos ao longo do tempo. Você pode monitorar as tendências desses dados nos últimos 30 dias. Você também pode filtrar os dados usando os filtros Categoria de ativo .
IVs em esforços de correção	Número de IVs ativos do número total de IVs que já estão nos esforços de correção ativos.
Esforços de correção ativos	Lista dos esforços de correção ativos.
ICs afetados	
ICs distintos	Número de itens de configuração (ICs) (ativos) afetados por essas vulnerabilidades.
IVs por classe de IC	Número de itens vulneráveis (IVs) para cada Configuration Management Database (CMDB) classe de IC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guias de itens relacionados e visualização em um tópico de observação

Guia e visualização de itens relacionados	Descrição
	Nota: Este widget aparece somente para os tópicos de observação no módulo de vulnerabilidades de host, aplicação e contêiner.
Problemas de configuração por classe de IC	Número de ICs para cada Configuration Management Database (CMDB) classe de IC. **Nota:** Este widget aparece somente para os tópicos de observação no módulo Problemas de configuração.
IVs voltados para a Internet	Número de IVs ativos do número total de IVs para seus ativos que estão expostos à Internet. **Nota:** Este widget aparece somente para os tópicos de observação no módulo de vulnerabilidades de host, aplicação e contêiner.
Problemas de configuração voltados para a Internet	Número de ICs ativos em relação ao total de ICs para seus ativos que estão expostos na Internet. **Nota:** Este widget aparece somente para os tópicos de observação no módulo Problemas de configuração.
Vulnerabilidades distintas	
IVs com explorações existentes	IVs ativos com explorações conhecidas.
Vulnerabilidades distintas	Número de vulnerabilidades individuais distintas associadas aos seus ativos. As vulnerabilidades distintas podem ser filtradas com base no tipo de problema.
IVs com vulnerabilidades de PCI	Número de ativos individuais e distintos que têm IVs ativos com vulnerabilidades do Setor de cartão de pagamento (PCI).
Itens vulneráveis	
Itens vulneráveis de host	Lista de todos os itens vulneráveis do host. Você pode filtrar esta lista para que somente os registros que você deseja ver sejam exibidos. **Nota:** Esta lista aparece somente para os tópicos de observação no módulo Vulnerabilidades do host.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guias de itens relacionados e visualização em um tópico de observação

Guia e visualização de itens relacionados	Descrição
Itens vulneráveis da aplicação	Lista de todos os itens vulneráveis da aplicação. Você pode filtrar esta lista para que somente os registros que você deseja ver sejam exibidos. **Nota:** Esta lista aparece somente para os tópicos de observação no módulo Vulnerabilidades da aplicação.
Itens vulneráveis de contêiner	Lista de todos os itens vulneráveis de contêiner. Você pode filtrar esta lista para exibir para que somente os registros que você deseja ver sejam exibidos. **Nota:** Esta lista aparece somente para os tópicos de observação no módulo Vulnerabilidades do contêiner.
Guia**Visão geral** em um tópico de observação no módulo Resultados de testes de configuração	
Resultados de testes de configuração ativos ao longo do tempo	Número de resultados de testes de configuração ativos ao longo do tempo. Você pode monitorar as tendências desses dados nos últimos 30 dias.
Resultados de testes de configuração em esforços de correção	Número de resultados de testes de configuração ativos do número total de registros que já estão nos esforços de correção ativos.
Esforços de correção ativos	Lista dos esforços de correção ativos.
Guia**Testes de configuração distintos** em um tópico de observação no módulo Resultados de testes de configuração	
Resultados de testes de configuração via criticidade de teste	Resultados de testes de configuração baseados na criticidade dos problemas.
Testes de configuração distinta	Número de testes de configuração distintos.
Guia**Resultados de testes de configuração** em um tópico de observação no módulo Resultados de testes de configuração	Lista de resultados de testes de configuração.

Você pode adquirir os detalhes mais recentes de um tópico de observação selecionando o botão **Atualizar**. O status da atualização mais recente e o carimbo de data/hora são exibidos sob o nome do tópico de observação. Quando você atualiza um tópico de observação, todos os detalhes do tópico de observação, incluindo os gráficos e os esforços de correção, são atualizados. Um tópico de observação é atualizado automaticamente quando é criado ou atualizado.

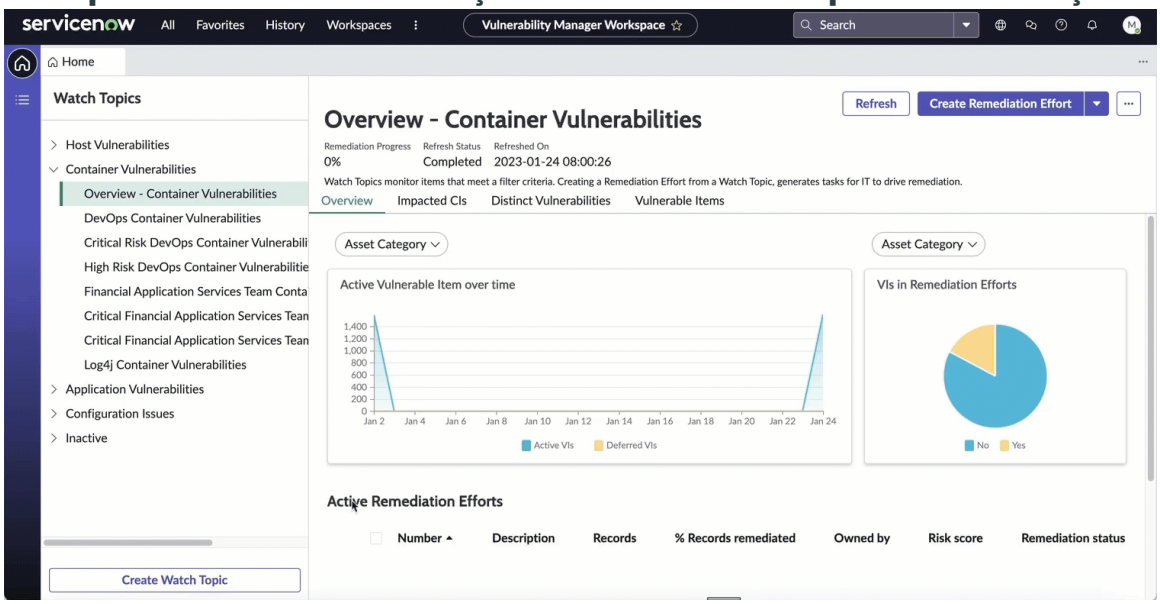
Nota:
Como você não pode atualizar um tópico de observação inativo, o botão **Atualizar** está inativo para um tópico de observação inativo.

Clique em um gráfico de dados em qualquer um dos widgets para exibir informações adicionais sobre os registros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example: Versão 18.0 Visualizações de dados em um tópico de observação



Visão geral dos esforços de correção

Um esforço de correção é um conjunto de registros associados a um tópico de observação. Os registros listados em um esforço de correção são estáticos. Eles não são atualizados por novos dados de importação ou mudanças feitas nos tópicos de observação.

Com **Ativo** selecionado na lista **Esforços** de correção, clique em um link de esforço de correção para abri-lo.

Os itens da lista relacionada no registro do esforço de correção permitem que você exiba o andamento e o status gerais da correção nos registros associados a ele.

- Na guia **Visão geral**, monitore os registros associados a este esforço de correção que foram encerrados ao longo do tempo. À direita do registro, clique no ícone de filtro no gráfico para ver os filtros aplicados à visualização de dados.
- Na guia **Detalhes**, exiba detalhes sobre o esforço de correção, incluindo o tópico de observação associado e o status (Ativo ou Inativo). Você pode desativar um esforço de correção nesta página. Se você desativar o esforço de correção antes que todos os registros sejam encerrados, todos os registros ativos se tornarão disponíveis para adicionar a novos esforços de correção.
- Na guia **Tarefas** de correção, exiba as Tarefas de correção associadas a este esforço de correção. Veja a porcentagem dos registros associados a esta tarefa que foram corrigidos.
- Na guia **Itens vulneráveis**, exiba os registros associados a este esforço de correção. Quando todos os registros em uma tarefa de correção são concluídos e encerrados, o esforço de correção muda para Inativo. Quando um esforço de correção está inativo, todos os registros encerrados associados ao esforço de correção não estão disponíveis para adicionar a novos esforços de correção.

Nota:
A partir da versão 18.0, a guia **Itens vulneráveis** aparece para os esforços de correção associados aos tópicos de observação nos módulos Vulnerabilidades do host, Vulnerabilidades da aplicação e Vulnerabilidades do contêiner.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Na guia **Resultados de testes de configuração**, exiba os Resultados de testes de configuração associados ao esforço de correção.

Nota:
A partir da versão 18.0, a guia **Resultados de testes de configuração** aparece para os esforços de correção associados aos tópicos de observação no módulo Resultados de testes de configuração.

Para obter mais detalhes e ações de IU que você pode executar em um esforço de correção, consulte Usar registros de esforço de correção.

Ciclos de vida de esforços de correção, tarefas de correção e registros nos espaços do Vulnerability Response

Os estados dos registros e suas tarefas de correção (RTs) associadas serão afetados se os registros forem adiados, resolvidos, reabertos e transferidos para outros esforços de correção (REs).

Funções necessárias: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin para o Vulnerability Manager Workspace.

Criando esforços de correção

A forma como os estados e os ciclos de vida dos esforços de correção, das tarefas de correção e dos registros são afetados depende de como um esforço de correção é criado, quando é criado e se é desativado.

Na lista no canto superior direito de um tópico de observação, você pode criar um esforço de correção clicando em **Criar um** esforço de correção ou **Criar esforço recorrente**. Você pode criar um esforço de correção recorrente por tópico de observação. Se você criar um esforço de correção recorrente, os esforços de correção subsequentes para o tópico de observação associado serão criados automaticamente com base nos critérios definidos. Em qualquer um dos casos:

- Para facilitar a correção, somente registros ativos são adicionados aos esforços de correção.
- Todos os registros em novos esforços de correção são colocados em novas tarefas de correção. Os registros podem existir em várias tarefas de correção, mas somente um registro pode ser associado a um esforço de correção.

Nota:
Um esforço de correção é desativado automaticamente quando não há registros ativos.

Transferindo registros ou transferência de registro

Você pode transferir registros de um esforço de correção para outro ao criar um esforço de correção, marcando a caixa de seleção **Transferir registros correspondentes de outros esforços de correção ativos**. Para obter mais informações sobre como transferir os registros, consulte Transferir registros para esforços de correção nos espaços Vulnerability Response. Se os registros forem transferidos de um esforço de correção ou transferidos para esforços de correção recorrentes:

Para um novo esforço de correção no mesmo tópico de observação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Todas as tarefas de correção do antigo esforço de correção são movidas para o novo esforço de correção.
- Novas Tarefas de correção são criadas com base nos critérios de agrupamento escolhidos para os registros que anteriormente não faziam parte de nenhuma Tarefa de correção.
- O esforço de correção antigo está desativado.

Para um novo esforço de correção em um tópico de observação diferente

Todos os registros do antigo Esforço de correção são movidos para o novo Esforço de correção, e as Tarefas de correção são criadas com base nos critérios de agrupamento escolhidos.

- Se todos os registros nas Tarefas de correção associadas ao Esforço de correção antigo forem transferidos, essas Tarefas de correção serão encerradas/canceladas.
- Se apenas um subconjunto de registros for transferido, as Tarefas de correção associadas ao antigo Esforço de correção serão divididas e permanecerão ativas.

As tarefas de correção encerradas associadas ao esforço de correção antigo não são afetadas.

Nota:
Você não pode transferir registros de esforços de correção recorrentes para novos esforços de correção. No entanto, você pode transferir registros de esforços de correção existentes e não recorrentes para novos esforços de correção. Consulte Transferir registros para esforços de correção nos espaços Vulnerability Response para obter mais informações sobre como transferir registros.

Visão geral dos painéis

Você pode exibir os painéis na IU Next Experience no Vulnerability Manager Workspace e usar esses painéis para rastrear e analisar as vulnerabilidades.

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul.app_sec_manager, sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Você pode exibir os painéis no Vulnerability Manager Workspace navegando até **Espaços** > **Espaço para gerentes de vulnerabilidades**. O painel padrão é exibido com base na sua função.

A tabela a seguir mostra o painel padrão que é exibido para uma função específica.

Painel padrão

Painel padrão	Função
Painel unificado	sn_vul_cmn_vulnerability_admin ou sn_vul_cmn_vulnerability_analyst
Painel de Vulnerabilidade de PA	sn_vul_vulnerability_admin ou sn_vul_vulnerability_analyst
Visão geral da aplicação	sn_vul_app_sec_manager
Visão geral do contêiner	sn_vul_container_vulnerability_admin ou sn_vul_container_analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode exibir os seguintes painéis para as tarefas que deseja executar, selecionando-os no menu suspenso na página Painéis.

Painéis no Vulnerability Manager Workspace

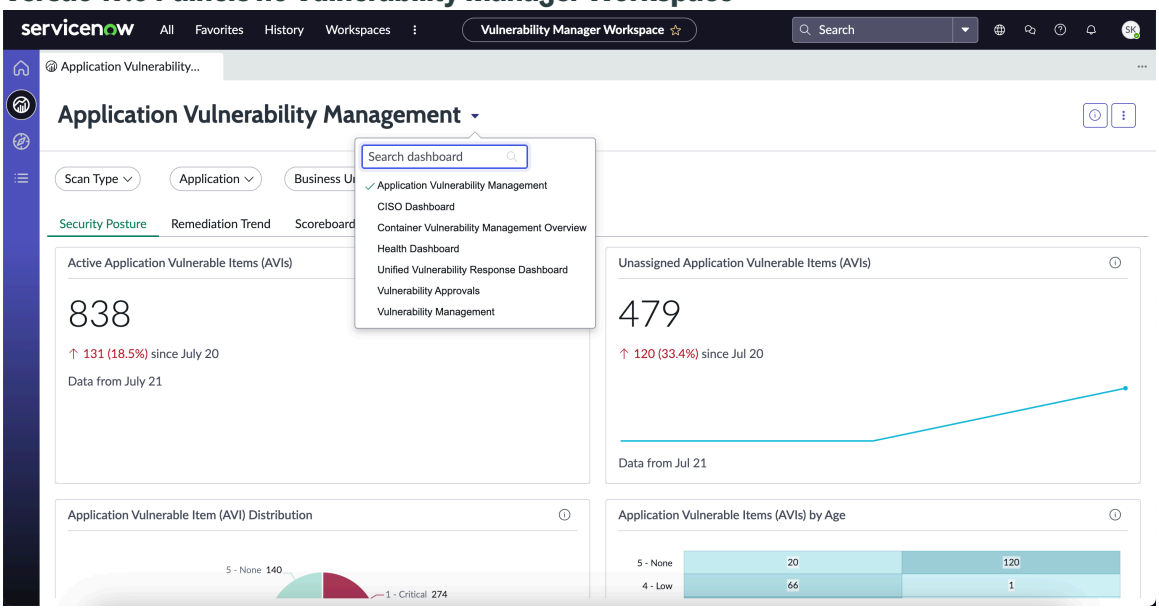
Painel	Descrição
Gestão de vulnerabilidade (PA)	Rastreie o volume, o desempenho e o andamento das vulnerabilidades do host, desde a análise e detecção iniciais até a contenção ou correção. Para obter mais informações, consultePainel Vulnerability Management (PA).
Aprovações de vulnerabilidade	Exiba o número de solicitações de aprovação aprovadas, rejeitadas e pendentes para você. Para obter mais informações, consulteUsando os painéis padrão Vulnerability Response.
Painel do CISO	Revela a postura geral de segurança da sua organização, incluindo a vulnerabilidade de segurança e os incidentes. Para obter mais informações, consulte Painel do CISO.
Visão geral da gestão de vulnerabilidade do contêiner	Rastreie o volume, o desempenho e o andamento das vulnerabilidades do contêiner, desde a análise e detecção iniciais até a contenção ou correção. Para obter mais informações, consulte Painel do Vulnerability Response contêiner.
Painel de gestão de vulnerabilidades da aplicação	Rastreie o volume, o desempenho e o andamento das vulnerabilidades da aplicação, desde a análise e detecção iniciais até a contenção ou correção.Gerenciamento de vulnerabilidade de aplicação Painel (PA)
Painel de integridade do Vulnerability Response unificado	Fornece visibilidade de vários scanners de vulnerabilidade e ferramentas de segurança para fornecer uma exibição abrangente das vulnerabilidades e riscos de uma organização. Para obter mais informações, consulte Soluções de análise e relatório para o painel unificado do Vulnerability Response.
Painel do Health Vulnerability Response	Exibe a pontuação de integridade geral da aplicação Vulnerability Response.

A imagem a seguir mostra a página Painéis no Vulnerability Manager Workspace.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versão 19.0 Painéis no Vulnerability Manager Workspace



Você pode criar um painel personalizado selecionando o ícone ⋮ e, em seguida, selecionando **Criar novo painel**.

Visão geral de listas

A exibição de lista no espaço do Vulnerability Manager permite que os gerentes e analistas de vulnerabilidade e segurança exibam o andamento da correção nos registros, façam uma busca detalhada nos registros do Vulnerability Response e exibam o status de suas solicitações de aprovação e exceções.

Essas listas e links fornecem acesso fácil a registros e tarefas. Ele contém duas guias:

- Guia**Listas** : exibe as listas padrão de esforços de correção, tarefas de correção, itens vulneráveis, soluções, exceções e resultados de testes de configuração.
- Guia**Minhas listas** : exibe todas as listas que você renomeou na guia Lista e todas as listas que você criou.

  Você também pode criar sua própria lista para monitorar o andamento da correção. Para obter mais informações, consulte Criar uma lista personalizada de registros.

Guia Listas

As seguintes listas são exibidas:

- Esforços de correção (REs) - Mostra os REs ativos e todos os REs atribuídos aos seus grupos.
- Tarefas de correção (VULs) - Mostra as Tarefas de correção ativas e todas as Tarefas de correção atribuídas aos seus grupos.

> **Nota:**
> A partir da versão 18.0, a lista de tarefas de correção mostra as tarefas de correção criadas na IU clássica e no espaço para Vulnerability Response, Application Vulnerability Response, Vulnerability Response contêinere Configuration Compliance.

- Itens vulneráveis - Mostra registros ativos (em aberto) e todos os registros atribuídos aos seus grupos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Soluções: mostra todas as soluções para itens vulneráveis.
- Exceções: mostra os estados de aprovação de todas as solicitações de exceção e falso-positivo de seus grupos.
- Aprovações: mostra as solicitações de aprovação atribuídas a você para processamento. Para processar suas aprovações no espaço de trabalho, consulte Aprovar solicitações no Vulnerability Manager Workspace.
- A partir da versão 18.0, as listas a seguir também são exibidas na exibição de lista:
  - Itens vulneráveis de host: mostra os itens vulneráveis de host (IVs) ativos e todos os IVs de host do módulo Vulnerabilidades do host.
  - Itens vulneráveis da aplicação: mostra os itens vulneráveis da aplicação (AVITs) e todos os AVITs do módulo Vulnerabilidades da aplicação.
  - Itens vulneráveis de contêiner: mostra os itens vulneráveis de contêiner ativos (CVITs) e todos os CVITs do módulo Vulnerabilidades do contêiner.
  - Resultados de testes de configuração: mostra os resultados de testes de configuração ativos e todos os resultados de testes de configuração do módulo Resultados de testes de configuração.

    Nota:
    A partir da v19.0 de Vulnerability Response, os seguintes termos foram renomeados:

    Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

  - Bibliotecas - Mostra as seguintes bibliotecas, políticas e testes.
    - CVEs: mostra todas as vulnerabilidades e exposições comuns (CVEs) de Vulnerability Response, Application Vulnerability Responsee Vulnerability Response contêiner.
    - TPEs — Mostra todas as entradas de terceiros (TPEs) de Vulnerability Response.
    - CWEs — Mostra todas as Enumerações de Pontos Fracos Comuns (CWEs) de Vulnerability Response, Application Vulnerability Responsee Vulnerability Response contêiner.
    - Vulnerabilidades da aplicação: mostra todas as entradas de vulnerabilidade da aplicação de terceiros.
    - Políticas - Mostra todas as políticas Configuration Compliance.
    - Testes - Mostra todos os testes de Configuration Compliance.
    - Controles de compensação - Mostra todos os controles de compensação usados para solicitações de redução de risco. Você pode adicionar um controle de remuneração clicando em **Novo**. Para obter mais informações sobre como adicionar um controle de compensação, consulte Adicionar um controle de compensação à biblioteca.

      Nota:
      A lista de controles de remuneração aparece a partir da v20.0 de Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Noções básicas sobre controles de compensação para redução de risco

Controles de compensação são as medidas tomadas para reduzir o risco apresentado por vulnerabilidades que não podem ser corrigidas imediatamente. Eles podem ser usados para reduzir a probabilidade ou o impacto de uma exploração bem-sucedida.

Nota:
O recurso de controles de compensação está disponível somente para vulnerabilidades de host.

Aplicar controles de compensação pode ajudar a reduzir o risco de uma vulnerabilidade.

A tabela a seguir mostra os casos de uso para controles de compensação:

Casos de uso para controles de compensação

Caso de uso	Controle de compensação
Uma vulnerabilidade em um servidor Web que permite que os invasores executem código arbitrário.	Implemente um WAF (Web Application Firewall) para bloquear solicitações mal-intencionadas ao servidor Web.
Uma vulnerabilidade em um sistema operacional que permite que os invasores escalem privilégios para raiz.	Implemente o controle de aplicações para restringir quais aplicações podem ser executadas no sistema host.
Uma vulnerabilidade em um servidor de banco de dados que permite que os invasores acessem dados confidenciais.	Implemente a segmentação de rede para isolar o servidor de banco de dados de outros hosts e sistemas críticos.

Para obter mais informações sobre o impacto dos controles de compensação na pontuação de risco de um item vulnerável e da tarefa de correção, consulte Impacto dos controles de remuneração na pontuação de risco e na data de vencimento.

Tópicos relacionados

Adicionar um controle de compensação à biblioteca

Associar controles de compensação com CVEs ou TPEs para solicitações de redução de risco

Desabilitar ou habilitar a redução de risco para um CVE ou TPE

Soluções de análise e relatório para o painel unificado do Vulnerability Response

Soluções Análise da plataforma contêm conteúdo Platform Analytics] pré-empacotado para uso com outros produtos Now Platform. O painel unificado do Vulnerability Response é um painel agregado centralizado que fornece visibilidade de vários scanners de vulnerabilidade e ferramentas de segurança para fornecer uma exibição abrangente das vulnerabilidades e riscos de uma organização.

Funções necessárias

As funções e tarefas a seguir estão associadas a esta Solução. Eles são necessários para exibir e compartilhar os relatórios:

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

Tópicos relacionados

Soluções de análise e relatório

Painel de integridade do Vulnerability Response unificado

O painel Unified Vulnerability Response fornece uma exibição abrangente das vulnerabilidades e riscos de uma organização. As vulnerabilidades relacionadas à infraestrutura, nuvem, aplicações e contêineres podem ser exibidas em um painel centralizado para melhor visibilidade e correção.

Funções necessárias de Now Platform

As funções a seguir estão associadas a esta solução. Eles são necessários para exibir, editar e compartilhar os relatórios:

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.vulnerability_analyst
- sn_vul.app_developer
- sn_vulc.vulnerability_analyst

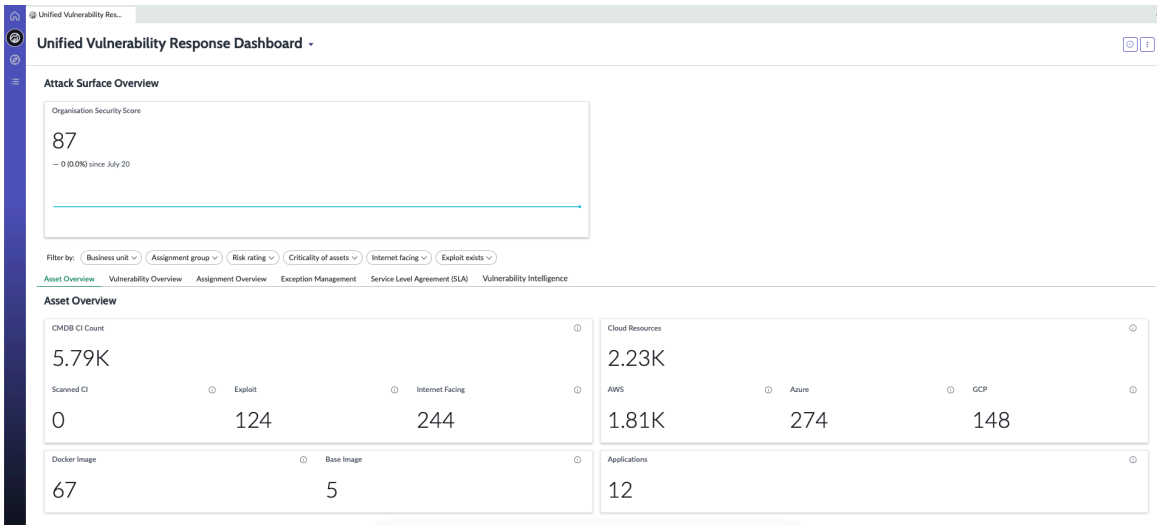
Acesse o painel unificado do Vulnerability Response

Para abrir o painel, navegue até:

- **Todos** > **Vulnerability Response** > **Espaço para gerentes de vulnerabilidades** e selecione o ícone **Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir o painel unificado do Vulnerability Response, selecione o menu suspenso ao lado do nome do painel.
- **Espaços** > **Espaço de Análise da plataforma** > **Painéis** > **Painel de integridade do Vulnerability Response unificado**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Casos de uso

Para obter exemplos de como diferentes pessoas de sua organização podem usar este painel, consulte estes casos de uso.

Usuário	Uso do painel
• Gerenciadores de vulnerabilidade • Analistas de Vulnerabilidade	• Fornece visibilidade em tempo real dos riscos presentes na infraestrutura, aplicações, configurações e contêineres. Epermite a eles priorizar e corrigir as vulnerabilidades em tempo hábil. • Fornece uma visão geral da superfície de ataque de ativos críticos, que pode ser usada para rastrear o andamento e os esforços de correção. • Fornece uma visão geral dos riscos nas unidades de negócios (BUs). Você pode usar filtros para selecionar BUs e comparar o andamento para realocar recursos, conforme necessário. O acesso no nível da função deve ser fornecido ao chefe da BU. • Fornece visibilidade sobre o possível impacto por BUs. Você pode usar o filtro Vulnerabilidade e exposição comuns (CVE) para identificar exposições em toda a organização. • Fornece visibilidade das pontuações de EPSS obtidas por entradas vulneráveis que existem no catálogo CISA KEV para itens vulneráveis de aplicativo, host e contêiner.

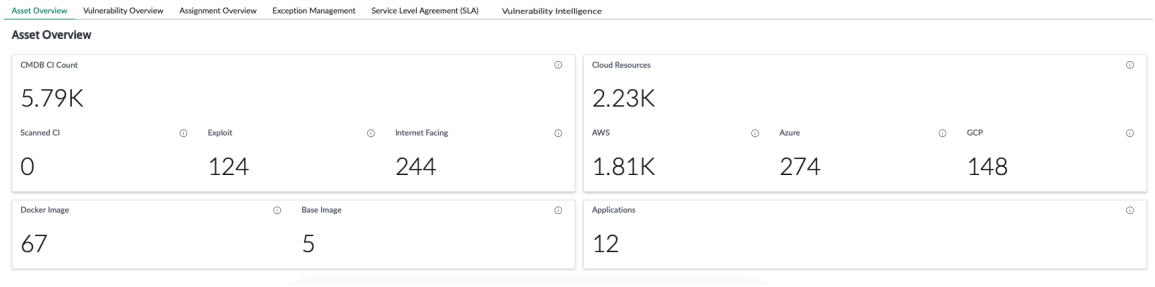
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

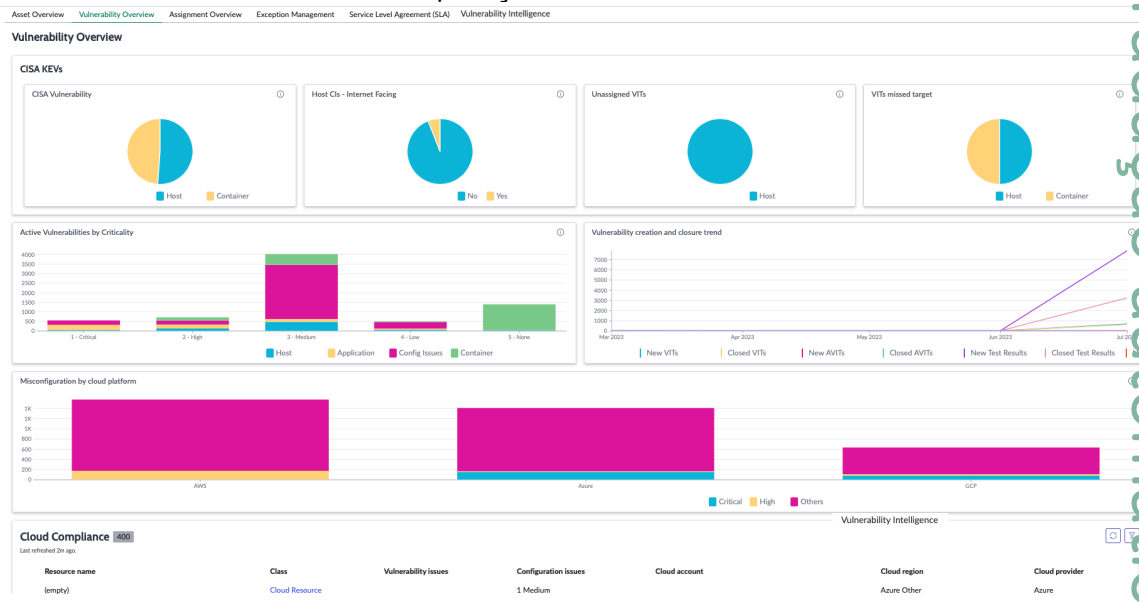
Guias do painel unificado do Vulnerability Response

Este painel permite que você veja as vulnerabilidades ou problemas que estão presentes em hosts, nuvem, configurações, aplicações e contêineres. Você pode exibir as vulnerabilidades com base na unidade de negócios, grupo de atribuição, classificação de risco, criticidade e se existe uma exploração para as vulnerabilidades.

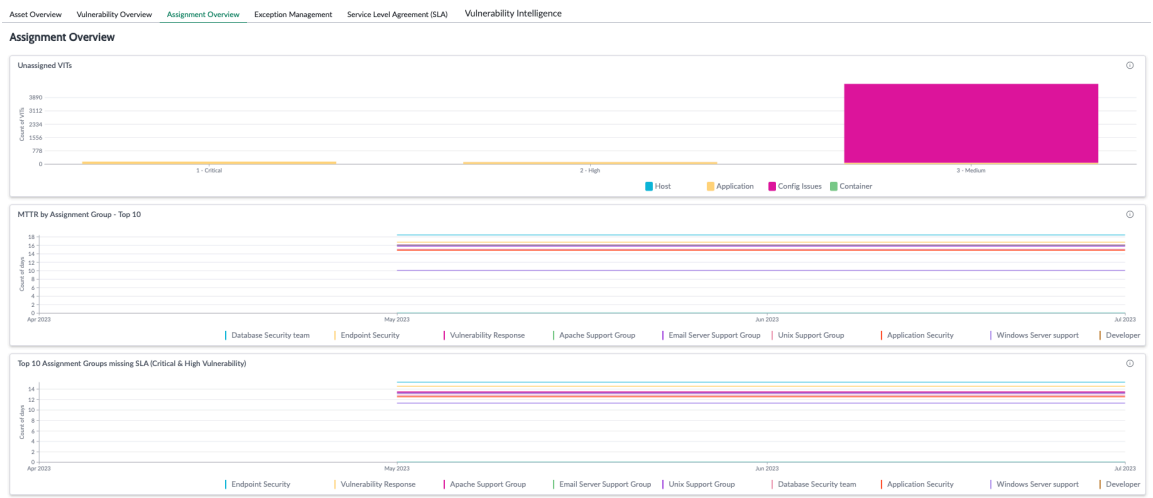
A guia **Visão geral** do ativo fornece o status geral dos itens de configuração (ICs) no sistema.



A guia **Visão geral de vulnerabilidade** fornece um status dos tipos de vulnerabilidades, como host, aplicação, contêiner.



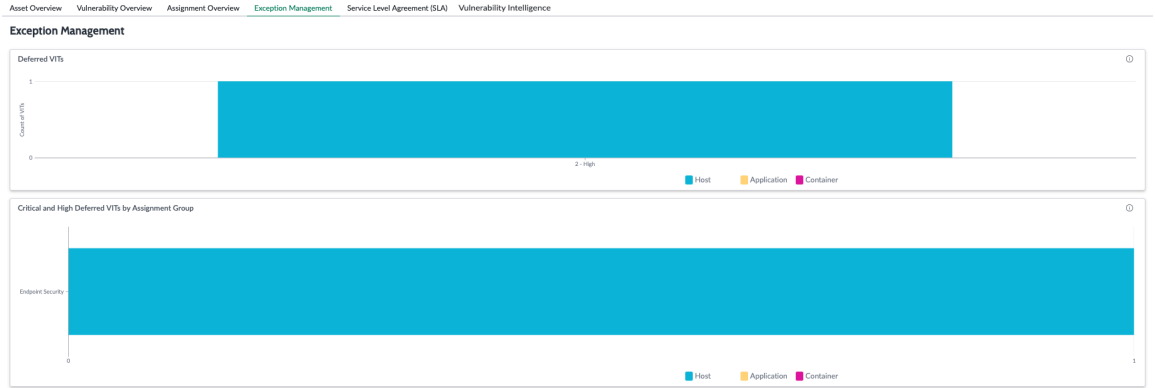
A guia **Visão geral da atribuição** fornece um status na atribuição das vulnerabilidades.



Tradução automática

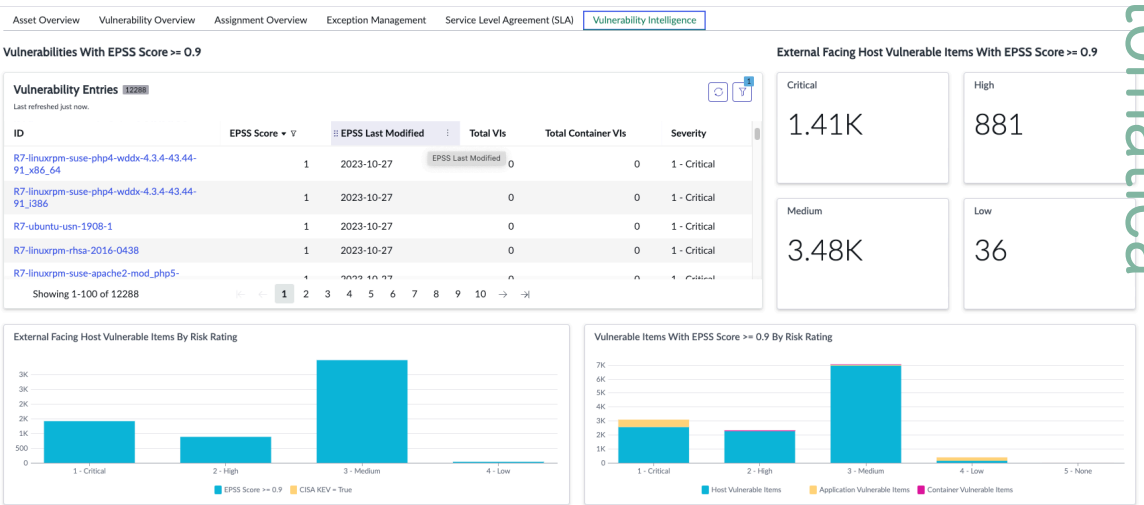
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A guia **Gerenciamento de exceções** fornece um status das vulnerabilidades adiadas.



A guia **Acordo de nível de serviço (ANS)** fornece um status no acordo de nível de serviço alcançado por diferentes grupos de atribuição.

A guia **Inteligência de vulnerabilidade** fornece um status nas pontuações de EPSS obtidas por vulnerabilidades com o sinalizador CISA KEV verdadeiro e Pontuação de EPSS > = 0,9 para itens vulneráveis de aplicativo, host e contêiner.



Filtros

Você pode filtrar os widgets com base no seguinte:

- Unidade de negócios
- Grupo de atribuição
- Pontuação de risco
- Criticidade de ativos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Voltado para a internet
- Explorar itens existentes

Quando um filtro é selecionado, os dados em todos os widgets são atualizados. No entanto, se um filtro não for aplicável a um widget, um símbolo de cruz será mostrado ao lado do nome do filtro.

Nota:
Somente os filtros de Unidade de negócios e Grupo de atribuição estão disponíveis em Tokyo. Todos os filtros estão disponíveis de Utah em diante.

Indicadores

Ativos verificados

Indicador de fórmula para ativos verificados nos últimos 60 dias. Contém ativos de item descoberto verificados, ativos de versão da aplicação verificados, ativos de imagem de contêiner descobertos verificados como indicadores de contribuição.

Ativos - Existe exploração

Indicador de fórmula para ativos em que existe exploração nas vulnerabilidades. Contém ativos de host – existe exploração, ativos da aplicação – existe exploração, ativos de contêiner – existe exploração como indicadores que contribuem.

Ativo de infraestrutura – Voltado para a internet

Indicador para buscar a contagem de ativos, que são voltados para a internet.

Itens descobertos com base no tipo de recurso de nuvem

Indicador para buscar a contagem de ativos com uma categoria de ativo, como nuvem.

Imagens base

Indicador para buscar a contagem de imagens de base.

Tipo de ativo de KEVs de CISA

Indicador de fórmula, que fornece a contagem de itens vulneráveis de contêiner e host em que a vulnerabilidade tem o sinalizador CISA KEV (BOD 22-01) definido como verdadeiro. Contém CISA existe CVR e CISA existe itens vulneráveis como indicadores contribuintes.

Existem itens vulneráveis CISA - não atribuídos

Indicador de fórmula, que fornece a contagem de itens vulneráveis de contêiner e host em que a vulnerabilidade tem o sinalizador CISA KEV (BOD 22-01) definido como verdadeiro e os itens vulneráveis não estão atribuídos. Contém itens de vulnerabilidade de contêiner não atribuídos e item de vulnerabilidade de host não atribuído como indicadores de contribuição.

Existem Itens Vulneráveis CISA – Meta não Atingida

Indicador de fórmula, que fornece a contagem de itens vulneráveis de contêiner e host em que a vulnerabilidade tem o sinalizador CISA KEV (BOD 22-01) definido como verdadeiro e os itens vulneráveis não atingiram a meta. Contém Itens Vulneráveis existentes na CISA, CVR existente na CISA como indicadores contribuintes.

VITs de host ativo

Contagem de itens vulneráveis de host (VITs) ativos.

VITs da aplicação ativos

Contagem de itens vulneráveis da aplicação (AVITs) ativos.

VITs de contêiner ativo

Contagem de itens vulneráveis de contêiner ativos (CVITs).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Novos VITs

Contagem de VITs abertos em um dia.

Novos AVITs

Contagem de AVITs que abriram em um dia.

Novos CVITs

Contagem de CVITs que abriram em um dia.

Novos Resultados de testes

Contagem de resultados de testes (TRs) que foram criados em um dia.

AVITs encerrados

Contagem de VITs encerrados em um dia.

VITs encerrados

Contagem de AVITs encerrados em um dia.

CVITs encerrados

Contagem de CVITs encerrados em um dia.

Resultados de testes fechados

Contagem de TRs encerrados em um dia.

Problemas de configuração em aberto – Resultados de testes

Contagem de todos os resultados de testes abertos, que estão em estado de falha.

Pontuação de risco da organização

Pontuação de risco de uma organização da tabela de pontuação de risco da aplicação de acúmulo.

Itens vulneráveis de aplicação não atribuídos

AVITs sem grupo de atribuição ou atribuídos a.

Item Vulnerável de Host Não Atribuído

VITs sem grupo de atribuição ou atribuídos a.

Itens vulneráveis de contêiner não atribuídos

CVITs sem grupo de atribuição ou atribuídos a.

Problemas de configuração não atribuídos

TRs sem grupo de atribuição ou atribuídos a.

VITs adiados

VITs no estado adiado.

AVITs adiados

AVITs no estado adiado.

CVITs adiados

CVITs no estado adiado.

ANS de host – Encerrado

Idade média dos VITs encerrados.

ANS de aplicação – Encerrado

Idade média de encerramento de AVITs.

ANS de contêiner – Encerrado

Idade média de encerramento de CVITs encerrados.

ANS de Resultado de testes – Aprovado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Idade média de encerramento dos TRs aprovados.

ANS de host – Encerrado (crítico e alto)

Idade média de encerramento dos VITs críticos e altos encerrados.

ANS de aplicação – Encerrado (crítico e alto)

Idade média de encerramento de AVITs críticos e altos.

ANS de contêiner – Encerrado (crítico e alto)

Idade média de encerramento dos CVITs críticos e altos encerrados.

ANS do resultado de testes – Aprovado (crítico e alto)

Idade média de encerramento dos TRs críticos e altos aprovados.

MTTR agregado

Idade média de encerramento de VITs, AVITs, CVITs e TRs.

ANS não Atingido

Idade média de encerramento de VITs, AVITs, CVITs e TRs encerrados e não atingidos.

Vulnerabilidades com pontuações de EPSS >= 0,9

Contagem de entradas de vulnerabilidade com pontuações de EPSS maiores ou iguais a 0,9.

Detalhamentos

- Tipo de VIT (unificado)
- Voltado para a internet (unificado)
- Classificação de risco (unificada)
- Existe exploração (unificada)
- Tipo de recurso de nuvem do item descoberto (unificado)
- Existe CISA (unificado)
- Classe do CMDB (unificada)
- Unidade de negócios (unificada)
- Essencial para os negócios (unificado)
- Motivo adiado (unificado)
- Grupo de atribuição (unificado)
- Status de correção (unificado)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações de dados

Guia Visão geral do ativo

Título	Tipo	Descrição
Visão geral da superfície de ataque	Pontuação única	Número que representa a pontuação agregada da segurança de uma organização.
Contagem de IC do CMDB	Pontuação única	Número de ICs na organização que estão registrados e rastreados no Configuration Management Database (CMDB). Fornece um detalhamento dos seguintes ICs: • ICs verificados: número de ICs verificados • Exploração: número de explorações disponíveis • Voltados para a Internet: número de ICs voltados para a Internet
Recurso de Nuvem	Pontuação única	Número de ICs com categoria de ativo, como nuvem. Fornece um detalhamento dos seguintes ativos de nuvem: • AWS • Azure • GCP
Imagem do Docker	Pontuação única	Número de imagens do docker, incluindo o número de imagens de base.

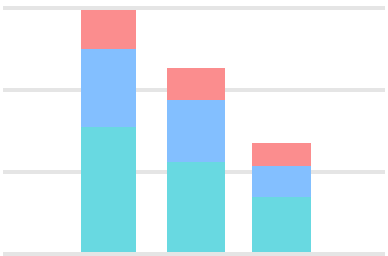
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral do ativo

Título	Tipo	Descrição
Candidaturas	Pontuação única	Número de aplicações na organização.

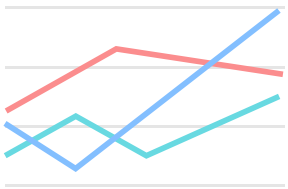
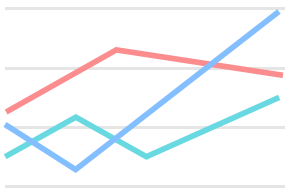
Guia Visão geral de vulnerabilidade

Título	Tipo	Descrição
KEVs de CISA	Gráfico de Pizza	Número de vulnerabilidades associadas ao catálogo CISA e ao sinalizador CISA como verdadeiro. Fornece um detalhamento com base no seguinte: • Vulnerabilidade CISA: tipos de vulnerabilidades com sinalizador CISA como verdadeiro • ICs do host – Voltados para a Internet: ICs voltados para a Internet • VITs não atribuídos: VITs não atribuídos com sinalizador CISA como verdadeiro • VITs não atingiram a meta: VITs que não atingiram a meta com o sinalizador CISA como verdadeiro
Vulnerabilidades ativas por criticidade	Barra 	Número de VITs, AVITs e CVITs ativos com base na criticidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

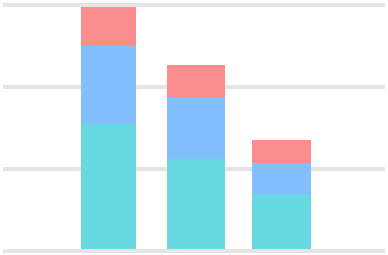
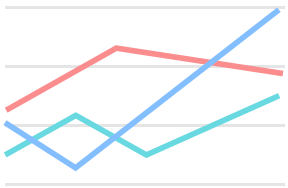
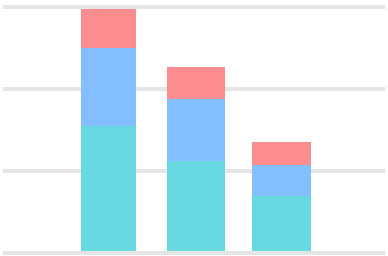
Guia Visão geral de vulnerabilidade

Título	Tipo	Descrição
Tendência de criação e fechamento de vulnerabilidade	Linha 	Número de vulnerabilidades novas e encerradas para todas as aplicações. Fornece uma tendência para os últimos três meses.
Configuração incorreta por plataforma de nuvem	Linha 	Número de problemas de configuração com base na classificação de risco de cada ativo de nuvem.
Conformidade de nuvem	Tabela	Lista de recursos com a categoria de ativo como nuvem junto com os seguintes detalhes: • Nome do recurso • Classe • Problemas de vulnerabilidade: número de problemas presentes no recurso que são agregados com base na classificação de risco. • Problemas de configuração: número de recursos com problemas de configuração junto com a classificação de risco. • Conta de nuvem: ID da conta de nuvem. • Região da nuvem: local dos recursos de nuvem. • Provedor de nuvem: nome do provedor de nuvem.

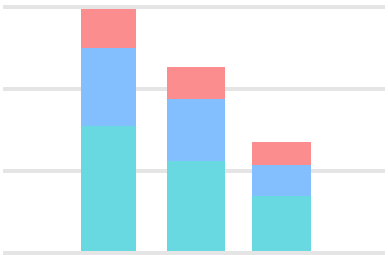
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral da atribuição

Título	Tipo	Descrição
VITs não atribuídos	Barra 	Número de vulnerabilidades que não são atribuídas a nenhum grupo ou indivíduo junto com a classificação de risco.
MTTR por grupo de atribuição – 10 principais	Linha 	Tempo médio gasto por um grupo de atribuição para identificar e corrigir vulnerabilidades ou problemas de segurança. Os 10 principais grupos de atribuição são exibidos que têm o maior tempo médio de correção.
10 principais grupos de atribuição sem ANS (vulnerabilidade crítica e alta)	Barra 	10 principais grupos de atribuição que não atingiram a data de meta de correção de vulnerabilidades críticas e altas.

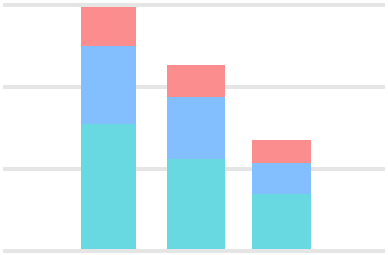
Guia Gestão de exceções

Título	Tipo	Descrição
VITs adiados	Barra 	Número de vulnerabilidades no estado adiado com base na classificação de risco.

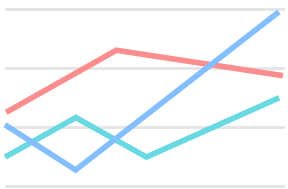
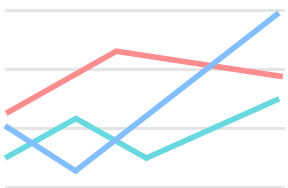
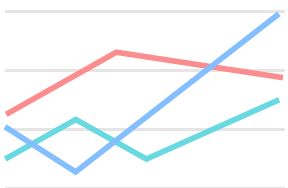
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Gestão de exceções

Título	Tipo	Descrição
VITs críticos e altos adiados por grupo de atribuição	Barra 	Número de vulnerabilidades com classificações de risco crítico e alto no estado adiado que é categorizado com base nos grupos de atribuição.

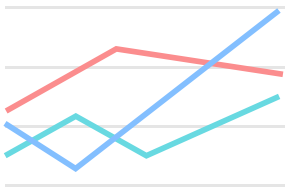
Guia Acordo de nível de serviço (ANS)

Título	Tipo	Descrição
Vulnerabilidade do host: obtenção de ANS por grupo de atribuição	Linha 	Tempo gasto por um grupo de atribuição para corrigir vulnerabilidades do host. Fornece uma tendência para os últimos 10 meses.
Problemas de conformidade: obtenção de ANS por grupo de atribuição	Linha 	Tempo gasto por um grupo de atribuição para corrigir problemas de conformidade. Fornece uma tendência para os últimos 10 meses.
Vulnerabilidade da aplicação: obtenção de ANS por grupo de atribuição	Linha 	Tempo gasto por um grupo de atribuição para corrigir vulnerabilidades da aplicação. Fornece uma tendência para os últimos 10 meses.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Acordo de nível de serviço (ANS)

Título	Tipo	Descrição
Vulnerabilidade da contêiner: obtenção de ANS por grupo de atribuição	Linha 	Tempo gasto por um grupo de atribuição para corrigir vulnerabilidades de contêiner. Fornece uma tendência para os últimos 10 meses.

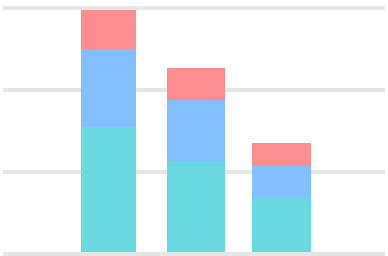
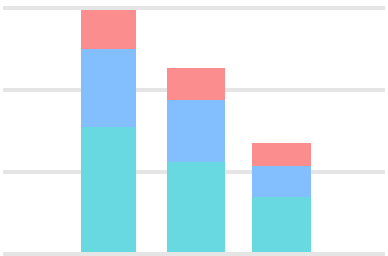
Guia Inteligência de vulnerabilidade

Título	Tipo	Descrição
Vulnerabilidades com Pontuação de EPSS>= 0,9	Tabela	Exibição de lista completa de todas as entradas vulneráveis (CVEs ou TPEs) que têm uma pontuação de EPSS maior ou igual a 0,9 junto com os detalhes a seguir. • ID: ID de CVE da vulnerabilidade • Pontuação de EPSS • Última modificação de EPSS • CISA KEV BOD 22-01: indica se a entrada existe no CISA KEV BOD (diretiva operacional de vinculação 22-01) • Total de IVs: contagem total de IVs existentes para esta entrada de vulnerabilidade. • Total de IVs de contêiner: contagem total de IVs de contêiner existentes para esta entrada de vulnerabilidade. • Gravidade

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Inteligência de vulnerabilidade

Título	Tipo	Descrição
Itens vulneráveis do host externo com pontuação EPSS >= 0,9	Pontuação única	Número que indica a contagem agregada de itens vulneráveis de host externos com uma pontuação de EPSS maior ou igual a 0,9. Fornece pontuações únicas classificadas por severidade da classificação de risco.
Itens vulneráveis de host voltados externamente por avaliação de risco	Barra 	Número de itens vulneráveis de host externos por classificação de risco. As barras da pilha são categorizadas por Pontuação de EPSS > = 0,9 e CISA KEV = Verdadeiro.
Itens vulneráveis com pontuação de EPSS >= 0,9 por avaliação de risco	Barra 	Número de vulnerabilidades com pontuação de EPSS maior ou igual a 0,9 classificadas por classificação de risco. Fornece um detalhamento por itens vulneráveis de host, itens vulneráveis de aplicação e itens vulneráveis de contêiner.

Trabalhos programados para coleta de dados

Os trabalhos de coleta de dados coletam pontuações automaticamente para detalhamentos e indicadores automatizados. Os trabalhos programados a seguir são executados para coletar pontuações em novos dados automaticamente.

Aviso:
Por padrão, os seguintes trabalhos de coleta de dados são desativados no sistema de base:

- Coleta diária de dados do painel unificado
- Coleta de dados semanais do painel unificado
- Coleta de dados históricos do painel unificado

Antes de habilitar os trabalhos, consulte a base de conhecimento .

Trabalho programado	Frequência	Descrição
Coleta de dados históricos do painel unificado	Uma vez	Coleta pontuações e snapshots de registros existentes.
Coleta de dados semanais do painel unificado	Semanalmente	Coleta dados semanalmente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho programado	Frequência	Descrição
Coleta diária de dados do painel unificado	Diariamente	Coleta dados todos os dias.
Acumular pontuações de risco para a organização	Diariamente	Coleta a pontuação de risco agregada de uma organização.
Preencher contagens diárias de conformidade da nuvem	Diariamente	Coleta dados para conformidade da nuvem.
Trabalho diário de EPSS	Diariamente	Coleta dados de EPSS de First.org.

Uma nova tabela de pontuação de risco da aplicação de acúmulo [sn_vul_cmn_rollup_app_risk_score] é criada no escopo comum de vulnerabilidade. Esta tabela é preenchida usando as seguintes calculadoras de acúmulo por meio dos trabalhos programados todos os dias.

Nome da calculadora de acúmulo	Descrição
Acúmulo de pontuação de risco da organização	Agrega as pontuações de risco de todos os itens vulneráveis e problemas de configuração em uma organização. Ele fornece uma pontuação de risco geral para uma organização.
Acúmulo do item vulnerável	Agrega as pontuações de risco de todos os itens vulneráveis em uma organização para contribuir com a pontuação de risco geral de uma organização.
Acúmulo de item vulnerável da aplicação	Agrega as pontuações de risco de todos os itens vulneráveis da aplicação em uma organização para contribuir com a pontuação de risco geral de uma organização.
Acúmulo do item vulnerável de contêiner	Agrega as pontuações de risco de todos os itens vulneráveis de contêiner em uma organização para contribuir com a pontuação de risco geral de uma organização.
Acúmulo do resultado de testes	Agrega as pontuações de risco de todos os resultados de testes em uma organização para contribuir com a pontuação de risco geral de uma organização.
Acumular pontuações de EPSS de NVDs para TPEs	Agrega pontuações de EPSS de NVDs para TPEs, para contribuir com a pontuação de risco geral de uma organização.

Tradução automática

Usando o Vulnerability Manager Workspace

No Vulnerability Manager Workspace, você pode agrupar um conjunto de vulnerabilidades em um tópico de observação definindo uma condição e pode rastrear o andamento da correção criando esforços de correção.

Crie filtros para visualizar o resumo de registros ativos

Como gerente e analista de vulnerabilidade, você pode criar filtros para visualizar o resumo dos registros desejados no Vulnerability Manager Workspace.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Página inicial**.
2. Na página inicial, selecione o ícone de ícone de engrenagem em qualquer uma das guias Vulnerabilidades do host, Vulnerabilidades do contêiner, Vulnerabilidades da aplicação ou Resultados de testes de configuração.
3. No modal Filtros salvos, preencha os campos.

Modal de filtros salvos

Campo	Descrição
Nome do filtro	Nome do filtro
Condições	Condição para listar os registros para os quais você deseja ver as visualizações.

4. Selecione **Salvar**.
   O filtro criado aparece no menu suspenso **Exibir por**.
5. Selecione o filtro no campo **Exibir por** para exibir as visualizações dos registros filtrados.
   Para obter mais informações sobre os widgets, consulte Visão geral da página inicial.
6. Para atualizar ou excluir um filtro:

   a. Selecione o ícone de ícone de Engrenagem .

   b. No formulário Filtros salvos, selecione **Usar filtros existentes**, preencha os campos e selecione **Atualizar**.

Formulário Filtros salvos

Campo	Descrição
Selecionar filtro	Lista de filtros existentes.
Nome do filtro	Nome descritivo do filtro.
Condições	As condições do filtro existente. Edite a condição para um novo conjunto de registros.

   c. Para excluir um filtro, selecione **Excluir**.

Usar tópicos de observação no Vulnerability Manager Workspace

Use os tópicos de observação no Vulnerability Manager Workspace para exibir as vulnerabilidades que são filtradas dos dados importados dos critérios que você definiu. Use essas informações para determinar como as vulnerabilidades em cada tópico de observação podem afetar seu ambiente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul_container.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Nos tópicos de observação, você pode executar as seguintes tarefas:

- Monitore o número de esforços de correção e registros de itens vulneráveis para ver o andamento da correção de vulnerabilidade.
- Edite ou exclua os tópicos de observação existentes e crie tópicos.
- Crie os esforços de correção e entregue automaticamente as tarefas de correção para suas equipes de TI somente para as vulnerabilidades que você deseja corrigir.

Nota:

A partir da v19.0 de Vulnerability Response, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

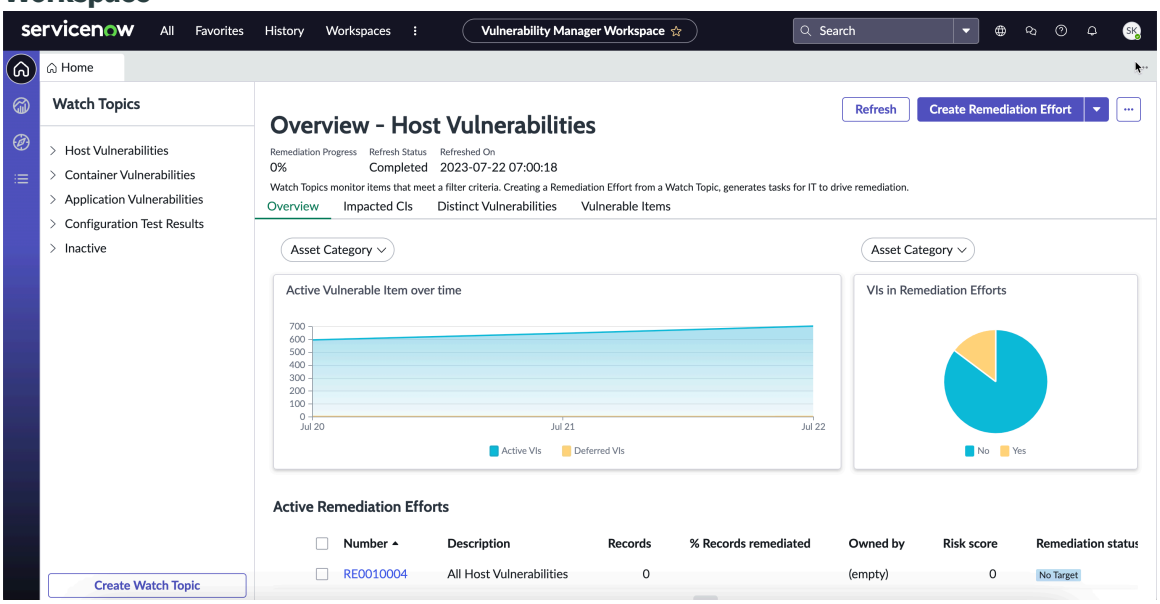
Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Espaço para gerentes de vulnerabilidades**.
2. Selecione um tópico de observação.

   Quando você seleciona um tópico de observação, a guia **Visão geral** é exibida por padrão.

   Para obter mais informações sobre os tópicos de observação, consulte Visão geral dos tópicos de observação.

Guia Visão geral da versão 19.0 na página inicial do Vulnerability Manager Workspace



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os painéis são dinâmicos e os novos dados de vulnerabilidade são atualizados na importação.

3. Selecione uma **guia de Itens relacionados** para exibir mais dados.

   Para obter atualizações na lista de itens relacionados e visualizações em um tópico de observação a partir da versão 18.0, consulte Lista de itens relacionados e visualizações em um tópico de observação.

4. Realize as ações de IU na página Tópicos de observação.

5. **Opcional:** Selecione um registro para exibir mais detalhes.

Criar um tópico de observação no Vulnerability Manager Workspace

Os gerentes e analistas de vulnerabilidade podem criar tópicos de observação usando um conjunto de condições para filtrar subconjuntos de itens vulneráveis que eles desejam monitorar.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Na guia Visão geral dos tópicos de observação, um relatório de tendências que é atualizado todas as noites, junto com outros relatórios, mostra o status atual dos registros desse tópico de observação.

Nota:
A partir da v19.0 de Vulnerability Response, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Espaço para gerentes de vulnerabilidades**.
   A página inicial (inicial) é exibida com os tópicos de observação atuais.
2. **Opcional:** Como alternativa, à direita do botão Criar esforço de correção, clique nos três pontos, seguidos por editar para modificar um tópico de observação existente.

   Nota:
   Você pode observar um atraso antes que os dados atuais sejam exibidos para um tópico de observação depois de alterar a filtragem.

3. No canto inferior esquerdo da página, clique em **Criar tópico**de observação.
4. No modal exibido, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

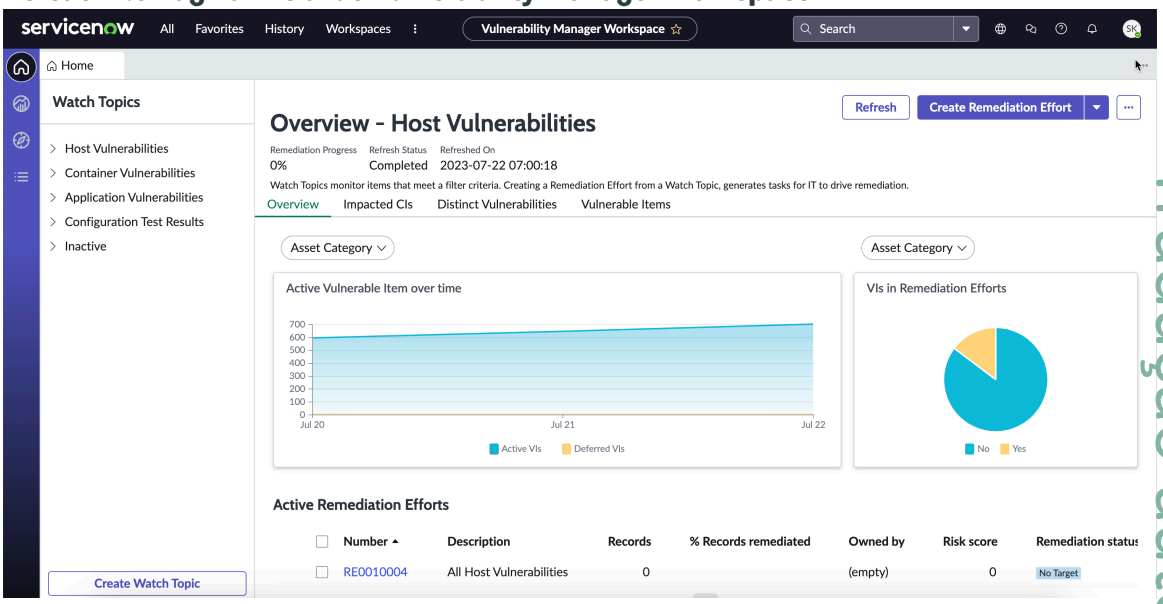
Para obter mais informações sobre os campos Criar modal de tópico de observação, consulteCriar campos de formulário de tópico de observação.

5. A partir da versão 18.0, você pode definir condições para a categoria de registro selecionada.

> **Nota:**
> Se você não definir nenhuma condição no tópico de observação, nenhum dado será extraído para o painel.

6. Clique em **Enviar**.
Seu novo tópico de observação é exibido na página inicial do. A partir da versão 18.0, os tópicos de observação são categorizados por tipo de registro no painel de navegação.

Versão 19.0 Página inicial do Vulnerability Manager Workspace



O que Fazer Depois

Crie um esforço de correção.

Editar ou excluir um tópico de observação

Como administrador ou analista de vulnerabilidade, você pode editar ou excluir um tópico de observação existente.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Se você editar um tópico de observação existente:

- Os dados no painel são atualizados para refletir suas mudanças.
- Os registros que estão atualmente nos Esforços de correção existentes permanecem inalterados.
- Os registros que não estão nos Esforços de correção são exibidos com base nos critérios inseridos no construtor de condição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você excluir um tópico de observação antes que todos os registros associados sejam corrigidos, os registros exibidos com esse tópico de observação não serão afetados.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
   A página inicial (inicial) é exibida com os tópicos de observação atuais.
2. Abra o tópico de observação que você deseja editar.
3. Clique nos três pontos e clique em **Editar**.

   Nota:
   Você não pode editar um tópico de observação inativo.

4. No modal Editar tópico de observação que, modifique os campos.
5. Clique em **Enviar**.

   Nota:
   Você pode observar um atraso antes que os dados atuais sejam exibidos para um tópico de observação depois de alterar a filtragem.

   Você também pode editar os esforços de correção recorrentes existentes. Se houver um esforço de correção recorrente para um tópico de observação, **Editar esforço recorrente** estará disponível no menu. Selecione esta opção para editar o esforço recorrente.

   As mudanças feitas e salvas no registro do esforço de correção não afetam nenhum outro esforço de correção que você já criou a partir do tópico de observação.

6. **Opcional:** Para excluir um tópico de observação, selecione o menu de três pontos no tópico de observação e selecione **Excluir**.

Desativar ou ativar um tópico de observação

A partir da versão 18.0, você pode desativar ou ativar um tópico de observação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul_container.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

- Todos os tópicos de observação inativos são exibidos no módulo **Inativo** no painel de navegação.
- Você não pode criar um esforço de correção ou um esforço de correção recorrente para um tópico de observação inativo.
- Você não pode atualizar um tópico de observação inativo.
- Os detalhes de um tópico de observação inativo e seus esforços de correção associados não são atualizados.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
   A página inicial (inicial) é exibida com os tópicos de observação atuais.
2. Abra o tópico de observação que você deseja desativar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique nos três pontos e em **Desativar**.
   O tópico de observação aparece no módulo Inativo.
4. Para ativar um tópico de observação, selecione um tópico de observação no módulo Inativo, selecione o menu de três pontos e selecione **Ativar**.
   O tópico de observação ativado é movido para o módulo apropriado no painel de navegação.

Usar registros de esforço de correção

Quando os gerentes e analistas de vulnerabilidade criam esforços de correção (REs), as tarefas de correção (VUL) são atribuídas automaticamente às equipes de TI para correção.

Antes de Iniciar

Você precisa criar um esforço de correção antes de usá-lo para monitorar o andamento da correção nas Tarefas de correção.

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Procedimento

1. Se não estiver selecionado, no canto superior esquerdo, clique no ícone Lista.

   A exibição de lista com registros de esforço de correção ativos é exibida.
2. Na página principal da exibição de lista, com os Esforços de correção ativos selecionados nas listas filtradas, clique em um registro para abri-lo.
   O registro é exibido. Você pode exibir as tarefas de correção e registros que estão associados ao esforço de correção selecionado.
3. Consulte a tabela a seguir para obter as ações que você pode executar no registro do esforço de correção.

   Depois de criar um registro, pode levar alguns minutos para que as tarefas de correção e um grande número de registros sejam exibidos.

Ação de IU	Descrição
Adicionar um marcador	À direita do cabeçalho, clique no ícone de marcador pequeno. Você pode adicionar um texto que ajude a identificar este registro. Por exemplo, você pode adicionar um marcador informando que este registro tem PCI ou outros dados críticos.
Adicionar uma anotação de trabalho ao registro	Na extremidade direita da tela, clique no ícone **Atividade** (ícone de iluminação) e insira uma anotação de trabalho. Clique no ícone para alternar o painel.
Atualizar o registro	Na guia **Detalhes**, para todos os campos editáveis, clique em um campo para selecioná-lo, faça suas mudanças e clique em **Salvar** para atualizar o registro.
Quando exibido, clique no ícone de filtro para refinar os dados na página exibida	Com qualquer uma das guias Tarefas de correção, Itens vulneráveis our Resultados de testes de configuração selecionadas, na extremidade direita, clique no ícone de filtro para mostrar os filtros que se aplicam à guia.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação de IU	Descrição
	No painel exibido, clique **em Exibição avançada** para adicionar ou alterar as condições do filtro dos itens na página. Clique em **Atualizar** para salvar suas mudanças. Por exemplo, na guia **Itens vulneráveis**, talvez você prefira adicionar o campo Idade e inserir um intervalo para exibir somente registros de um período específico. Os registros que correspondem às condições definidas são exibidos na lista.
Refinar filtros para itens em uma coluna	Selecione uma coluna e clique no menu de três pontos verticais para expandi-la e inserir condições para refinar e agrupar os dados na coluna.
Filtrar itens ou corresponder itens de uma linha em uma coluna	Digamos, por exemplo, que você queira exibir somente registros que tenham uma vulnerabilidade específica. Na lista de registros, selecione a linha do registro na coluna **Resumo**. Clique no menu de pontos verticais exibido e escolha um: ○ **Mostrar correspondência** : mostra todos os outros registros que têm esta vulnerabilidade. ○ **Filtrar** - mostra todos os registros que não têm esta vulnerabilidade.

4. Nas guias Tarefas de correção, Itens vulneráveis e Resultados de testes de configuração, você pode fazer uma busca detalhada em registros individuais de Tarefa de correção (VUL), Item vulnerável (VIT) e Resultado de teste (CTR) .

O que Fazer Depois

Se você quiser criar uma tarefa de correção sob demanda a partir de um esforço de correção, consulte Criar uma tarefa de correção sob demanda no Vulnerability Manager Workspace. Você também pode Criar uma lista personalizada de registros para ajudá-lo a monitorar o andamento da correção.

Criar um esforço de correção no Vulnerability Manager Workspace

Um registro de esforço de correção é uma lista estática de registros que você cria a partir de um tópico de observação no espaço do Vulnerability Manager.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Você usa esforços de correção para entregar as tarefas que as equipes de TI usam para corrigir vulnerabilidades. A partir da v16.1:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você pode editar os esforços de correção existentes.
- Crie esforços de correção que são criados automaticamente nas datas e horas que você definir.
- Transfira registros de esforços de correção existentes para um novo esforço de correção.

A partir da versão 18.0, como não é possível criar um esforço de correção para um tópico de observação inativo, o botão **Criar** esforço de correção fica inativo.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Espaço para gerentes de vulnerabilidades**.
2. Na página inicial (Inicial), selecione um tópico de observação para o qual você deseja criar um esforço de correção.
3. Para exibir os registros associados ao tópico de observação selecionado, no cabeçalho do registro, clique no botão **Itens vulneráveis** guia.

   Os registros são exibidos.

   No cabeçalho da guia Itens vulneráveis, você pode exibir o número total de registros que este tópico de observação tem.

   As seguintes colunas e dados são exibidos:

Colunas na guia Itens vulneráveis

Coluna	Descrição
Número	O número do registro.
Resumo	Descrição da vulnerabilidade.
Item de configuração	O ativo associado à vulnerabilidade.
Pontuação de risco	Pontuação de risco quantificada que separa os registros em Crítico, Alto, Médio, Baixo e Nenhum.
Estado	Status do registro.
Status da Correção	Status de correção de um registro.
Grupo de atribuição	Grupos de atribuição responsáveis pela correção. A atribuição de registros a grupos é baseada nas regras de atribuição que você cria.
Esforço de correção	Se ele for atribuído a um esforço de correção, cada registro listará seu esforço de correção atribuído. Depois que ele for adicionado a um esforço de correção, um registro não será adicionado a nenhum outro esforço de correção criado.
Grupo de atribuição	Grupos de atribuição responsáveis pela correção. A atribuição de registros a grupos é baseada nas regras de atribuição que você cria.
Esforço de correção	Se ele for atribuído a um esforço de correção, cada registro listará seu esforço de correção atribuído. Depois que ele for adicionado a um esforço de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Coluna	Descrição
	correção, um registro não será adicionado a nenhum outro esforço de correção criado.
Na tarefa de correção	Se verdadeiro, este valor indica que um registro já está em uma tarefa de correção. Os registros podem estar em várias tarefas de correção, mas um registro pode ser adicionado somente a um esforço de correção.
Explorar itens existentes	Indica se existe uma exploração conhecida para um registro.
Aberto pela última vez	Data em que o registro foi aberto pela última vez no seu Now Platform. Se o registro foi fechado e reaberto, esta é a última vez em que o registro foi reaberto.

4. Para criar um esforço de correção, clique em **Criar**esforço de correção .

   Quando você cria um esforço de correção, os registros já existentes nos esforços de correção não são adicionados a novos esforços de correção criados a partir deste tópico de observação.

   Conforme os registros são atualizados ou novos registros são criados em tópicos de observação, você pode criar esforços de correção.

5. Como alternativa, você pode Criar um esforço de correção recorrente nos espaços do Vulnerability Response.

   O botão **Editar** está disponível no menu para esforços de correção existentes. Você tem a opção de modificar os campos e as condições de um modal exibido. As mudanças feitas e salvas no registro do esforço de correção não afetam nenhum dos outros esforços de correção que você já criou a partir do tópico de observação.

6. Na etapa 1 do modal Criar esforço de correção, preencha os campos.

   No campo Descrição resumida, insira o texto que descreve o esforço de correção recorrente e ajuda a localizá-lo e rastreá-lo na lista de esforços.

   No campo Descrição, insira mais texto sobre o contexto do esforço que ajuda a localizá-lo facilmente na lista de esforços de correção.

   A partir da versão 17.1, ao criar um esforço de correção para tópicos de observação que contêm vulnerabilidades de host, você pode atualizar automaticamente os itens vulneráveis duplicados nas tarefas de correção criadas. Para atualizar automaticamente os itens vulneráveis duplicados, você deve marcar a caixa de seleção **Atualizar automaticamente os itens vulneráveis duplicados para as tarefas de correção criadas**.

   Nota:
   A partir da versão 18.0, esta caixa de seleção aparece na etapa 2.

7. Na etapa 2, Geração de tarefas, escolha um método na lista para agrupar os registros nas tarefas de correção que você gera a partir deste esforço de correção depois que ele é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Para a versão 18.0, a opção **Nenhum** não está disponível.

8. Na etapa 3, Transferir, verifique quantos registros você deseja adicionar ao esforço de correção e veja quantos registros estão disponíveis para transferência de outros esforços de correção ativos.

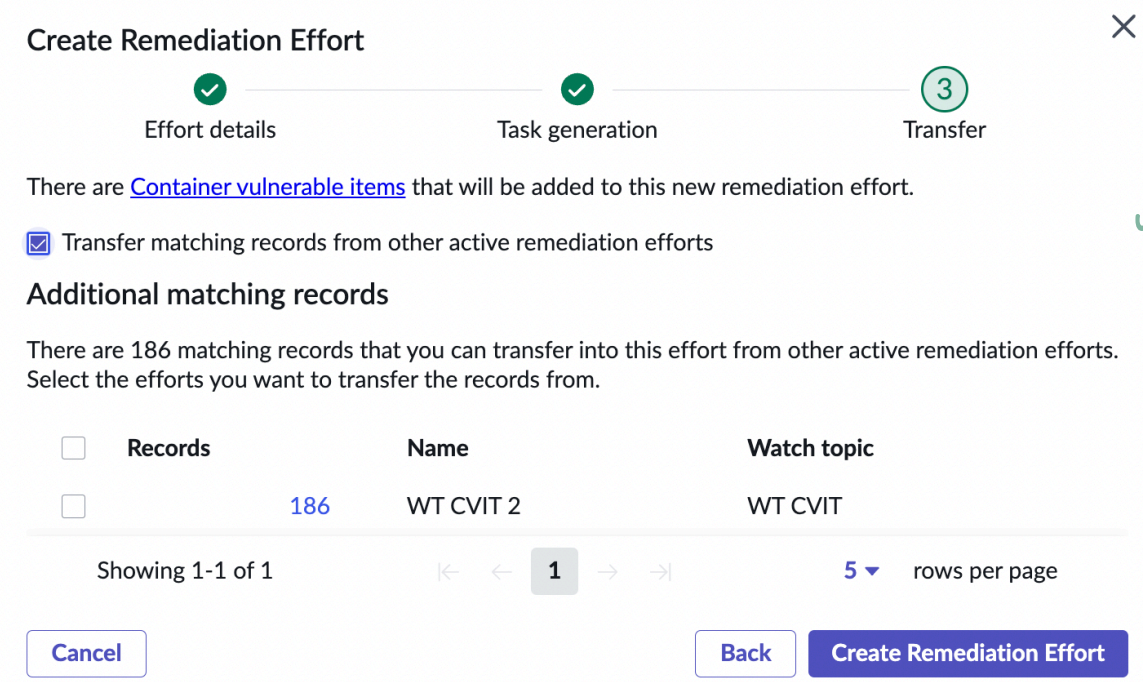
   Se não houver registros novos ativos para adicionar, o seguinte texto será exibido:

   Não há registros ativos disponíveis que você possa adicionar a este novo esforço de correção.

   Todos os registros adicionais disponíveis para transferência para este esforço são listados em Registros correspondentes adicionais .

   A partir da versão 18.0, marque a caixa de seleção **Transferir registros correspondentes de outros esforços de correção ativos** e marque as caixas de seleção dos registros que você deseja transferir de outros esforços de correção ativos.

Versão 18.0 Criar esforço de correção



Depois de clicar em **Criar esforço**de correção , o novo esforço de correção será exibido em alguns momentos. Dependendo do número de registros, pode levar algum tempo para preencher o novo registro. Uma mensagem indica se o registro ainda está sendo preenchido.

O novo esforço de correção é criado com todos os registros disponíveis no tópico de observação usado para criá-lo, além de todos os registros que você selecionou para transferência de esforços existentes.

Se você selecionar registros para transferir de um esforço existente e o esforço existente transferir todos os seus registros para o novo esforço, o esforço de correção do qual você moveu os registros será encerrado. Para obter mais informações sobre como as Tarefas de correção associadas aos Esforços de correção são afetadas pela transferência de registros, consulte Ciclos de vida de esforços de correção, tarefas de correção e registros nos espaços do Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Se não houver registros disponíveis no tópico de observação ou registros selecionados para transferência, o botão **Criar esforço** de correção será desativado.

O trabalho programado *Populate Efforts* é executado a cada 10 minutos para preencher os dados nos widgets com base na condição selecionada.

Clique na guia Progresso da correção para exibir o andamento da correção. Clique em qualquer item para exibir detalhes, incluindo tipo de registro, pontuação de risco, classificação de risco, porcentagem de registros corrigidos, registros no estado adiado e não adiado e número total de registros, condições usadas no tópico de observação e status de correção. As informações de Status de correção, como Meta de correção e Status da correção, são acumuladas da tabela Itens vulneráveis. A pontuação de risco mais alta do registro é acumulada da tabela Calculadoras de vulnerabilidade, enquanto a pontuação de risco é acumulada da **Calculadoras de acúmulo de vulnerabilidade** > **Agregar esforço de correção**.

A guia Tarefas de correção exibe as tarefas para todos os tipos de problemas. Os campos são preenchidos quando os seguintes trabalhos programados são executados. Eles são executados automaticamente a cada 15 minutos:

- Acumular valores de item vulnerável da aplicação para vulnerabilidade e grupo.
- Acumular valores de item vulnerável de contêiner para vulnerabilidade e grupo.
- Acumular valores de resultado de teste para testar o grupo de resultados e o teste de configuração.
- Acumular valores de item vulnerável para vulnerabilidade e grupo.

Na exibição Listas, você pode exibir os Esforços de correção, as Tarefas de correção, os Itens vulneráveis, os Resultados de testes de configuração e assim por diante. Você pode abrir uma tarefa de correção ou um item vulnerável e exibir a página Detalhes. Clique nas reticências Mais ações e em **Iniciar investigação** para resolver uma tarefa de correção.

9. **Opcional:** Você também pode editar os esforços de correção recorrentes existentes.

(Optional) Se houver um esforço de correção recorrente para um tópico de observação, **Editar esforço recorrente** estará disponível no menu no canto superior direito de um tópico de observação. Escolha esta opção para editar o esforço recorrente.

As mudanças feitas e salvas no registro do esforço de correção não afetam nenhum dos outros esforços de correção que você já criou a partir do tópico de observação.

Criar uma tarefa de correção sob demanda no Vulnerability Manager Workspace

Crie uma tarefa de correção sob demanda a partir de um esforço de correção. Se você criar uma tarefa de correção sob demanda, escolha os registros que deseja adicionar manualmente.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Para a versão 18.0 do Vulnerability Response, não é possível criar uma tarefa de correção a partir da exibição de registro de um esforço de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Espaço para gerentes de vulnerabilidades**.
2. Na parte superior esquerda do espaço com a página inicial exibida, clique no ícone de exibição de **lista** para exibir a página inicial da lista.
3. Em Esforços de correção, clique em **Ativo** ou em **Todos**.
4. Na lista exibida, clique em um registro para abri-lo.
   A guia de visão geral do registro é exibida.
5. Clique na guia **Itens vulneráveis**.
   A lista de registros será exibida.
6. Para criar uma nova tarefa de correção, na coluna Número, selecione os registros que você deseja adicionar.
7. Clique **em Criar tarefa de correção**.
8. No modal exibido, preencha os campos.
9. Clique em **Criar**.
10. A nova tarefa de correção é exibida com os registros ativos selecionados.

Criar um esforço de correção recorrente nos espaços do Vulnerability Response

Você pode criar e programar esforços de correção recorrentes que são gerados automaticamente nas datas e horas que você definir.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode criar automaticamente esforços de correção recorrentes em uma programação que ajuda a rastrear vulnerabilidades que podem surgir e exigir atenção imediata e contínua.

A partir da versão 18.0, como não é possível criar um esforço de correção recorrente para um tópico de observação inativo, a opção **Criar esforço recorrente** está inativa. Se você desativar um tópico de observação que tenha um esforço recorrente já programado, um novo esforço de correção não será criado até que o tópico de observação seja ativado. Além disso, os detalhes da **Recorrência do esforço** e da **Data da próxima recorrência** desaparecem no canto superior direito. Depois de ativar o tópico de observação, um esforço de correção será criado na próxima programação.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Espaço para gerentes de vulnerabilidades**.
2. Na página inicial (Inicial), selecione um tópico de observação para o qual você deseja criar um esforço de correção recorrente.

   Você pode criar um esforço de correção recorrente por tópico de observação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Você não pode transferir registros de esforços de correção recorrentes para novos esforços de correção. No entanto, você pode transferir registros de esforços de correção existentes e não recorrentes para novos esforços de correção. Consulte Transferir registros para esforços de correção nos espaços Vulnerability Response para obter mais informações sobre como transferir registros.

3. Em um tópico de observação, no canto superior direito da lista Criar esforço de correção, selecione **Criar esforço recorrente**.

   O modal Criar esforço recorrente é exibido.

4. Na etapa 1, Detalhes do esforço, preencha os campos obrigatórios.

   No campo Descrição resumida, insira o texto que descreve o esforço de correção recorrente que ajuda a localizá-lo e rastreá-lo na lista de esforços.

   No campo Descrição, insira mais texto sobre o contexto do esforço que ajuda a localizá-lo facilmente na lista de esforços de correção. Por exemplo, `Vulnerabilidades em ativos externos`.

   A partir da versão 17.1, ao criar um esforço de correção para tópicos de observação que contêm vulnerabilidades de host, você pode atualizar automaticamente os itens vulneráveis duplicados nas tarefas de correção criadas. Para atualizar automaticamente os itens vulneráveis duplicados, você deve selecionar a opção **Atualizar automaticamente os itens vulneráveis duplicados para as tarefas de correção criadas**.

   Nota:
   A partir da versão 18.0, esta caixa de seleção aparece na etapa 2.

5. Clique em **Avançar**.
   Os detalhes da geração de tarefa são exibidos.
6. Na etapa 2, Geração de tarefas, escolha um método na lista para agrupar os itens vulneráveis nas tarefas de correção que você gera a partir deste esforço de correção depois que ele é criado.
   - Por grupo de atribuição
   - Por grupo de atribuição e item de configuração
   - Por grupo de atribuição e vulnerabilidade
   - Nenhum (nenhuma tarefa de correção criada). Use este método se quiser adicionar registros manualmente a uma tarefa de correção para este esforço. Consulte Criar uma tarefa de correção sob demanda no Vulnerability Manager Workspace.

     Nota:
     Para a versão 18.0 de Vulnerability Response, a opção **Nenhum** não está disponível.

7. Clique em **Avançar** para continuar.
8. Na etapa 3, Recorrência, selecione a frequência.

   a. Defina a programação de recorrência.

      Use as listas para selecionar o mês/dia/hora/minuto em que você deseja que o esforço de correção seja criado. O fuso horário para programação é, por padrão, o seu fuso horário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Se você tiver muitas vulnerabilidades, talvez prefira definir a criação para fora do horário de expediente.

Se você quiser que o trabalho seja criado no último dia do mês, o trabalho programado criará o esforço de correção recorrente no último dia do mês. Uma mensagem será exibida se o mês não tiver 31 dias.

b. Opcional: Selecione **Transportar vulnerabilidades** para vulnerabilidades ativas neste esforço de correção para levar adiante em cada esforço de correção subsequente que for criado.

9. Clique **em Programar recorrência**.
Uma mensagem é exibida informando que o registro de correção recorrente foi criado. O novo esforço de correção não é exibido imediatamente, ele é criado quando você o programou. Ele é exibido em suas listas depois de criado pelo trabalho programado.

A data em que o esforço de correção será criado é mostrada no tópico de observação correspondente. Para obter mais informações sobre como as Tarefas de correção associadas aos Esforços de correção são afetadas pela transferência de registros, consulte Ciclos de vida de esforços de correção, tarefas de correção e registros nos espaços do Vulnerability Response.

Transferir registros para esforços de correção nos espaços Vulnerability Response

Você pode transferir registros de esforços de correção existentes para novos esforços de correção.

Antes de Iniciar

Se enfrentar uma ameaça de dia zero ou uma vulnerabilidade muito crítica que você deseja resolver rapidamente, convém consolidar todos os registros ativos que você já possui para esta vulnerabilidade em um esforço de correção. No entanto, cada registro só pode estar em um esforço e os registros podem se sobrepor entre os tópicos de observação. Portanto, para coletar todos eles, você precisa transferir esses registros de vários esforços existentes para um esforço de correção.

Digamos, por exemplo, que você criou um esforço de correção que tem uma vulnerabilidade de alta prioridade. Como esta vulnerabilidade é difundida e pode afetar outras áreas em seu ambiente, talvez você já tenha registros associados a esta vulnerabilidade nos esforços de correção existentes. Para combinar esses registros para que estejam todos em um esforço de correção, você pode transferir todos os registros dos esforços de correção existentes para um novo esforço de correção.

Nota:
Você não pode transferir registros de esforços de correção recorrentes para novos esforços de correção. Para obter mais informações, consulte Criar um esforço de correção recorrente nos espaços do Vulnerability Response.

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Espaço para gerentes de vulnerabilidades**.

2. Na página inicial (Inicial), selecione um tópico de observação para o qual você deseja criar um esforço de correção recorrente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique **em Criar esforço**de correção.
   O modal Criar esforço de correção é exibido.
4. Na etapa um, Detalhes do esforço, preencha os campos obrigatórios.

   No campo Descrição resumida, insira o texto que descreve o esforço de correção recorrente que ajuda a localizá-lo e rastreá-lo na lista de esforços.

   No campo Descrição, insira mais texto sobre o contexto do esforço que ajuda a localizá-lo facilmente na lista de esforços de correção. Por exemplo, Vulnerabilidades ativas do Log4J.

   a. No campo Nome, insira um nome para o novo esforço de correção.
      Por padrão, o nome do tópico de observação é exibido.

   b. No campo Descrição, insira um texto que o ajudará a localizar facilmente esse esforço de correção na lista de esforços de correção.

   A partir da versão 17.1, ao criar um esforço de correção para tópicos de observação que contêm vulnerabilidades de host, você pode atualizar automaticamente os itens vulneráveis duplicados nas tarefas de correção criadas. Para atualizar automaticamente os itens vulneráveis duplicados, você deve selecionar a opção **Atualizar automaticamente os itens vulneráveis duplicados para as tarefas de correção criadas**.

   Nota:
   A partir da versão 18.0, esta caixa de seleção aparece na etapa 2.

5. Clique em **Avançar**.
   Os detalhes da geração de tarefa são exibidos.
6. Na etapa 2, Geração de tarefas, escolha um método na lista para agrupar os registros nas tarefas de correção que você gera a partir deste esforço de correção depois que ele é criado.
   - Por grupo de atribuição
   - Por grupo de atribuição e item de configuração
   - Por grupo de atribuição e vulnerabilidade
   - Nenhum (nenhuma tarefa de correção criada). Use este método se quiser adicionar registros manualmente a uma tarefa de correção para este esforço. Consulte Criar uma tarefa de correção sob demanda no Vulnerability Manager Workspace.

     Nota:
     Para a versão 18.0, a opção **Nenhum** não está disponível.

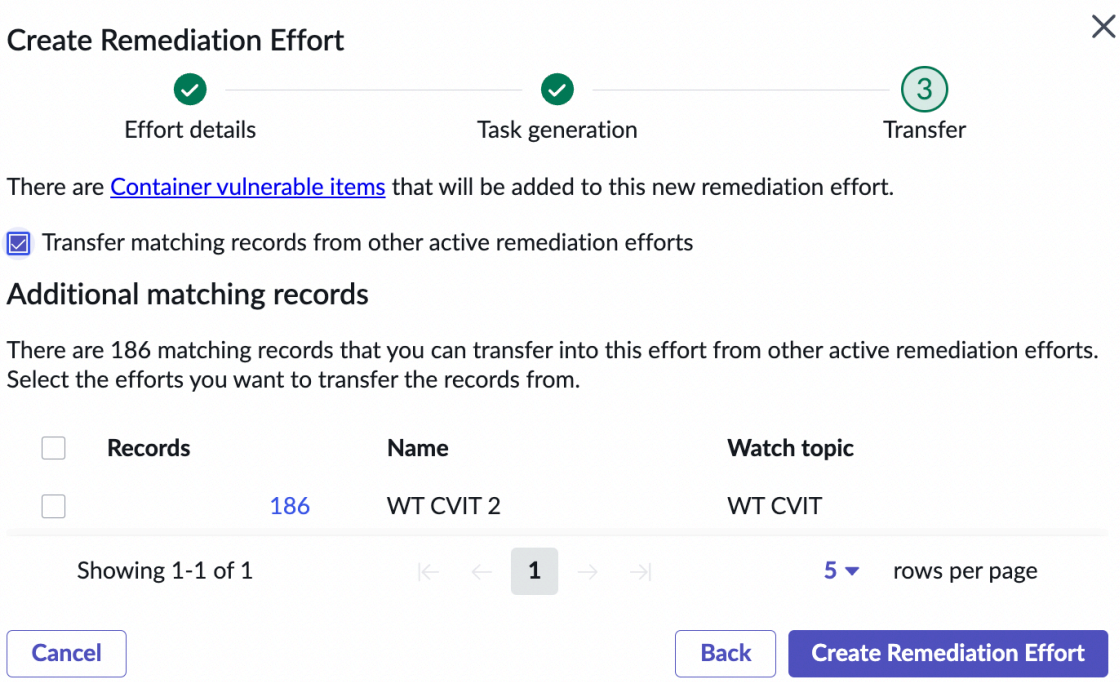
7. Clique em **Avançar**.
8. Na etapa 3, Transferir, verifique quantos registros serão adicionados ao esforço de correção e veja quantos registros estão disponíveis para transferência de outros esforços de correção ativos.
9. Para transferir registros de outros esforços, na lista, marque as caixas de seleção dos registros desejados.

   A partir da versão 18.0, marque a caixa de seleção **Transferir registros correspondentes de outros esforços de correção ativos** e marque as caixas de seleção dos registros que você deseja transferir de outros esforços de correção ativos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versão 18.0 Criar esforço de correção



10. Clique **em Criar esforço**de correção.

Após alguns momentos, o novo esforço de correção será exibido. Dependendo do número de registros, isso pode levar algum tempo. Uma mensagem indica que o registro está sendo preenchido.

O novo esforço de correção é criado com todos os registros disponíveis no tópico de observação usado para criá-lo, além de todos os registros que você selecionou para transferência de esforços existentes.

Se você selecionar registros para transferir de um esforço existente e o esforço existente transferir todos os seus registros para o novo esforço, o esforço de correção do qual você moveu os registros será encerrado.

Nota:
Se não houver registros disponíveis no tópico de observação nem registros selecionados para transferência, o botão **Criar esforço** de correção será desativado.

Para obter mais informações sobre como as Tarefas de correção associadas aos Esforços de correção são afetadas pela transferência de registros, consulte Transferência de registros ou transferênciade registro.

Adicionar um controle de compensação à biblioteca

Como gerente ou analista de vulnerabilidade, adicione uma lista de controles compensatórios que podem ser aplicados para a redução de risco de itens vulneráveis e tarefas de correção.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Alguns controles de compensação usados com frequência são enviados com o sistema básico. Você pode exibir esses controles de compensação navegando até **Espaços** > **Espaço para gerentes de vulnerabilidades** > **Listas** > **Bibliotecas** > **Controles de compensação**. Você pode ativar ou desativar esses controles de remuneração de acordo com seus requisitos.

Nota:
O recurso de controles de compensação está disponível somente para vulnerabilidades de host.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Lista em Bibliotecas, selecione **Controles de compensação**.
3. Clique em **Nova**.
4. No formulário Criar controles de remuneração, preencha os campos.

Criar campos de formulário de controles de remuneração

Campo	Descrição
Nome	Nome do controle de compensação, que aparece como uma opção no menu suspenso **Controles de compensação** do modal de exceção Solicitar.
Descrição	Informações resumidas que fornecem detalhes sobre o controle de compensação.
Ativo	Status do controle de compensação. Somente controles ativos aparecem no menu suspenso **Controles de compensação** do modal de exceção Solicitar.

5. Selecione **Salvar**.
6. Na lista Controles de compensação em Bibliotecas, selecione o controle de compensação desejado e selecione **Editar**, ative ou desative um controle de compensação e clique em **Salvar** para modificar os controles de compensação.
   Todos os controles de compensação ativos aparecem como uma opção no menu suspenso **Controles de compensação** do modal de exceção Solicitar para solicitações de redução de risco.

O que Fazer Depois

A partir da v21.0 de Vulnerability Response, você pode associar controles de compensação a CVEs ou TPEs depois de adicionar controles de compensação à biblioteca. Para obter mais informações sobre como associar controles de remuneração, consulte Associar controles de compensação com CVEs ou TPEs para solicitações de redução de risco.

Tópicos relacionados

- Noções básicas sobre controles de compensação para redução de risco
- Desabilitar ou habilitar a redução de risco para um CVE ou TPE
- Associar controles de compensação com CVEs ou TPEs para solicitações de redução de risco
- Impacto dos controles de remuneração na pontuação de risco e na data de vencimento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Associar controles de compensação com CVEs ou TPEs para solicitações de redução de risco

Como gerente ou analista de vulnerabilidade, você pode associar controles de compensação relevantes a um CVE ou TPE, que pode ser aplicado para solicitações de redução de risco.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

- Se você não associar controles de remuneração a um CVE ou TPE, todos os controles ativos serão exibidos no campo Selecionar controles de compensação do formulário de Exceção de solicitação.
- Se você associar um controle de compensação a um CVE, esse controle de compensação será associado automaticamente ao TPE, que será mapeado para o CVE.

Nota:
O recurso de controles de compensação está disponível somente para vulnerabilidades de host.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Listas, em Bibliotecas, abra um dos seguintes para os quais você deseja associar os controles:
   - **CVE** da lista de CVEs.
   - **TPE** da lista de TPEs.
3. Selecione **Associar controles**.

   Nota:
   O botão **Associar controles** aparece somente quando a redução de risco está habilitada para um CVE ou TPE. Em outras palavras, você pode associar controles de remuneração somente quando a redução de risco estiver habilitada para um CVE ou TPE. Se o botão **Associar controles** não estiver visível, selecione **Habilitar redução de risco**.

4. No modal Associar controles, selecione os controles de compensação que podem ser aplicados às vulnerabilidades associadas ao CVE ou TPE para redução de risco.
5. Selecione **Enviar**.
   - Os controles de compensação associados aparecem na guia Controles de compensação aplicáveis na exibição de registro do CVE e TPE.
   - Enquanto um proprietário de correção solicita redução de risco, esses controles de compensação associados aparecem no campo Selecionar controles de compensação no modal Solicitar exceção.

Tópicos relacionados

Noções básicas sobre controles de compensação para redução de risco

Desabilitar ou habilitar a redução de risco para um CVE ou TPE

Adicionar um controle de compensação à biblioteca

Impacto dos controles de remuneração na pontuação de risco e na data de vencimento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Desabilitar ou habilitar a redução de risco para um CVE ou TPE

Como gerente e analista de vulnerabilidade, você pode desabilitar ou habilitar as solicitações de redução de risco para as vulnerabilidades do host de uma entrada de vulnerabilidade comum (CVE) ou entrada de terceiros (TPE).

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
A redução de risco para um CVE e TPE está habilitada por padrão.

Nota:
O recurso de controles de compensação está disponível somente para vulnerabilidades de host.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
   Na página Listas, em Bibliotecas, abra um dos seguintes para os quais você deseja desabilitar as solicitações de redução de risco:
   - **CVE** da lista de CVEs.
   - **TPEs** da lista de TPEs.
2. Selecione **Desabilitar redução de risco**.
   O proprietário da correção não pode solicitar a redução de risco dos itens vulneráveis de host relacionados a este CVE ou TPE. Em outras palavras, a caixa de seleção Solicitação de redução de risco não aparece quando o **Motivo** é selecionado como Controle de atenuação no local no modal de exceção da solicitação.
3. Para habilitar as solicitações de redução de risco para itens vulneráveis de host, selecione **Habilitar redução de risco**.

Tópicos relacionados

Noções básicas sobre controles de compensação para redução de risco

Adicionar um controle de compensação à biblioteca

Associar controles de compensação com CVEs ou TPEs para solicitações de redução de risco

Impacto dos controles de remuneração na pontuação de risco e na data de vencimento

Editar itens vulneráveis de host em massa no Vulnerability Manager Workspace

A partir da v21.0 de Vulnerability Response, você pode atualizar o estado, a solução preferencial, o patch preferencial e o grupo de atribuição para vários host itens vulneráveis (VITs) no Vulnerability Manager Workspace.

Antes de Iniciar
Função necessária:sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin e qualquer função com a função granular sn_vul.bulk_edit.

Por Que e Quando Desempenhar Esta Tarefa
No Vulnerability Manager Workspace, o recurso de edição em massa é compatível somente com itens vulneráveis de host.

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Na página Lista, em Vulnerabilidades do host, selecione os itens vulneráveis executando uma das seguintes ações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Marque a caixa de seleção ao lado de cada item se quiser usar a opção **Somente itens selecionados** no campo Seleção de registro.
- Aplique filtros se quiser usar a opção de **filtro Todos os itens vulneráveis que correspondem** ao campo Seleção de registro.

3. Selecione **Edição em massa**.
4. No modal de edição em massa, preencha os campos.

Editar campos de modal em massa

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ○ Somente itens selecionados ○ Todos os itens vulneráveis que correspondem ao filtro ○ Tarefa de Correção ○ Entrada de Vulnerabilidade **Nota:** Registros com IC inválido ou IC desativado não são atualizados.
Estado	Mudança para o **Estado** no item vulnerável. As opções são: ○ Não Atualizar ○ Em aberto ○ Sob Investigação ○ Aguardando Implementação ○ Adiado **Nota:** ▪ Quando você seleciona essa opção, os campos Motivo, Descrição resumida, Até e Informações adicionais são exibidos. ▪ Quando você adia registros, uma tarefa de correção é criada e essa tarefa é enviada para aprovação. ○ Encerrado **Nota:** ▪ Quando você seleciona esta opção para marcar os registros como falso-positivos, os campos Motivo, Descrição resumida, Até e Informações adicionais são exibidos. ▪ Quando você marca os registros como falso-positivos, uma tarefa de correção é criada e essa tarefa é enviada para aprovação. ○ Resolvido

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Solução preferencial	Solução que é direcionada para corrigir todos os itens vulneráveis selecionados para edição em massa. Selecione a mudança para o campo **Solução preferencial** no item vulnerável. As opções são de uma lista de pesquisa de soluções preferenciais disponíveis para os VITs selecionados. **Nota:** ◦ O conjunto de soluções preferenciais disponíveis é uma interseção de todas as possíveis soluções das vulnerabilidades em todos os VITs selecionados. ◦ Ao selecionar **Seleção de registro** > **Entrada de Vulnerabilidade** para uma edição em massa, todos os VITs da vulnerabilidade serão definidos para a solução preferencial selecionada. **Nota:** Esta operação não define a **solução preferencial** no nível de entrada de vulnerabilidade. Definir a **solução preferencial** no nível de entrada de vulnerabilidade definiria a **solução preferencial** para todos os novos VITs daqui para frente. A edição em massa modifica somente o conjunto atual de VITs. ◦ As vulnerabilidades distintas nos critérios de seleção são limitadas a 500. Se houver mais de 500 vulnerabilidades distintas, uma mensagem de aviso será exibida solicitando que você selecione VITs com critérios diferentes para definir a **solução Preferencial**. ◦ O número total de soluções que podem ser mostradas na lista de pesquisa é limitado a 170. Se houver mais de 170 soluções, uma mensagem de aviso será exibida. O valor atualizado é mostrado na exibição de lista de itens vulneráveis.
Patch preferencial	Patch que é direcionado para corrigir todos os itens de vulnerabilidade selecionados para edição em massa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ◦ Você deve instalar o Patch Orchestration para exibir a lista de patches preferenciais. ◦ O conjunto de patches preferenciais disponíveis é uma interseção de todos os possíveis patches em todos os VITs selecionados. ◦ As vulnerabilidades distintas nos critérios de seleção são limitadas a 500. Se houver mais de 500 vulnerabilidades distintas, uma mensagem de aviso será exibida solicitando que você selecione VITs com critérios diferentes para definir o **patch Preferencial**. ◦ O número total de patches que podem ser mostrados na lista de pesquisa é limitado a 170. Se houver mais de 170 patches, uma mensagem de aviso será exibida.
Motivo	Motivo para adiar registros: ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Risco aceito ◦ Redução do controle no local ◦ Outro Motivo para fechar os registros: ◦ Falso-positivo **Nota:** ▪ Ao selecionar esta opção, os campos Descrição resumida, Até e Informações adicionais são exibidos. ▪ Uma tarefa de correção é criada quando você marca os registros como falso-positivos e essa tarefa é enviada para aprovação. ◦ Cancelado ◦ Corrigidos **Nota:** Este campo aparece quando você seleciona o Estado como Adiado ou Encerrado.
Descrição resumida	Breve nota que descreve os motivos do adiamento e da solicitação de falso-positivo . Essas informações são refletidas no campo Descrição da tarefa de correção criada para solicitações de adiamento e falso-positivo encerradas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Este campo aparece quando você seleciona o Estado como Adiado e Encerrado-Falso-positivo.
Até	Data até a qual o registro permanece adiado. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado.
Informações adicionais	Outras informações necessárias. Essas informações são refletidas no campo Informações adicionais na guia Visão geral da tarefa de correção criada para solicitações de adiamento e falso-positivo encerradas. Se sua solicitação de adiamento for aprovada, essas informações adicionais serão exibidas como anotações de adiamento para o VIT e a tarefa de correção. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado e Encerrado-Falso-positivo.
Cancelar atribuição	Todos os itens selecionados não estão atribuídos ao grupo de atribuição e ao proprietário de correção. **Nota:** ○ Este campo aparece quando você seleciona o Estado como Não atualizar. ○ Quando você cancela a atribuição de registros, uma tarefa de correção é criada e essa tarefa é enviada para aprovação.
Grupo de atribuição	Grupo de atribuição para os registros. Todos os grupos de atribuição ativos aparecem neste campo. **Nota:** Este campo é desativado quando você marca a caixa de seleção Cancelar atribuição.
Anotações de trabalho	Texto que você insere para descrever as mudanças.

5. Selecione **Editar**.
   Um trabalho assíncrono de edição em massa atualiza os registros selecionados. Uma tarefa de correção é criada com os itens vulneráveis selecionados ao adiar, cancelar a atribuição ou fechar (falso-positivo) itens vulneráveis em massa. E esta tarefa é enviada para aprovação. Você pode exibir a tarefa de correção na lista Tarefa de correção na página Lista.

Solicitar exceções para tarefas de correção e registros do Vulnerability Manager Workspace

No Vulnerability Manager Workspace, os gerentes e analistas de vulnerabilidade podem solicitar exceções e falsos positivos para tarefas e registros de correção. Você também pode dividir tarefas de correção e criar solicitações de mudança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul_container.vulnerability_analyst, sn_vul.app_sec_manager, sn_vul_container.vulnerability_admin ou sn_vulc.admin.

Como gerente ou analista de vulnerabilidade, você pode executar essas tarefas a partir da tarefa de correção e dos registros exibidos no Vulnerability Manager Workspace.

A partir da versão 19.0 do Vulnerability Response, você pode:

- divida uma Tarefa de correção, solicite exceções e exceções de política para Grupos de resultados de testes (TRGs) no Vulnerability Manager Workspace.
- solicite exceções de política para vulnerabilidades de contêiner (CVITs) no Vulnerability Manager Workspace.

Nota:
A partir da v19.0 de Vulnerability Response, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

A partir da versão 18.0 do Vulnerability Response, você pode:

- Solicite exceções para itens de vulnerabilidade da aplicação (AVITs) e itens de vulnerabilidade de contêiner (CVITs) e suas tarefas de correção no Vulnerability Manager Workspace.
- Solicite uma exceção de política para itens de vulnerabilidade de host, AVITs, CVITs e suas tarefas de correção no Vulnerability Manager Workspace.

Você inicia essas ações de IU a partir de registros no Vulnerability Manager Workspace, da mesma forma que os proprietários de correção executam essas tarefas no IT Remediation Workspace.

Consulte os seguintes tópicos para obter mais informações:

- Solicitar um falso-positivo no Espaço de correção de problemas de TI
- Solicitar uma exceção no Espaço de correção de problemas de TI
- Solicitar redução de risco no Espaço de correção de problemas de TI
- Dividir uma tarefa de correção no Espaço de correção de problemas de TI
- Criar uma solicitação de mudança no Espaço de correção de problemas de TI
- Solicitar uma exceção usando GRC: Policy and Compliance Management no Espaço de correção de problemas de TI

Solicitar uma extensão para um item vulnerável adiado no Espaço do gerenciador de vulnerabilidades

Solicite uma extensão para um item vulnerável adiado antes que ele atinja o adiado até a data de vencimento. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Por Que e Quando Desempenhar Esta Tarefa
Você também pode solicitar uma extensão do ambiente clássico.

Use o mesmo procedimento para solicitar uma extensão para um item vulnerável de aplicação, item vulnerável de contêiner, grupo de resultados de teste e uma tarefa de correção.

Procedimento
1. Navegar até **Espaços** > **Vulnerability Manager Workspaces**.
2. Selecione Listas.
3. Em Itens vulneráveis de host, selecione **Todos**.
4. Filtre a lista selecionando adiado na coluna Estado.
5. Selecione um item vulnerável adiado.

> **Nota:**
> O botão Solicitar extensão fica visível somente quando o estado do item vulnerável é Adiado.

6. Selecione o botão **Solicitar extensão**.
7. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até quando o item vulnerável adiado deve ser estendido para correção.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

8. Selecione **Solicitar extensão**.
   Um e-mail é acionado no envio da solicitação e na ação subsequente do aprovador.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

- A solicitação passa por dois níveis de aprovação.
- Se um item vulnerável adiado for estendido novamente, a contagem de adiamento de extensão aumentará no back-end.

9. Depois que a solicitação é aprovada, as anotações Até, Motivo e Adiamento são atualizadas.

Verificar novamente registros e tarefas de correção no Vulnerability Manager Workspace

Para verificar se suas tarefas e registros de correção foram resolvidos entre os ciclos de verificação programados, inicie novas verificações de seu Now Platform sob demanda.

Função necessária: sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin.

As novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

Os scanners Rapid7 e Qualys são desativados por padrão na aplicação Vulnerability Response. Se você tentar executar uma nova verificação a partir dos itens vulneráveis ou das tarefas de correção que têm essas aplicações como origem, o botão **Verificar novamente** não estará disponível.

Para ativar esses scanners, como um usuário com a função sn_vul.vulnerability_admin:

1. Navegar até **Todos** > **Vulnerability Response** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o scanner que você deseja ativar e clique no registro para abri-lo.
3. Marque a caixa de seleção Ativo.
4. Clique em **Atualizar**.

   O produto que você ativou é exibido no campo Origem no item vulnerável e nos registros da tarefa de correção após a próxima importação, e a **opção Nova verificação** está disponível como uma ação de IU.

A nova verificação é compatível com registros e tarefas de correção com as seguintes integrações no Vulnerability Manager Workspace. Consulte os seguintes tópicos para obter mais informações:

- Verificar novamente Rapid7 itens vulneráveis dos Vulnerability Response espaços
- Verificar novamente Qualys itens vulneráveis dos Vulnerability Response espaços
- Verificar novamente Tenable.io e Tenable.sc itens vulneráveis dos espaços Vulnerability Response

Para iniciar novas verificações no Espaço do gerenciador de vulnerabilidades a partir de itens vulneráveis e registros de tarefa de correção, os registros exigem um scanner compatível como origem.

Você pode preferir criar uma lista filtrada que exiba registros por origem. Consulte Criar uma lista personalizada de registros para obter um exemplo de como criar uma lista.

Usar a exibição de lista no Espaço do gerenciador de vulnerabilidades

A exibição de lista no espaço do Vulnerability Manager permite que os gerentes e analistas de vulnerabilidade e segurança exibam o andamento da correção nos registros, façam uma busca detalhada nos registros do Vulnerability Response e exibam o status de suas solicitações de aprovação e exceções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul.app_sec_manager, sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Espaço para gerentes de vulnerabilidades**.
2. Na parte superior esquerda do espaço com a página inicial exibida, clique no ícone **Lista**.
3. **Opcional:** Clique em **Minhas listas** para criar uma lista.
   Para obter mais informações sobre como criar uma lista, consulte Criar uma lista personalizada de registros.
4. Consulte a tabela a seguir para obter as ações que você pode executar na página Lista.

Ação de IU	Descrição
Abrir um esforço de correção	
À esquerda da coluna Número com uma lista exibida, passe o mouse sobre uma linha e clique no pequeno ícone de informações **(i)** de um registro.	Detalhes sobre os registros são exibidos no painel lateral direito da página. Os detalhes incluem: ○ Grupo de atribuição ○ Vulnerabilidade ○ Atribuído a ○ Descrição resumida ○ Descrição Você pode editar os campos. Se a caixa de seleção Ativo for exibida, você poderá ativar ou desativar o registro. Clique em **Atualizar** para salvar suas mudanças.
Atualizar lista	Com o ícone de atualização na parte superior direita da página, recarregue a página atual.
Redefinir larguras	Clique no ícone de engrenagem para ajustar a largura das colunas em suas listas. Uma cópia da lista original será salva em **Suas listas**.
Copiar a URL da página exibida	Copie o URL para uso em outro lugar.
Exportar a página	No modal, insira o arquivo e os tipos de entrega e clique em **Exportar**.
Refinar filtros para os dados na página.	Selecione uma coluna e expanda o menu de três pontos verticais para exibir opções que filtram ainda mais os dados na coluna. Por exemplo, talvez você prefira filtrar a coluna Grupo de atribuição da lista de tarefas de correção ativas por um grupo de atribuição específico.
Filtrar itens ou corresponder itens de uma linha em uma coluna	Selecione uma célula em uma coluna e refine os dados exibidos escolhendo um:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação de IU	Descrição
	○ Mostrar correspondência: exibe somente os itens que correspondem à célula selecionada na coluna. ○ Filtrar — Filtra os itens da coluna que correspondem à célula selecionada na coluna.

5. A partir da versão 18.0, você pode criar um item vulnerável da aplicação nas listas **Ativo** ou **Todos** em `Application Vulnerable items` clicando no botão **Novo** no canto superior direito.

Criar uma lista personalizada de registros

Você pode criar uma lista personalizada no espaço do gerenciador de vulnerabilidades.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin, sn_vul.app_sec_manager, sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin ou sn_vulc.admin

Procedimento

1. Navegar até **Espaços** > **Espaço para gerentes de vulnerabilidades**.
2. Selecione o ícone **Lista** e clique em **Minhas listas**.
3. Selecione **Nova lista**.
4. No modal Nova lista, clique em **Iniciar a partir de existente** e pesquise na lista de seleção Lista uma lista existente para usar como modelo.
5. Edite o Nome da Lista.
6. Adicionar filtros.
   Por exemplo, você pode criar uma lista de registros ativos para um scanner específico que deseja monitorar para novas verificações. Você pode usar os filtros: Ativo é verdadeiroe Origem contém (nome do seu scanner).
7. Edite as colunas que você deseja exibir na lista.
8. Clique em **Criar**.
   Sua nova lista será exibida.
9. Como alternativa, clique em **Criar seu próprio**, insira um nome e, em seguida, em **Selecionar origem**.
10. Comece a digitar no campo e selecione uma das fontes exibidas para sua nova lista.
11. Clique em **Criar**.
    Sua nova lista será exibida.

    Nota:
    Se você sair do módulo de lista, a lista exibida ao sair será a lista que você vê ao retornar.

12. Para excluir uma lista, com a lista exibida, clique no ícone de engrenagem no canto superior direito da página.

Aprovar solicitações no Vulnerability Manager Workspace

Aprove as solicitações enviadas de Espaço de correção de problemas de TI pelos responsáveis pela correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Funções necessárias:

Funções de aprovador necessárias para várias solicitações de aprovação

Tipo de aprovação	Níveis de aprovação necessários	Funções de aprovador	Informações adicionais
Aprovações de falso-positivos	Um	• Função granular sn_vul.false_positive_approver para itens vulneráveis (VITs). • sn_vul.app_false_positive_approver para itens vulneráveis da aplicação (AVITs) • sn_vul_container.false_positive_approver para itens vulneráveis de contêiner (CVITs) Ou Os aprovadores devem estar no grupo de usuários Aprovadores de falso-positivo.	-
Aprovações de exceção (adiamentos)	Dois	• É necessário um aprovador no grupo Aprovador - Nível 1 • É necessário um aprovador no grupo Aprovador - Nível 2	Uma solicitação de exceção para um registro ou tarefa de correção é aprovada usando um fluxo de trabalho de aprovação padrão de dois níveis. A solicitação de exceção requer dois níveis de aprovadores. Depois que a solicitação é aprovada pelo aprovador de nível 1, ela é enviada para o aprovador de segundo nível e fica visível na fila do aprovador 2.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções de aprovador necessárias para várias solicitações de aprovação

Tipo de aprovação	Níveis de aprovação necessários	Funções de aprovador	Informações adicionais
Desatribuir aprovações	É necessário um aprovador no grupo Aprovador - Nível 1	• sn_vul.unassign_appr para AVITs e VITs • sn_vul_container.unas para CVITs • sn_vulc.unassign_app para problemas de configuração (ICs)	**Nota:** Por padrão, uma configuração de aprovação é fornecida e um grupo de aprovação de desatribuição é criado. Os usuários (Cancelar atribuição de aprovador - Nível 1) deste grupo podem aprovar a solicitação. Este grupo contém uma função de aprovador de desatribuição, sn_vul.unassign_approver, por padrão. Você pode modificar ou criar um novo grupo e atualizar a configuração de aprovação. Para configurar regras de aprovação, navegue até o respectivo módulo Regras de aprovação, selecione qualquer uma das seguintes regras de aprovação e navegue até a configuração de aprovação na guia **Configurações** de aprovação: • *Vulnerable item field change request* para um item vulnerável. • *Vulnerability field change request* para uma tarefa de correção. • *Application vulnerability*

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções de aprovador necessárias para várias solicitações de aprovação

Tipo de aprovação	Níveis de aprovação necessários	Funções de aprovador	Informações adicionais
Aprovações de redução de risco	Dois	• É necessário um aprovador no grupo Aprovador - Nível 1 • É necessário um aprovador no grupo Aprovador - Nível 2	O fluxo de aprovação para redução de risco é o mesmo que as aprovações de exceção (adiamentos).

Consulte Vulnerability Response personas e funções granulares e Atribua as funções de persona Vulnerability Response usando o Assistente de configuração para obter mais informações sobre como atribuir funções de persona a usuários e usuários a grupos.

Nota:
Adicione usuários aos grupos de aprovação antes de enviar solicitações de aprovação. Se você criar solicitações antes de adicionar usuários aos grupos de aprovação, as solicitações podem não ficar visíveis para os usuários que têm a permissão de aprovação.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Espaço para gerentes de vulnerabilidades**.
   Se um aprovador não tiver acesso ao espaço, as aprovações poderão ser processadas em **Vulnerability Response** > **Minhas aprovações** no ambiente clássico.
2. Selecione o ícone de exibição de lista (de exibição de lista).
   A página Lista é exibida.
3. Na lista filtrada de Aprovações, selecione **Atribuído a mim**.
4. Localize uma solicitação que você deseja processar e selecione o link na coluna Estado.
   O registro de aprovação de mudança de estado de vulnerabilidade (VCA#) é exibido.
5. Escolha uma das opções a seguir para aprovar ou rejeitar a solicitação.

Configurar notificações por e-mail nos espaços Vulnerability Response

Identifique usuários para lembretes de e-mail automáticos enviados a usuários no grupo de usuários do responsável pela correção.

Antes de Iniciar

Função necessária: administrador

Este recurso gera automaticamente um resumo de e-mail para usuários no grupo de usuários do Proprietário da correção. Adicione os usuários que você deseja que recebam notificações por e-mail, conforme descrito em Use o resumo de e-mail nos Espaços do Vulnerability Response.

Verifique se os usuários têm um endereço de e-mail ativo inserido no registro do usuário e se você os adicionou ao grupo de usuários do responsável pela correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você quiser mudar a frequência de entrega, o dia ou a hora dos e-mails, ou desativar o recurso, siga estas etapas.

Procedimento

1. Navegar até **Todos** > **Trabalhos programados**.
2. Localize **Gerar resumo de correção** e clique nele para abrir o registro.

   Você pode preferir deixar os campos em suas configurações padrão até verificar se as notificações estão sendo enviadas. Por padrão, os e-mails são enviados semanalmente nas manhãs de segunda-feira às 9h no fuso horário da instância que está executando o trabalho.

3. Modifique os campos no formulário.
   Para obter mais informações sobre os campos de formulário, consulteGerar campos de formulário de resumo de correção.
4. Clique em **Atualizar**.

O que Fazer Depois

Caso você tenha verificado que todas as informações listadas anteriormente estão corretas e se você tiver usuários no grupo de usuários Proprietário da correção, mas os e-mails não forem enviados conforme o esperado, verifique se há canais ativados para receber notificações por e-mail. Consulte Create notification channels .

Informações de referência do Vulnerability Manager Workspace

Os tópicos a seguir fornecem links, informações de referência, além de dados de campo nos formulários e registros encontrados no espaço do Vulnerability Manager.

Criar campos de formulário de tópico de observação

A tabela a seguir descreve os campos no formulário Criar tópico de observação no Vulnerability Manager Workspace.

Campo	Descrição
Nome	Nome do tópico de observação, por exemplo, IVs críticos.
Pertence a	O nome do usuário que possui o tópico de observação.
Ordem de exibição	Insira um valor entre 100 e 1000. 100 é o valor padrão. Valores menores que começam com 100 são exibidos em ordem crescente nas listas.
Grupo responsável	O nome do grupo que possui o tópico de observação.
Ativo	Ativar ou desativar o tópico de observação. O padrão é selecionado (Ativo).
Lista de observação	Adicione nomes de usuários que recebem notificações e podem exibir o tópico de observação.
Descrição	Texto que descreve o tópico de observação. Este texto é exibido no campo Descrição ao criar um esforço de correção a partir deste tópico de observação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Categoria	Tipo de registro para o qual o tópico de observação está sendo criado. **Nota:** O campo **Categoria** aparece a partir da versão 18.0.
Visualização	Clique em **Visualizar** para ver uma lista de quantos registros suas condições de filtro retornam. **Nota:** A partir da versão 18.0, o botão **Visualizar** não está disponível.

Tópicos relacionados

Criar um tópico de observação no Vulnerability Manager Workspace

Gerar campos de formulário de resumo de correção

A tabela a seguir mostra os campos no formulário Gerar resumo de correção.

Gerar campos de resumo de correção

Campo	Descrição
Caixa de seleção ativa	Essa caixa de seleção está ativada por padrão. Se você não quiser enviar notificações por e-mail, desative este campo.
Executar	Semanalmente é o padrão. Escolha uma opção na lista.
Dia	Segunda-feira é o padrão. Escolha uma opção na lista.
Hora	Defina um horário para entregar os e-mails. Selecione um fuso horário se quiser um fuso horário diferente do usado pela instância que executa o trabalho.

Impacto dos controles de remuneração na pontuação de risco e na data de vencimento

A partir da v20.0 do Vulnerability Response, como Proprietário de correção, você pode solicitar a redução de risco de um item vulnerável de host ou tarefa de correção, e os aprovadores podem aprovar as solicitações de redução de risco.

Para obter mais informações sobre como solicitar a redução de risco e aprovar a aprovação de redução de risco, consulte Solicitar redução de risco no Espaço de correção de problemas de TI e Aprovar solicitações no Vulnerability Manager Workspace respectivamente.

Quando você aprova uma solicitação de redução de risco, a pontuação de risco é reduzida de acordo com o **Valor desejado** (classificação de risco) na aprovação de mudança de estado (VCA#). A pontuação de risco mais alta da classificação de risco desejada é atribuída ao registro quando sua solicitação de redução de risco é aprovada. O exemplo a seguir mostra como a Pontuação de risco e a Pontuação de risco original são atualizadas quando os controles de compensação são aplicados. As pontuações de risco mais altas padrão das classificações de risco são usadas no exemplo a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Impacto dos controles de compensação na pontuação de risco e na pontuação de risco original

Cenário	Pontuação de risco	Pontuação de risco	Pontuação de risco original (pontuação de risco calculado)
Dados anteriores à v20.0	2 - Alta	80	O campo não está disponível antes da v20.0.
Depois de atualizar para v20.0	2 - Alta	80	Nulo
A pontuação de risco calculado muda para 90 durante a ingestão	1 - Crítica	90	Nulo
Quando você aplica controles de compensação	3 – Médio	69	90
A pontuação de risco calculado muda para 70 durante a ingestão	3 – Médio	69	70
A pontuação de risco calculado muda para 50 durante a ingestão	3 – Médio	50	50
A pontuação de risco calculado muda para 80 durante a ingestão	3 – Médio	50	80
Quando os controles de compensação expiram em **Até a data para redução de risco**	2 - Alta	80	Nulo

Impacto dos controles de compensação em uma tarefa de correção

Quando sua solicitação de redução de risco é aprovada para uma tarefa de correção, o impacto dos controles de compensação em seus itens vulneráveis é o seguinte:

- Os controles de compensação aplicados na tarefa de correção são aplicados aos itens vulneráveis (exceto aqueles no estado Encerrado) que têm pontuação de risco maior do que a pontuação de risco correspondente ao **valor desejado** na aprovação de mudança de estado de uma tarefa de correção. E a pontuação de risco desses itens vulneráveis é reduzida de acordo com o **valor desejado**.
- A **data Até para redução de risco** permanece inalterada para os itens vulneráveis aos quais um controle de compensação já foi aplicado. Ele não é atualizado com a **data Até para redução de risco** da Tarefa de correção.
- A **data Até da redução de risco** é transferida para os itens vulneráveis somente quando um controle compensatório não é aplicado a nenhum item vulnerável anteriormente. Se você aplicar os controles compensatórios na tarefa de correção novamente, a **data Até**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

para redução de risco não será revertida para os itens vulneráveis, já que a **data Até existente para redução de risco** dos itens vulneráveis terá prioridade.

- Quando um novo item vulnerável é adicionado a uma tarefa de correção na qual os controles compensatórios já estão aplicados, o risco não é transferido para os itens vulneráveis.

Impacto de um controle de compensação em um item vulnerável

Quando sua solicitação de redução de risco é aprovada para um item vulnerável:

- Its nova pontuação de risco é exibida no campo **Pontuação de risco** e a pontuação de risco antiga (pontuação de risco calculada) é movida para o campo **Pontuação de risco original**. Esta mudança é válida até a data especificada no campo **Até a data para redução de risco**.
- Quando um item vulneráveltem controles de compensação já aplicados, durante a ingestão:
  - Se a pontuação de risco calculada for maior do que a pontuação de risco, a pontuação de risco permanecerá a mesma e a pontuação de risco original será atualizada com a pontuação de risco calculada.
  - Se a pontuação de risco calculada for menor do que a pontuação de risco, a pontuação de risco e a pontuação de risco original serão atualizadas com a pontuação de risco calculada.
- Se um item de configuração(IC) for alterado para um item vulnerável com o controle de compensação já aplicado:
  - o IC é atualizado para um item vulnerável por padrão, já que a propriedade do sistema `sn_sec_cmn.update_on_ci_change` é definida como verdadeiro.

    Os controles de compensação ainda serão aplicáveis ao item vulnerável.
  - o item vulnerável será encerrado e um novo VIT será criado se a propriedade do sistema `sn_sec_cmn.update_on_ci_change` estiver definida como falsa.

    Os controles de compensação ainda serão aplicáveis ao novo item vulnerável e o **Até a datapara redução de risco**, **Pontuação de risco original e Pontuação** de **risco** permanecem as mesmas.
- Quando um item vulnerável é reaberto pelo scanner e os controles de compensação já estão aplicados a ele, o mesmo controle de compensação é aplicado depois que ele é reaberto.

Tópicos relacionados

Noções básicas sobre controles de compensação para redução de risco

Adicionar um controle de compensação à biblioteca

Associar controles de compensação com CVEs ou TPEs para solicitações de redução de risco

Desabilitar ou habilitar a redução de risco para um CVE ou TPE

#unique_1317_Connect_42_li-risk-reduction-vmws

Espaço de correção de problemas de TI

As equipes de TI exibem tarefas e informações centradas em TI, como soluções e itens de configuração afetados. As equipes de TI podem economizar tempo na resolução de

Tradução automática

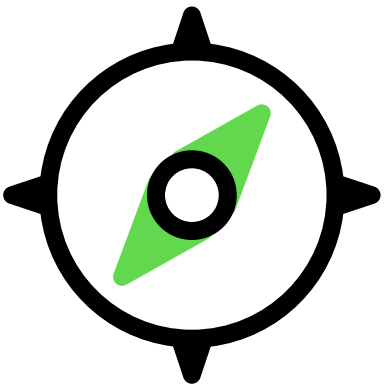
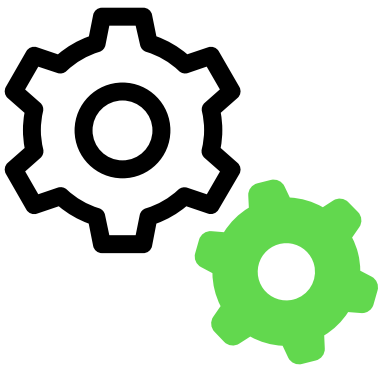
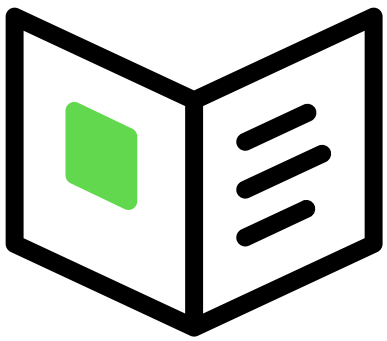
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidades criando facilmente solicitações de mudança, verificando novamente itens vulneráveis e enviando solicitações de exceção a partir do espaço de correção de TI.

Visão geral

v18.0 Demonstração do espaço de correção de TI

Iniciar

Explorar	Corrigir	Referência
		
Saiba mais sobre o Espaço de correção de TI	Saiba como corrigir vulnerabilidades e configurações incorretas no Espaço de correção de TI	Saiba mais sobre as informações adicionais necessárias para usar o Espaço de correção de TI

Solucionar problemas e obter ajuda

- Security Operations na Comunidade da ServiceNow
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Explorando o Espaço de correção de problemas de TI

O Espaço de correção de problemas de TI é destinado a responsáveis pela correção de TI e grupos de TI. Ela é composta por exibições iniciais e de lista, bem como visualizações de dados nas quais você pode clicar que permitem ver as tarefas de correção que foram atribuídas a você e quantos registros atribuídos a você têm soluções.

Função necessária: sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A partir da v19.0 de Vulnerability Response, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

O Espaço de correção de problemas de TI consiste nas seguintes páginas principais, listas e formulários:

Página principal (Inicial)

A página inicial consiste em uma lista de tarefas de correção atribuídas a você e quais registros atribuídos a você têm soluções.

Você pode clicar em uma tarefa de correção para exibir os detalhes e iniciar uma investigação. Na exibição Listas, você pode exibir os Esforços de correção, as Tarefas de correção, os Itens vulneráveis, os Resultados de testes de configuração e assim por diante. Você pode abrir uma tarefa de correção e clicar em **Atribuir a mim** para atribuir a tarefa a você e iniciar a investigação.

Nota:
Se você não atribuir a tarefa a si mesmo na tarefa de correção, não poderá exibir nenhuma ação de IU no nível de item vulnerável.

Clique nas reticências Mais ações e em **Iniciar investigação** para resolver uma tarefa de correção.

Um cartão de pontuação adicional, **ICs vulneráveis**, é exibido na exibição inicial. A visualização de dados de ICs vulneráveis mostra os itens de configuração que têm IVs atribuídos a você ou seus grupos. Para obter mais informações, consulte Exibir itens de configuração com vulnerabilidades no Espaço de correção de problemas de TI.

A página exibida inclui as seguintes informações:

- Tarefas de correção ativas atribuídas a você.
- Registros atribuídos a você que têm soluções preferenciais.
- A lista de tarefas de correção atribuídas a você.

Para obter mais informações sobre o que você pode fazer nesta página, consulte Usar registros de tarefa de correção no Espaço de correção de problemas de TI.

Página Painéis

A página de painéis consiste no painel de correção de vulnerabilidade. Para obter mais informações sobre a página Painéis, consulte Visão geral dos painéis.

Página de lista

Essa exibição consiste em páginas de lista padrão e personalizadas para tarefas de correção, itens vulneráveis, soluções e solicitações de exceções atribuídas a você.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Listas: listas padrão de Tarefas de correção, Itens vulneráveis de host, Itens vulneráveis de aplicação, Itens vulneráveis de contêiner e Resultados de testes de configuração, atribuídos a você e seu grupo, Soluções e Solicitações de exceção.
- Minhas Listas - Esta exibição mostra todas as listas que você renomeou na página principal Lista e todas as listas que você criou.

A exibição de lista é exibida com links para trabalhos atribuídos a você e seus grupos, itens vulneráveis atribuídos a você e seus grupos, soluções e suas solicitações de exceção.

Você também pode criar suas próprias listas para ajudá-lo a monitorar o andamento da correção.

As listas de **ICs vulneráveis** são exibidas na exibição de lista. A lista de Soluções será exibida se a aplicação Vulnerability Solution Management estiver instalada. Este cartão mostra dados de solução, soluções potenciais e preferenciais de fornecedores terceirizados sobre seus itens vulneráveis.

Para obter mais informações sobre o que você pode fazer nesta página, consulte Use a exibição de lista no Espaço de correção de problemas de TI.

Exibir um exemplo de fluxo de trabalho no Espaço de correção de problemas de TI

Exiba um exemplo de um fluxo de trabalho de ponta a ponta no Espaço de correção de problemas de TI. Veja como os especialistas de TI podem usar o espaço para monitorar itens vulneráveis críticos e corrigir as vulnerabilidades atribuídas a eles.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner

Procedimento

Clique na imagem a seguir para exibir as etapas do fluxo de trabalho.
Demonstração do espaço de correção de TI

A imagem inclui as seguintes tarefas:

- Na página inicial (página principal do responsável pela correção de TI), exiba as tarefas de correção atribuídas a você. Alterne entre o trabalho atribuído a você e ao seu grupo. Consulte as tarefas de correção que têm soluções.
- Clique na exibição de **lista** para ver as listas do seu trabalho atribuído.
- Na exibição de lista com a lista **Atribuído ao meu grupo** selecionada, identifique e atribua o trabalho a você.
- Em um registro de tarefa de correção em aberto:
  - Clique na guia **Visão geral** para ver os itens vulneráveis (IVs) e os itens de configuração (ICs) afetados que estão associados ao registro.
  - Clique na guia **Soluções** para ver as soluções preferenciais e possíveis.
  - Clique na guia **Detalhes** para modificar os campos editáveis.
  - Clique nas ações de IU: **Marcar como falso positivo**, **Criar mudança**, **Dividir tarefa**, **Solicitar exceção**. Siga as instruções nas caixas de diálogo para ajudá-lo na correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral dos painéis

A página Painéis no Espaço de correção de problemas de TI fornece o painel Correção de vulnerabilidade na IU Next Experience, que pode ser usado para se concentrar nas tarefas de correção e nos itens vulneráveis.

Função necessária: sn_vul.remediation_owner

Você pode exibir o painel de Correção de vulnerabilidades navegando até **Espaços** > **Espaço de correção de TI** e selecionando o ícone Painéis. Para obter mais informações sobre o painel Vulnerability Remediation, consulte Usando os painéis padrão Vulnerability Response.

Você pode criar um painel personalizado selecionando o ícone Mais opções e selecionando **Criar novo painel**.

Usando o Espaço de correção de problemas de TI

O Espaço de correção de TI fornece uma lista consolidada de vulnerabilidades de host, vulnerabilidades de aplicação, vulnerabilidades de contêiner e configurações incorretas que são atribuídas a você e seu grupo. Você pode usar este espaço para corrigir e solicitar exceções para vulnerabilidades e configurações incorretas.

Use o resumo de e-mail nos Espaços do Vulnerability Response

Use notificações por e-mail para exibir o andamento da correção e lembrá-lo quando as tarefas estiverem se aproximando ou o ANS tiver passado.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa

Como proprietário de correção, entre em sua área de trabalho e veja sua notificação por e-mail como um resumo do seu trabalho. Veja o que você realizou, o que está se aproximando e o que está atrasado. Use a notificação para ajudá-lo a organizar e priorizar suas ações de correção críticas. Clique em um link no e-mail para acessar diretamente o seu espaço. As notificações podem ajudar os especialistas de TI com o status instantâneo de seu trabalho. Como gerente de vulnerabilidade, ajude seus especialistas de TI a entrar na plataforma diretamente do serviço de e-mail para tarefas de correção.

Consulte Configurar notificações por e-mail nos espaços Vulnerability Response para obter mais informações sobre como configurar este recurso.

Por padrão, o e-mail mostra as tarefas que você encerrou, o total de tarefas ativas atribuídas a você e seus grupos, recém-atribuídas, VITs encerradas e outras informações.

Procedimento

1. Navegue até o seu e-mail, localize uma notificação e clique para abri-la.
   A notificação é exibida com informações sobre seu status de trabalho.
2. Clique **em Ir para o espaço** para navegar até sua área de trabalho.

Usar registros no Espaço de correção de problemas de TI

Use registros para ajudá-lo a exibir o andamento da correção e o impacto dos itens vulneráveis em seus ativos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner

Procedimento
1. Em sua instância Now Platform, navegue até **Todos** > **Vulnerability Response** > **Espaço de correção de TI**.
   A página inicial do é exibida.
2. Navegue até um registro de item vulnerável e abra-o na página inicial ou na exibição de lista.

   A guia de detalhes inclui informações no cabeçalho do formulário na parte superior que estão relacionadas à natureza da vulnerabilidade, por exemplo, CVE-2013-5014 detectado em LINUX-DAL-4331. No cabeçalho do formulário, os valores de Estado, Classificação de risco e Data de destino da correção são exibidos.
3. Consulte a tabela a seguir para obter as ações de IU que você pode executar no registro da tarefa de correção.

Usar registros de tarefa de correção no Espaço de correção de problemas de TI

As tarefas de correção são criadas e atribuídas automaticamente a partir dos esforços de correção. As equipes de TI e os responsáveis pela correção exibem as tarefas de correção no Espaço de correção de problemas de TI.

Antes de Iniciar
Função necessária: sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa
Quando os gerentes e analistas de vulnerabilidade criam esforços de correção para orientar a correção, as tarefas de correção são criadas automaticamente e atribuídas às equipes de TI com base no grupo que está associado aos registros em um esforço de correção.

Veja os ICs vulneráveis atribuídos a você e seus grupos que têm vulnerabilidades na guia **ICs vulneráveis** ou na lista de ICs vulneráveis atribuídos a você e seu grupo na exibição Lista.

Procedimento
1. Em sua instância Now Platform, navegue até **Vulnerability Response** > **Espaço de correção de TI**.
   A página inicial do é exibida.
2. Na seção Tarefas de correção, clique em um registro de tarefa de correção (VUL) para abri-lo.
3. **Opcional:** Como alternativa, você pode clicar no ícone Lista no canto superior esquerdo da página inicial para ver todas as tarefas de correção e registros (trabalho) atribuídos a você e seus grupos.
   Para obter mais informações sobre como usar a exibição de lista, consulte Use a exibição de lista no Espaço de correção de problemas de TI.
4. Na página inicial ou na exibição de lista, clique em um registro de tarefa de correção (VUL) para abri-lo.

   A imagem a seguir mostra as seções de um registro de tarefa de correção e os dados disponíveis.

   Entre as guias **Soluções** e **Solicitações de mudança** nas guias da lista relacionada mostradas na imagem a seguir, você pode clicar na guia **Detalhes** para atualizar algumas das informações no registro, como o grupo de atribuição, por exemplo. Clique em **Salvar** para aplicar suas mudanças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A guia de detalhes inclui informações no cabeçalho do formulário na parte superior que estão relacionadas à natureza da tarefa, por exemplo, Vulnerabilidades nos servidores XYZ (San Diego). No cabeçalho do formulário, são exibidos os valores de Estado, Classificação de risco, Grupo de atribuição, Status da correção e o percentual de registros ativos que você corrigiu.

5. Consulte a tabela a seguir para obter as ações de IU que você pode executar a partir do registro da tarefa de correção.

   A guia Soluções mostra informações da solução preferencial e potencial que melhor corresponde à vulnerabilidade associada ao registro da tarefa. Soluções são patches que suas equipes de TI aplicam para resolver vulnerabilidades.

   Se a aplicação Vulnerability Solution Management estiver instalada, as *Soluções preferenciais* serão as soluções de substituição mais altas aplicadas a registros. A lista de soluções é baseada nos registros na tarefa de correção.

   Para exibir as soluções, no registro da tarefa de correção, navegue até **Soluções** > **Soluções preferenciais**.

   Possíveis soluções. Todas as soluções disponíveis para IVs nesta tarefa. Navegar até **Soluções** > **Soluções potenciais**.

   Você pode exibir os ICs (ativos) afetados por esta vulnerabilidade no registro da tarefa de correção, navegando até **Visão geral** > **ICs afetados**.

Use a exibição de lista no Espaço de correção de problemas de TI

Com a exibição de lista no Espaço de correção de problemas de TI, você pode exibir tarefas de correção e registros atribuídos a você e seus grupos. Você também pode rastrear suas solicitações de exceção e falso-positivo para tarefas de correção e itens vulneráveis e exibir soluções.

Antes de Iniciar
Função necessária: sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Espaço de correção de TI**.
2. Clique no ícone Lista.
   A exibição de lista é exibida.
   - Clique em uma lista filtrada para exibir o número total de tarefas de correção ativas ou registros atribuídos a você ou seu grupo. Consulte Usar registros de tarefa de correção no Espaço de correção de problemas de TI para obter mais informações sobre o que você pode fazer com esses registros.
   - Exiba o número total de IVs atribuídos a você ou seus grupos que têm soluções. Clique no cartão **Soluções preferenciais em IVs** para exibir a lista.
   - Veja os ICs vulneráveis atribuídos a você e seus grupos que têm vulnerabilidades na guia **ICs vulneráveis** ou na lista de ICs vulneráveis atribuídos a você e seu grupo na exibição Lista.
3. **Opcional:** Clique **em Minhas listas**.

   (Optional) Para criar uma nova lista, siga estas etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. No canto inferior esquerdo da página, clique em **Nova lista**.

b. No modal Nova lista, clique em **Iniciar a partir de existente** e pesquise na lista de seleção Lista uma lista existente para usar como modelo.

c. Edite o Nome da Lista.

d. Adicionar filtros.
Por exemplo, você pode criar uma lista de itens vulneráveis ativos para um scanner específico que deseja monitorar. Por exemplo, você pode usar os filtros: Ativo é verdadeiroe Origem contém (nome do scanner).

e. Edite as colunas que você deseja exibir na lista.

f. Clique em **Criar**.
Sua nova lista será exibida.

g. Como alternativa, clique em **Criar seu próprio**, insira um nome e, em seguida, em **Selecionar origem**.

h. Comece a digitar no campo e selecione uma das fontes exibidas para sua nova lista.

i. Clique em **Criar**.
Sua nova lista será exibida.

Nota:
Se você sair do módulo de lista, a lista exibida ao sair será a lista que você vê ao retornar. Para excluir as listas personalizadas que você cria, com a lista exibida, à direita do painel, clique no ícone de engrenagem.

4. Consulte a tabela a seguir para saber o que você pode fazer na exibição de lista.

Atribuir uma tarefa de correção a si mesmo no Espaço de correção de problemas de TI

Em um registro de tarefa de correção, atribua o registro a você mesmo no espaço Vulnerability Response.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner

Esta opção está disponível somente em registros de tarefa de correção que ainda não foram atribuídos a você.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Espaço de correção de TI** > **Exibição em lista** > **Trabalho do Meu Grupo**.
2. Clique em uma tarefa de correção (VUL#) para abri-la.
3. Nos botões de ação de IU à direita, clique em **Atribuir a mim**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A tarefa de correção é exibida na lista Meu trabalho em Tarefas de correção na exibição de lista.

4. Você também pode atribuir registros a si mesmo seguindo as mesmas etapas de registros abertos.
   O botão **Atribuir a mim** só estará disponível se o registro ainda não estiver atribuído a você.

Exibir itens de configuração com vulnerabilidades no Espaço de correção de problemas de TI

Os aprimoramentos a seguir foram adicionados às tarefas de correção com a versão 16.1 da aplicação Vulnerability Response.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_owner ou sn_vulc.remediation_owner. A função itil ou cmdb_read também será necessária se você quiser exibir dados de IC nos espaços.

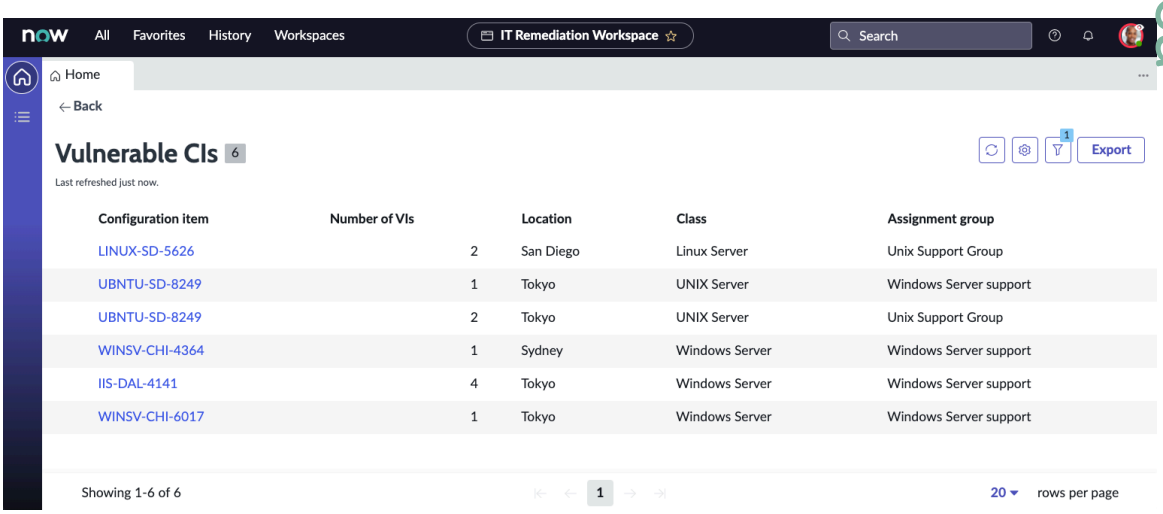
Por Que e Quando Desempenhar Esta Tarefa

Veja os itens de configuração (IC) atribuídos a você que têm vulnerabilidades. Clique em Cartão de pontuação de **ICs vulneráveis**. Clique na lista Filtrar no canto superior esquerdo para alternar entre **Atribuído a mim** e **Atribuído aos meus grupos**. Na exibição de lista, clique nos links.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Espaço de correção de TI**.
   A página inicial do é exibida.
2. Como alternativa, você pode exibir essas listas nos links na exibição de lista ou navegando até seus módulos, por exemplo, **Todos** > **Vulnerability Response** > **Tarefas de correção**.
3. Escolha um para continuar.
   Dependendo do que for selecionado na alternância de filtro, exiba as listas dos seguintes registros atribuídos a você ou a você e seus grupos.
4. Clique no cartão de pontuação **ICs vulneráveis**.

   A lista de registros de IC é exibida.



5. Clique em um item de configuração para abrir seu registro.
   O registro é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As listas relacionadas permitem que você exiba detalhes e vários registros associados. Os novos dados disponíveis neste registro com esta versão incluem:

- Uma linha do tempo que mostra a atividade recente neste registro.
- Todas as solicitações de mudança associadas a este IC.
- Navegue facilmente pelos cartões de pontuação e exiba as tarefas de correção, itens vulneráveis e soluções preferenciais associadas a este IC.
- A partir de 18.0 , você pode navegar até os cartões de pontuação e exibir os patches preferenciais associados a este IC. Patches preferenciais são os patches associados aos itens vulneráveis. A guia Patches na lista relacionada exibe os patches instalados e ausentes para os ICs.
- Informações sobre o IC que incluem classe, local, acesso à Internet, ambiente e programação de manutenção.

Solicitar um falso-positivo no Espaço de correção de problemas de TI

Em um registro de tarefa de correção, marque um falso positivo no espaço Vulnerability Response.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner, sn_vul.app_security_campion ou sn_vul_container.remediation_owner

Um falso positivo é uma condição em que o scanner relata que existe uma vulnerabilidade no sistema, mas, na realidade, não há nenhuma vulnerabilidade. Pode haver vários motivos, como classificação incorreta, lógica ou algoritmo inadequado no scanner. Um proprietário de correção pode enviar uma solicitação de aprovação para falsos positivos de itens vulneráveis (IVs) ou registros de tarefas de correção (RTs).

A partir da versão 18.0, você pode solicitar exceções para itens de vulnerabilidade da aplicação e itens de vulnerabilidade de contêiner.

Para obter mais informações sobre falsos positivos no ambiente clássico na aplicação Vulnerability Response, consulte Falso-positivo visão geral.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Espaço de correção de TI**.
2. Localize uma tarefa de correção ou itens vulneráveis que você deseja marcar como falso-positivo.
3. Nos botões de ação de IU à direita, clique em **Marcar como falso-positivo**.
4. Na caixa de diálogo exibida, insira as informações sobre a solicitação e clique em **Solicitar aprovação**.
5. No modal Responder ao questionário, responda às perguntas e clique em **Enviar**.

Nota:
A partir da versão 18.0, você pode responder ao questionário para fornecer informações adicionais sobre sua solicitação para o aprovador. O modal Responder questionário aparece somente quando a caixa de seleção **Habilitar questionário para marcar como falso-positivo** está marcada no formulário Configuração de gestão de exceções. Para obter mais informações, consulte Configurar Gestão de exceções para Vulnerability Response.

Sua solicitação foi enviada para aprovação. Uma mensagem será exibida indicando que a solicitação foi enviada com sucesso. Uma solicitação de falso positivo para um item vulnerável ou uma tarefa de correção requer apenas um único aprovador.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para exibir o status das solicitações de aprovação no Espaço de correção de TI, em Solicitações de exceção na página Lista, clique em **Minhas solicitações**. O número da solicitação (VCA#) é exibido quando você abre o IV ou o registro da tarefa de correção na lista.

Depois que a solicitação é aprovada, o Estado do IV ou o registro da tarefa muda para Encerrado. Os IVs ativos em registros de tarefa marcados como falso-positivos também são fechados.

Se a solicitação for rejeitada:

- O estado não muda no IV ou no registro da tarefa. Os IVs ativos permanecem abertos.
- O registro de solicitação (nº do VCA) exibe **Rejeitado** na coluna Estado de aprovação na exibição de lista em Minhas solicitações.

Criar uma solicitação de mudança no Espaço de correção de problemas de TI

Em um registro de tarefa de correção, crie uma solicitação de mudança. Como alternativa, adicione uma tarefa de correção a uma solicitação de mudança existente.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_ownerou sn_vulc.admin

Nota:
A função itli será necessária se você quiser enviar solicitações de mudança do Espaço de correção de problemas de TI.

Por Que e Quando Desempenhar Esta Tarefa

Pode haver vários motivos pelos quais você deseja criar uma solicitação de mudança para uma tarefa de correção. Normalmente, é porque sua investigação requer intervenção manual para corrigir as vulnerabilidades.

Para obter mais informações sobre as solicitações de mudança e como criar solicitações de mudança no ambiente clássico, consulte Change Management para Vulnerability Response.

A partir da versão 19.0 do Vulnerability Response, você pode criar solicitações de mudança para Grupos de resultados de testes (TRGs) no Espaço de correção de problemas de TI.

Nota:
A partir da v19.0 de Vulnerability Response, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI**.
2. Localize uma tarefa de correção para a qual você deseja criar uma solicitação de mudança.
3. Nos botões de ação de IU à direita, expanda a lista e escolha um:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Clique **em Criar mudança**
- **Adicionar a uma mudança existente**

4. Para criar uma nova solicitação de mudança, preencha os campos no modal exibido.
   Para obter mais informações sobre os campos de formulário, consulte Criar campos de formulário de solicitação de mudança.
5. Selecione **Criar solicitação de mudança**.
   O registro da tarefa de correção é exibido e uma mensagem indica que a solicitação de mudança foi criada com sucesso.

   Clique no link relacionado Solicitações de mudança em um registro para exibir todas as solicitações de mudança associadas ao registro.

6. Como alternativa, para adicionar esta tarefa de correção a uma solicitação de mudança existente, siga estas etapas.

   a. Clique na seta para baixo para expandir a lista no botão **Criar mudança**.

   b. Selecione **Adicionar à mudança existente**.

   c. No modal exibido, clique no ícone de pesquisa para exibir a lista de solicitações de mudança existentes.

   d. Para adicionar condições à lista para enfocar a lista de solicitações de mudança, no canto superior direito do modal, clique no ícone de filtro (funil).

   e. No novo painel exibido, clique **em Exibição avançada**.

   f. Use o construtor de condição para criar suas condições.

   g. Selecione **Atualizar**.

   h. Na lista, clique em uma solicitação de mudança para selecioná-la.
   Um modal atualizado será exibido com sua escolha.

   i. **Opcional:** No modal, marque a caixa de seleção Adicionar ICs ao CR para adicionar itens de configuração de todos os itens vulneráveis ativos à solicitação de mudança.

   j. Selecione **Adicionar mudança**.
   O registro de correção é exibido e uma mensagem indica que a solicitação de mudança foi criada com sucesso e enviada para aprovação.

   - Clique no link **Exibir mudança** na mensagem para abrir o registro de solicitação de mudança (CHG).
   - Selecione o link do menu do item relacionado a **solicitações de mudança** no registro da tarefa de correção para exibir todas as solicitações de mudança associadas ao registro.

   Como alternativa, no ambiente clássico, navegue até **Autoatendimento** > **Minhas solicitações**. Depois de enviar a mudança e ela ser implementada, se a sincronização de estado estiver habilitada, a tarefa de correção será movida automaticamente para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resolvido. Para obter mais informações sobre estados e sincronização de estado em solicitações de mudança, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção.

Dividir uma tarefa de correção no Espaço de correção de problemas de TI

Em um registro de tarefa de correção, identifique um subconjunto de itens vulneráveis e crie uma nova tarefa de correção para eles.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_owner, ou sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode selecionar itens vulneráveis individuais na lista exibida na guia Itens vulneráveis e movê-los para uma nova tarefa de correção.

Os casos de uso para dividir IVs de tarefas de correção existentes em novas tarefas podem incluir os seguintes exemplos:

- Você deseja criar uma solicitação de mudança ou solicitações de mudança para um grupo de divisão.
- Você deseja reatribuir um grupo de divisão a outro usuário em seu grupo de atribuição.
- Você solicita um adiamento ou exceção para um grupo de divisão porque sabe que algumas vulnerabilidades em itens de configuração (ICs) específicos não podem ser corrigidas até a data de destino.

Para obter mais informações sobre solicitações de mudança e divisão de uma tarefa de correção no ambiente clássico e para versões de Vulnerability Response anteriores à v15.0, consulte Dividir uma tarefa de correção.

A partir da v19.0 de Vulnerability Response, você pode dividir tarefas em grupos de resultados de testes.

Nota:
A partir da v19.0 de Vulnerability Response, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

A partir da versão 18.0, você pode dividir tarefas para itens de vulnerabilidade da aplicação e itens de vulnerabilidade de contêiner.

Procedimento

1. Com uma tarefa de correção exibida, clique na guia **Itens vulneráveis**, se ainda não estiver selecionada.
2. Na lista, selecione os IVs que você deseja mover para uma nova tarefa de correção.
3. Clique **em Dividir tarefa**.
4. Na caixa de diálogo exibida, o número de IVs selecionados na lista é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique **em Dividir tarefa** novamente.
   A mensagem de confirmação a seguir é exibida com um link para a nova tarefa de correção.

   Como alternativa, você pode usar o construtor de condição para filtrar IVs.

6. Localize uma tarefa de correção que você deseja dividir.
7. Nos botões de ação de IU à direita, clique em **Dividir tarefa**.
   Após alguns momentos, o construtor de condição será exibido.
8. No modal exibido, use o construtor de condição para identificar o subconjunto de itens vulneráveis que você deseja a adicionar a uma nova tarefa de correção.
9. Clique **em Dividir tarefa**.
   Se uma mensagem exibir que nenhum item vulnerável corresponde às suas condições, você deverá ajustar seus critérios e clicar em **Dividir tarefa** novamente. Edite o campo de descrição resumida conforme necessário. Este campo pode ajudá-lo a encontrar sua nova tarefa de correção depois que ela é criada.

   Se os IVs corresponderem às suas condições, o número de IVs correspondentes será exibido em uma mensagem, conforme mostrado na imagem anterior.

10. **Opcional:** Clique no link **Visualizar itens** para exibir os IVs que correspondem às condições do filtro.
    A nova tarefa de correção é exibida como uma nova guia na parte superior do registro.

Solicitar uma exceção no Espaço de correção de problemas de TI

Em um registro de tarefa de correção, solicite uma exceção para uma tarefa de correção.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_owner, ou sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Algumas vulnerabilidades podem não ter um patch, correção ou solução existente. Ou você pode determinar que uma tarefa de correção não pode ser resolvida até a data de destino. Quando sua correção não puder estar em conformidade com uma gestão de vulnerabilidades ou política de segurança, padrão ou diretriz publicada, você poderá solicitar uma exceção.

Você pode solicitar exceções para tarefas de correção e itens vulneráveis do Espaço de correção de TI que foram atribuídos a você.

A partir da versão 19.0 do Vulnerability Response, você pode solicitar exceções para os resultados de testes .

Nota:
A partir da v19.0 de Vulnerability Response, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

A partir da versão 18.0, você pode solicitar exceções para itens de vulnerabilidade da aplicação e itens de vulnerabilidade de contêiner.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como solicitar exceções no ambiente clássico, consulte Solicitar uma exceção para uma tarefa de correção.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Espaço de correção de TI**.
2. Localize uma tarefa de correção para a qual você deseja solicitar uma exceção.
3. Nos botões de ação de IU à direita, clique em **Solicitar exceção**.
4. Na caixa de diálogo exibida, preencha a data de término da exceção, selecione um motivo na lista e adicione outras informações necessárias.
5. Clique **em Solicitar exceção**.
6. No modal Responder ao **questionário**, responda às perguntas e clique em **Enviar**.

Nota:
A partir da versão 18.0, você pode responder ao questionário para fornecer informações adicionais sobre sua solicitação para o aprovador. O modal Responder **questionário** aparece somente quando a caixa de seleção **Habilitar questionário para solicitar exceção** está marcada no formulário **Configuração de gestão de exceções**.

Uma mensagem informa que sua solicitação foi enviada com sucesso para aprovação.

Uma solicitação de exceção para uma tarefa de correção é aprovada usando um fluxo de trabalho de aprovação padrão de dois níveis. Depois que a solicitação é aprovada pelo aprovador de nível 1, ela é enviada para o aprovador de nível 2.

- O registro da tarefa de correção ou o IV muda para Em revisão enquanto a solicitação de exceção está aberta.
- O registro da tarefa de correção ou o IV muda para Adiado se a solicitação for aprovada.
- O registro de solicitação de exceção é encerrado depois que sua solicitação de exceção é aprovada.

Para exibir o status de suas solicitações de aprovação, em Solicitações de exceção na página Lista, clique em **Minhas solicitações**. O número da solicitação (#VCA) é exibido quando você abre o IV ou o registro da tarefa de correção na lista.

- Se a solicitação for rejeitada, o registro da solicitação (número do VCA) exibirá **Rejeitado** na coluna Estado de aprovação na exibição de lista em Minhas solicitações.
- Você precisará enviar uma nova solicitação de exceção se ainda quiser adiar este item.

Solicitar uma exceção usando GRC: Policy and Compliance Management no Espaço de correção de problemas de TI

A partir da versão 18.0, você pode solicitar as exceções de política para itens vulneráveis de host (IVs), itens de vulnerabilidade da aplicação (AVITs), tarefas de correção (VULs) e tarefas de correção de aplicação (AVULs) do Espaço de correção de problemas de TI.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner, sn_vul.app_security_campion, sn_vul_container.remediation_owner ou sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

A partir da versão 19.0 do Vulnerability Response, você também pode solicitar exceções de política para grupos de resultados de testes (TRGs), itens de vulnerabilidade de contêiner (CVITs) e suas Tarefas de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A partir da v19.0 de Vulnerability Response, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v19.0	Terminologia v19.0 em diante
Grupos de resultados de testes	Tarefas de correção
Problemas de configuração	Resultados de testes de configuração
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Espaço de correção de TI**.
2. No navegador de aplicações, selecione o ícone de lista (ícone de).
3. Na página Lista, em Itens vulneráveis de host, Itens vulneráveis da aplicação ou Tarefas de correção, selecione o registro para o qual você deseja solicitar uma exceção.
   O registro selecionado deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
4. Selecione o botão **Solicitar exceção**.
5. No formulário, preencha os campos.
   Para obter mais informações sobre os campos de formulário, consulte Solicitar campos do formulário de exceção para exceções de política.
6. Selecione **Exceção de solicitação**.
7. No modal Responder ao questionário, responda às perguntas para fornecer informações adicionais sobre sua solicitação e selecione **Enviar**.

   Nota:
   O modal Responder ao questionário aparece somente quando os detalhes do questionário são adicionados ao respectivo registro de integração.

   Uma mensagem é exibida informando que sua solicitação foi enviada com sucesso para aprovação.

   Para obter mais informações sobre a integração de exceção de política e a transferência entre o proprietário de correção e o gerente de conformidade, consulte Configuração opcional do Policy and Compliance Management .

Tradução automática

Solicitar redução de risco no Espaço de correção de problemas de TI

A partir da v20.0 de Vulnerability Response, você pode solicitar a redução no risco de um item vulnerável de host ou uma tarefa de correção.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa

A partir da v21.0 de Vulnerability Response:

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você pode solicitar a redução de risco para uma tarefa de correção se seus itens de vulnerabilidade estiverem associados a uma mesma entrada de vulnerabilidade comum (CVE) ou entrada de terceiro (TPE) para a qual a redução de risco está habilitada.
- Você não pode solicitar a redução de risco para uma tarefa de correção com itens vulneráveis associados a diferentes CVEs, embora a redução de risco esteja habilitada para CVEs.

Nota:
O recurso de controles de compensação está disponível somente para vulnerabilidades de host.

Procedimento

1. Navegar até **Espaços** > **Espaço de correção de TI**.
2. Na página Lista, abra um item vulnerável de host ou uma tarefa de correção.
3. Selecione o menu de três pontos e selecione **Solicitar exceção**.
4. No pop-up Solicitar exceção, preencha os campos.

Solicitar modal de exceção

Campo	Descrição
Motivo	Motivo da sua solicitação de exceção. Selecione *Controle de mitigação no local* para a solicitação de redução de risco. Para ver como adicionar novas opções de motivo, consulte Definir mapeamento do motivo da política.
Solicitação de adiamento	Difere o registro. Este campo é selecionado por padrão. **Nota:** Este campo aparece somente quando a opção *Controle de mitigação no local* é selecionada no campo **Motivo**.
Solicitação de redução de risco	Permite que você solicite a redução da pontuação de risco. **Nota:** Essa caixa de seleção aparece somente quando a opção *Controle de mitigação no local* está marcada no campo **Motivo**.
Classificação de risco atual	Severidade atual do risco. **Nota:** Este campo é exibido somente quando a caixa de seleção **Solicitação de redução de risco** está marcada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Classificação de risco desejada	Nova classificação de risco que você deseja atribuir ao registro. A pontuação de risco mais alta neste intervalo de classificação de risco é aplicada ao registro quando sua solicitação é aprovada. **Nota:** Este campo é exibido somente quando a caixa de seleção **Solicitação de redução de risco** está marcada.
Selecionar controles de remuneração	Motivo da sua solicitação para reduzir a classificação de risco.
Até	Data em que a solicitação de adiamento ou redução de risco expira. Quando a solicitação de exceção expira: ○ O registro será revertido para o estado Aberto. ○ Os controles de compensação expiram. ○ A pontuação calculada substituirá uma pontuação reduzida.
Observações de justificativas	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita.

5. Selecione **Exceção de solicitação**.
6. No modal Responder ao questionário, responda às perguntas para fornecer informações adicionais sobre sua solicitação e selecione **Enviar**.

   Nota:
   O modal Responder ao questionário aparece somente quando o questionário está habilitado para gerenciamento de exceções. Para obter mais informações, consulte Configurar Gestão de exceções para Vulnerability Response.

   Uma mensagem será exibida informando que sua solicitação foi enviada com sucesso para aprovação. Uma notificação é enviada ao aprovador sobre sua solicitação.

   ○ Se você solicitar um adiamento e redução de risco:
   - Duas aprovações de mudança de estado (VCA#) são criadas para adiamento e redução de risco.
   - O estado do registro muda para Em revisão.

   ○ Se você solicitar somente a redução de risco:
   - Uma aprovação de mudança de estado (VCA#) é criada.
   - O estado não muda.

   Na aprovação ou rejeição da sua solicitação, você receberá uma notificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como a **data Até da redução de risco** é atualizada para uma tarefa de correção e item vulnerável quando uma solicitação de redução de risco é aprovada, consulte Impacto dos controles de remuneração na pontuação de risco e na data de vencimento.

O que Fazer Depois

Você receberá uma notificação quando sua solicitação for aprovada ou rejeitada pelo aprovador. Para obter mais informações sobre o processo de aprovação, consulte Aprovar solicitações no Vulnerability Manager Workspace.

Tópicos relacionados

Noções básicas sobre controles de compensação para redução de risco

Desabilitar ou habilitar a redução de risco para um CVE ou TPE

Adicionar um controle de compensação à biblioteca

Impacto dos controles de remuneração na pontuação de risco e na data de vencimento

Verifique novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Inicie novas verificações de Espaço de correção de problemas de TI em seu Now Platform sob demanda.

As novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

A nova verificação é compatível com as seguintes integrações no Espaço de correção de problemas de TI. Consulte os seguintes tópicos para obter mais informações:

- Verificar novamente Qualys itens vulneráveis dos Vulnerability Response espaços
- Verificar novamente Rapid7 itens vulneráveis dos Vulnerability Response espaços
- Verificar novamente Tenable.io e Tenable.sc itens vulneráveis dos espaços Vulnerability Response

Funções necessárias: sn_vul.remediation_owner para Espaço de correção de problemas de TI.

Verificar novamente Qualys itens vulneráveis dos Vulnerability Response espaços

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Inicie novas verificações no produto Qualys sob demanda de Espaço de correção de problemas de TI em sua instância Now Platform.

Antes de Iniciar

Para iniciar uma nova verificação do produto Qualys no ambiente clássico, consulte Iniciar nova verificação para Qualys Vulnerability Integration.

Os scanners Qualys são desativados por padrão na aplicação Vulnerability Response. Se você tentar executar uma nova verificação a partir dos itens vulneráveis ou das tarefas de correção que têm essas aplicações como origem, o botão **Verificar novamente** não estará disponível.

Para ativar esses scanners, como um usuário com a função sn_vul.vulnerability_admin:

1. Navegar até **Todos** > **Vulnerability Response** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o scanner que você deseja ativar e clique no registro para abri-lo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Marque a caixa de seleção Ativo.
4. Clique em **Atualizar**.

   O produto que você ativou é exibido no campo Origem no item vulnerável e nos registros de tarefa de correção após a próxima importação, e a **opção Nova verificação** está disponível como uma ação de IU.

Para obter mais informações sobre como configurar o scanner Qualys, consulte Configurar dispositivos scanner e Configurações e modificações avançadas do Qualys.

- Você pode iniciar novas verificações sob demanda para itens vulneráveis e tarefas de correção que tenham o produto Qualys como origem de Espaço de correção de problemas de TI em seu Now Platform.
- Em um registro de tarefa de correção, o registro pode estar em qualquer estado diferente de **Encerrado**e todos os IVs associados devem ser do produto Qualys.
- Para iniciar novas verificações no espaço de correção de TI a partir de itens vulneráveis e registros de tarefa de correção, esses registros devem ser atribuídos a você.

Funções necessárias:

- sn_vul.remediation_owner para Espaço de correção de problemas de TI.
- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin do Vulnerability Manager Workspace.

Procedimento

1. Navegue até um item vulnerável ou uma tarefa de correção que foi atribuída a você e abra-o.

   Nota:
   Se você escolher um esforço de correção para iniciar uma nova verificação, todos os IVs associados a esse registro serão verificados.

2. No canto superior direito do registro, clique em **Verificar novamente**.
3. No modal Verificar novamente, escolha um perfil de opção.
   Um perfil de opção é necessário ao iniciar uma verificação de [Qualys de seu Now Platform®. Os perfis de opção contêm Qualys configurações de verificação.
4. No modal Nova verificação, clique em **Solicitar nova verificação**.
   A mensagem A solicitação de verificação está sendo processada é exibida.
5. Clique no link **Exibir status** na mensagem para exibir o andamento da verificação.

   O registro de verificação (VSCAN#) é exibido. Abaixo do cabeçalho do registro com o número da verificação, as listas de itens relacionados exibem as seguintes informações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A lista Detalhes exibe o número da verificação primária, a origem do scanner e o estado. Exiba verificações concluídas e com falha na seção Resumo da verificação.
- A lista Verificações exibe todas as verificações secundárias e seus estados. Quando todas as verificações secundárias forem concluídas, o estado da verificação primária mudará para Concluído.
- A lista Origem exibe o item vulnerável usado para a verificação, o item de configuração e a vulnerabilidade associados, o estado do IV e seu status de correção.

Sua instância Now Platform® rastreia o status de nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro.

O tempo limite não interrompe a verificação. O tempo limite se refere a quando Now Platform® parou de acompanhar seu status de nova verificação, não quando a nova verificação real parou.

Todos os IVs que fizeram a transição ou farão a transição para Encerrado/Corrigido são importados com a próxima importação programada das integrações Qualys.

Verificar novamente Rapid7 itens vulneráveis dos Vulnerability Response espaços

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Inicie novas verificações no produto Rapid7 sob demanda do Espaço de correção de TI em sua instância Now Platform.

Antes de Iniciar

Para iniciar uma nova verificação do produto no ambiente clássico, consulte Iniciar nova verificação para a integração de vulnerabilidade Rapid7. Este tópico também inclui informações sobre como programar verificações com os parâmetros de integração na instância de integração Rapid7.

Os scanners Rapid7 são desativados por padrão na aplicação Vulnerability Response. Se você tentar executar uma nova verificação dos itens vulneráveis ou das tarefas de correção que têm a aplicação Rapid7 como origem, o botão **Verificar novamente** não estará disponível.

Para ativar esses scanners, como um usuário com a função sn_vul.vulnerability_admin:

1. Navegar até **Todos** > **Vulnerability Response** > **Verificação de Vulnerabilidades** > **Scanners**.
2. Localize o scanner que você deseja ativar e clique no registro para abri-lo.
3. Marque a caixa de seleção Ativo.
4. Clique em **Atualizar**.

   O produto que você ativou é exibido no campo Origem no item vulnerável e nos registros de tarefa de correção após a próxima importação, e a **opção Nova verificação** está disponível como uma ação de IU.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Você pode iniciar novas verificações sob demanda para itens vulneráveis e tarefas de correção que tenham o produto Rapid7 InsightVM como origem do espaço de correção de TI em seu Now Platform.
- Em um registro de tarefa de correção, o registro pode estar em qualquer estado diferente de **Encerrado**e todos os IVs associados devem ser do produto Rapid7.
- Para iniciar novas verificações no espaço de correção de TI a partir de itens vulneráveis e registros de tarefa de correção, esses registros precisam ser atribuídos a você.

Funções necessárias: sn_vul.remediation_owner para o espaço de correção de TI

sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin do Vulnerability Manager Workspace

Procedimento

1. Navegue até um item vulnerável ou uma tarefa de correção que foi atribuída a você e abra-o.

   Nota:
   Se você escolher um esforço de correção para iniciar uma nova verificação, todos os IVs associados a esse registro serão verificados.

2. No canto superior direito do registro, clique em **Verificar novamente**.
3. No modal Confirmar nova verificação, clique em **Solicitar nova verificação**.
   A mensagem A solicitação de verificação está sendo processada é exibida.
4. Clique no link **Exibir status** na mensagem para exibir o andamento da verificação.

   O registro de verificação (VSCAN#) é exibido. Abaixo do cabeçalho do registro com o número da verificação, as listas de itens relacionados exibem as seguintes informações:

   - A lista Detalhes exibe o número da verificação primária, a origem do scanner e o estado. Exiba verificações concluídas e com falha na seção Resumo da verificação.
   - A lista Verificações exibe todas as verificações secundárias e seus estados. Quando todas as verificações secundárias forem concluídas, o estado da verificação primária mudará para Concluído.
   - A lista Origem exibe o item vulnerável usado para a verificação, o item de configuração e a vulnerabilidade associados, o estado do IV e seu status de correção.

   Sua instância Now Platform® rastreia o status de nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro.

   O tempo limite não interrompe a verificação. O tempo limite se refere a quando Now Platform® parou de acompanhar seu status de nova verificação, não quando a nova verificação real parou.

   Todos os IVs que fizeram a transição ou farão a transição para Encerrado/Corrigido são importados com a próxima importação programada das integrações Rapid7.

Verificar novamente Tenable.io e Tenable.sc itens vulneráveis dos espaços Vulnerability Response

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados. Inicie novas verificações nos produtos Tenable.io e Tenable.sc sob demanda do Espaço de correção de TI na sua instância Now Platform.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Para iniciar uma nova verificação dos produtos Tenable.io e Tenable.sc do ambiente clássico de Vulnerability Response, consulte Iniciar nova verificação para a integração Tenable.sc e Iniciar nova verificação para a integração Tenable.io.

Para executar novas verificações de seu Now Platform, você precisa de suas credenciais da Tenable. Para obter mais informações sobre como configurar seus scanners Tenable.io e Tenable.sc e importar suas credenciais da Tenable, consulte Configurar a integração de vulnerabilidade da Tenable usando o assistente de configuração.

- Você pode iniciar novas verificações sob demanda para itens vulneráveis e tarefas de correção que tenham o produto Tenable.io ou Tenable.sc como origem do espaço de correção de TI no seu Now Platform.
- Em um registro de tarefa de correção, o registro pode estar em qualquer estado diferente de **Encerrado**e todos os IVs associados devem ser do produto Tenable.io ou Tenable.sc.
- Para iniciar novas verificações no Espaço de correção de problemas de TI de itens vulneráveis e registros de tarefa de correção, esses registros devem ser atribuídos a você.

Funções necessárias:

- sn_vul.remediation_owner para o Espaço de correção de problemas de TI
- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin do Vulnerability Manager Workspace

Procedimento

1. Navegue até um item vulnerável ou uma tarefa de correção que foi atribuída a você e abra-o.

   Nota:
   Se você escolher um esforço de correção para iniciar uma nova verificação, todos os IVs associados a esse registro serão verificados.

2. No canto superior direito de um registro, clique em **Verificar novamente**.
   Você será solicitado a escolher a instância ou as instâncias para a nova verificação e as credenciais do scanner que deseja usar para acessar o scanner. As credenciais exibidas são aquelas importadas pelas integrações de credenciais de verificação Tenable.io e Tenable.sc.

3. No modal, clique no ícone de pesquisa.

   No modal Selecionar uma credencial de verificação exibido, use os filtros nos títulos das colunas para selecionar o nome, a instância e ou as instâncias e os tipos de credencial que você deseja usar.

   Consulte a tabela a seguir para obter mais informações.

4. No modal de nova verificação atualizado, clique em **Solicitar nova verificação**.
   A mensagem A solicitação de verificação está sendo processada é exibida.

5. Clique no link **Exibir status** na mensagem para exibir o andamento da verificação.

   O registro de verificação (VSCAN#) é exibido. Abaixo do cabeçalho do registro com o número da verificação, as listas de itens relacionados exibem as seguintes informações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A lista Detalhes exibe o número da verificação primária, a origem do scanner e o estado. Exiba verificações concluídas e com falha na seção Resumo da verificação.
- A lista Verificações exibe todas as verificações secundárias e seus estados. Quando todas as verificações secundárias forem concluídas, o estado da verificação primária será alterado para Concluído.
- A lista Origem exibe o item vulnerável usado para a verificação, o item de configuração e a vulnerabilidade associados, o estado do IV e seu status de correção.

Sua instância Now Platform® rastreia o status de nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro.

O tempo limite não interrompe a verificação. O tempo limite se refere a quando Now Platform® parou de acompanhar seu status de nova verificação, não quando a nova verificação real parou.

Todos os IVs que fizeram a transição ou farão a transição para Encerrado/Corrigido são importados com a próxima importação programada das integrações Tenable.io ou Tenable.sc.

Espaço de correção de problemas de TI informações de referência

Os tópicos a seguir fornecem links, informações de referência, além de dados de campo nos formulários e registros encontrados em Espaço de correção de problemas de TI.

Criar campos de formulário de solicitação de mudança

A tabela a seguir mostra os campos e suas descrições no formulário Criar solicitação de mudança.

Campo	Descrição
Tipo de mudança	Normal – Normal é o padrão. Padrão - dois campos adicionais são exibidos: Categoria de mudança padrão - Selecione uma categoria na lista Modelo de mudança padrão: selecione um modelo na lista de seleção para usar nesta solicitação de mudança Emergência - Prioridade crítica
Adicionar ICs à solicitação de mudança	O padrão é habilitado. Se habilitada, a solicitação de mudança adiciona todos os itens de configuração (IC) que pertencem aos itens vulneráveis ativos neste esforço de correção que são adicionados a esta solicitação de mudança.
Prioridade	Alto é o padrão. Selecione uma prioridade na lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Grupo de atribuição	O grupo de atribuição é obtido por padrão do tópico de observação. Clique no ícone de pesquisa e, no modal, escolha outro grupo de atribuição.
Data de término planejada	Clique no ícone de calendário para selecionar uma data de término planejada.
Atribuído a	O usuário atual é atribuído por padrão à tarefa de correção. Clique no ícone de pesquisa e escolha outro usuário no modal.
Descrição resumida	A descrição resumida é obtida da tarefa de correção. Clique no texto para editá-lo.
Descrição	A descrição é obtida da tarefa de correção. Clique no texto para editá-lo.
Justificativa	A justificativa obtida da tarefa de correção. Clique no texto para editá-lo.
Plano de implementação	Pré-preenchido com informações da solução preferencial, se disponível. Exiba a solução ou insira um plano de justificativa.

Tópicos relacionados

Criar uma solicitação de mudança no Espaço de correção de problemas de TI

Solicitar campos do formulário de exceção para exceções de política

A tabela a seguir mostra os campos que você deve preencher no formulário Solicitar exceção para exceções de política.

Formulário de Exceção de solicitação

Campo	Descrição
Política	Política de gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle que estão associados à política que você selecionou. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válido de	Data em que a exceção começa. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até	Data em que a exceção de política expira e o estado do item ou grupo vulnerável muda de Adiado para Aberto. **Nota:** O número de dias em que a exceção de política é válida não pode exceder a **Duração máxima da exceção (dias)** que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Criar uma política .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de Exceção de solicitação

Campo	Descrição
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser preenchido pelo responsável pela correção.

Tópicos relacionados

Solicitar uma exceção usando GRC: Policy and Compliance Management no Espaço de correção de problemas de TI

Solicitar campos do formulário de exceção para redução de risco

A tabela a seguir mostra os campos que você deve preencher no formulário de exceção Solicitar para solicitações de redução de risco.

Formulário de Exceção de solicitação

Campo	Descrição
Motivo	Motivo da sua solicitação de exceção. Selecione *Controle de mitigação no local* para a solicitação de redução de risco. Para ver como adicionar novas opções de motivo, consulte Definir mapeamento do motivo da política.
Solicitação de adiamento	Difere o registro. Este campo é selecionado por padrão. **Nota:** Este campo aparece somente quando a opção *Controle de mitigação no local* é selecionada no campo **Motivo**.
Solicitação de redução de risco	Permite que você solicite a redução da pontuação de risco. **Nota:** Essa caixa de seleção aparece somente quando a opção *Controle de mitigação no local* está marcada no campo **Motivo**.
Classificação de risco atual	Severidade atual do risco. **Nota:** Este campo é exibido somente quando a caixa de seleção **Solicitação de redução de risco** está marcada.
Classificação de risco desejada	Nova classificação de risco que você deseja atribuir ao registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de Exceção de solicitação

Campo	Descrição
	A pontuação de risco mais alta neste intervalo de classificação de risco é aplicada ao registro quando sua solicitação é aprovada. **Nota:** Este campo é exibido somente quando a caixa de seleção **Solicitação de redução de risco** está marcada.
Selecionar controles de remuneração	Motivo da sua solicitação para reduzir a classificação de risco.
Até	Data em que a solicitação de adiamento ou redução de risco expira. Quando a solicitação de exceção expira: • O registro será revertido para o estado Aberto. • Os controles de compensação expiram. • A pontuação calculada substituirá uma pontuação reduzida.
Observações de justificativas	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita.

Explore o Espaço de avaliação de vulnerabilidade

O Espaço de avaliação de vulnerabilidade foi projetado para o gerenciador de eventos de vulnerabilidade executar a avaliação de exposição e gerenciar proativamente eventos de vulnerabilidade crítica, especialmente durante os eventos de vulnerabilidade crítica, como um evento de dia zero.

Depois que uma vulnerabilidade crítica é identificada, os gerentes de evento de vulnerabilidade podem avaliar o possível impacto e o risco associado à vulnerabilidade. Os analistas podem analisar o sistema, as aplicações ou os componentes de rede afetados para entender a severidade e os possíveis vetores de ataque na organização.

O Espaço de avaliação de vulnerabilidade contém:

Página Avaliação de exposição

Fornece visibilidade detalhada dos ativos expostos a vulnerabilidades e software vulnerável. A funcionalidade de avaliação de exposição fornece:

- Visibilidade dos ativos afetados para vulnerabilidade e software afetado
- Capacidade de executar avaliações autônomas para um único CVE ou software vulnerável
- Visibilidade dos ativos afetados para CVEs da vulnerabilidade explorada conhecida da CISA

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Visibilidade para exposição de modelo de descoberta adicional e ativos.
- Capacidade de criar itens vulneráveis

Página de avaliação de vulnerabilidade

A página Avaliação de vulnerabilidade, na qual você pode lidar com eventos de crise de vulnerabilidade, desde a avaliação até a resolução, usando o fluxo de trabalho de gestão de crises de vulnerabilidade. O fluxo de trabalho permite rastrear eventos de vulnerabilidade de interesse, analisar o risco associado a eles, executar a avaliação de exposição em vários inventários (por exemplo, inventário de instalações de software) e declará-lo como uma crise para um compromisso de resposta elevado. Você pode associar o registro de avaliação de vulnerabilidade a um incidente de segurança grave e permitir que a equipe de resposta a incidentes de segurança responda à crise.

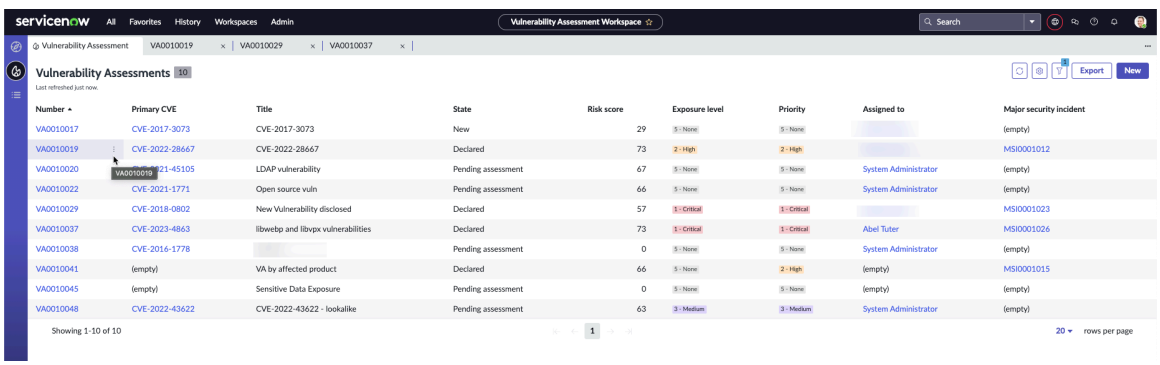
- Criar e modificar avaliações de vulnerabilidade para eventos de vulnerabilidade crítica
- Registrar os principais atributos da vulnerabilidade para calcular o risco
- Realizar avaliação de vulnerabilidade para determinar o nível de exposição e a prioridade
- Declare a avaliação de vulnerabilidade como um evento crítico
- Associe a avaliação de vulnerabilidade a um incidente de segurança grave vinculando, propondo ou promovendo a avaliação de vulnerabilidade a um incidente de segurança grave.

Página de lista

A página Lista compreende uma biblioteca que contém:

- CVEs
- TPEs
- CWEs

A imagem a seguir mostra a página inicial do Vulnerability Assessment Workspace.



Explorando a avaliação de exposição

A avaliação de exposição usa a estrutura de enumeração de plataforma comum (CPE), que faz parte do sistema de Vulnerabilidades e exposições comuns (CVEs), para avaliar a exposição de vulnerabilidade de seus ativos ao software de vulnerabilidade. Esta avaliação é realizada usando um modelo de descoberta de software.

Ao empregar um algoritmo de correspondência, os CPEs relevantes são associados e mapeados para o modelo de descoberta de software, permitindo a identificação de possíveis exposições.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode usar a avaliação de exposição por CVE ou software para identificar a exposição a possíveis vulnerabilidades para os seguintes cenários:

- Vulnerabilidades que podem não ser identificadas por scanners tradicionais
- Vulnerabilidades de dia zero antes do scanner fornecerem a assinatura para detecção de vulnerabilidade

A avaliação de exposição fornece um aviso antecipado para corrigir essas vulnerabilidades e melhorar a maturidade do programa de gestão de vulnerabilidades.

Pré-requisitos para avaliação de exposição

Versões disponíveis

Aplicação	Versão
Plug-in Vulnerability Emergency Response (sn_vul_analyst)	2.0
Vulnerability Response	20,0
Vulnerability Response com NVD	1,3
Vulnerability Response Integration with CISA	1,2
Vulnerability Response Integration with NVD **Nota:** Para obter mais informações, consulte Noções básicas sobre as integrações do NVD.	1,3
Gestão de ativos de software	Plug-in Software Asset Management Foundation ou Software Asset Management Professional plug-in

Requisitos de compatibilidade e sistema

A aplicação Vulnerability Response está disponível no ServiceNow Store. A aplicação Gestão de ativos de software ITSM (com.snc.asset_management) é necessária para o módulo Avaliação de exposição. Esta aplicação gerencia todos os seus ativos e licenças de software, e a versão SAM Foundation desta aplicação faz parte da aplicação Vulnerability Response que você baixa do ServiceNow Store.

Importante:
A aplicação Exposure Assessment funciona com os seguintes plug-ins:

- Plug-in Software Asset Management Foundation (com.snc.sams)
- Software Asset Management Professional (com.snc.pa.samp)
- Plug-in de Gestão de ativos de software (com.snc.software_asset_management)

Para verificar se a aplicação SAM Foundation está instalada em sua instância, navegue até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e pesquise por com.snc.asset_management. Se a aplicação não estiver instalada, selecione **Instalar**. Como a aplicação de avaliação de exposição requer acesso aos dados de ativos em sua instância Now Platform®, as aplicações de gestão de ativos devem ter dados para referência. A tabela de modelos de descoberta de software (cmdb_sam_sw_discovery_model) e as instalações de software (cmdb_sam_sw_install) exigem dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de algoritmo de correspondência para modelos de descoberta de software

A aplicação Software Asset Management Professional permite editar um modelo de descoberta de software para normalizar manualmente o software descoberto que não foi totalmente normalizado (parcialmente normalizado, fornecedor normalizado ou correspondência não encontrada) no formulário de modelos de descoberta de software para que possa ser reconciliado. A partir da versão 20.0 de Vulnerability Response oferece suporte ao modelo de descoberta normalizado que vem de Software Asset Management Professional. Os campos a seguir são usados para o algoritmo de correspondência para modelos de descoberta de software.

CPE (modelo de software)	Noções básicas do SAM	Profissional de SAM
Fornecedor	Chave primária	Chave primária
Produto	Nome de exibição	Nome de exibição
Versão	Fornecedor descoberto	Fornecedor descoberto
Edição	Produto Descoberto	Produto Descoberto
	Versão descoberta	Versão descoberta
		Fornecedor Normalizado
		Produto normalizado
		Versão normalizada

Nota:
A aplicação SAM Professional não faz parte do produto principal Vulnerability Response da ServiceNow Store e requer uma assinatura separada.

Propriedade do sistema

Para processar as vulnerabilidades exploradas pela CISA automaticamente para avaliação de exposição, defina a propriedade do sistema `sn_vul_analyst.enable_exposure_for_cisa` como `true`. O valor padrão é `false`.

Trabalhos programados

A seguir estão os trabalhos programados.

Nome do trabalho programado	Descrição
Verificar possível exposição de vulnerabilidade	Processa os CVEs delta, o software e as instalações para obter a exposição. **Nota:** Este trabalho programado é executado a cada 12 horas. Ele é executado por um período mais longo do que os outros trabalhos programados.
Inserir CVE explorado CISA na configuração de exposição	Sob demanda. Insere os CVEs CISA na tabela Configuração de exposição para calcular a exposição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do trabalho programado	Descrição
Executar avaliação de exposição para CVEs configurados	Sob demanda. Calcula a exposição de todos os registros de CVE na tabela Configuração de exposição.
Executar exposição de software	Sob demanda. Calcula a exposição de todos os registros de software na tabela Configuração de exposição.

Termos-chave

- Pontuação de**confiança:** uma pontuação de confiança é uma medida da confiabilidade ao fornecer uma recomendação para um campo. Quanto maior a pontuação, mais confiável será a recomendação. Para obter exemplos de cálculos, consulte Exemplo de cálculo de pontuação de confiança.
- **Contagem de instalação de software:** número de ativos de software afetados pela vulnerabilidade.
- Modelo de**software: modelo** de software associado ao produto. Faça uma busca detalhada no modelo de software para ver o resultado do modelo de software. Para obter mais informações, consulte Software Asset Management Foundation plugin discovery models and software installations .

Avaliação de exposição por CVE

A avaliação de exposição usa Vulnerabilidades e exposições comuns (CVEs) para avaliar a exposição de seus ativos usando o modelo de descoberta de software. Você pode usar a avaliação de exposição por CVE para identificar a exposição a possíveis vulnerabilidades.

Para obter informações sobre como avaliar a exposição por CVE, consulte:

- Adicionar CVEs para avaliar a exposição
- Criar IVs para CVEs para avaliação de exposição
- Ativar ou desativar CVEs para avaliação de exposição
- Exportar ICs afetados para avaliação de exposição
- Exemplo de cálculo de pontuação de confiança

Adicionar CVEs para avaliar a exposição

Adicione Vulnerabilidades e exposições comuns (CVEs) à lista de configuração de exposição de CVEs na avaliação de exposição para avaliar o impacto de uma nova vulnerabilidade ou vulnerabilidade de dia zero.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por CVE**.
2. Selecione **Adicionar**.
3. Na caixa de diálogo Adicionar CVE, selecione os CVEs que você deseja adicionar à lista e selecione a opção **Adicionar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os CVEs que já estão na lista não são adicionados novamente. O restante é adicionado à lista de CVEs.

Nota:
Selecione o ícone de filtro para navegar até a **exibição Avançado** e especificar os CVEs que você deseja exibir.

Criar IVs para CVEs para avaliação de exposição

Crie itens vulneráveis (IVs) na página Avaliação de exposição. Os gerentes de eventos de vulnerabilidade analisam essa lista de IVs e recomendam soluções e patches que ajudam a equipe de TI a corrigir essas vulnerabilidades.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa
Depois que a exposição é avaliada, a lista da avaliação potencial é exibida no registro de avaliação de exposição com a contagem de itens de configuração (ICs). Você pode selecionar os registros e, na ação da lista, selecionar **Criar itens vulneráveis** para criar itens vulneráveis (IVs) para os ICs em que o software vulnerável está presente e nas vulnerabilidades e exposições comuns (CVEs). Os IVs são criados em segundo plano. Esse processo pode levar algum tempo. Depois que os itens forem criados, você poderá navegar até a tabela IV para exibir os registros criados.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por CVE**.
2. Selecione os CVEs necessários e selecione a opção **Criar itens vulneráveis**.
3. Na caixa de diálogo Criar itens vulneráveis, selecione a opção **Criar itens vulneráveis**.
4. Selecione o link **Exibir status** para exibir o status do trabalho em segundo plano usado para criar os IVs.

Ativar ou desativar CVEs para avaliação de exposição

Para o processamento delta de um CVE, você pode ativá-lo, adicionando-o à lista ativa de CVEs.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por CVE**.
2. Selecione os CVEs ativos necessários e selecione a opção **Desativar**.
   Os CVEs estão desativados.

   Nota:
   Para ativar o software, siga o mesmo processo e selecione a opção **Ativar**.

3. Atualize a página para exibir o status atualizado (falso) na coluna Ativo.

Exportar ICs afetados para avaliação de exposição

Você pode rastrear a lista de ativos afetados para um novo CVE exportando os itens de configuração (ICs) relacionados a um registro de avaliação de exposição para uma

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

planilha do Excel. Esta planilha pode ser usada para compartilhar os detalhes dos ativos e os proprietários para criar incidentes com os ativos afetados conhecidos para as vulnerabilidades de dia zero.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por CVE**.
2. Selecione o modelo do Discovery para o registro cujos ICs você deseja exportar.
   A guia Instalações de software contém os ICs ativos relacionados ao registro de software. Esses ICs são armazenados na coluna **Instalado em**.
3. Selecione a opção **Exportar**.
4. Na caixa de diálogo Exportar, selecione o Tipo de arquivo e o Tipo de entrega para exportar os ICs relacionados.
5. Selecione a opção **Exportar**.

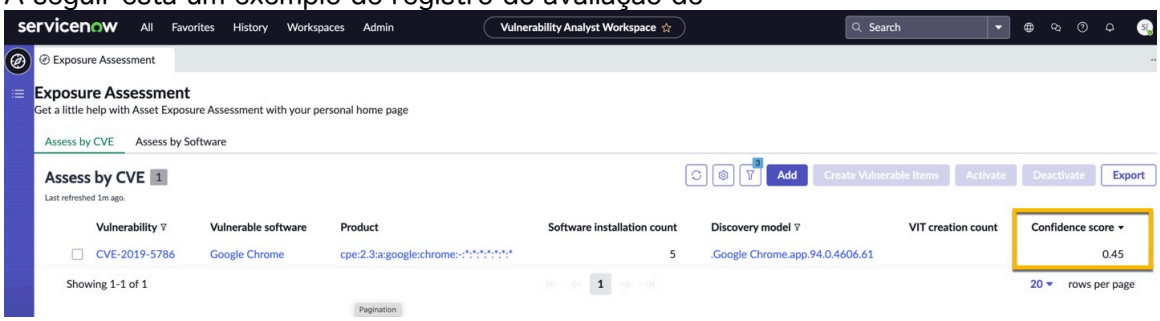
Exemplo de cálculo de pontuação de confiança

Exemplo de cálculo da confiança de uma vulnerabilidade de dia zero com base em suas informações de vulnerabilidades e exposições comuns (CVE).

A seguir está um exemplo de cálculo da pontuação de confiança das informações de enumeração de plataforma comum (CPE) de **CVE-2019-5786**.

Nota:
Para exibir os CPEs, você pode agrupar a coluna Vulnerabilidade por vulnerabilidade. Para obter detalhes sobre como exibir os detalhes do software vulnerável, consulte Exibir detalhes do software vulnerável.

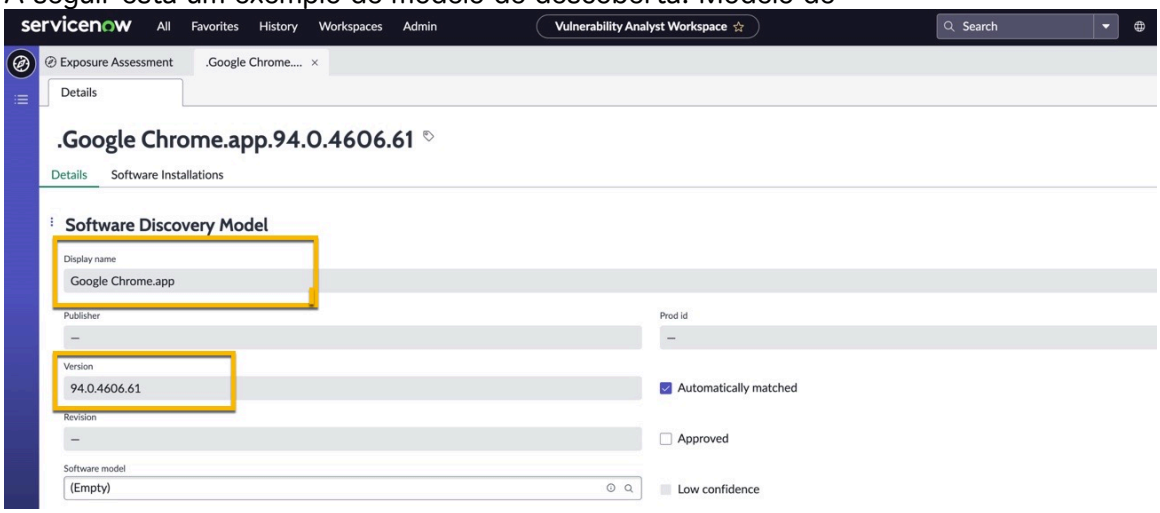
A seguir está um exemplo de registro de avaliação de



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seguir está um exemplo de modelo de descoberta: Modelo de



Como calcular a pontuação de confiança

O intervalo de pontuação de confiança é de 0 a 1. Com base nas informações de CPE, a pontuação de confiança é calculada usando a seguinte fórmula:

```
((BASE SCORE) + (publisher score) +(product score) + (version score) + (edition score) + (display name score)) / 100
```

=

```
((25) + (10) + (10)) / 100
```

=

```
45 / 100
```

=

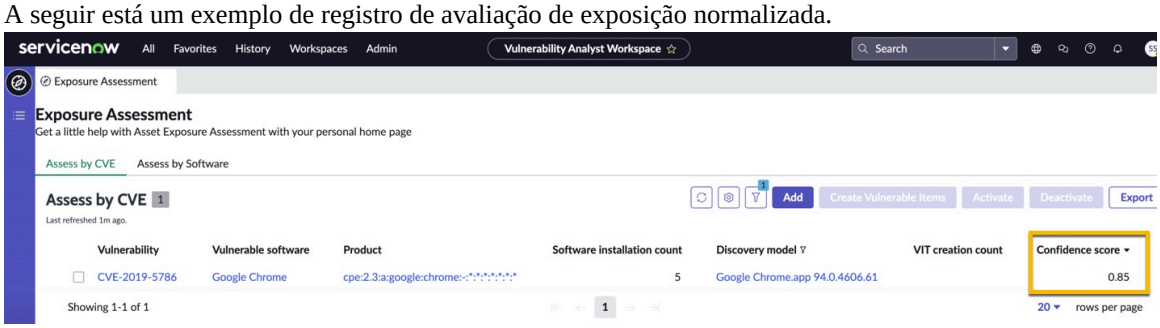
```
.45
```

Nota:
Para consultar os valores usados para calcular a pontuação de confiança, consulte Tabelas de referência de pontuação de confiança para avaliação de exposição.

Como calcular a pontuação de confiança quando o modelo de software corresponde ao modelo de descoberta normalizado

Se você estiver usando o modelo de descoberta normalizado, as informações adicionais disponíveis para o modelo de descoberta de software fornecerão uma pontuação de confiança aprimorada. A seguir está o cálculo de amostra:

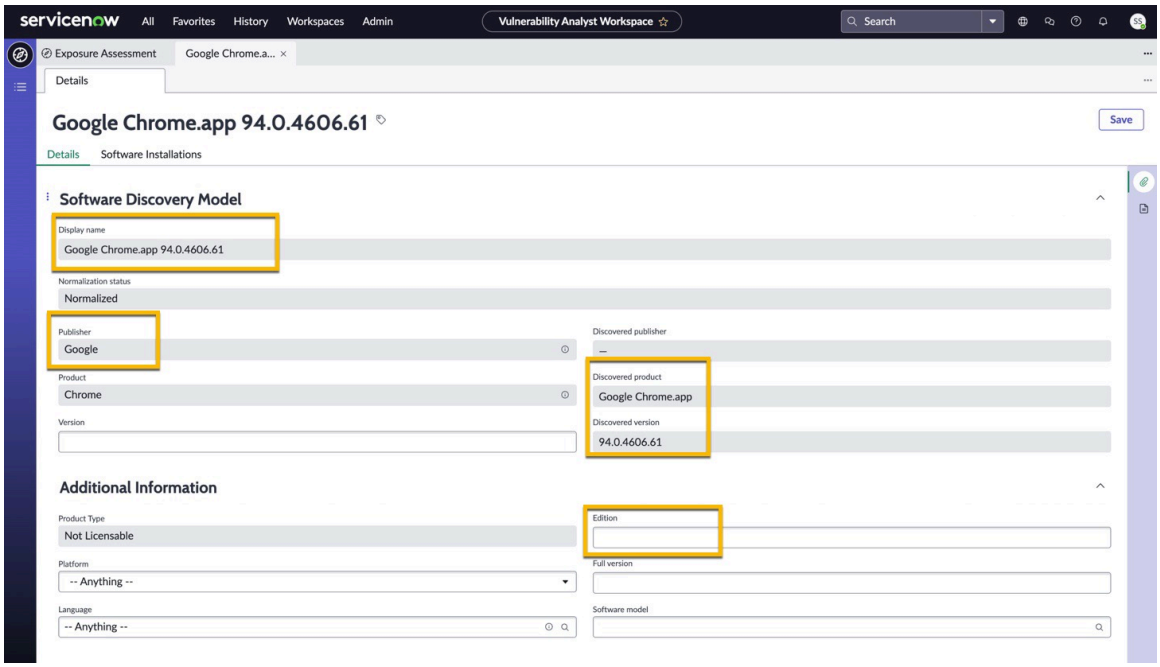
A seguir está um exemplo de registro de avaliação de exposição normalizada.



A seguir está um exemplo de modelo de descoberta normalizado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.




```
((BASE SCORE) + (publisher score) +(product score) + (version score) + (edition score) +
 (display name score)) / 100
```

=

```
((25) + (15) + (15) + (15) + (15) + (10)) / 100
```

=

```
85 / 100
```

=

```
.85
```

Nota:
Para consultar os valores usados para calcular a pontuação de confiança, consulte Tabelas de referência de pontuação de confiança para avaliação de exposição.

Exibir detalhes do software vulnerável

Exiba os detalhes do software vulnerável, neste caso, o Google Chrome. Ele é comparado ao modelo de descoberta e à enumeração de plataforma comum (CPE). Esta versão de CPE afeta todas as versões do Google Chrome.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegue até **Todos** e digite *sn_vul_software.LIST*.
2. Na lista de software vulnerável, pesquise por **cpe:2.3:a:google:chrome:-:*:*:*:*:*:*:*** para exibir as informações.

Tabelas de referência de pontuação de confiança para avaliação de exposição

Valores de referência usados para calcular a pontuação de confiança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabelas de referência

Tabela de referência do cálculo de pontuação de confiança

Segmento de software vulnerável	Segmento do modelo de descoberta	Pontuação	Segmento de correspondência exata do modelo de descoberta	Pontuação de correspondência exata
Fornecedor	Nome de exibição	15	Fornecedor	5
Modelo	Nome de exibição	15	Modelo	5
Versão	Nome de exibição	10	Versão	5
Nome de exibição	Nome de exibição	10	Nome de exibição	5

Tabela de resumo da pontuação de confiança

Pontuação	Valor
Soma de todas as pontuações	75
Pontuação base **Nota:** Pontuação mínima fornecida a todos os modelos de descoberta correspondentes.	25
Pontuação total	100

Avaliação de exposição por software

Avaliação de exposição para vulnerabilidades de dia zero, quando Vulnerabilidades e exposições comuns (CVEs) para o ativo ou item de configuração não estão disponíveis. Ele usa as informações do software para avaliar a exposição, usando o modelo de descoberta de software.

Para obter informações sobre como avaliar a exposição por software, consulte:

- Adicionar software para avaliação de exposição
- Criar IVs para software para avaliação de exposição
- Ativar ou desativar o software para avaliação de exposição
- Exporte ICs afetados para software no espaço de avaliação de vulnerabilidade

Adicionar software para avaliação de exposição

Adicione um novo software ao módulo Avaliação de exposição para avaliar o impacto de uma nova vulnerabilidade ou vulnerabilidade de dia zero.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por software** > **Adicionar**.
2. No formulário, preencha os campos.

Campo	Descrição
Fornecedor	Fornecedor do software.
Produto	Nome do produto do software.
Versão	Versão do produto de software.
Edição	Edição do software

Nota:
Se você tentar adicionar a exposição de um software existente na tabela com o status "falso", um registro duplicado não será criado. O status do software existente é atualizado para "verdadeiro".

3. Selecione a opção **Adicionar**.

Criar IVs para software para avaliação de exposição

Crie itens vulneráveis (IVs) na página Avaliação de exposição. Os gerentes de eventos de vulnerabilidade analisam essa lista de IVs e recomendam soluções e patches que ajudam a equipe de TI a corrigir essas vulnerabilidades.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por software**.
2. Selecione os registros para os quais você deseja criar IVs.
3. Selecione a opção **Criar itens vulneráveis**.
4. Na caixa de diálogo Criar itens vulneráveis, selecione:
   - Vulnerabilidade Existente
   - Nova Vulnerabilidade
5. Selecione a opção **Criar itens vulneráveis**.

Ativar ou desativar o software para avaliação de exposição

Para interromper o processamento delta do software, você pode desativá-lo, removendo-o da lista ativa de software.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por software**.
2. Para desativar, selecione o software ativo necessário e selecione a opção **Desativar**.
   O software está desativado.

   Nota:
   Para ativar o software, siga o mesmo processo e selecione a opção **Ativar**.

3. Atualize a página para exibir o status atualizado (falso) na coluna Ativo.

Exporte ICs afetados para software no espaço de avaliação de vulnerabilidade

Você pode rastrear a lista de ativos afetados para o novo software exportando os itens de configuração (ICs) relacionados a um registro de avaliação de exposição para uma planilha do Excel. Esta planilha pode ser usada para compartilhar os detalhes dos ativos e os proprietários para criar incidentes com os ativos afetados conhecidos para as vulnerabilidades de dia zero.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de Exposição** > **Avaliar por software**.
2. Selecione o modelo de descoberta para o registro cujos ICs você deseja exportar.
   A guia Instalações de software contém os ICs ativos relacionados ao registro de software. Esses ICs são armazenados na coluna **Instalado em**.
3. Selecione a opção **Exportar**.
4. Na caixa de diálogo Exportar, selecione o Tipo de **arquivo e o Tipo** de **entrega** para exportar os ICs relacionados.
5. Selecione a opção **Exportar**.

Explorando a avaliação de vulnerabilidade

O Vulnerability Assessment Workspace foi projetado para o Vulnerability Event Manager criar um evento de vulnerabilidade e executar uma avaliação de vulnerabilidade, especialmente durante a análise de vulnerabilidade de dia zero.

Você pode usar o espaço de avaliação de vulnerabilidade para gerenciar vulnerabilidades críticas, como:

- Vulnerabilidades de dia zero de severidade crítica ou alta
- Nova inteligência de ameaça identificada para uma vulnerabilidade
- Exploração rápida de uma vulnerabilidade de severidade crítica ou alta.

Espaço de avaliação de vulnerabilidade e Vulnerability Crisis Management

Como gerenciador de eventos de vulnerabilidade, identifique e crie um registro de evento de vulnerabilidade para vulnerabilidades de interesse. Depois de criar o evento vulnerável, você pode executar a avaliação de risco, atualizar manualmente os atributos de risco e calcular a pontuação de risco automaticamente. Usando o Espaço de avaliação de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

vulnerabilidade, você pode executar as seguintes ações para lidar com eventos de crise de vulnerabilidade, desde o início até a resolução.

- Criar um registro de avaliação de vulnerabilidade
- Modificar o registro de avaliação de vulnerabilidade
- Executar uma avaliação de vulnerabilidade
- Revisar os detalhes da avaliação
- Atribua uma prioridade e um nível de exposição ao registro de avaliação de vulnerabilidade
- Adicionar ICs afetados ao registro de avaliação
- Criar itens vulneráveis para o IC afetado ou o componente de software afetado
- Vincule o registro de avaliação de vulnerabilidade ao incidente de segurança grave no Gestão de incidentes graves de segurança

Pré-requisitos para avaliação de vulnerabilidade

Versões disponíveis

Aplicação	Versão
Plug-in Vulnerability Emergency Response (sn_vul_analyst)	2.0
Vulnerability Response	20,0
Vulnerability Response com NVD **Nota:** Para obter mais informações, consulte Noções básicas sobre as integrações do NVD.	1.4.2
Vulnerability Response Integration with CISA	1,2
Modelo de dados para SBOM	1.1.2
Lista de materiais de software Núcleo	2.0.2
Gestão de ativos de software	Plug-in Software Asset Management Foundation ou Software Asset Management Professional plug-in
Gestão de incidentes graves de segurança	2.2.5

Trabalhos programados

A seguir estão os trabalhos programados.

Nome do trabalho programado	Descrição
Avaliação de vulnerabilidade	Atualiza a tabela de itens de configuração afetados e a origem do IC se itens vulneráveis (VITs ou AVITs) forem criados após a avaliação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do trabalho programado	Descrição
	Nota: Este trabalho programado é executado diariamente. Ele é executado por um período mais longo do que os outros trabalhos programados.

Tópicos relacionados

Vulnerability Cris Management

Criar um registro de avaliação de vulnerabilidade

Crie registros de avaliação para vulnerabilidades de interesse. Depois de criar a avaliação, você pode iniciar a avaliação de risco inicial, atualizar manualmente o registro e calcular a pontuação de risco automaticamente.

Antes de Iniciar

Você precisa fazer parte do grupo de atribuição do gerenciador de eventos de avaliação de vulnerabilidade do sistema básico para executar as tarefas associadas à avaliação de vulnerabilidade. Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa

Você pode criar um registro de avaliação de vulnerabilidade para vulnerabilidades de interesse associando o registro de evento a um CVE primário ou a um produto afetado.

Procedimento

1. Navegar até **Todos** > **Espaços** > **Espaço de avaliação de vulnerabilidade**.
2. Selecione o ícone **Avaliação de vulnerabilidade**.
3. Selecione **Novo**.
4. Insira um título apropriado no campo **Título**.
5. **Opcional:** Selecione um CVE primário para associar ao novo registro de avaliação do campo **CVE primário**.

   Nota:
   Todos os detalhes preliminares no registro de avaliação são preenchidos com base no produto que você seleciona ou cria ou no CVE primário que você associa ao registro.

6. Selecione **Enviar**.
   O registro de avaliação de vulnerabilidade com o título que você inseriu é criado e exibido em uma nova guia de avaliação de vulnerabilidade. Por padrão, o registro de avaliação de vulnerabilidade é exibido na guia **Detalhes**.

   Nota:
   Por padrão, os detalhes do CVE primário associado/mapeado são exibidos.

   - Se nenhum CVE primário for selecionado durante a criação do registro de evento de avaliação de vulnerabilidade, um registro padrão será criado.
   - Se o CVE primário tiver CVEs associados, os CVEs relacionados serão preenchidos na guia **Entradas de vulnerabilidade**. Você pode adicionar mais CVEs associados na guia **Entradas de vulnerabilidade**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Navegue até a guia **Produtos afetados**.

   a. Selecione **Novo**.

   b. No formulário, preencha os campos.

Campo	Descrição
Fornecedor	Fornecedor do software. Este é um campo obrigatório.
Produto	Nome do produto do software. Este é um campo obrigatório.
Versão	Versão do produto de software.
Edição	Edição do software

   Nota:
   Se você tentar adicionar uma vulnerabilidade a um software existente na tabela com o status "falso", um registro duplicado não será criado. O status do software existente é atualizado para "verdadeiro".

   c. Selecione **OK**.

8. Selecione **Salvar**.

Atualizar o registro de limpeza automática de avaliação de vulnerabilidade

Atualize o registro de liberação automática de avaliação de vulnerabilidade.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa
No sistema de base, o período de retenção de registros de avaliação de vulnerabilidade é definido como 6 meses. Se qualquer estado de registro de avaliação de vulnerabilidade for encerrado, os registros de avaliação de vulnerabilidade serão armazenados somente até o período de retenção definido e os registros relacionados dessa avaliação serão removidos após 6 meses de todas as tabelas relacionadas.

Procedimento

1. Navegar até **Todos** > **Limpezas automáticas**.
2. Abra o registro com a tabela, sn_vul_analyst_vulnerability_assessment.
3. Marque a caixa de seleção **Ativa** para ativar a opção de limpeza automática do registro de avaliação de vulnerabilidade.
4. Clique em **Atualizar**.

Modificar o registro de avaliação de vulnerabilidade

Atualize o registro de avaliação de vulnerabilidade, publique sua criação. Com base nos valores do campo, você pode calcular a pontuação de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa
Depois que o CVE primário é adicionado à avaliação de vulnerabilidade, o registro é movido para um estado de avaliação pendente. Você pode adicionar outros CVEs relacionados na guia **Entradas de vulnerabilidade**ou adicionar os produtos afetados por esta vulnerabilidade na guia **Produtos afetados**. Você pode fazer mais modificações nos campos de **avaliação de risco** e a **pontuação** de risco do registro de avaliação será atualizada automaticamente de acordo.

Procedimento
1. Navegar até **Todos** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de vulnerabilidade**.
2. Na guia **Detalhes**, atualize os campos.

Campo	Descrição
Título	Título que descreve o registro do evento de vulnerabilidade .
CVE primário	CVE primário que você associou ao registro do evento.
Estado	Estado atual do registro do evento.
Prioridade	Prioridade do registro do evento em uma escala de 1 a 5.
Origem do alerta	Origem do possível evento de vulnerabilidade.
Pontuação de risco	Pontuação de risco calculada automaticamente. Não editável por padrão.
Nível de exposição	O nível de exposição do evento de vulnerabilidade em uma escala de 1 a 5.
Grupo de atribuição	O grupo de atribuição ao qual o registro de evento é atribuído.
Atribuído A	O usuário ao qual o registro de evento está atribuído.
Descrição	Descrição detalhada do registro do evento.

3. Navegue até a guia **Entradas de vulnerabilidade** para adicionar CVEs associados ou relacionados.
   a. Selecione **Novo**.
   b. Pesquise o registro no campo de **entrada de vulnerabilidade**.
   c. Selecione o registro de vulnerabilidade que você deseja associar ao registro de avaliação.
   d. **Opcional:** Selecione **Procurar** para navegar e anexar um arquivo.
   e. Selecione **Salvar**.
   Os registros de vulnerabilidade selecionados são adicionados ao registro de avaliação e exibidos na guia **Entradas de vulnerabilidades**.
4. **Opcional:** Adicione produtos afetados.
5. Adicionar link relacionado ao registro de avaliação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Modifique os **atributos de risco** do CVE primário associado ao registro de evento de avaliação de vulnerabilidade.

Campo	Descrição
Corrupção de memória	Indica se este registro de evento pode corromper a memória.
Executável de código remoto	Indica se a execução remota de código é possível.
Escalação de privilégio local	Indica se existe uma vulnerabilidade de escalação de privilégio local.
Acesso não autorizado	Indica se existe uma vulnerabilidade de acesso não autorizado.
DDOS	Indica se o possível evento pode envolver negação de serviço distribuída.
Complexidade de ataque	Indica a complexidade da anexação. As opções são Baixo, Médio ou Alto.
Vetor de ataque	Indica o possível caminho ou método de ataque. As opções são: Rede, Rede adjacente, Local, Física, Nenhuma.
Privilégios necessários (PN):	Indica o nível de privilégios que um invasor precisa para explorar a vulnerabilidade. As opções são Nenhum, Baixo ou Alto.
Interação do usuário	Indica se a interação do usuário é necessária para explorar a vulnerabilidade.
Impacto da confidencialidade	Indica a medida do possível impacto na confidencialidade da vulnerabilidade. As opções são Nenhum, Baixo ou Alto
Mudança de escopo	Indica se o escopo da avaliação foi alterado.
Impacto na disponibilidade	Indica o possível impacto na disponibilidade de uma vulnerabilidade de uso indevido explorada com sucesso. Disponibilidade se refere à acessibilidade dos recursos de informação. As opções são Nenhum, Baixo ou Alto
Impacto na integridade	Indica o possível impacto na integridade de uma vulnerabilidade de uso indevido explorada com sucesso. Integridade se refere à confiabilidade e à veracidade garantida das informações. As opções são Nenhum, Baixo ou Alto
Nível de correção	Indica o status ou a disponibilidade de correção para a vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	As opções são Correção oficial, Correção temporária, Solução alternativa, Indisponível, Não definido.
Maturidade do código de exploração	Indica a probabilidade de a vulnerabilidade ser explorada com base no estado existente das técnicas de exploração e na disponibilidade do código. As opções são Não comprovado, Prova de conceito, Funcional, Alto e Não definido.
Confiança do relatório	Indica o quanto você está confiante de que a vulnerabilidade existe.

7. Insira comentários relevantes no campo **Compor**.
   - Insira suas anotações de trabalho no campo Anotações de **trabalho (privadas)**.
   - Insira seus comentários (visíveis para todos) no campo **Comentários**.
8. **Salve** o registro de avaliação.
   Com base nas atualizações feitas nos campos de **atributo de risco** do CVE primário ou do produto afetado associado ao registro de avaliação, o campo **Pontuação de risco** é atualizado automaticamente.

> **Nota:**
> Para modificar as regras ou os critérios da calculadora de pontuação de risco do sistema de base, navegue até **Todos** > **Calculadoras de avaliação de vulnerabilidade** > **Calculadora de risco da avaliação de vulnerabilidade** > **Regra de risco de avaliação de vulnerabilidade**. Você pode adicionar critérios e modificar a ponderação do nível de campo para os critérios existentes, conforme necessário.

O que Fazer Depois
Realize uma avaliação inicial do registro do evento.

Excluir CVEs associados ou produtos afetados do registro de avaliação de vulnerabilidade

Exclua um registro de evento de vulnerabilidade se ele não for mais necessário.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa
Você pode excluir CVEs ou produtos afetados associados ao registro de avaliação de vulnerabilidade. Você só poderá excluir entradas de vulnerabilidade/CVEs associados ou produtos afetados se eles estiverem nos estados de avaliação **Novo** ou **Pendente**.

Procedimento
1. Navegar até **Todos** > **Espaços** > **Avaliação de vulnerabilidade**.
2. Selecione o registro de avaliação de vulnerabilidade.
3. Selecione a guia **Entradas de vulnerabilidade** ou a guia **Produtos afetados**.
4. Selecione o CVE associado ou o registro do produto afetado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione **Excluir**.

> **Nota:**
> O botão **Excluir** é exibido somente para um registro de avaliação quando ele está nos estados **Nova** ou **Avaliação pendente**.

Adicionar link relacionado ao registro de avaliação

Adicione links e informações adicionais relacionados ao registro de avaliação.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade**.
2. Selecione a entrada de registro de avaliação.
3. Selecione a guia **Links relacionados**.
4. Insira uma descrição relevante no campo **Descrição**.
5. Insira o URL no campo **Link**.
6. Selecione **OK**.
   O link relacionado é adicionado e listado na guia Links relacionados.

Realizar uma avaliação

Depois de criar o registro de avaliação de vulnerabilidade e atualizar os campos de atributo de risco, execute uma avaliação do registro de evento.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa
Realize uma avaliação inicial depois que um evento para uma vulnerabilidade de interesse tiver sido criado e determinado como apresentando risco para sistemas e dados. O objetivo desta atividade é analisar melhor a ameaça atualizando a avaliação de risco com uma avaliação de exposição detalhada.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliação de vulnerabilidade**.
2. Selecione o registro relevante na lista de registros de evento de avaliação de vulnerabilidade.
3. Selecione **Avaliar** para executar a avaliação de vulnerabilidade.
   O trabalho em segundo plano do evento Vulnerability Response - Avaliação de vulnerabilidade do processo é iniciado e uma notificação relevante é exibida.
4. Selecione **Exibir status** na notificação para exibir o status do trabalho em execução.
5. Selecione **Salvar**.

   A guia **Avaliações** exibe os detalhes da avaliação. Quando a avaliação é processada, os VITs ou AVITs associados às entradas vulneráveis ou CVEs são exibidos nos **Itens vulneráveis** ou na guia **Itens vulneráveis da aplicação**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado

- Itens vulneráveis ou TPEs relacionados aos CVEs associados são obtidos durante a avaliação. Os ICs relacionados aos itens vulneráveis também são identificados e exibidos na tabela Itens de configuração afetados.
- Se os ICs associados não existirem na tabela de ICs afetados, os ICs identificados serão adicionados à tabela e o valor do campo **Tem item vulnerável** será definido como **Verdadeiro**e o valor do campo **Origem** será definido como Scanner.
- Se o IC já existir na tabela de IC afetada, somente o valor do campo **Tem item vulnerável** será definido como **Verdadeiro** e o valor dos Campos de **origem** do IC permanecerá o mesmo de quando o registro de avaliação foi criado.
- Se itens vulneráveis forem criados após a avaliação, um trabalho programado de avaliação de vulnerabilidade será executado para atualizar a tabela de ICs afetados e a origem do IC.

O que Fazer Depois

- Atribua uma prioridade e um nível de exposição ao registro de avaliação de vulnerabilidade
- Adicionar ICs afetados ao registro de avaliação
- Criar itens vulneráveis para o IC afetado ou o componente de software afetado
- Adicionar link relacionado ao registro de avaliação

Tópicos relacionados

Guia Avaliação

Guia Visão geral

Guia Avaliação

Revise os resultados da avaliação na guia de avaliação. Depois de executar uma avaliação do evento de vulnerabilidade, o registro é correlacionado aos dados de Lista de materiais de software e Gestão de ativos de software e exibido com visualizações.

A guia de avaliação preenche os dados (se disponíveis) com base no registro de avaliação que você cria e correlaciona os detalhes com as avaliações de Gestão de ativos de software e Lista de materiais de software dados de componente no CMDB.

Como funciona a avaliação

Ao selecionar o botão **Avaliar**, uma avaliação de todos os CVEs relacionados e produtos afetados usando os dados Gestão de ativos de software e SBOM é iniciada. Um trabalho em segundo plano é acionado e, quando a avaliação é processada, os VITs ou AVITs associados às entradas vulneráveis ou CVEs são exibidos nas guias Itens vulneráveis e **Itensvulneráveis da aplicação**.

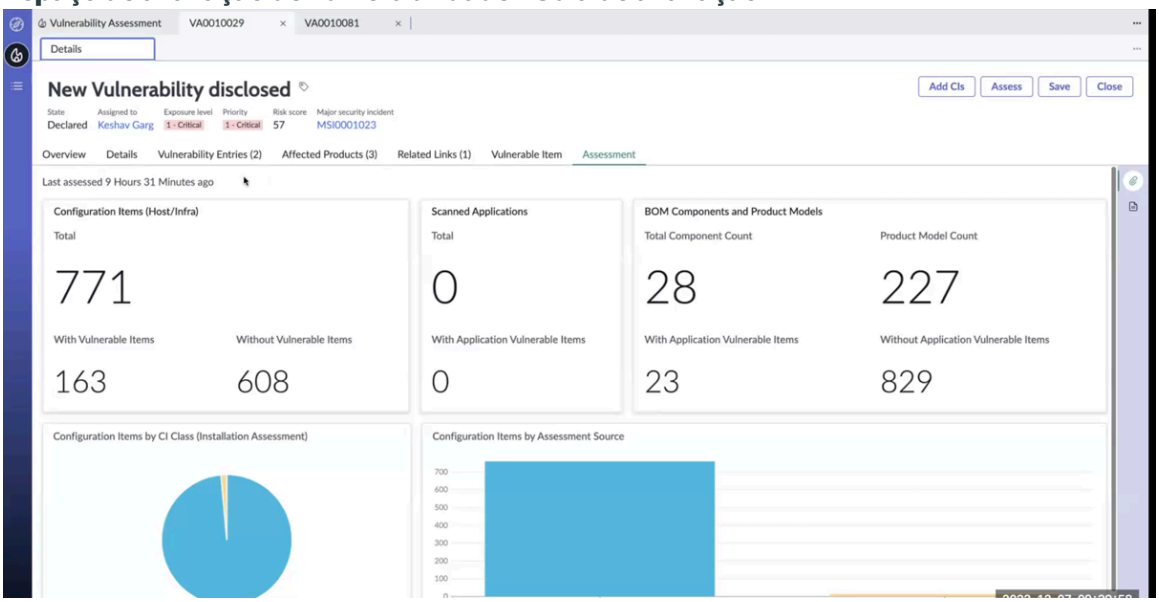
- Todos os itens vulneráveis ou TPEs relacionados ao CVE são identificados.
- Os itens de configuração (ICs) relacionados aos itens vulneráveis também são identificados e exibidos na tabela de itens de configuração afetados.
- Se os ICs não estiverem presentes na tabela de ICs afetados, os ICs identificados serão adicionados à tabela, o sinalizador **Tem item vulnerável** será definido como verdadeiro e o valor do campo **Origem** será definido como Scanner.
- Se o IC já existir na tabela de itens de configuração afetados, somente o sinalizador **Tem item vulnerável** será definido como verdadeiro e a **Origem** permanecerá inalterada desde quando o registro de avaliação foi criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se itens vulneráveis forem criados após a avaliação, um trabalho programado de avaliação de vulnerabilidade será executado para atualizar a tabela de ICs afetados e a origem do IC.
- No espaço de avaliação, você pode exibir carimbos de data/hora para ver a última avaliação dos eventos. A guia **Avaliação** fica visível somente quando as novas avaliações são criadas. Se a avaliação estiver no estado em andamento, o status da última avaliação aparecerá como a avaliação está em andamento. Para exibir o status da avaliação atualizado, atualize a página. Depois que a avaliação for concluída, o usuário poderá ver todas as guias relacionadas a essa avaliação.

Espaço de avaliação de vulnerabilidade - Guia de avaliação



Os detalhes da avaliação são exibidos para os widgets a seguir.

- Itens de configuração (host/infraestrutura)
- Aplicações escaneadas
- Componentes da BOM e modelos de produto
- Itens de configuração por classe de IC (avaliação de instalação)
- Itens de configuração por origem de avaliação: exibe a lista de itens de configuração afetados.

Visualizações de dados

Nome	Tipo	Descrição
Itens de configuração (host/ infraestrutura)	Pontuação única	Exibe a contagem de ICs com e sem IVs. O widget Itens de configuração exibe a contagem total de ICs associados ao registro de avaliação. O widget exibe ainda mais os itens de configuração com itens

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
		vulneráveis e sem itens vulneráveis.
Aplicações escaneadas	Contagem	Contagem total de aplicações verificadas com AVITs. **Nota:** Você pode exibir a contagem de aplicações verificadas para CVEs primários e secundários.
Componentes da BOM e modelos de produto	Pontuação única	Contagem total de componentes, contagem de modelo de produto, com itens vulneráveis de aplicação, sem contagem de itens vulneráveis de aplicação.
Itens de configuração por origem de avaliação	Barras empilhadas	Itens de configuração afetados empilhados pela origem da avaliação.
Itens de configuração por classe de IC (avaliação de instalação)	Gráfico de Pizza	Itens de configuração empilhados por classe de IC.

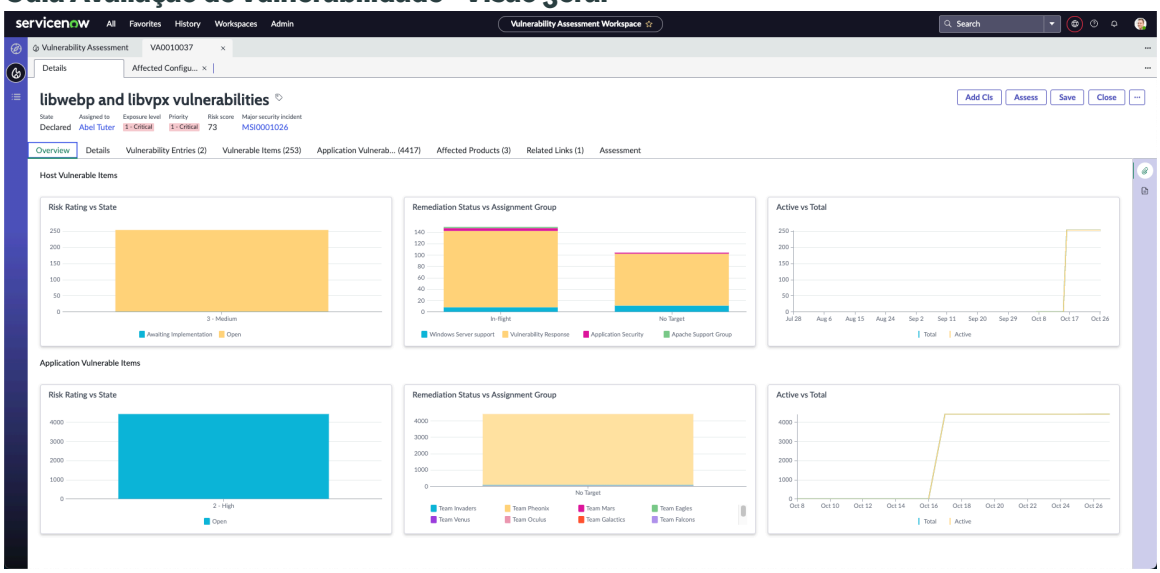
Guia Visão geral

A visão geral dos detalhes da avaliação é exibida na guia Visão geral. Depois de executar a avaliação inicial, o registro é correlacionado aos dados de Lista de materiais de software e Gestão de ativos de software e exibido com visualizações.

Guia Visão geral

A guia Visão geral preenche os dados (se disponíveis) com base no registro de avaliação que você cria e correlaciona os detalhes com as avaliações de Gestão de ativos de software e Lista de materiais de software dados no CMDB. O

Guia Avaliação de vulnerabilidade - Visão geral



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os detalhes da avaliação são exibidos para os widgets a seguir.

- Itens vulneráveis de host (host/infraestrutura)
  - Classificação de risco x estado
  - Status de correção x Grupo de atribuição
  - Ativo x Total
- Itens vulneráveis da aplicação
  - Classificação de risco x estado
  - Status de correção x Grupo de atribuição
  - Ativo x Total

Visualizações de dados

Itens vulneráveis de host

Nome	Tipo	Descrição
Classificação de risco x estado	Barras empilhadas	Estado dos itens vulneráveis empilhados por sua classificação de risco.
Status de correção x Grupo de atribuição	Barras empilhadas	Status de correção do item vulnerável empilhado por seu grupo de atribuição.
Ativo x Total	Lista e linha	Total de itens vulneráveis associados a esta entrada versus itens vulneráveis ativos.

Itens vulneráveis da aplicação

Nome	Tipo	Descrição
Classificação de risco x estado	Barras empilhadas	Estado dos itens vulneráveis da aplicação empilhados por sua classificação de risco.
Status de correção x Grupo de atribuição	Barras empilhadas	Status de correção do item vulnerável da aplicação empilhado por seu grupo de atribuição.
Ativo x Total	Lista e linha	Total de itens vulneráveis da aplicação associados a esta entrada versus itens vulneráveis ativos.

Atribua uma prioridade e um nível de exposição ao registro de avaliação de vulnerabilidade

Atribua manualmente a prioridade e o nível de exposição ao registro de avaliação de vulnerabilidade.

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade**.
2. Selecione um registro de avaliação de vulnerabilidade.
3. Navegue até **Atributos de risco** na guia **Detalhes**.
4. Selecione uma **Prioridade** na lista de opções.
5. Selecione um **Nível de exposição** na lista de opções.
6. Selecione **Salvar**.

Adicionar ICs afetados ao registro de avaliação

Adicione manualmente os ICs em sua organização que você acha que devem estar associados ao registro de avaliação de vulnerabilidade, mas não são exibidos nos ICs afetados após a] avaliação inicial .

Antes de Iniciar
Função necessária: sn_vul_analyst.vul_event_manager

Por Que e Quando Desempenhar Esta Tarefa
Adicione ICs que você sabe que podem ter sido afetados, mas não aparecem após a conclusão da avaliação. Você só pode adicionar ICs quando o registro de avaliação está no estado de avaliação **Declarado** ou **Pendente**.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade**.
2. Selecione o registro de avaliação necessário na lista.
3. Selecione **Adicionar ICs**.
4. Selecione os itens de configuração na caixa de diálogo Itens de configuração.
5. Selecione **Adicionar ICs**.
   O trabalho em segundo plano do Vulnerability Response - Adicionar itens de configuração ao evento é iniciado e uma notificação relevante é exibida.
6. Selecione **Exibir status** na notificação para exibir o status do trabalho em execução.

Resultado
Os registros são adicionados à tabela Itens de configuração afetados com **Origem** como *Manual*.

O que Fazer Depois
Navegue até a guia **Avaliação** e atualize o widget **Itens de configuração (host/infraestrutura)** para exibir os ICs que você adicionou.

Criar itens vulneráveis para o IC afetado ou o componente de software afetado

Crie itens vulneráveis (IVs) ou itens vulneráveis da aplicação (AVITs) a partir do Espaço de avaliação de vulnerabilidade. Os analistas de vulnerabilidade analisam a lista de IVs e recomendam soluções e patches que ajudam a equipe de TI a corrigir essas vulnerabilidades.

O gerenciador de eventos de vulnerabilidade deve ser capaz de selecionar um, muitos ou todos os resultados da pesquisa de exposição para criar itens de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Item vulnerável da aplicação para resultados de avaliação SBOM que não têm AVITs associados
- Itens vulneráveis para itens de configuração que não têm VITs associados
- Associe o CVE primário aos itens de vulnerabilidade.

Criar IVs para itens de configuração sem itens vulneráveis associados

Crie VITs de itens vulneráveis para itens de configuração identificados por meio da avaliação de vulnerabilidade, mas não tenham VITs associados ao registro.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliações**.
2. Selecione o registro de avaliação para o qual você precisa criar o VIT.
3. Selecione a guia **Avaliação**.
4. Selecione **Sem** contagem de itens de **configuração no widget Itens de configuração (infraestrutura do host)**.
5. Selecione os Itens de configuração para os quais você deseja criar VITs na lista **Itens de configuração afetados**.
6. Selecione **Criar item vulnerável**.
   O trabalho em segundo plano Vulnerability Response - Criar avaliação de vulnerabilidade de VITs manuais é iniciado e uma notificação relevante é exibida.
7. Selecione **Exibir status** na notificação para exibir o status do trabalho em execução.
   Itens vulneráveis para os itens de configuração afetados que você selecionou são criados.

   O widget de **itens de configuração (infraestrutura do host)** agora exibirá o mesmo IC na contagem de **itens vulneráveis**.

Criar itens vulneráveis da aplicação (AVITs) para modelos de produtos afetados ou componentes sem itens vulneráveis da aplicação associados

Crie itens vulneráveis da aplicação (AVITs) para produtos afetados ou itens de componentes identificados por meio da avaliação de vulnerabilidade, mas não têm AVITs associados ao registro.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade** > **Avaliações**.
2. Selecione o registro de avaliação para o qual você precisa criar o VIT.
3. Selecione a guia **Avaliação**.
4. Selecione **Sem contagem de itens vulneráveis da aplicação** no widget **Componentes da lista de materiais e Modelos de produto**.
5. Selecione os modelos de produto afetados para os quais você deseja criar AVITs na lista **Modelos de produto afetados**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Selecione **Criar item vulnerável da aplicação**.
   O trabalho em segundo plano Vulnerability Response - Criar avaliação de vulnerabilidade de VITs manuais é iniciado e uma notificação relevante é exibida.
7. Selecione **Exibir status** na notificação para exibir o status do trabalho em execução.
   Itens vulneráveis da aplicação para os itens de modelos de produto afetados que você selecionou são criados. para o CVE primário associado ao registro.

   O widget **de modelos de produto e componentes da lista de materiais** agora exibirá o mesmo modelo de produto ou componente na contagem de **itens vulneráveis da aplicação**.

Vincule o registro de avaliação de vulnerabilidade ao incidente de segurança grave no Gestão de incidentes graves de segurança

Você pode vincular, propor ou promover o registro de avaliação para um Incidente de segurança grave, desde que tenha acesso à aplicação Gestão de incidentes graves de segurança.

Antes de Iniciar

Função necessária: sn_vul_analyst.vul_event_manager, sn_si.analyst, sn_msi.workspace_admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode mover o registro de avaliação para ser associado a um incidente de segurança grave existente, criar um novo ISG a partir do registro de avaliação ou promover o registro de avaliação de vulnerabilidade a um incidente de segurança grave. Aproveite os recursos Gestão de incidentes graves de segurança, como as integrações com Microsoft Teams e Microsoft SharePoint.

Você também pode exibir o link para os incidentes de segurança graves no Vulnerability Manager Workspace para itens vulneráveis. O link MSIM será associado à avaliação vulnerável que será mostrada nos itens de vulnerabilidade e também em outros espaços de Vulnerability Response.

Procedimento

1. Navegar até **Espaços** > **Espaço de avaliação de vulnerabilidade**.
2. Selecione o registro de avaliação que você deseja vincular a um incidente de segurança grave.
3. Selecione o ícone **Mais ações**, na guia **Detalhes**.
4. Selecione uma das seguintes opções.

Opção	Descrição
Link para o incidente de segurança grave	Selecione o registro MSI existente na lista de Incidentes de segurança graves. O registro de avaliação de vulnerabilidade está vinculado ao incidente de segurança grave existente.
Propor como incidente de segurança grave	Insira os seguintes detalhes e selecione **Propor**. ○ Data de detecção ○ Justificativa ○ Impacto potencial

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Promover como incidente de segurança grave	Insira os seguintes detalhes e selecione **Promover**. ○ Data de detecção ○ Data de resolução estimada ○ Justificativa ○ Impacto potencial

5. Selecione **Salvar**.

O que Fazer Depois

Selecione o registro MSI para abrir o registro na exibição Gestão de incidentes graves de segurança.

Tópicos relacionados

Link para Incidente de segurança grave

Propor como Incidente de segurança grave

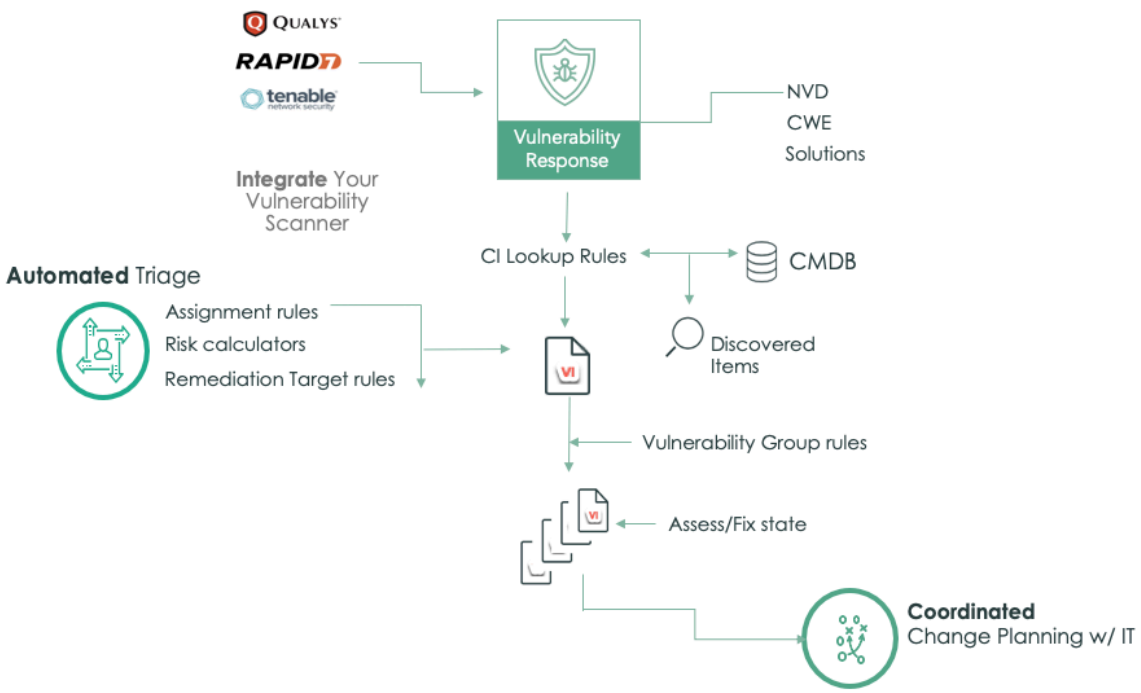
Promover a um Incidente de segurança grave

Vulnerability Response visão geral da correção

Vulnerability Response A correção é um processo em fases que consiste na verificação da conclusão da importação, na triagem de novas vulnerabilidades e no monitoramento do andamento até a conclusão. Abordada dessa forma, a correção se torna gerenciável, oportuna e, de várias maneiras, automatizada.

Entender sua postura de segurança nos ativos da empresa ajuda a identificar as vulnerabilidades mais críticas para correção. Este processo de correção requer que Vulnerability Response e uma integração de terceiros, como Qualys Vulnerability Integration estejam instalados e configurados.

Fluxo do processo de integração do Vulnerability Response



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verificar a conclusão bem-sucedida das importações de integração de terceiros

A primeira fase neste processo é garantir que tudo esteja funcionando corretamente. Vulnerability Response é predefinido para baixar vulnerabilidades do National Vulnerability Database (NVD) e Common Enumeration Weakness (CWE). As importações de terceiros fornecem os dados necessários para criar itens vulneráveis e tarefas de correção. A correção bem-sucedida depende da importação consistente e bem-sucedida de vulnerabilidades e itens vulneráveis.

Durante a importação, as Regras de pesquisa de IC correspondem aos ativos de terceiros com os ativos no Configuration Management Database (CMDB). Todos os ativos são armazenados no módulo Itens descobertos. As informações de IC são críticas para a implementação da solução.

Nota:
Depois que uma integração de terceiros foi instalada e configurada, há algumas instâncias em que uma importação pode falhar, por exemplo, se o fornecedor de terceiros limitar suas chamadas de API. Quando as importações falham, elas exigem atenção imediata.

Os relatórios de execução de status da integração para as integrações de terceiros compatíveis são enviados com as aplicações para fornecer uma visão geral gráfica de suas importações. Use este relatório, ou crie o seu próprio, para determinar facilmente se a importação mais recente foi bem-sucedida. Para obter mais informações sobre integrações compatíveis, consulte Integrações do Vulnerability Response.

Analisar e fazer a triagem de vulnerabilidades e itens vulneráveis

A próxima fase de correção exige a revisão de novas vulnerabilidades e itens vulneráveis. Um item vulnerável (IV) é uma combinação detectada de vulnerabilidade e item de configuração (IC). Conforme os itens vulneráveis são formados, várias regras são executadas que atribuem IVs, determinam o risco que eles representam e definem metas de correção. Ajuste as regras, conforme necessário, para garantir que os itens vulneráveis sejam triados com sucesso.

Monitorar o andamento da correção de vulnerabilidade existente

A fase final da correção consiste em monitorar seu andamento.

- Analise o status das importações para implementações de patch que não foram exibidas e faça o acompanhamento com as operações de TI.
- Rastreie o andamento das obrigações de conformidade regulatória e garanta sua conclusão.
- Revise o status do item adiado e revise ou implemente correções.
- Monitore os painéis do Vulnerability Management. Para revisar tendências, exibir relatórios em tempo real e usar métricas que rastreiam suas taxas de cumprimento da meta de correção, talvez você prefira monitorar seus processos com a aplicação Performance Analytics para Vulnerability Response.
- Fechando detecções obsoletas em Vulnerability Response.

Verificar a conclusão bem-sucedida das importações de integração de Vulnerability Response

A maneira mais fácil de determinar se as importações foram bem-sucedidas é usar um painel de status de execução de integração. O painel Status da execução de integração

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

fornece um exemplo de exibição gráfica do status das execuções de integração de terceiros.

As integrações de vulnerabilidade Qualys e Rapid7 têm um painel de status de execução de integração. Consulte Qualys gráfico de status de execução de integração ou Rapid7 Vulnerability Integration gráfico de status de execução para obter informações detalhadas sobre o conteúdo do gráfico.

Nota:
Gráficos, para integrações não fornecidas por ServiceNow®, podem ser criados a partir de relatórios em um painel, mas podem exigir ServiceNow experiência. Para obter mais informações sobre como criar relatórios e painéis, consulte Introdução a relatórios e painéis.

Exibir Vulnerability Response dados de detecção de item vulnerável

Os dados completos coletados por suas integrações de scanner de terceiros com Vulnerability Response são exibidos nas guias Detecções e Detecções iniciais nos registros de item vulnerável (VIT). Também é exibido em registros de detecção na lista de detecção de item vulnerável na sua instância Now Platform®.

Antes de Iniciar

As integrações de terceiros recuperam dados de detecção de item vulnerável. As detecções são ocorrências distintas de vulnerabilidades, conforme relatado pelos scanners. Os dados de detecção são emparelhados com itens vulneráveis e o estado do IV é atualizado com base no estado das detecções. Se um IV não for encontrado, um novo será criado. As detecções são abertas ou encerradas somente pelos dados encontrados diretamente por um scanner.

Função necessária:

sn_vuln.admin inicia execuções de integração e exibe dados de detecção de item vulnerável

sn_vul.remediation_owner está atribuído a itens vulneráveis criados a partir de detecções de item vulnerável e exibe dados em registros de IV

Procedimento

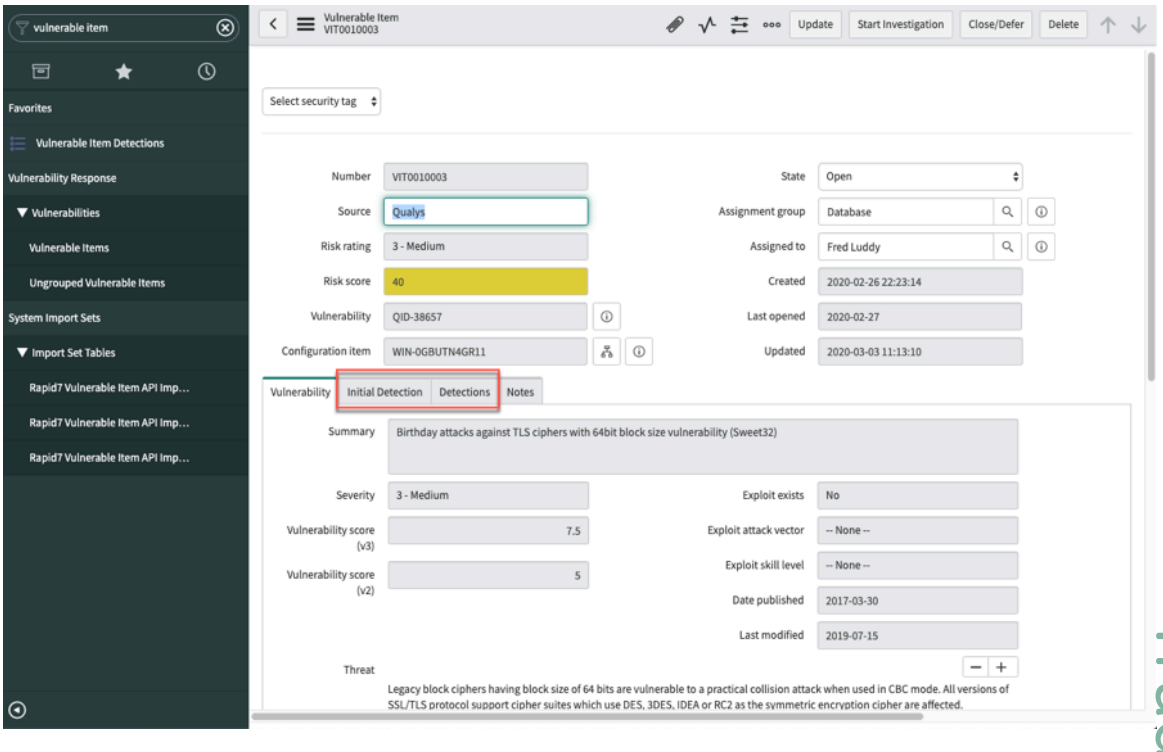
1. Para exibir os dados de detecção de item vulnerável, navegue até um registro de item vulnerável e abra-o.

   O registro é exibido com as guias Detecções iniciais e Detecções.

   Nota:
   Os dados exibidos anteriormente na guia Detalhes da configuração são exibidos junto com outros dados de detecção nas guias Detecção inicial e Detecções.

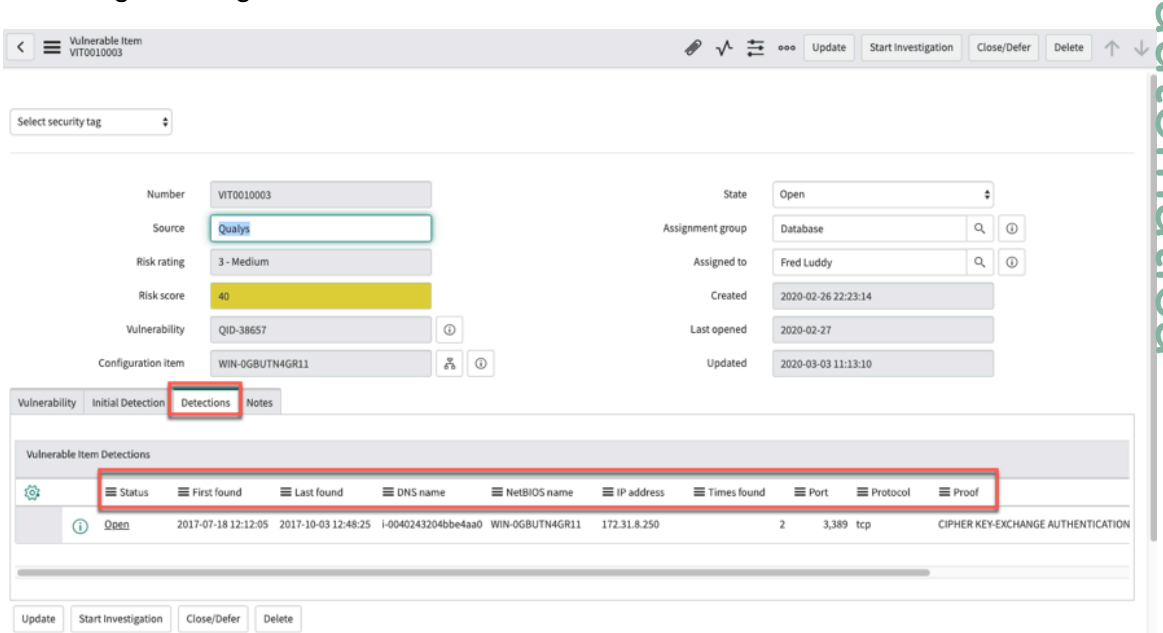
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Clique na guia **Detecções**.

Quando um item vulnerável é criado a partir dos resultados de uma verificação de terceiros, os dados da verificação são exibidos no registro de detecção, conforme mostrado na figura a seguir.



Cada linha na seção Detecções de item vulnerável representa dados de uma detecção distinta. Na coluna Primeiro encontrado, a data em que o item vulnerável foi detectado pela primeira vez pelo scanner é exibida. Na coluna Último encontrado, a data da detecção mais atual é exibida. O campo Origem exibe o scanner que recuperou os dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Para Qualys, com detecções de item vulnerável, os seguintes campos estão obsoletos no registro IV e não são mais preenchidos:

- Qualys severidade
- Última atualização pela origem

Também para Qualys, conforme mostrado na figura anterior, quando um IV é criado a partir de uma verificação, o valor da verificação para Resultados é exibido na coluna Prova no registro de detecção. No entanto, este valor não é exibido na parte superior do registro IV.

Para Rapid7, quando um IV é criado a partir de uma verificação, o valor da Prova da verificação pode ser exibido na coluna Prova no registro de detecção e na parte superior do registro de IV, mas não por padrão. Para exibir este valor na parte superior do registro IV, selecione o campo Prova no layout do formulário.

3. **Opcional:** Para configurar o layout da guia Detecções no registro, siga estas etapas.

   a. As colunas a seguir são exibidas na guia Detecções por padrão.

   - Status
   - Encontrado pela primeira vez (dados)
   - Último encontrado (data)
   - Nome DNS
   - Net BIOSname
   - Endereço IP
   - Horas encontradas
   - Porta
   - Protocolo
   - Prova
   - SSL

   Nota:

   (Optional) Observação: se não houver valor em uma coluna, os dados desse campo não foram detectados pelo scanner.

   b. Clique no ícone de engrenagem (ícone de) para personalizar sua exibição.

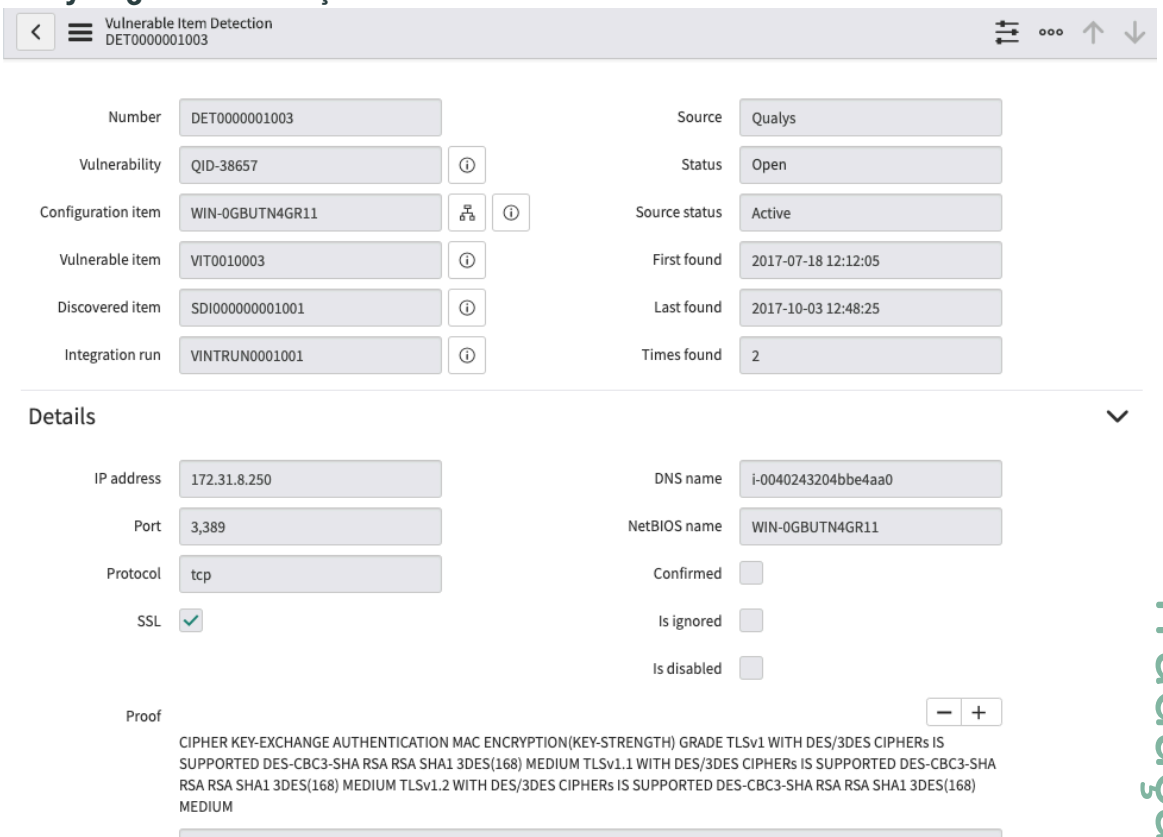
   c. Selecione as colunas da interface de caixa de listagem dupla para exibir dados específicos e clique em **OK**.

4. Com a guia Detecções selecionada, na coluna Status, clique em um item para abrir o registro de detecção e exibir os detalhes associados a esse item vulnerável, incluindo um resumo da solução (somente integração do Rapid7 InsightVM).

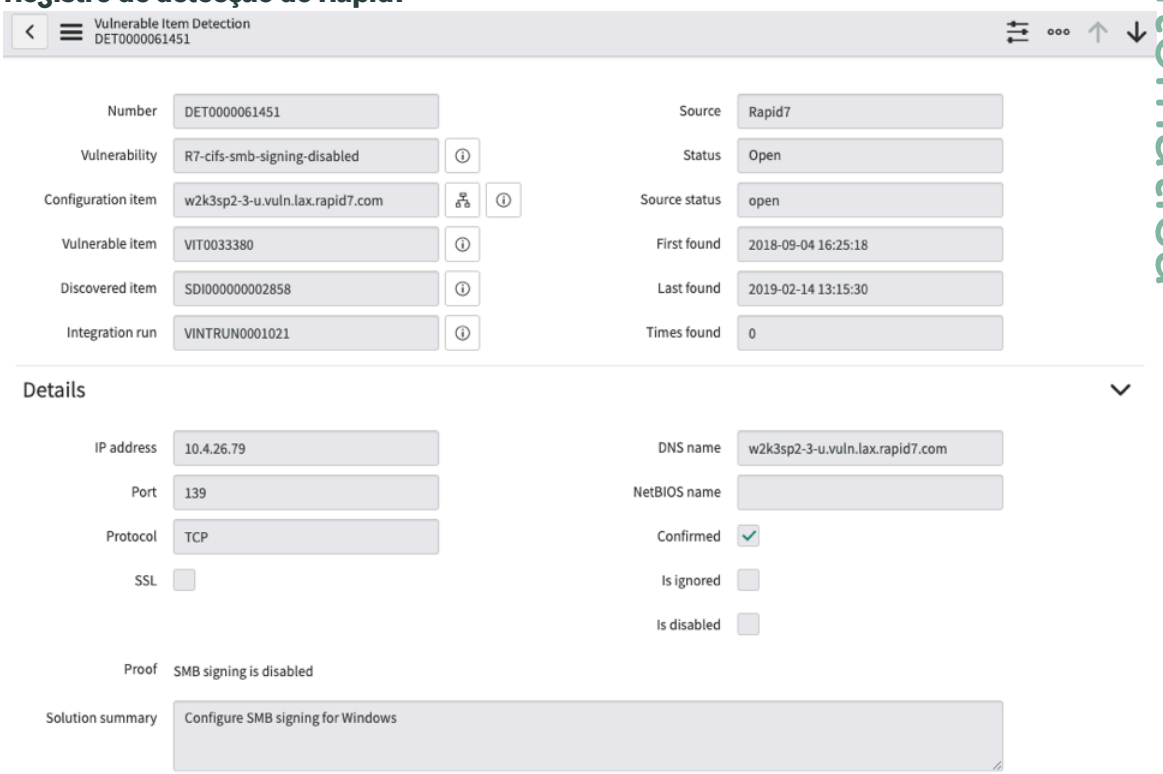
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Qualys registro de detecção



Registro de detecção do Rapid7

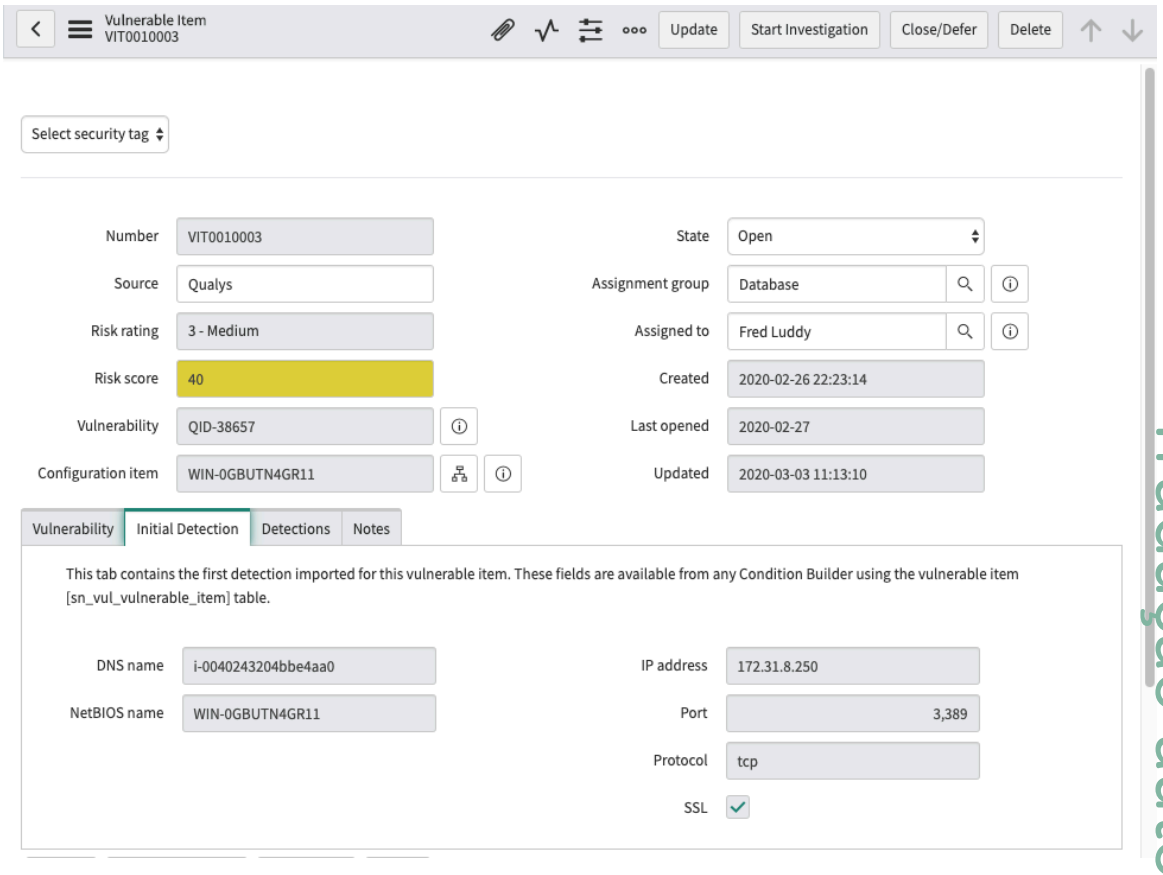


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

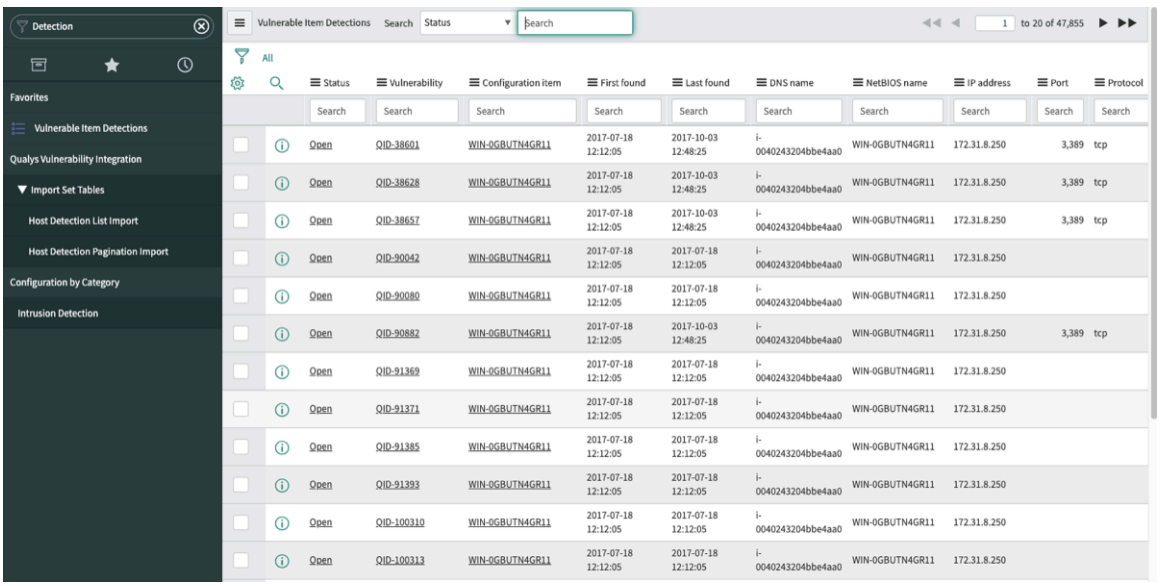
5. Retorne ao registro e selecione a guia Detecção inicial.

A guia Detecções iniciais exibe os dados importados do scanner de terceiros na primeira ocorrência da detecção. Essas informações na guia de detecção inicial não mudam conforme os dados de detecção são atualizados.



6. Opcional: Navegue até Detecções de item vulnerável para exibir a Lista de detecção de item vulnerável.

(Optional) A lista de Detecção de item vulnerável é exibida. Cada linha na lista de Detecções de itens vulneráveis representa uma detecção distinta. As colunas exibem os mesmos dados que o registro IV.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As detecções são abertas ou encerradas somente pelos dados encontrados por um scanner, elas não são revertidas dos IVs. Conforme as detecções são importadas, elas são usadas para criar IVs e atualizar os estados dos IVs⌧Se todas as detecções de um item vulnerável forem encerradas, esse item vulnerável será encerrado. No registro IV, o estado é fechadoe o subestado é fixo.

Nota:
Os erros são registrados enquanto:

- Processando anexos recuperados do scanner.
- Criar ou atualizar detecções ou itens vulneráveis.

Para obter informações sobre como lidar com erros de detecção, consulte Tratamento de erros para detecções.

Quando todos os IVs são encerrados para uma tarefa de correção, a tarefa de correção é encerrada.

Os IVs encerrados com um subestado **fixo** ou **obsoleto** serão reabertos se uma nova detecção for criada e os IVs puderem ser correspondidos com a nova vulnerabilidade.

Itens vulneráveis definidos como **Resolvidos** em sua instância, mas não transicionados para **Encerrado/Corrigido** pelas execuções de integração subsequentes serão reabertos se forem detectados durante novas verificações.

Quando todos os IVs são encerrados para uma tarefa de correção, o registro é encerrado.

Itens vulneráveis definidos como "Resolvidos" em sua instância, mas não transicionados para "Encerrado/Corrigido" pelas execuções de integração subsequentes, serão reabertos se forem detectados durante novas verificações.

Para Rapid7 detecções, agora está disponível uma opção na página de configuração do Rapid7 em sua instância para reabrir IVs resolvidos por idade. Se habilitado, os IVs definidos como **Resolvidos**, mas não transicionados para **Encerrado/Corrigido** pelas verificações subsequentes, retornam para **Aberto** após o número de dias inserido.

Para Qualys detecções, se o scanner continuar a encontrar IVs que foram definidos como "Resolvido", mas não transicionados para **Encerrado/Corrigido** pelas verificações subsequentes, esses IVs retornam para **Aberto** quando a última data encontrada for posterior à data Resolvido.

O que Fazer Depois

Para exibir mais dados, incluindo contagens de item e detecção, você pode Verificar Vulnerability Response registros de dados de detecção de item vulnerável na execução de integração (VINTRUN).

Verificar Vulnerability Response registros de dados de detecção de item vulnerável na execução de integração (VINTRUN)

A partir de registros de execução de integração em sua instância Now Platform®, você pode localizar dados de detecção de item vulnerável de integração de terceiros com base na data e hora das verificações. Verifique se a verificação foi concluída com sucesso, exiba o número (contagens) de detecções individuais, bem como todos os itens vulneráveis (IVs) que foram criados ou atualizados diretamente como resultado das verificações.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vuln.admin (obsoleto)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Você pode preferir ter as informações de execução da integração, data e hora da verificação ou o número do registro de execução da integração (VINTRUN#) do item vulnerável ou registros de detecção para ajudá-lo a localizar registros específicos das listas a seguir.

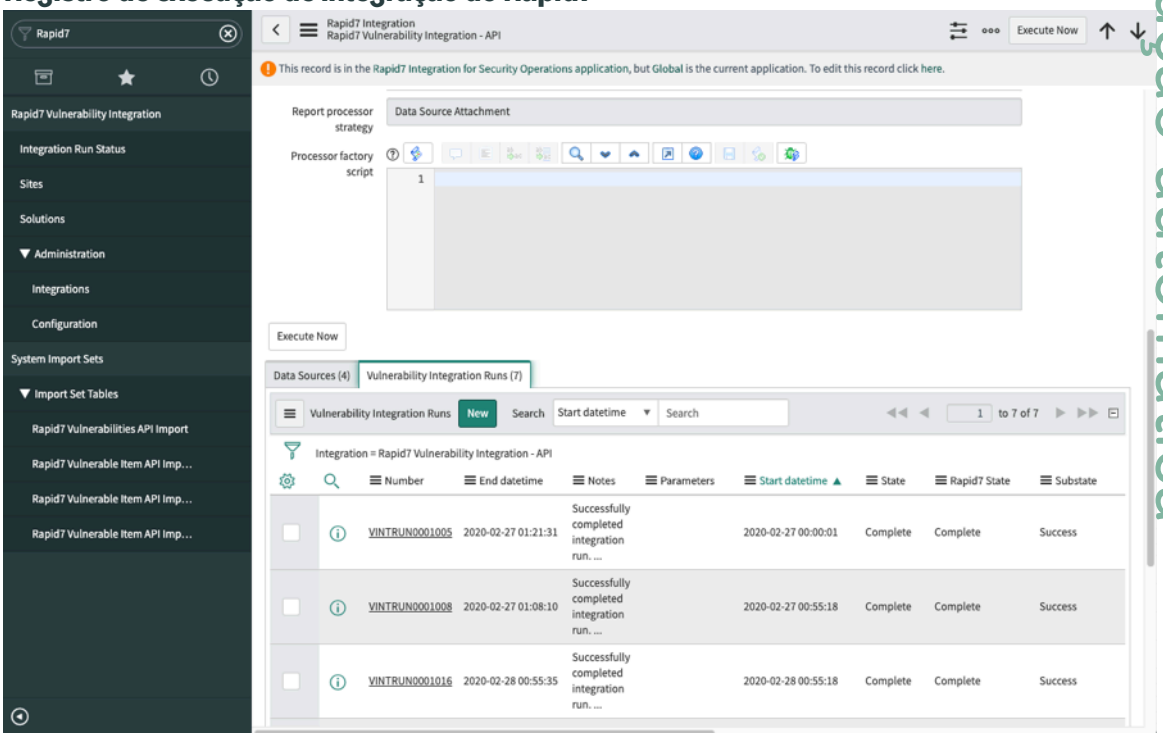
Procedimento

1. Escolha um para continuar.

2. Na parte inferior da página exibida, clique na guia **Execuções de integração de vulnerabilidade**.
3. Clique em um item nas colunas Número ou Origem da importação para abrir um registro.

   O registro de execução da integração é exibido.

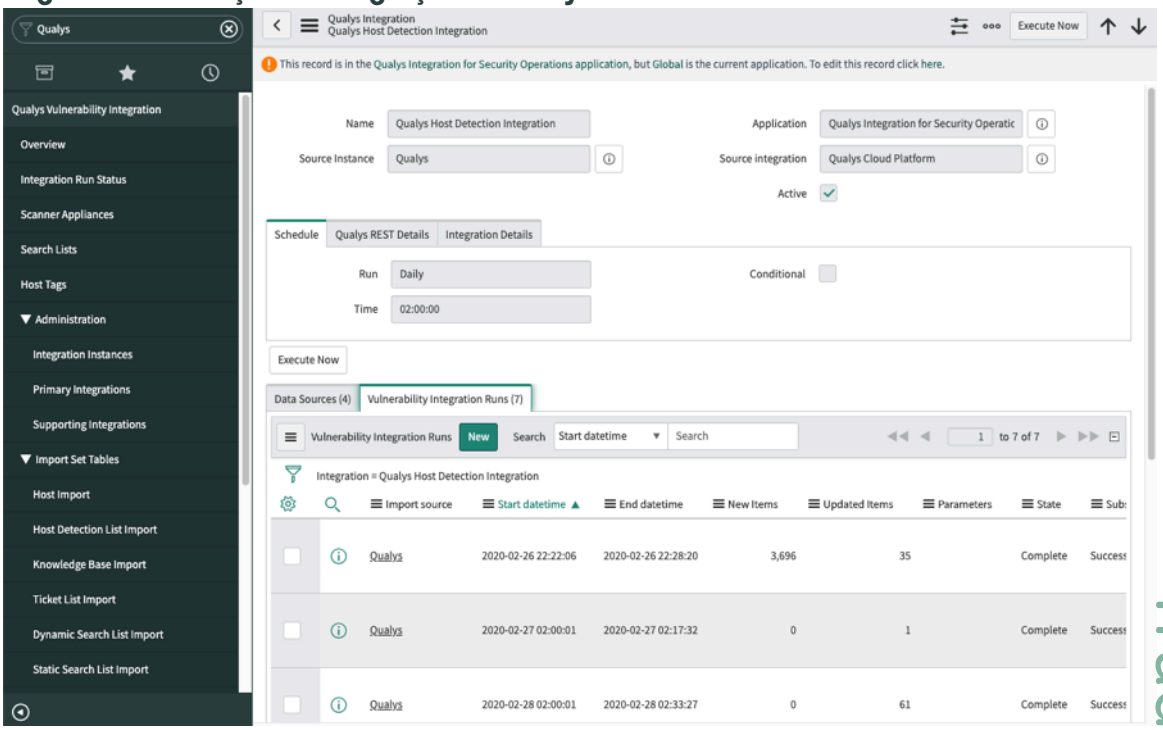
Registro de execução de integração do Rapid7



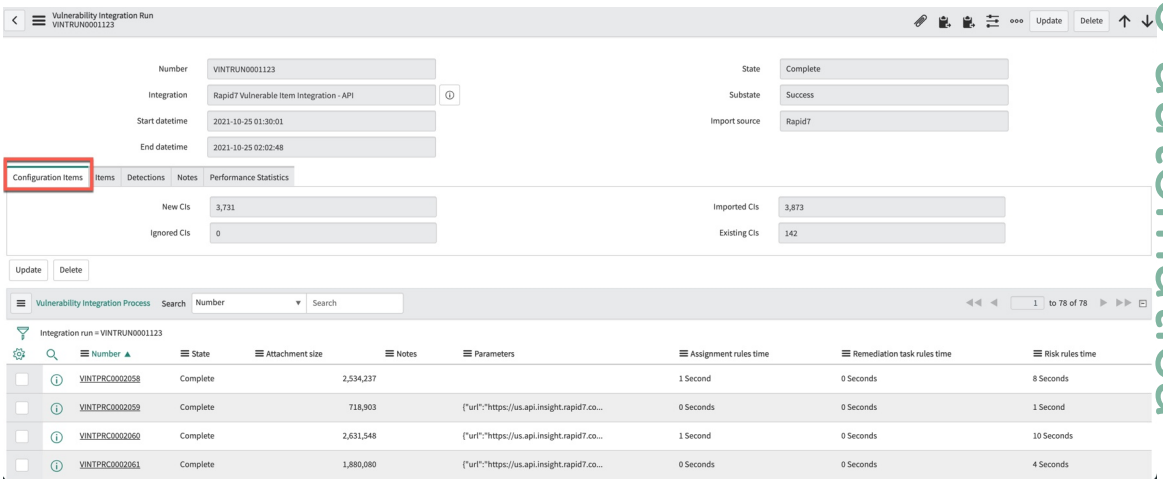
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Registro de execução de integração da Qualys



O registro de execução da integração é exibido. Você pode verificar no campo Estado que a integração foi executada com sucesso. Selecione a guia **Itens de configuração**.



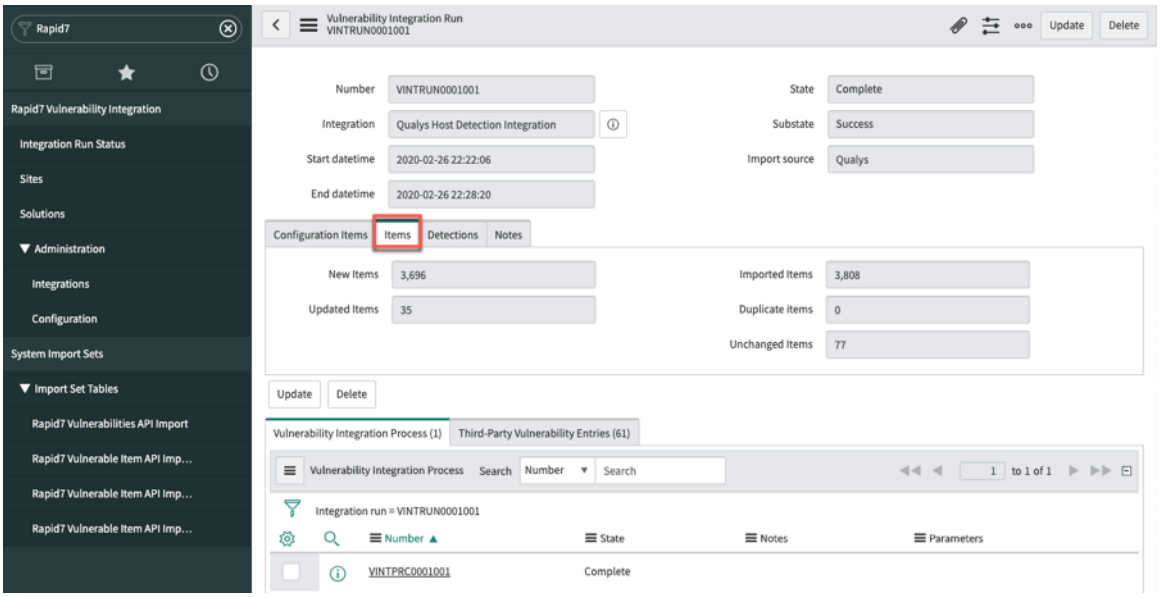
A guia Itens de configuração exibe as seguintes informações:

- A guia Itens de configuração exibe o número total de itens de configuração importados.
- O campo Novos ICs exibe o número de ICs criados como parte desta execução de integração.
- O campo ICs importados exibe a soma de todos os ICs nesta seção.
- O valor do campo ICs ignorados é sempre 0 para as Vulnerability Response integrações.
- O campo ICs existentes exibe o número total de ICs que já existem.

Clique na guia **Itens**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A guia Itens exibe as seguintes informações:

- A guia Itens exibe o número total de IVs importados. Você pode ver o total de detecções importadas adicionando os números listados na guia Detecções.
- O campo Novos itens exibe o número de itens vulneráveis criados a partir desta execução de integração.
- O campo Itens importados exibe a soma de todos os campos nesta seção.
- O campo Itens duplicados não está mais preenchido.
- O campo Itens atualizados exibe o número de vezes que os itens vulneráveis são atualizados durante esta execução de integração. Este valor não é o número de itens vulneráveis exclusivos que são atualizados. Se, por exemplo, um item vulnerável for atualizado duas vezes durante a execução da integração, ele será contado duas vezes e exibido como dois itens atualizados.
- O campo Itens inalterados exibe itens vulneráveis encontrados durante a execução da integração que já existem no banco de dados, mas não foram atualizados porque nenhum dos valores de campo relevantes foi alterado.

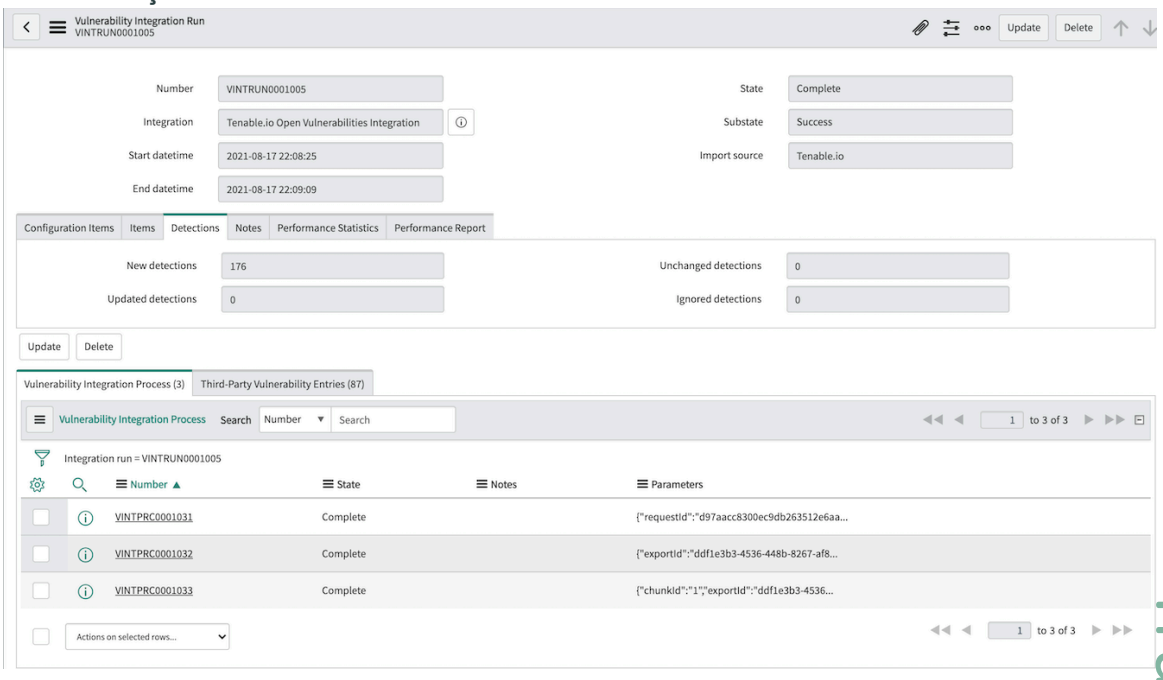
4. Clique na guia **Detecções**.

   Esta guia será exibida somente se a execução da integração tiver alguma detecções. Você pode verificar o total de detecções importadas adicionando os números listados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Detecções de VR v15.0



Nota:
Antes da v15.0, não havia campo para detecções ignoradas.

A guia Detecções exibe as seguintes informações:

- A partir da v15, um novo campo Detecções ignoradas foi adicionado para rastrear as detecções que antes eram ignoradas. Com esta implementação, a contagem de detecções importadas e a contagem rastreada nos registros de execução de integração se tornam consistentes. Esta funcionalidade foi implementada para todos os scanners, ou seja, Qualys Vulnerability Integration, Rapid7 Vulnerability Integration, Tenable Vulnerability Integration e Microsoft TVM.
- O campo Novas detecções exibe novas detecções criadas durante essa execução de integração.
- O campo Detecções inalteradas exibe as detecções encontradas durante a execução da integração que já existem no banco de dados, mas não foram atualizadas porque nenhum dos valores de campo relevantes foi alterado.
- O campo Detecções atualizadas exibe o número de vezes que as detecções são atualizadas durante esta execução de integração. Este valor não é o número de detecções exclusivas atualizadas. Se, por exemplo, uma detecção for atualizada duas vezes como parte da execução da integração, ela será contada duas vezes e exibida como duas detecções atualizadas.

Nota:
As detecções que não são exibidas nessas contagens são detecções que estão em um estado encerrado (Corrigido), porque os registros fixos são usados para atualizar os IVs existentes. Se você quiser mais visibilidade para esses registros de detecção, poderá exibir os IVs encerrados que são criados quando não há um IV correspondente existente em um estado aberto. Para obter mais informações sobre vulnerabilidades no estado corrigido que você pode habilitar no Assistente de configuração para a integração da Qualys, consulte Configuração de Vulnerability Response usando o Assistente de configuração.

5. Clique em um item nas colunas Número ou Origem da importação para abrir um registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de dados de patch e programação de patches no Vulnerability Response

A partir da v16.1 de Vulnerability Response, você pode programar patches e exibir dados de patch junto com a solução e outras informações de vulnerabilidade em registros no ambiente clássico e nos espaços Vulnerability Response na sua instância Now Platform.

Funções necessárias

Os usuários precisam de funções específicas para a integração de orquestração de patches que você está usando para importar seus patches para exibir dados e programar patches. Consulte as integrações compatíveis para obter mais informações.

- Noções básicas sobre a integração de orquestração de patches do BigFix HCL com Vulnerability Response e Noções básicas sobre a integração de orquestração de patches [Vulnerability Response com Microsoft SCCM.
- Exibição de dados de orquestração de patches nos painéis Vulnerability Response no ambiente clássico.
- Exiba dados em cartões de pontuação no Vulnerability Response Espaços.

Programação de patches

Você pode programar patches dos seguintes registros:

- Atualização de patch (VPU)
- Tarefa de correção (RT)
- Item descoberto (SDI)

Dados de patch no ambiente clássico

No ambiente clássico na aplicação Vulnerability Response :

- Para exibir registros de atualização de patch, navegue até **Todos** > **Vulnerability Response** > **Patches**.
- Para exibir Soluções, navegue até **Todos** > **Vulnerability Response** > **Soluções**.
- Para exibir IVs atribuídos a você que tenham patches, navegue até **Todos** > **Vulnerability Response** > **Itens vulneráveis** > **Atribuído a mim com patches**.
- Para exibir tarefas de correção, navegue até **Todos** > **Vulnerability Response** > **Itens vulneráveis** > **Atribuído a mim com patches**
- Para exibir registros de item descoberto, navegue até **Todos** > **Security Operations** > **Itens descobertos**.

Dados de patch e acúmulo de estado para orquestração de patches no Vulnerability Response

A partir da v16.1 de Vulnerability Response, os dados e os estados do patch são acumulados para a atualização de patch e outros registros na aplicação Vulnerability Response.

Registros de atualização de patch nos espaços no ambiente clássico em Vulnerability Response

Informações sobre patches, soluções de vulnerabilidade e vulnerabilidades estão todas conectadas na aplicação Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os dados de patch e os dados e status de rollup de patch são exibidos nos registros em sua instância. Os registros de patch são incluídos como parte do recurso de orquestração de patches desta integração com Vulnerability Response. Exiba registros de patch (VPU) em espaços do Vulnerability Response na exibição de lista no espaço de correção de TI. Os registros de atualização de patch na exibição clássica e nos espaços do Vulnerability Response incluem os seguintes dados:

- Dados de solução de vulnerabilidade e informações de fornecedores de patch importados pela aplicação Vulnerability Solution Management.
- Status de correção de origem que inclui o número total de dispositivos com uma vulnerabilidade que pode ser corrigida por um patch e todos os dispositivos que não tenham atualizações.
- Status de correção que inclui % de IVs corrigidos e o total de IVs que têm um patch como preferencial.
- Dispositivos associados, itens vulneráveis, implantações de patch e solicitações de patch nos links relacionados em registros na exibição de classe. Esses dados são exibidos em guias em registros nos espaços do Vulnerability Response.
- Solicitações de patch que os responsáveis pela correção enviaram para aprovação.

Funções necessárias

Os usuários precisam de funções específicas para a integração de orquestração de patches que você está usando para exibir dados e programar patches. Consulte as integrações compatíveis para obter mais informações.

- Noções básicas sobre a integração de orquestração de patches do BigFix HCL com Vulnerability Response e Noções básicas sobre a integração de orquestração de patches [Vulnerability Response com Microsoft SCCM.
- Exibição de dados de orquestração de patches nos painéis Vulnerability Response no ambiente clássico.
- Exiba dados em cartões de pontuação no Vulnerability Response Espaços.

Dados de patch e acúmulo de estado

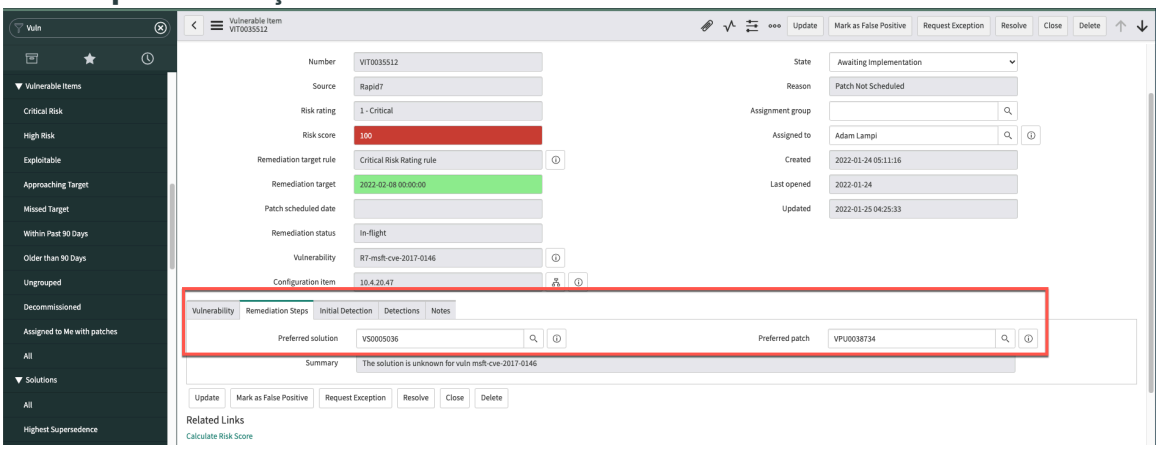
Para exibir os itens vulneráveis que têm patches e que estão atribuídos a você no ambiente clássico, navegue até **Todos** > **Vulnerability Response** > **Itens vulneráveis** > **Atribuído a mim com patches**.

Se um registro de item vulnerável for preenchido com um patch preferencial, ele fará a transição automaticamente para **Aguardando implementação** somente se o estado do IV não for **Encerrado**, **Resolvido**, **Adiado** ou **Em revisão**. Para fazer uma busca detalhada nos dados para exibir a solução preferencial e outros dados, clique na guia **Correção** no registro IV.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Etapas de correção



Um IV com um patch preferencial muda para **Aguardando implementação** nos seguintes casos:

- Se um patch estiver programado para implantação em um IC que faz parte de uma importação de coleção e o IC tiver um IV associado, o motivo pelo qual o IV está **Aguardando implementação** é **Patch programado**.
- Se um patch estiver programado para implantação em um IC que faz parte de uma importação de coleção e o IC tiver um IV associado e a data de destino da correção (prazo) posterior à data do tempo de correção (TTR), o estado de o IV está **Aguardando implementação** com o motivo como **Patch programado (data de destino ausente)**.
- Se um patch não estiver programado para implantação em um IC que faz parte de uma importação de coleção, o estado do IV será **Aguardando implementação**, com o motivo como **Patch não programado**.

Clique no ícone de informações do **patch preferencial** para abrir as atualizações de patch e exibir as seguintes informações nos links relacionados:

Itens vulneráveis

Itens vulneráveis associados a este patch.

Dispositivos associados

Dispositivos que têm atualizações e aqueles que não têm atualizações.

Implantações de patch

Implantações programadas para este patch em máquinas individuais (ativos) ou em grupos de ativos.

Solicitações de patches

Uma lista de solicitações de patch que foram enviadas para aprovação antes de serem programadas para implantação.

Patches em potencial

Patches que podem solucionar uma vulnerabilidade.

Clique no ícone de **informações do patch preferencial** para abrir o registro e exibir as informações listadas anteriormente, além dos seguintes dados de atualização do patch:

Status de correção da fonte

O total de dispositivos que exigem este patch e todos os dispositivos que não tenham o patch.

Status da Correção

O status (total de IVs, percentual corrigido, IVs adiados) dos IVs que têm este patch preferencial.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Patches e soluções preferenciais

Quando uma vulnerabilidade importada corresponde a um ativo em seu Configuration Management Database (CMDB), um item vulnerável (IV) é criado em Vulnerability Response. Se o item de configuração (IC) associado a este IV também for importado de um fornecedor de patch de terceiros e for mostrado como sem um patch para a mesma vulnerabilidade, um patch preferencial será listado e implementado em suas soluções. Essas informações permitem que você saiba que um ativo (IC) tem uma correção de um patch disponível que é a melhor correspondência para sua vulnerabilidade.

Exibição de patches sem soluções

Após uma importação, se nenhum dado de solução de vulnerabilidade estiver disponível, o campo de **solução de vulnerabilidade** no registro de atualização de patch será deixado em branco. Para obter mais informações sobre como exibir informações para esses tipos de patches, consulte Exibir patches sem soluções em Vulnerability Response.

Exibir patches sem soluções em Vulnerability Response

A partir da v16.0 de Vulnerability Response, para patches que não têm soluções após uma importação, o sistema pesquisa IDs de patch nos dados de referência de vulnerabilidade para que você possa exibir esses patches em registros de vulnerabilidade.

Patches sem soluções

Função necessária: sn_vul.vulnerability_admin.

Os dados importados da orquestração de patches e das aplicações de solução de vulnerabilidade, bem como das integrações do scanner de patch, são processados, conectados e exibidos na aplicação Vulnerability Response em registros de atualização de patch.

Quando existe uma solução para uma vulnerabilidade, as informações relacionadas são correlacionadas em sua instância e acumuladas dos patches, para as soluções de vulnerabilidade e para as vulnerabilidades. Para exibir essas informações, navegue até **Todos** > **Vulnerability Response** > **Patches** > **Todos**.

Após uma importação, se nenhum dado de solução de vulnerabilidade estiver disponível, o campo de **solução de vulnerabilidade** no registro de atualização de patch será deixado em branco. Para que você possa ver as informações da solução relacionada a esses patches, uma propriedade do sistema, [**sn_vul_patch_orch.no_solution_patch_rollup**], é ativada por padrão em sua instância. Esta propriedade pesquisa IDs de boletim e IDs de artigo nos dados de referência de vulnerabilidade das importações do scanner. Se uma correspondência for encontrada, os dados associados serão preenchidos na tabela de possíveis patches e essas informações serão exibidas nas listas relacionadas de registros de vulnerabilidade.

Se você tiver um grande número de vulnerabilidades ou o trabalho programado de acúmulo estiver demorando muito para ser concluído, convém desativar esta propriedade do sistema para evitar possíveis problemas de desempenho. No entanto, observe que se você desativar esta propriedade do sistema, os dados da solução importada não serão pesquisados nem acumulados para suas vulnerabilidades sem soluções.

Como um usuário com a função sn_vul.vulnerability_admin, para desativar a propriedade do sistema, siga estas etapas:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegar até **sys.properties.list**.
2. Localize **sn_vul_patch_orch.no_solution_patch_rollup** e clique nele para abrir o registro.
3. No campo Valor, digite `false`.
4. Clique em **Atualizar**.

Exibição de dados de orquestração de patches nos painéis Vulnerability Response

A partir da v16.1, você pode exibir dados de atualização de patch no ambiente clássico nos painéis incluídos com a aplicação Vulnerability Response.

Os espaços Vulnerability Response incluem visualizações de dados que podem ajudar a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a severidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizadas conforme os dados de vulnerabilidade mudam. Para obter mais informações, consulte Espaço para gerentes de vulnerabilidades e Explorando o Espaço de correção de problemas de TI.

Você também pode exibir esses dados nos painéis do CISO e do Vulnerability Management (PA) se tiver uma assinatura do Performance Analytics.

Você também pode exibir dados de patch no ambiente clássico. Para obter mais informações sobre as funções necessárias e como exibir dados nos painéis Vulnerability Response no ambiente clássico que estão incluídos com a aplicação Vulnerability Response e aqueles que exigem uma assinatura separada, consulte Usando os painéis padrão Vulnerability Response.

Exibir uma solução

Exiba todas as soluções, soluções com maior substituição e soluções associadas a itens vulneráveis para informar suas atividades de correção.

Antes de Iniciar

Função necessária:
sn_vul.read, sn_vul.vulnerability_admin ou sn_vul.remediation_owner

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa

Como analista de vulnerabilidade ou proprietário de correção, você pode exibir diferentes conjuntos de soluções relacionados a itens vulneráveis.

Nota:
Os registros de solução são somente leitura, exceto em **Anotações** na seção **Anotações internas** ou soluções criadas pelo usuário.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Soluções**.
2. Escolha uma lista de soluções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Você pode filtrar uma lista de soluções usando caracteres curinga para o nome do produto.

3. Para revisar, clique em cada item.
4. **Opcional:** Insira anotações na guia **Anotações** e clique com o botão direito do mouse em **Salvar** para permanecer na página ou clique em **Atualizar** para salvar e retornar à lista de **Soluções de vulnerabilidade**.

Nota:
Se você tiver apenas a função sn_vul.read, não poderá executar esta etapa.

Criar uma solução de vulnerabilidade

Crie uma solução de vulnerabilidade para que você possa rastrear soluções de vulnerabilidade que não sejam cobertas pelo conteúdo da solução de terceiros.

Antes de Iniciar

Função necessária: admin, sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) ou Vulnerability.write
Solução de gerenciamento de vulnerabilidade é um recurso disponível na aplicação Vulnerability Response. Solução de gerenciamento de vulnerabilidade requer uma assinatura separada.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa

Você pode criar uma solução a partir de qualquer uma das listas de soluções. Você deve instalar a aplicação Vulnerability Solution Management antes de criar uma solução.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Soluções**.
2. Escolha uma lista de soluções: **Todos**, **Maior substituição** ou **Com itens vulneráveis**.
3. Clique em **Nova**.
4. Preencha os campos editáveis no formulário, conforme apropriado.
   Você pode deixar os campos não utilizados em branco. Para obter mais informações sobre campos individuais, consulte Campos de formulário de solução.
5. Clique com o botão direito do mouse em **Salvar** no cabeçalho.
   O registro da solução é adicionado e aparece nas listas **Todos** e **Substituição mais alta**, por padrão.
6. As Listas relacionadas são exibidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode associar esta solução às seguintes listas relacionadas: **Itens vulneráveis , Vulnerabilidadesde terceiros**, **CVEs**, **Soluções substitutas** e **Soluções anteriores**. Escolha uma vulnerabilidade ou solução e clique em **Enviar**.

Nota:

Solução de gerenciamento de vulnerabilidade associa automaticamente itens vulneráveis e tarefas de correção a soluções quando os registros de vulnerabilidade são associados manualmente a soluções.

Itens vulneráveis reatribuídos manualmente a outra solução não são atualizados automaticamente com as mudanças de solução no nível de vulnerabilidade.

Se você quiser excluir o relacionamento entre uma vulnerabilidade de terceiros e uma solução porque não é relevante para o IC que você está corrigindo ou não é uma preocupação em seu ambiente, consulte Excluir manualmente soluções de registros de terceiros ou vice-versa.

Excluir manualmente soluções de registros de terceiros ou vice-versa

Exclua o relacionamento entre uma vulnerabilidade de terceiros e uma solução porque ele não é relevante para o IC que você está corrigindo ou não é uma preocupação em seu ambiente. Exclua manualmente as soluções usando uma vulnerabilidade de terceiros ou um registro de solução.

Antes de Iniciar

Função necessária: sn_vul.write
sn_vul.remediation_owner

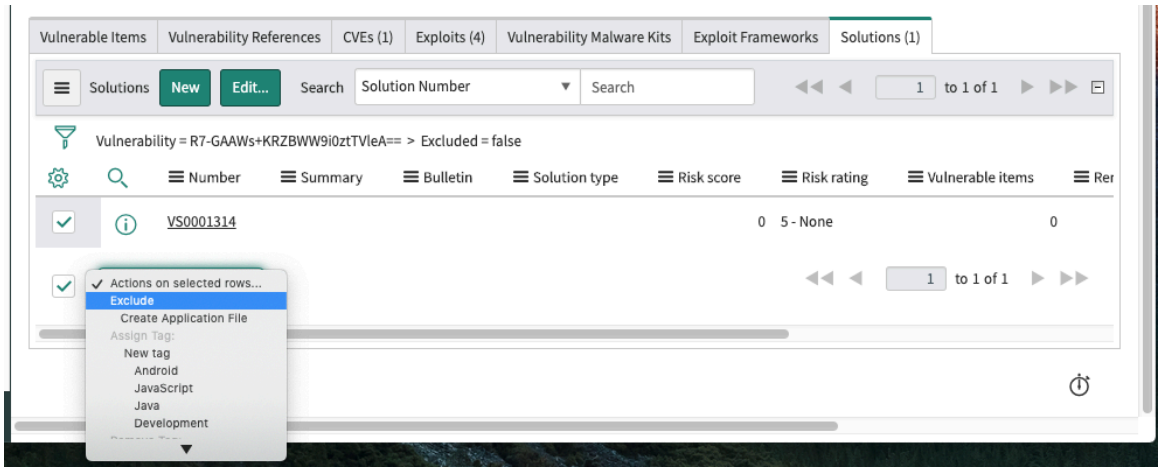
Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Bibliotecas** > **Terceiros** ou **Vulnerability Response** > **Todas as soluções**
2. Abra uma vulnerabilidade de terceiros ou registro de solução.
   a. Para um registro de terceiros: selecione a guia relacionada **Soluções**.
   b. Para obter um registro de solução: selecione a guia relacionada **Vulnerabilidades de terceiros**.
3. Marque a caixa ao lado de cada registro de vulnerabilidade ou solução que você deseja excluir.
4. No menu suspenso **Ações em linhas selecionadas**, escolha **Excluir**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



O registro do terceiro ou da solução não aparece mais na guia relacionada.

Os relacionamentos de vulnerabilidade de terceiros com as soluções também são excluídos quando as soluções são atualizadas ou se o trabalho noturno estiver habilitado.

Os relacionamentos de vulnerabilidade de terceiros com as soluções são excluídos durante o trabalho programado à noite.

Excluir vulnerabilidades de terceiros significa que a solução não é mais um fator para qualquer avaliação de solução preferencial. Impactos da exclusão:

- Todas as contagens para soluções, já que a vulnerabilidade de terceiros, os itens vulneráveis (IVs) e os itens de configuração (ICs) anexados à vulnerabilidade de terceiros não contam mais para a solução.
- Determinar a solução preferencial para a vulnerabilidade de terceiros e, por extensão, a solução preferencial de quaisquer IVs anexados e tarefas de correção que contenham o IV.

Triagem de vulnerabilidades automaticamente

A revisão e a triagem de novas vulnerabilidades são necessárias para garantir a correção bem-sucedida. Transforme as importações de vulnerabilidades em tarefas de correção com atribuição automatizada de item vulnerável (IV), cálculo de risco, metas de correção e agrupamento de IV.

Começando com vulnerabilidades importadas, reconcilie os ativos não encontrados no CMDB, priorize os resultados, traduza isso em atividades de correção que são atribuídas automaticamente, orquestre o processo de correção e confirme a conclusão com uma verificação de validação.

Novos itens vulneráveis geralmente são classificados em tarefas de correção na importação, com base nas regras de tarefas de correção. Às vezes, os itens vulneráveis não podem ser agrupados ou não contêm um item de configuração reconhecido.

Uma visão geral do processo de triagem de vulnerabilidade:

- Faça login na sua instância Vulnerability Response.
- Valide se suas regras (Pesquisa de IC, Atribuição) para o item vulnerável estão funcionando conforme o esperado. Para obter informações sobre como revisar as Regras de pesquisa de IC, consulte Regras de pesquisa de IC para identificar itens de configuração de Vulnerability Response integrações de vulnerabilidade de terceiros. Para obter informações sobre regras de atribuição, consulte Vulnerability Response visão geral de regras de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Devido ao grande volume nas importações de dados, é necessário ter cuidado com a atribuição automatizada de itens vulneráveis.

- Valide se as metas de correção estão corretas. Consulte Vulnerability Response regras de destino de correção para obter informações sobre como as regras de destino de correção funcionam e como revisá-las.
- Exiba itens vulneráveis desagrupados.
  - Observando os itens vulneráveis desagrupados, considere revisar as regras do grupo e executar uma nova verificação. Para obter mais informações, consulte Criar ou editar Vulnerability Response regras de tarefa de correção.
  - Agrupe manualmente os itens vulneráveis. Como criar manualmente uma tarefa de correção no Vulnerability Response para obter mais informações.
  - Revise as pontuações de risco dos itens vulneráveis em suas tarefas de correção. Para obter mais informações, consulte Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade.
  - Feche itens vulneráveis mais antigos não detectados recentemente por suas integrações de terceiros. Para obter mais informações, consulte Fechamento automático de itens vulneráveis e detecções.
- Exibir e reclassificar itens de configuração incompatíveis.
- Pesquise o que precisa ser feito para correção.

  Esta etapa pode incluir:

  - Determine com o que lidar agora e o que você pode adiar. Essa determinação geralmente é baseada na pontuação de risco, nos sistemas afetados e nos patches com janelas de mudança.

    Nota:
    As regras de destino de correção pertencem a itens vulneráveis. Essas regras são executadas quando o item vulnerável é importado. Essas regras foram criadas anteriormente no Assistente de configuração.

  - Atualizar itens vulneráveis, se necessário, e Exibir o status da meta de correção de um item vulnerável Vulnerability Response.
  - Crie uma **solicitação de mudança** e atribua a tarefa de correção a um grupo de atribuição (Operações de TI) para correção.

    Nota:
    Se a vulnerabilidade constitui um incidente de segurança e o plug-in Security Incident Response (com.snc.security_incident) estiver ativado, você poderá criar registros de incidentes de segurança a partir das tarefas de correção.

  - Depois de enviar uma ou mais solicitações de mudança, mova o estado do grupo para Sob investigação.

Editar itens vulneráveis em massa no Vulnerability Response

Edite itens vulneráveis em massa para economizar tempo selecionando campos e executando um trabalho de edição em massa assíncrono em segundo plano.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Por Que e Quando Desempenhar Esta Tarefa

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

A partir de Vulnerability Response v21.0, você pode cancelar a atribuição de itens vulneráveis de host em massa na página Lista em Vulnerability Manager Workspace. Para obter mais informações, consulte Editar itens vulneráveis de host em massa no Vulnerability Manager Workspace.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Vulnerabilidades** > **Itens vulneráveis**.
2. Selecione os itens vulneráveis executando uma das seguintes ações:
   - Marque a caixa de seleção ao lado de cada item se quiser usar a opção **Somente itens selecionados** no campo Seleção de registro.
   - Aplique filtros se quiser usar a opção de **filtro Todos os itens vulneráveis que correspondem** ao campo Seleção de registro.
3. Selecione o botão **Edição em massa**.
4. No modal de edição em massa, preencha os campos.

Campo	Descrição
Seleção de registro	Registros a serem atualizados. As opções são: ○ Somente Itens vulneráveis selecionados ○ Todos os itens vulneráveis que correspondem ao filtro ○ Tarefa de correção ○ Entrada de vulnerabilidade
Estado	Mudança para o **Estado** no item vulnerável. As opções são: ○ Não Atualizar ○ Em aberto ○ Sob Investigação ○ Aguardando Implementação ○ Adiado **Nota:** ▪ Quando você seleciona essa opção, os campos Motivo, Descrição resumida, Até e Informações adicionais são exibidos. ▪ Quando você adia VITs, uma tarefa de correção é criada e essa tarefa é enviada para aprovação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Encerrado **Nota:** ▪ Quando você seleciona esta opção para marcar os registros como falso-positivos, os campos Motivo, Descrição resumida, Até e Informações adicionais são exibidos. ▪ Quando você marca os registros como falso-positivos, uma tarefa de correção é criada e essa tarefa é enviada para aprovação. ○ Resolvido
Solução preferencial	Solução que é direcionada para corrigir todos os itens vulneráveis selecionados para edição em massa. Selecione a mudança para o campo **Solução preferencial** no item vulnerável (VITs). As opções são de uma lista de pesquisa de soluções preferenciais disponíveis para os VITs selecionados. **Nota:** ○ O conjunto de soluções preferenciais disponíveis é uma interseção de todas as possíveis soluções das vulnerabilidades em todos os VITs selecionados. ○ Ao selecionar **Seleção de registro** > **Entrada de Vulnerabilidade** para uma edição em massa, todos os VITs da vulnerabilidade serão definidos para a solução preferencial selecionada. **Nota:** Esta operação não define a **solução preferencial** no nível de entrada da vulnerabilidade. Definir a **solução preferencial** no nível de entrada de vulnerabilidade definiria a **solução preferencial** para todos os novos VITs daqui para frente. A edição em massa modifica somente o conjunto atual de VITs. ○ As vulnerabilidades distintas nos critérios de seleção são limitadas a 500. Se houver mais de 500 vulnerabilidades distintas, uma mensagem de aviso será exibida solicitando que você selecione VITs com critérios diferentes para definir a **solução Preferencial**. ○ O número total de soluções que podem ser mostradas na lista de pesquisa é limitado a 170. Se houver mais de 170 soluções, uma mensagem de aviso será exibida. O valor atualizado é mostrado na exibição de lista de itens vulneráveis.
Patch preferencial	Patch que é direcionado para corrigir todos os itens de vulnerabilidade selecionados para edição em massa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: ◦ Você deve instalar o Patch Orchestration para exibir a lista de patches preferenciais. ◦ O conjunto de patches preferenciais disponíveis é uma interseção de todos os possíveis patches em todos os VITs selecionados. ◦ As vulnerabilidades distintas nos critérios de seleção são limitadas a 500. Se houver mais de 500 vulnerabilidades distintas, uma mensagem de aviso será exibida solicitando que você selecione VITs com critérios diferentes para definir o **patch Preferencial**. ◦ O número total de patches que podem ser mostrados na lista de pesquisa é limitado a 170. Se houver mais de 170 patches, uma mensagem de aviso será exibida.
Motivo	Motivo para adiar registros: ◦ Aguardando janela de manutenção ◦ Correção indisponível ◦ Risco aceito ◦ Redução do controle no local ◦ Outro Motivo para fechar os registros: ◦ Falso-positivo **Nota:** ▪ Quando você seleciona esta opção, os campos Descrição resumida, Até e Informações adicionais são exibidos. ▪ Uma tarefa de correção é criada quando você marca os registros como falso-positivos e essa tarefa é enviada para aprovação. ◦ Cancelado ◦ Corrigidos **Nota:** Este campo aparece quando você seleciona o Estado como Adiado ou Encerrado.
Descrição resumida	Breve nota que descreve o motivo do adiamento e das solicitações de falso-positivo encerradas. Essas informações são refletidas no campo Descrição da tarefa de correção criada para solicitações de adiamento e falso-positivo encerradas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Este campo aparece quando você seleciona o Estado como Adiado e Encerrado-Falso-positivo.
Até	Data até a qual o registro permanece adiado. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado.
Informações adicionais	Outras informações necessárias. Essas informações são refletidas no campo Informações adicionais na guia Visão geral. Se sua solicitação de adiamento for aprovada, essas informações adicionais aparecerão como anotações de adiamento no VIT e na tarefa de correção. **Nota:** Este campo aparece quando você seleciona o Estado como Adiado e Encerrado-Falso-positivo.
Cancelar atribuição	Todos os itens selecionados não estão atribuídos ao grupo de atribuição e ao proprietário de correção. Para obter mais informações sobre como um proprietário de correção pode remover as atribuições de itens vulneráveis, consulte Remover atribuições de itens vulneráveis para você ou seus grupos. **Nota:** ○ Este campo aparece quando você seleciona o Estado como Não atualizar. ○ Quando você cancela a atribuição de registros, uma tarefa de correção é criada e essa tarefa é enviada para aprovação.
Grupo de atribuição	Grupo de atribuição para o VIT. Selecione manualmente ou use Recomendações de atribuição se estiver habilitado. **Nota:** Este campo é desabilitado quando você marca a caixa de seleção **Cancelar atribuição**.
Anotações de trabalho	Texto que você insere para descrever as mudanças.

5. Selecione **OK**.
   Um trabalho assíncrono de edição em massa atualiza os registros selecionados. O número do trabalho com um link é exibido na página Itens vulneráveis, onde você pode exibir seu status. Uma tarefa de correção é criada com os itens vulneráveis selecionados ao adiar, cancelar a atribuição ou fechar (falso-positivo) itens vulneráveis em massa. E esta tarefa é enviada para aprovação.

Itens vulneráveis não agrupados Vulnerability Response

Itens vulneráveis são atribuídos automaticamente a uma tarefa de correção quando são importados. No entanto, às vezes, se um item vulnerável (IV) for criado manualmente, por exemplo, o IV pode se tornar um órfão. O módulo de item vulnerável não **agrupado** lista os itens vulneráveis sem um grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Os processos automatizados de integração não criam órfãos, portanto, espera-se que este caso de uso seja pequeno.

O desagrupamento ocorre se um item vulnerável foi criado sem uma vulnerabilidade ou se não houver nenhuma regra de tarefa de correção que atribua o IV a um grupo.

Nesse caso, revise a lista de itens vulneráveis desagrupados navegando até **Todos** > **Vulnerability Response** > **Itens vulneráveis** > **Desagrupado**.

Após a revisão, suas opções são as seguintes:

- Você pode Criar ou editar Vulnerability Response regras de tarefa de correção para capturar todos os itens que aparecem nesta lista.
- Você pode Como criar manualmente uma tarefa de correção no Vulnerability Response e adicionar manualmente itens desta lista ao grupo ou definir uma condição que corresponda a esses itens.
- Você pode abrir uma tarefa de correção existente e adicionar itens vulneráveis relevantes ao grupo, desde que ele esteja no estado Aberto ou Em investigação.

Nota:
Itens vulneráveis adicionados manualmente não são removidos automaticamente das tarefas de correção por regras de tarefa de correção ou condições de grupo.

Para obter mais informações sobre como as tarefas de correção e as regras de tarefa se comportam, consulte Vulnerability Response tarefas de correção e regras de tarefa visão geral.

Exibir itens vulneráveis desagrupados Vulnerability Response

Itens vulneráveis que não são atribuídos a um grupo são colocados em uma lista visível.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)
Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Vulnerabilidades** > **Itens vulneráveis desagrupados**.
2. Revise os itens vulneráveis na lista.
3. Clique em cada item vulnerável para exibir e determinar como incluir em um grupo.

Adicionar manualmente um item vulnerável a uma tarefa de correção

Se um item vulnerável for deixado desagrupado, você poderá adicioná-lo a uma tarefa de correção.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)
Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Procedimento

1. Registre o número vulnerável.
2. Navegar até **Todos** > **Vulnerability Response** > **Tarefas de correção**.
3. Escolha uma tarefa de correção (VUL) para o item vulnerável.
4. Selecione **Editar** no canto inferior direito.
5. Insira o número do **item vulnerável** no campo de pesquisa da Coleção.
6. Selecione o item vulnerável da coleção e adicione à lista.
7. Clique em **Salvar**.

Remover atribuições de itens vulneráveis para você ou seus grupos

Reatribua registros de item vulnerável nas aplicações Vulnerability Response e Application Vulnerability Response.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa

Se você determinar que os itens vulneráveis (VITs) não estão dentro do seu escopo de correção ou se achar que os registros foram atribuídos incorretamente a você ou aos seus grupos, poderá remover a si mesmo ou aos seus grupos dos campos **Atribuído a** e **Grupo de atribuição** no item vulnerável e nos registros de tarefa de correção.

O botão **Cancelar atribuição** é exibido nos seguintes registros em qualquer estado diferente de Encerrado ou Resolvido:

- Tarefas de correção (VULs) no ambiente clássico e nos espaços Vulnerability Response. Se uma tarefa de correção for atualizada com este recurso, os campos **Atribuído a** e**Grupo de atribuição** em todos os VITs associados também serão limpos.
- Itens vulneráveis (VITs) no ambiente clássico e nos espaços Vulnerability Response.
- Itens vulneráveis da aplicação (AVITs).
- Itens vulneráveis de contêiner (CVITs).

Procedimento

1. No ambiente clássico ou no Espaço de trabalho do proprietário de correção de TI, navegue até um registro de item vulnerável (VIT) atribuído a você que esteja em qualquer estado diferente de Encerrado ou Resolvido.
2. Para limpar os campos **Atribuído a** e **Grupo de atribuição**, na parte superior do registro, selecione **Cancelar atribuição**.
3. **Opcional:** Como alternativa, navegue até um AVIT atribuído a você ou aos seus grupos e clique em **Cancelar atribuição** para limpar os campos de atribuição.
4. Na caixa de diálogo Cancelar atribuição, forneça as anotações de trabalho e selecione **Enviar**.
5. **Opcional:** Se você quiser limpar os campos de atribuição de vários VITs em uma lista, selecione os VITs desejados e selecione **Edição em massa**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Na caixa de diálogo Edição em massa do item vulnerável, selecione **Somente itens vulneráveis selecionados** no campo **Seleção de registro**, marque a caixa de seleção **Cancelar atribuição** e clique em **OK**.
Para obter mais informações sobre edições em massa, consulte Edição em massa de itens vulneráveis do Vulnerability Response.

b. Selecione o ID da tarefa de correção que é exibido na notificação.

6. Exiba as seguintes informações:
   - As anotações de trabalho que você forneceu são exibidas na seção Anotações.
   - Na guia **Aprovação** de mudança de estado, o registro de aprovação de mudança de estado é exibido com o estado Em revisão, o que ajuda a rastrear o fluxo de trabalho de aprovação.
   - Na guia **Aprovações solicitadas**, a solicitação para a remoção de você ou do seu grupo de atribuição é exibida no estado Solicitado.

Resultado

A solicitação é aprovada usando um fluxo de trabalho de aprovação padrão de um nível. Para obter mais informações, consulte Aprovar solicitações no Vulnerability Manager Workspaces.

- Se sua solicitação for aprovada, o registro de aprovação de mudança de estado e o registro de aprovação solicitado passarão para o estado Aprovado. Você e seus grupos serão removidos dos campos **Atribuído a** e **Grupo de atribuição**. Não atribuído é exibido no campo **Tipo de atribuição** e a tarefa de correção e os VITs são exibidos na lista do módulo Não atribuído para Configuration Compliance.

  Notificações de que os registros não estão atribuídos são enviadas automaticamente para gerentes de vulnerabilidade ou analistas no grupo de notificação de cancelamento de atribuição. Para configurar o sinalizador de aprovação, as notificações e o grupo de atribuição padrão, consulte Remoção de atribuições de itens vulneráveis e tarefas de correção.

- Se sua solicitação for rejeitada, o estado do registro de aprovação de mudança e o registro de aprovação solicitada mudarão para o estado Rejeitado.

Nota:
Como administrador de vulnerabilidade, você pode definir a propriedade do sistema `sn_vul.unassign_vr.approval_required` como **falsa** para desabilitar o processo de aprovação.

O que Fazer Depois

Navegue até os módulos Não atribuídos das aplicações Vulnerability Response e Application Vulnerability Response Vulnerability Response contêiner, monitore todos os registros não atribuídos para itens que possam se enquadrar no seu escopo e reatribua-os a você.

Aprovar uma solicitação de cancelamento de atribuição no Vulnerability Response

Aprove solicitações para a remoção de itens vulneráveis de um grupo de atribuição ou de um usuário individual na aplicação Vulnerability Response.

Antes de Iniciar

Função necessária: para aprovações de cancelamento de atribuição, um aprovador é necessário no grupo Aprovador - Nível 1.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_vul.unassign_approver para AVITs e VITs
- sn_vul_container.unassign_approver para CVITs

Por Que e Quando Desempenhar Esta Tarefa

Por padrão, uma configuração de aprovação é fornecida e um grupo de aprovação de desatribuição é criado. Usuários do grupo Aprovador não atribuído - Nível 1 podem aprovar a solicitação. Este grupo contém uma função de aprovador de desatribuição, sn_vul.unassign_approver, por padrão. Você pode modificar ou criar um novo grupo e atualizar a configuração de aprovação. Para configurar uma regra de aprovação, selecione qualquer uma das seguintes regras de aprovação no módulo Regras de aprovação e navegue até a configuração de aprovação na guia **Configurações** de aprovação:

- *`Vulnerable item field change request`* para um item vulnerável.
- *`Vulnerability field change request`* para uma tarefa de correção.
- *`Application vulnerability field change request`* para um item vulnerável da aplicação (AVIT).
- *`Approval for container management`* para um item vulnerável de contêiner (CVIT).

Para obter mais informações sobre regras de aprovação e configurações, consulte Configurações de fluxo de trabalho de aprovação para solicitação de cancelamento de atribuição.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Minhas aprovações** para VITs e AVITs. Como alternativa, navegue até **Todos** > **Vulnerability Response do contêiner** > **Minhas aprovações** para CVITs.
2. Selecione uma solicitação da sua fila.
3. Aprove ou rejeite a solicitação adicionando os comentários apropriados.

Fechamento automático de itens vulneráveis e detecções

Você pode fechar automaticamente detecções obsoletas e itens vulneráveis (IVs) associados a ICs desativados usando o módulo Configuração de fechamento automático.

Para configurar a opção de fechamento automático, navegue até **Todos** > **Vulnerability Response** > **Administração** > **Configuração de fechamento automático**. Você pode fechar automaticamente detecções e IVs obsoletos nos seguintes cenários:

- Encerrar automaticamente detecções obsoletas no Vulnerability Response
- Fechar automaticamente itens vulneráveis relacionados a ICs desativados

Para obter informações sobre como trabalhar com itens de configuração desativados, consulte Como trabalhar com itens de configuração desativados.

Como trabalhar com itens de configuração desativados

Os itens de configuração (ICs) desativados são movidos para o estado desativado, arquivado ou excluído no Configuration Management Database (CMDB). Vulnerability Response contém itens vulneráveis (IVs) que são compostos por ICs. Quando o estado de um IC é atualizado para desativado, os IVs associados são encerrados com o subestado "IC desativado".

Se o CMDB mudar o status da fase do ciclo de vida de um IC para desativado, você poderá optar por fechar automaticamente os IVs associados. Para obter mais informações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

sobre como fechar automaticamente os IVs associados, consulte Fechar automaticamente itens vulneráveis relacionados a ICs desativados.

O IC desativado é eventualmente arquivado ou excluído permanentemente do CMDB.

Impacto da desativação dos ICs:

- **Impacto nos itens descobertos:** quando o IC é desativado, o item descoberto (DI) relacionado é marcado como "IC desativado".
- **Impacto em itens vulneráveis:** quando o estado de um DI é atualizado para "IC desativado", o IV associado é encerrado e a seção de anotações é atualizada automaticamente.

Nota:
O estado de um DI é atualizado automaticamente para "IC desativado" sempre que o estado do ciclo de vida de um IC é atualizado. Por outro lado, o estado de um IV é atualizado para Encerrado somente quando a opção **Fechar automaticamente IVs vinculados a ICs desativados** está habilitada. Para obter mais informações sobre como fechar automaticamente os IVs associados, consulte Fechar automaticamente itens vulneráveis relacionados a ICs desativados.

O trabalho programado *`Close detections/VIs for decommissioned CIs`* é executado diariamente para os DIs atualizados. Se a opção de configuração de fechamento automático estiver habilitada para ICs desativados, ela identificará o DI que contém um IC desativado e fechará o IV relacionado com o subestado "IC desativado". Se todos os IVs em uma tarefa de correção estiverem encerrados e seu subestado for IC desativado, a tarefa de correção também será encerrada com o subestado "Cancelado". Para exibir os IVs desativados, navegue até **Vulnerability Response** > **Itens vulneráveis** > **Desativado**.

Nota:
Se um IC voltar para o estado original do estado "Descontinuado", a entrada "Itens descobertos" também será atualizada. Os IVs são abertos automaticamente quando os dados são ingeridos novamente do scanner.

Fechar automaticamente itens vulneráveis relacionados a ICs desativados

Se o Configuration Management Database (CMDB) mudar o status da fase do ciclo de vida de um item de configuração (IC) para desativado, você poderá optar por fechar automaticamente os itens vulneráveis (IVs) e as detecções associados.

Antes de Iniciar
Função necessária: sn_vul.admin

Por Que e Quando Desempenhar Esta Tarefa
Para fechar automaticamente os IVs e as detecções associados, você deve habilitar a opção de fechar automaticamente os IVs que estão associados a ICs desativados. Se esta opção estiver habilitada, os IVs e as detecções novos e existentes relatados para o mesmo IC serão criados ou atualizados automaticamente no estado "Encerrado". Eles são baseados no ID do ativo na carga do scanner e no status de entrada dos itens descobertos. Para obter mais informações sobre o impacto de ICs desativados, consulte Como trabalhar com itens de configuração desativados.

Nota:
O estado de um DI é atualizado para "IC desativado" sempre que o estado do ciclo de vida de um IC é atualizado. Por outro lado, o estado de um IV é atualizado para Encerrado somente quando a opção **Fechar automaticamente IVs vinculados a ICs desativados** está habilitada.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Configuração de fechamento automático** > **Ciclo de vida do item de configuração**.
2. Para fechar automaticamente itens vulneráveis associados aos ICs desativados, marque a caixa de seleção Fechar automaticamente **IVs vinculados a ICs desativados**.
3. Selecione **Atualizar**.

Nota:
Se um IC já tiver sido desativado antes que a opção **Fechar automaticamente VIs vinculados a ICs desativados** seja habilitada, os IVs serão criados somente para novas detecções de scanners. O estado desses IVs é Encerrado e o subestado é IC desativado.

Você não pode reabrir manualmente os IVs cujo estado é IC desativado, usando as opções **Reabrir** ou **Edição em massa**.

Os IVs encerrados com um subestado fixo ou obsoleto serão reabertos se uma nova detecção for criada e os IVs puderem ser correspondidos com a nova vulnerabilidade. Para obter mais informações, consulte Detecções, tarefas de correção e estados de item vulnerável.

Fechando detecções obsoletas em Vulnerability Response

O módulo Encerrar automaticamente detecções obsoletas ajuda a limpar automaticamente detecções vulneráveis mais antigas que não foram encontradas recentemente por suas integrações de terceiros. Mover essas detecções para Encerrado reduz o número de itens vulneráveis ativos e tarefas de correção em sua instância Now Platform e ajuda a reconciliar ativos no seu CMDB.

Visão geral e principais termos

Para acumular dados de detecção com mais precisão para seus itens vulneráveis, o módulo Encerrar automaticamente detecções obsoletas ajuda a limpar detecções de itens vulneráveis mais antigas que não foram encontradas recentemente por suas integrações de terceiros. Para obter mais informações sobre este recurso, consulte o caso de uso abaixo e o artigo Encerrar automaticamente detecções obsoletas [KB 0958638] .

Em versões anteriores do Vulnerability Response, o módulo Fechar itens vulneráveis automaticamente transicionava itens vulneráveis não encontrados recentemente ou atualizados por suas integrações de scanner de terceiros para Encerrado - Obsoleto.

Antes de habilitar o recurso Encerrar automaticamente detecções obsoletas, revise os termos a seguir, como os estados se acumulam para itens vulneráveis e tarefas de correção e os pré-requisitos para suas integrações de terceiros que importam dados de detecção.

Para habilitar o recurso, consulte Encerrar automaticamente detecções obsoletas no Vulnerability Response.

Termos-chave

Detecções obsoletas

Refere-se a detecções associadas a itens vulneráveis na sua instância Now Platform® que são antigos e não foram encontrados, atualizados ou detectados por verificações de integração de terceiros por um período significativo.

Últimas detecções encontradas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta opção de pesquisa usa uma data e hora fornecidas pelo scanner de terceiros. Este termo se refere à data e hora mais atuais ou mais recentes em que as detecções foram encontradas novamente pelo scanner.

Ativos verificados pela última vez

Esta opção de pesquisa usa uma data e hora fornecidas pelo scanner de terceiros. Este termo se refere à data e hora mais atuais em que um ativo foi verificado pela última vez por um scanner de terceiros.

Caso de uso

Às vezes, os ativos (itens de configuração) podem ser desativados em seu ambiente ou limpos por scanners de terceiros, e suas detecções associadas não são atualizadas por detecções de item vulnerável. Como resultado, as detecções e seus itens vulneráveis relacionados não são atualizados na aplicação Vulnerability Response e se tornam inativos (obsoletos).

Para fechar essas detecções antigas que têm dados de item vulnerável inalterados e, em seguida, reduzir o número de IVs ativos e tarefas de correção (RTs), habilite o fechamento automático de detecções obsoletas. Este recurso fecha automaticamente as detecções de itens vulneráveis que não foram encontrados recentemente ou atualizados por suas integrações de scanner de terceiros com base nos critérios de pesquisa e em uma idade em número de dias que você definiu.

Como exemplo, suponha que um item de configuração (IC) específico tenha vários IDs de ativo e um desses IDs não tenha sido importado em uma detecção de um scanner de terceiros nos últimos 90 dias. Este recurso fecha automaticamente esta detecção que não tem novos dados de vulnerabilidade para que o IV associado possa ser fechado.

Como um IV pode ter mais de uma detecção associada a ele, este recurso faz a transição somente das detecções determinadas como obsoletas pelos parâmetros definidos. Por exemplo, se um IV tiver quatro detecções associadas a ele e duas detecções estiverem obsoletas, ou seja, nenhum novo dado de vulnerabilidade foi importado nos últimos 90 dias, este recurso fechará somente as detecções obsoletas. Antes que o IV possa ser encerrado, você deve primeiro corrigir as outras duas detecções em aberto.

Acúmulo de estados de detecção para IVs

Para diferenciar as detecções encerradas automaticamente das detecções encerradas por scanners de terceiros, um novo valor para o campo Status, Obsoleto, foi adicionado. Os valores possíveis possíveis para este campo são Aberto, Encerrado e Obsoleto. Obsoleto indica que uma detecção foi encerrada pelo recurso de detecção de fechamento automático.

Precedência de estado: Aberto > Encerrado > Obsoleto.

1. Se alguma detecção estiver Aberta, o estado de IV associado permanecerá Aberto.
2. Se nenhuma detecção estiver Aberta, algumas estiverem Encerradas e algumas estiverem Obsoletas, o estado de IV associado mudará para Encerrado - Corrigido.
3. Se todas as detecções estiverem obsoletas, o estado do IV associado mudará para Encerrado - Obsoleto.

   Declarando com Vulnerability Response 20.0, se uma detecção estiver no estado Encerrado - Obsoleto, o IV associado estiver no estado Encerrado, o estado do IV não fará a transição para Encerrado - Obsoleto. Isso evita que o IV seja reaberto quando uma nova detecção é identificada para que você possa evitar passar por todo o. Para reverter esse comportamento, desmarque a caixa de seleção **Ignorar detecções obsoletas para**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

IVs encerrados no formulário Configuração de fechamento automático. Para obter mais informações, consulte Encerrar automaticamente detecções obsoletas no Vulnerability Response.

4. Se a detecção for Obsoleta e o IV associado estiver no estado Encerrado, o estado do IV não fará a transição para Encerrado - Obsoleto. Isso evita que o IV seja reaberto quando uma nova detecção é identificada para que você possa evitar passar por todo o processo de aprovação e solicitação de falso-positivo. Para reverter esse comportamento, desmarque a caixa de seleção **Ignorar detecções obsoletas para IVs encerrados** no formulário Configuração de fechamento automático. Para obter mais informações, consulte Encerrar automaticamente detecções obsoletas no Vulnerability Response.

Acúmulo de estados de IV para tarefas de correção (VUL)

Precedência de estado: Aberto > Encerrado - Corrigido > Encerrado - Obsoleto.

1. Se algum IVs em uma VUL (tarefa de correção) estiver Aberto, o estado da VUL não será alterado.
2. Se pelo menos um IV for Encerrado - Corrigido e o restante for Encerrado - Obsoleto, o estado do VUL muda para Encerrado - Corrigido.
3. Se todos os IVs em um VUL forem Encerrado - Obsoleto, o estado do VUL mudará para Encerrado - Cancelado.

Detecções de encerramento automático e requisitos de integração de terceiros

Usuários do Microsoft TVM e Detecções obsoletas de fechamento automático

Item de check-list	Descrição
Integração de vulnerabilidade do Microsoft TVM	Com a Integração de vulnerabilidades do Microsoft TVM, se você selecionar **Detecções encontradas pela última vez** para basear sua pesquisa, este recurso exigirá uma execução bem-sucedida da Integração de vulnerabilidades da máquina Microsoft TVM (importação completa) nos últimos sete dias. Esta integração é executada semanalmente. Se o encerramento automático de detecções obsoletas estiver habilitado e configurado para **Detecções encontradas pela última vez**e a integração de vulnerabilidades de máquina com Microsoft TVM estiver desabilitada ou uma importação de dados não for concluída com êxito nos últimos sete dias, o trabalho programado para fechar detecções ainda será executado diariamente, mas alguns detecções obsoletas podem não ser encerradas conforme o esperado. Se você selecionar **Ativos verificados pela última vez** para basear sua pesquisa, a execução da integração de vulnerabilidades da máquina com Microsoft TVM não será necessária. Para ativar esta integração:

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item de check-list	Descrição
	1. Navegar até **Integração de vulnerabilidade Microsoft VTM** > **Administração** > **Integração**. 2. Localize e habilite a **integração de vulnerabilidades da máquina com Microsoft TVM (importação completa)**.
(Opcional) Implante várias instâncias das integrações do Microsoft TVM em seu ambiente.	Opcionalmente, você pode implantar várias instâncias das integrações em seu ambiente. O encerramento automático de detecções obsoletas não é específico da instância e está habilitado ou desabilitado em seu ambiente. As detecções obsoletas são transicionadas automaticamente para Obsoleto nas instâncias que concluíram com êxito as execuções de integração. Se o fechamento automático de detecções obsoletas estiver habilitado e você desabilitar as integrações que são executadas semanalmente em uma instância, o trabalho programado para fechar detecções ainda será executado diariamente, mas algumas detecções podem não fazer a transição para obsoletas automaticamente como esperado.

Qualys Usuários e itens vulneráveis obsoletos de encerramento automático

- Todas as integrações de terceiros ativadas Qualys que recuperam dados de detecção podem ser executadas com este módulo. Não há aplicações Qualys específicas necessárias.
- Opcionalmente, você pode implantar várias instâncias das integrações Qualys em seu ambiente.
- O encerramento automático de detecções obsoletas não é específico da instância e está habilitado ou desabilitado em seu ambiente. As detecções obsoletas são transicionadas automaticamente para Obsoleto em todas as instâncias.

Rapid7 Usuários e Encerramento automático de detecções obsoletas

Item de check-list	Descrição
A integração de vulnerabilidade Rapid7	Se você selecionar **Detecções encontradas pela última vez** para basear sua pesquisa, este recurso exigirá uma execução bem-sucedida de uma das Rapid7 Integrações de item vulnerável abrangente nos últimos sete dias. Essas integrações abrangentes são executadas semanalmente: • Para o data warehouse Rapid7 Nexpose, é necessária uma execução bem-sucedida da Integração de item vulnerável abrangente Rapid7. • Para Rapid7 InsightVM, é necessária uma execução bem-sucedida da Rapid7 Integração de item vulnerável abrangente - API. Se o encerramento automático de detecções obsoletas estiver habilitado e configurado para **Detecções encontradas pela última vez**e as Rapid7 Integrações de

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item de check-list	Descrição
	item vulnerável abrangente estiverem desabilitadas ou uma importação de dados não for concluída com êxito nos últimos sete dias, o trabalho programado para fechar detecções ainda será executado diariamente, mas algumas detecções obsoletas podem não ser encerradas conforme o esperado. Se você selecionar **Ativos verificados pela última vez** para basear sua pesquisa, nenhuma execução de integração abrangente Rapid7 será necessária. Para ativar essas integrações: **1.** Navegar até **Rapid7 Vulnerability Integration** > **Administração** > **Integração**. **2.** Localize e habilite a Integração Abrangente de Item Vulnerável Rapid7 que você precisa. **Nota:** Além dessas integrações que são executadas semanalmente, Rapid7 Nexpose e Rapid7 InsightVM têm integrações de IV que são executadas diariamente, a Rapid7 Vulnerable Item Integration e a Rapid7 Vulnerable Item Integration - API. Se as integrações diárias e semanais Rapid7 estiverem habilitadas, somente uma integração será executada de cada vez. Se um desses trabalhos de integração estiver em execução, o trabalho da outra integração será ignorado até o próximo trabalho programado.
(Opcional) Implante várias instâncias das integrações Rapid7 em seu ambiente.	Opcionalmente, você pode implantar várias instâncias das integrações abrangentes em seu ambiente. O encerramento automático de detecções obsoletas não é específico da instância e está habilitado ou desabilitado em seu ambiente. As detecções obsoletas são transicionadas automaticamente para Obsoleto nas instâncias que concluíram com êxito as execuções de integração. Se o encerramento automático de detecções obsoletas estiver habilitado e você desabilitar as integrações que são executadas semanalmente em uma instância, o trabalho programado para fechar detecções ainda será executado diariamente, mas algumas detecções podem não fazer a transição para obsoletas automaticamente como esperado.

Usuários de integração de vulnerabilidade da Tenable e itens vulneráveis obsoletos de fechamento automático

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Todas as integrações ativadas do Tenable Vulnerability Integration que recuperam dados de detecção podem ser executadas com este módulo. Não há integrações de vulnerabilidade específicas da Tenable necessárias.
- Opcionalmente, você pode implantar várias instâncias da integração de vulnerabilidade da Tenable em seu ambiente.
- O encerramento automático de detecções obsoletas não é específico da instância e está habilitado ou desabilitado em seu ambiente. As detecções obsoletas são transicionadas automaticamente para **Obsoleto** em todas as instâncias.

Depois de verificar se suas integrações estão configuradas corretamente, consulte Encerrar automaticamente detecções obsoletas no Vulnerability Response para habilitar o recurso.

Atualizar informações de itens vulneráveis obsoletos de fechamento automático para detecções obsoletas de fechamento automático

Para o módulo Encerrar automaticamente detecções obsoletas, se você usou anteriormente Encerrar automaticamente itens vulneráveis obsoletos:

- O valor do número de dias que você inseriu para a **última** opção de **Ativos verificados em Encerrar automaticamente itens vulneráveis obsoletos é preservado automaticamente para os Ativos verificados pela última vez** em Encerrar automaticamente detecções obsoletas.
- O valor do número de dias que você inseriu para a opção Itens vulneráveis **encontrados** pela última vez em Encerrar automaticamente itens vulneráveis obsoletos é preservado automaticamente para as **Detecções encontradas pela última vez** em Encerrar automaticamente detecções obsoletas.
- As detecções em aberto existentes com itens vulneráveis como Encerrado - Obsoleto serão transicionadas para Obsoleto de acordo com as definições de configuração de fechamento automático quando o trabalho programado `Auto-Close Stale Detections` for executado após o upgrade.

Informações de acúmulo

- Se um item vulnerável foi Encerrado - Obsoleto antes da atualização e todas as suas detecções forem marcadas como Obsoletas após a atualização, o estado do IV permanecerá Encerrado - Obsoleto.
- Se um item vulnerável foi Encerrado - Obsoleto antes do upgrade e apenas algumas de suas detecções estiverem marcadas como Obsoletas após o upgrade e o restante tiver sido encerrado pelo scanner, o item vulnerável será transicionado para Encerrado - Corrigido de acordo com a lógica de acúmulo.

Encerrar automaticamente detecções obsoletas no Vulnerability Response

Habilite o fechamento automático de detecções obsoletas para fechar automaticamente detecções vulneráveis obsoletas que não foram encontradas recentemente por suas integrações de terceiros.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vuln.admin (obsoleto) ou um gerenciador de vulnerabilidades com a função granular sn_vul.manage_auto_close_stale_vi.

Para obter mais informações sobre este recurso, os principais termos e qualquer configuração que possa ser necessária para suas integrações de terceiros que importam dados de detecção, consulte Fechando detecções obsoletas em Vulnerability Response para obter mais informações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Vulnerability Response** > **Administração** > **Configuração de fechamento automático** > **Detecções obsoletas**.
   O formulário Configuração obsoleta de encerramento automático é exibido.
2. Preencha os campos.
3. Para o campo **Fechar automaticamente detecções obsoletas com base em**, escolha uma opção para sua pesquisa.

   Ambas as pesquisas correspondem à idade das detecções mais antigas em número de dias até uma data fornecida pelo seu scanner.

   - **Últimas detecções encontradas**. Esta opção pesquisa a data mais atual ou mais recente em que as detecções foram encontradas novamente pelo scanner.

     Nota:
     Para usuários de Rapid7 e Microsoft TVM, uma mensagem de aviso é exibida sobre a solicitação de informações de detecção atuais.

     Se você selecionar **Detecções encontradas pela última vez** para basear sua pesquisa, este recurso exigirá uma execução de integração bem-sucedida de uma das Rapid7 integrações de item vulnerável abrangente nos últimos sete dias.

     Se você selecionar **Detecções encontradas pela última vez** para basear sua pesquisa, este recurso exigirá uma execução bem-sucedida da integração de vulnerabilidades de máquina Microsoft TVM (importação completa) nos últimos sete dias.

   - **Última verificação dos ativos**. Esta opção pesquisa a data mais atual em que um ativo foi verificado pela última vez por um scanner de terceiros.
4. Somente para usuários de Rapid7 e Microsoft TVM, verifique se todas as integrações necessárias estão habilitadas.
   Para obter mais informações, consulte Noções básicas sobre o Rapid7 Vulnerability Integration e Noções básicas sobre a integração de vulnerabilidade do Microsoft Threat and Vulnerability Management.
5. Para habilitar o módulo, clique na caixa de seleção Ativo para selecioná-lo.
6. No campo **Últimas detecções encontradas (dias atrás)**, insira a idade das detecções mais antigas no número de dias.

   O padrão é 90 dias. Você pode inserir qualquer valor positivo para o número de dias. Este valor é usado para corresponder a uma data fornecida pelo scanner. Com 90 e **Últimas detecções encontradas** exibidas, todas as detecções não encontradas nos últimos 90 dias serão encerradas automaticamente. Com 90 e **Ativos verificados pela última vez** exibidos, todas as detecções associadas a ativos não verificados nos últimos 90 dias são encerradas automaticamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Há uma relação entre o campo **Detecções encontradas pela última vez/Ativos verificados pela última vez (dias atrás)** para este recurso e o campo **Importar desde** na API Integração abrangente de item vulnerável da Rapid7 e na integração de vulnerabilidades da máquina com Microsoft TVM.

Para essas integrações, o campo **Importar desde** nas páginas de configuração está vazio por padrão.

Se você não inserir um valor ou o campo não tiver nenhum valor, os dados do número de dias configurados no campo **Detecções encontradas/Última verificação de ativos (dias atrás)** serão usados.

Por exemplo, se o número de dias definido no formulário de configuração de fechamento automático for 90e o campo **Importar desde** estiver vazio nas páginas de configuração da integração, a primeira execução de integração importará os dados dos últimos 90 dias. Os campos **Importar desde** da Rapid7 Integração de item vulnerável abrangente - API e a integração de vulnerabilidades da máquina Microsoft TVM são editáveis, portanto, você também pode fornecer os valores desejados. O valor de 90 dias será fornecido como padrão se o campo permanecer vazio para que o recurso de fechamento automático não feche os falsos positivos.

Este relacionamento entre esses campos se aplica somente à primeira execução de integração. Depois disso, alterar o campo **Detecções encontradas pela última vez/ Ativos verificados pela última vez (dias atrás)** no formulário Fechar automaticamente detecções vulneráveis obsoletas não afeta o campo **Importar desde** nas páginas de configuração da integração. O campo é alterado para a hora de início da primeira execução para que as execuções de integração subsequentes importem somente as informações delta.

7. **Opcional:** Marque a caixa de seleção **Ignorar detecções obsoletas para IVs adiados** para ignorar detecções obsoletas que são mapeadas para IVs adiados ou para IVs atualmente em revisão para adiamento.

   (Optional) Se você deixar esta opção desabilitada, todas as detecções que corresponderem aos seus critérios serão fechadas e mapeadas para IVs adiados ou para IVs que estão em revisão para adiamento. Os IVs adiados ou IVs que estão em revisão que correspondem a essas detecções também são encerrados automaticamente com base na lógica de acúmulo. Para obter mais informações sobre a lógica de acúmulo, consulte Fechando detecções obsoletas em Vulnerability Response.

   Se você habilitar esta opção, todas as detecções que correspondam aos seus critérios que mapeiam para IVs adiados ou para IVs que estão em revisão para adiamento serão ignoradas durante o fechamento automático.

8. **Opcional:** Desmarque a caixa de seleção **Ignorar detecções obsoletas para IVs encerrados**. Por padrão, esta caixa de seleção é marcada para que o IV encerrado não seja reaberto quando uma nova detecção relacionada a este IV encerrado for identificada.

   (Optional) Para obter mais informações sobre a lógica de acúmulo, consulte Fechando detecções obsoletas em Vulnerability Response.

9. Clique em **Atualizar** para salvar suas mudanças.

   O trabalho programado, Encerrar automaticamente detecções obsoletas, é executado diariamente. O trabalho identifica se você selecionou a data em que as detecções

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

foram encontradas ou se os ativos foram verificados pela última vez. As detecções correspondentes transicionam para Obsoleto. O recurso Fechar detecção obsoleta automaticamente fecha somente detecções obsoletas para instâncias de integração ativas. Os itens vulneráveis e as detecções associadas às instâncias de integração ativas são encerrados.

Depois que as detecções forem marcadas como Obsoletas, se o scanner relatar que encontrou essa detecção novamente, o campo Status das detecções será alterado para Aberto. Os itens vulneráveis correspondentes da detecção também são reabertos.

Além disso, se a detecção estiver marcada como Obsoleta e o scanner descobrir que ela é Corrigida, a detecção muda para Encerrado. O estado também é acumulado para os IVs.

Como criar manualmente uma tarefa de correção no Vulnerability Response

A criação manual de uma tarefa de correção é feita quando você deseja agrupar itens vulneráveis por algo diferente dos critérios de Regras de tarefa de correção. Por exemplo, você pode criar tarefas para um gerente específico ou para novas explorações ativas, como ransomware que incluem diferentes vulnerabilidades. Você também pode usá-lo para agrupar itens vulneráveis desagrupados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Tarefas de correção**.

   As regras de tarefa de correção funcionam da mesma forma que as regras de grupo de vulnerabilidades e ainda estão disponíveis para você. No entanto, talvez você prefira deixar as regras de tarefa de correção inativas enquanto se acostuma com os recursos que estão disponíveis para seus gerentes de segurança e equipes de TI nos espaços.

2. Selecione uma das categorias de tarefas para abrir a lista.
3. Clique em **Nova**.
4. Preencha os campos no formulário, conforme apropriado.
   Para obter informações sobre campos específicos, consulte Campos de formulário de tarefa de correção.
5. Clique em **Enviar**.
   Quando a tarefa é criada, usando o tipo de filtro **Condição** ou **Grupo** de filtros, a lista relacionada **Item vulnerável** pesquisa e exibe todos os itens vulneráveis correspondentes.

   Você pode usar o link relacionado, Verificar novamente se **há vulnerabilidades** para acionar manualmente uma verificação iniciada em ServiceNow®. Para obter informações sobre como configurar um scanner de vulnerabilidade, consulte Configurar e gerenciar scanners e verificações de vulnerabilidade Qualys.

   Para uma integração de vulnerabilidade da Qualys, um scanner padrão é pré-instalado no módulo **Scanners de vulnerabilidade**. Este scanner está desabilitado por padrão. Marque as caixas de seleção **Ativo** e **Padrão** para ativar o scanner Qualys para funcionar usando o link relacionado **Verificar vulnerabilidades** na tarefa de correção e nos formulários de item vulnerável.

   O link relacionado **Atualizar status** exibe a data e a hora da última atualização. Ele acumula informações dos IVs na tarefa de correção. Para obter mais informações, consulte Campos de formulário de tarefa de correção. Quando uma tarefa é formada com base

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

em uma vulnerabilidade específica, essa vulnerabilidade é listada no formulário de tarefa de correção.

Se você abrir um item vulnerável associado, todas as entradas de tarefa de correção associadas serão exibidas na guia da lista relacionada **Tarefa** de correção.

Adicionar usuários ao grupo do Vulnerability Response

Quando o recurso Fechar/Adiar é usado para adiar ou fechar um item vulnerável sem exigir uma verificação, o grupo Vulnerability Response é notificado para aprovar ou rejeitar a solicitação. Você pode atribuir os usuários apropriados.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Grupos**.
2. Abra o grupo Vulnerability Response.
3. Clique na lista relacionada **Membros do grupo** e clique em **Editar**.
4. Selecione um ou mais nomes na lista **Coleção**.
5. Clique em **Adicionar**.
6. Clique em **Salvar**.

Tópicos relacionados

Criar um usuário

Gerenciar itens vulneráveis individuais manualmente

Itens vulneráveis representam um item de configuração (IC) com uma determinada vulnerabilidade. Itens vulneráveis são importados de fontes de terceiros ou usando as informações do NVD do SAM (link) para comparar as entradas de vulnerabilidade com os registros de software recuperados do módulo Software Gestão de ativos.

Itens vulneráveis estão contidos em tarefas de correção definidas por regras de vulnerabilidade. Normalmente, as tarefas de correção são o local onde os grupos de itens vulneráveis são atribuídos e trabalhados.

Itens vulneráveis podem ser exibidos e editados em massa no módulo **Itens vulneráveis**. Os registros de item vulnerável exibem informações da vulnerabilidade na guia **Vulnerabilidade**. Esta guia pode indicar se há explorações públicas ou ativas para ela. Além disso, ele mostra se ele pode ser corrigido por meio de um patch, mudança de configuração ou combinação de ambos. Se houver endereços IP encontrados durante a desduplicação, eles serão exibidos em uma lista relacionada.

Se um IC for removido do CMDB, todos os itens vulneráveis associados também serão removidos.

Quando um item vulnerável é adicionado a uma tarefa de correção, o grupo aparece na lista **Tarefas** de correção de itens vulneráveis.

Quando é criada uma tarefa que afeta um item vulnerável, a tarefa aparece na lista relacionada **Tarefas que afetam** os itens vulneráveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Itens vulneráveis podem ser criados manualmente. Você pode criar incidentes de segurança ou solicitações de mudança e fechá-los ou adiá-los manualmente. As regras de tarefa de correção podem ser aplicadas a itens vulneráveis criados manualmente.

Tarefas de correção e regras de tarefa de correção foram aprimoradas para assumir a funcionalidade da tarefa. Itens vulneráveis não podem ser vinculados como uma tarefa primária.

Criar Vulnerability Response itens vulneráveis

Vários métodos criam itens vulneráveis (IV). Mais comumente, uma integração para um scanner de vulnerabilidade é instalada e configurada para importar resultados todas as noites. Há casos, como vulnerabilidades de segurança física, em que você pode preferir adicionar manualmente registros de item vulnerável.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_write

Por Que e Quando Desempenhar Esta Tarefa
Os IVs que você cria manualmente e os IVs criados automaticamente são adicionados e removidos automaticamente das tarefas de correção por regras de tarefa de correção e condições de grupo.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Itens vulneráveis**.
2. Selecione uma categoria para abrir a lista.
3. Clique em **Nova**.
4. Preencha os campos no formulário, conforme apropriado.
   Para obter informações sobre os campos de itens vulneráveis, consulte Vulnerability Response campos de formulário de item vulnerável.
5. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**.

   As regras de tarefa de correção avaliam o item vulnerável e o adicionam a uma tarefa existente ou criam uma nova tarefa. Se a avaliação falhar, o item vulnerável será adicionado à lista de **itens vulneráveis** não agrupados.

   Quando você salva um novo item vulnerável, todas as calculadoras habilitadas são executadas.

   Nota:
   Somente uma calculadora por **campo de destino** pode estar ativa de cada vez. Quando você ativa um, todos os outros com o mesmo **campo de destino** são desativados.

6. Você pode clicar em qualquer uma das listas relacionadas para exibir informações adicionais.

   Você pode usar o link relacionado, **Verificação de vulnerabilidades**, para acionar manualmente uma verificação iniciada por ServiceNow®. Para obter informações sobre como configurar um scanner de vulnerabilidade, consulte Configurar e gerenciar scanners e verificações de vulnerabilidade Qualys.

   Para uma integração de vulnerabilidade da Qualys, um scanner padrão é pré-instalado no módulo **Scanners de vulnerabilidade**. Este scanner está desabilitado por padrão. Marque as caixas de seleção **Ativo** e **Padrão** para ativar o scanner Qualys para funcionar usando o link relacionado **Verificar vulnerabilidades** na tarefa de correção e nos formulários de item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As seguintes opções de edição e correção ficam disponíveis na barra de cabeçalho:

- Atualizar: salva as atualizações do formulário.
- Criar incidente de segurança: cria um incidente de segurança.
- Fechar: fecha o item. Se todos os itens em seu grupo estiverem fechados, a tarefa de correção será fechada automaticamente.
- Exceção de solicitação: envia uma solicitação para adiar um item.
- Resolver: resolve o item.
- Excluir: remove o item vulnerável.

Tópicos relacionados

Editar itens vulneráveis em massa no Vulnerability Response

Adiar um item vulnerável

Se você determinar que o problema associado a um item vulnerável (VIT) é de baixo risco e pode ser adiado imediatamente sem análise adicional, você pode usar o recurso **Adiar**.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa

Um trabalho programado é executado todos os dias na verificação de itens vulneráveis adiados que atingiram a data de reabertura. No dia em que o adiamento do IV expirar, o registro será reaberto.

A partir da Vulnerability Response v20.0, antes de reabrir um IV adiado, o trabalho programado Verificar itens vulneráveis e Expiração do adiamento de grupos verifica se alguma regra de exceção é aplicável em um IV adiado e atualiza os campos **Motivo** e **Até** de acordo com a regra de exceção. O estado do IV permanece Adiado até a data de vencimento mais recente.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Itens vulneráveis**.
2. Abra um item vulnerável.
3. Clique **em Solicitar exceção**.
4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Até	Selecione a data em que o estado Adiado expira e a tarefa de correção é reativada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: A partir da versão 18.0 do Vulnerability Response (VR), se um item vulnerável adiado for fechado e reaberto por um scanner antes que a janela de exceção expire, o estado do VIT será revertido para o estado adiado, respeitando a janela de exceção ativa. Para habilitar essa funcionalidade, defina o valor da propriedade do sistema sn_vul.auto_defer_vit_in_active_exception_window como verdadeiro. Além disso, a data adiada até persiste mesmo depois que o item vulnerável é encerrado ou a exceção expira. A função necessária é sn_vul.manage_exception_configuration para leitura e gravação. Depois que o registro for enviado, se as notificações por e-mail forem definidas, os membros do grupo Vulnerability Response receberão um e-mail quando a data de expiração estiver dentro de uma semana. Quando a data de adiamento expira, o item vulnerável é definido novamente como Aberto e uma segunda notificação por e-mail é enviada.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Falso positivo ○ Correção indisponível ○ Risco aceito ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

Tradução automática

5. Clique em **Enviar**.
   O grupo está marcado **em revisão**. Um link relacionado **Reabrir** é exibido. A data e o motivo de reabertura aparecem nas anotações de trabalho na guia **Aprovações de mudança de estado**.

Solicitar uma extensão para um item vulnerável adiado

Solicite uma extensão para um item vulnerável adiado antes que ele atinja o adiado até a data de vencimento. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão nos espaços Vulnerability Response. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no Espaço do gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Itens vulneráveis**.
2. Abre um item vulnerável adiado.
3. Selecione **Solicitar extensão**.

Nota:
O botão Solicitar extensão fica visível somente quando o estado do item vulnerável é Adiado.

4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até quando o item vulnerável adiado deve ser estendido para correção.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
Um e-mail é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:
- A solicitação passa por dois níveis de aprovação.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

6. Depois que a solicitação é aprovada, as anotações Até, Motivo e Adiamento são atualizadas.

Atualizar Vulnerability Response itens vulneráveis

O link relacionado **Atualizar status** é usado para inspecionar itens vulneráveis para ver se há itens vulneráveis adicionais que pertençam a uma tarefa de correção. Use-o se uma atualização for garantida fora do trabalho programado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write ou, sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa

O link relacionado **Atualizar status** só pode ser editado no formulário de tarefa de correção nos estados **Aberto** ou **Sob investigação**, usando um grupo de filtros ou quando o tipo de filtro for condição. Esta inspeção é feita independentemente do status da caixa de seleção **Atualizar itens vulneráveis** automaticamente.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Tarefas de correção**.
2. Abra qualquer registro nos estados **Aberto** ou **Em investigação**.
3. Clique no link **Atualizar status**.
   Novos itens vulneráveis aparecem na guia **Itens vulneráveis**.

Identificar e escalar problemas de segurança em software de terceiros

Você pode exibir vulnerabilidades de software retornadas de entradas de terceiros para determinar a correção. Use essas informações para corresponder as entradas de software vulneráveis a um modelo de descoberta de Software Gestão de ativos.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Bibliotecas** > **Terceiro**.
   Uma lista de software vulnerável baixado é mostrada.
2. Clique em um registro de software para exibir informações de vulnerabilidade.
3. Clique nas seguintes listas relacionadas para obter mais informações para identificar vulnerabilidades.
   Se vulnerabilidades foram identificadas e itens vulneráveis foram criados, você pode Resolver tarefas de correção, conforme necessário.

Identificar e escalar problemas de segurança usando o NVD

Quando os registros do Identificador de vulnerabilidades e exposições comuns (CVE-ID) são baixados do NVD (National Vulnerability Database), eles são comparados ao software na rede da sua empresa, conforme identificado pelo modelo de descoberta de ativos de software. Quando um CVE-ID corresponde a um software vulnerável ou item

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de configuração em sua rede, um item vulnerável é criado. Você usa as informações no registro CVE-ID para decidir se deve escalar o item vulnerável para correção.

Antes de Iniciar

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Bibliotecas** > **NVD**.
   Uma lista de IDs de CVE que foram baixados do NVD é mostrada. As atualizações do NVD podem ser realizadas sob demanda e por execuções programadas dos registros do NIST National Vulnerability Database Integration localizados em **Todos** > **Administração** > **Integrações**.
2. Clique em um registro CVE para exibir as seguintes informações:
   - um resumo para o CVE-ID.
   - uma referência a uma entrada de CWE (Common Weakness Enumeration), se aplicável.
   - a pontuação de vulnerabilidade do CVE-ID no Common Vulnerability Scoring System (CVSS). Para obter mais informações sobre o CVSS, consulte o site do National Vulnerability Database .
3. Clique nas listas relacionadas para obter mais informações sobre vulnerabilidades.

   Referências de vulnerabilidade

   Nome, descrição e URL da vulnerabilidade fornecida e onde ela é referenciada.

   Explorações

   Detalhes.

   Pontos fracos

   Lista de pontos fracos do CWE.
4. Clique nas seguintes listas relacionadas para obter mais informações para identificar vulnerabilidades.
   Se vulnerabilidades foram identificadas e itens vulneráveis foram criados, você pode Resolver tarefas de correção, conforme necessário.

Identificar e escalar problemas de segurança usando o CWE

Exiba a biblioteca de registros de Enumeração de Pontos Fracos Comuns (CWE) do Banco de Dados de Vulnerabilidades Nacionais (NVD) para entender como eles se relacionam com os registros de Vulnerabilidade e Exposição Comuns (CVE). Em seguida, use essas informações para corresponder as entradas de software vulneráveis a um modelo de descoberta de Software Gestão de ativos.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_write

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Bibliotecas** > **CWE**.
   Uma lista de software vulnerável baixado é mostrada.
2. Clique em um registro de software CWE para exibir informações de vulnerabilidade.
3. Clique nas seguintes listas relacionadas para obter mais informações para identificar vulnerabilidades.
   Se vulnerabilidades foram identificadas e itens vulneráveis foram criados, você pode Resolver tarefas de correção, conforme necessário.

Exibir o status da meta de correção de um item vulnerável Vulnerability Response

Quando um item vulnerável quase atinge (ou ultrapassa) sua data de destino de correção, conforme definido por uma regra de destino de correção, o registro do item vulnerável é atualizado com um status. Essas informações podem ajudar o analista a monitorar proativamente as próximas atividades de correção.

Antes de Iniciar

Função necessária:
sn_vul.vulnerability_admin

sn_vul.read_remediation_target_rules [somente leitura]

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa

Um trabalho programado chamado **Avaliar destinos de correção** é executado uma vez por dia para comparar a data atual com a data de correção do item vulnerável especificada na regra de destino de correção associada. Quando a data atual está dentro do número de dias antes do vencimento da correção, um status de correção é adicionado ao registro do item vulnerável.

Para obter mais informações sobre regras de destino de correção, consulte Vulnerability Response regras de destino de correção.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Itens vulneráveis**.
2. Clique no item vulnerável que você deseja revisar.
   Se a data de correção do item vulnerável estiver dentro do intervalo das condições definidas na regra de destino de correção, a guia **Status** do destino de correção ficará visível.
3. Clique na guia **Status do destino de correção**.
4. Clique no registro de status do destino de correção para revisá-lo.

> **Nota:**
> Para exibir o número de itens vulneráveis que estão se aproximando da meta, em curso e meta anterior, consulte Usando os painéis padrão Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Criar ou editar Vulnerability Response regras de destino de correção

Como trabalhar com ICs incompatíveis

Como gerente e analista de vulnerabilidade, você pode exibir e reclassificar itens de configuração (ICs) incompatíveis, reconciliar itens descobertos incompatíveis, reaplicar regras de pesquisa de IC nos itens descobertos selecionados e desduplicar ICs existentes.

Reclassificar hardware não classificado

Reclassifique o hardware não classificado atualizando as regras de pesquisa de IC.

Antes de Iniciar
Função necessária: sn_sec_cmn.admin

Por Que e Quando Desempenhar Esta Tarefa
A tabela Mapa de importação de host [sn_sec_cmn_src_cmdb_map] exibe as variáveis de entrada da carga útil e suas atribuições correspondentes na tabela Itens descobertos. Ocasionalmente, discrepâncias nas convenções de nomenclatura entre o scanner e o Discovery podem fazer com que o hardware seja deixado sem classificação. Ao criar um novo IC de hardware não classificado, certifique-se de que o nome na carga útil contenha somente o nome do host. Posteriormente, quando o Discovery identificar o ativo, ele poderá ser reclassificado na classe de IC apropriada. Se necessário, um script pode ser gravado para gerar um valor derivado que se alinhe ao nome dos ICs no Discovery e no Configuration Management Database (CMDB).

Se o mecanismo de Identificação e Reconciliação (IRE) estiver ativado, a opção de reclassificação de Itens descobertos não será compatível.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Mapas de importação de host**.
2. Selecione uma origem.
3. Na lista Campo de destino, selecione **Nome**.
   A caixa de seleção **Usar script** se torna visível.

   Nota:
   - O script estará disponível somente se **Nome** for selecionado na lista Campo de destino.
   - Para adicionar um script para outras opções na lista do campo de destino, você deve desabilitar a política de IU:
     - Desabilitando o "Definir script de uso falso".
     - Desabilitando "Mostrar ou Ocultar Usar Script".
     - Removendo a condição "o campo de destino é o nome" na política "Mostrar ou ocultar script".
   - A tabela Mapas de importação de host é atualizada com duas novas colunas: Script e Usar script.
4. Marque a caixa de seleção **Usar script**.
   O campo **Script** exibe o script padrão, mas você tem a opção de criar um personalizado. Nesse campo, você pode especificar os valores de origem e derivados para alinhar com a convenção de nomenclatura do banco de dados. O valor gerado pelo script é armazenado em sourcePayload['DERIVED'][rule.source_field].

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Certifique-se de que as regras de pesquisa de IC sejam ajustadas para utilizar a carga útil de origem, os valores de atributo derivados e de destino ao fazer o check-in das tabelas correspondentes.

5. Para aplicar o script a registros duplicados mais antigos, faça o seguinte:

   a. Navegar até **Todos** > **Vulnerability Response Itens descobertos**.

   b. Selecione os registros duplicados.

   c. Na lista Ação nas linhas selecionadas, selecione **Reaplicar regras de pesquisa de IC**.
   Ele mostra uma correspondência com um ativo existente.

6. Para aplicar o script para Tenable.io, faça o seguinte:

   a. Navegar até **Vulnerability Response Mapas de importação de host**.

   b. Selecione o script para a linha com o nome NetBIOS, HOSTNAMES e FQDNS como o campo **Origem**.

   c. Atualize o script para cada elemento.

   Nota:
   Para Tenable.io, o scanner retorna uma matriz para NetBIOS, HOSTNAMES e nome FQDNS, para o qual o script não funciona conforme o esperado.

   Como o Mapa de importação de host para Tenable.io contém **netbios_name** no campo **Origem**, você deve gravar um script. Durante a pesquisa, outro campo de origem **NETBIOS** é usado, que tem uma matriz de valores. Portanto, uma nova linha é adicionada à tabela e a mesma lógica deve ser gravada em um loop no script. Da mesma forma, para **FQDNS** e **HOSTNAMES**.

7. Para aplicar o script para Rapid7, faça o seguinte:

   a. Navegar até **Todos** > **Vulnerability Response Mapas de importação de host**.

   b. Para Rapid7 linhas com FQDN e HostName, atualize o Método de pesquisa para Script.

   Nota:
   Para Rapid7, o método Pesquisa de IC é definido como Correspondência de campo para FQDN e Nome do host, o que ajuda a impedir que ele use o script.

Exibir e reclassificar itens de configuração incompatíveis

Os itens de configuração (ICs) que não são encontrados no Configuration Management Database (CMDB) são colocados em uma lista visível de itens descobertos. Esta lista oferece uma maneira conveniente de reclassificar ICs incompatíveis.

Antes de Iniciar

Função necessária:

sn_vul.read (mínimo para exibir ICs incompatíveis)

e

itil ou ativo (para reclassificar)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa

Como analista de vulnerabilidade, você pode exibir ICs incompatíveis.

A ação de reclassificação está disponível somente em ICs de classe `sn_sec_cmn_unmatched_ci`, quando você tem as funções itil ou de ativo. Depois que um IC tiver sido reclassificado, ele não poderá ser reclassificado usando a IU. Você pode reclassificar, no formulário de IC ou na exibição de lista de IC, alterando o valor da **classe**. Para obter mais informações, consulte Reclassify a CI .

Procedimento

1. Navegar até **Todos** > **Security Operations** > **CMDB** > **Itens Descobertos**.
2. Para revisar, clique em cada item.
3. Para fazer correções nas informações nos campos de formulário de **Item descoberto**, edite nesta página e clique com o botão direito do mouse em **Salvar**.
   Todos os dados adicionados ou deixados nesses campos são transferidos para o **Item de configuração** resultante quando ele é reclassificado.
4. Se tudo estiver correto, clique em **Reclassificar**.
5. Na lista de seleção, selecione um **Nome de classe** e clique em **Enviar**.
   A **classe** do **item descoberto** é atualizada, o campo **Estado** é alterado para Reclassificado e todos os dados estão no CMDB.

Reconciliar itens descobertos sem correspondência

Crie um trabalho programado para reconciliar itens descobertos incompatíveis.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Um item vulnerável (IV) consiste em uma vulnerabilidade e um item de configuração (IC). Quando um IV é criado, o IC adicionado a ele no momento da criação pode estar desatualizado. As informações de IC incompatíveis não serão reconciliadas se as informações no CMDB forem alteradas. Para reconciliar, aplique as regras de pesquisa de Item de configuração (IC) nos itens que estão em um estado incompatível quando o CMDB é atualizado com os ICs mais recentes.

Você pode executar uma demanda de trabalho programada para reaplicar a regra de correspondência de IC para os itens descobertos em um estado incompatível. Se o IC mudar após a reaplicação das regras de pesquisa, os itens descobertos serão atualizados com o novo IC. As detecções afetadas e os itens vulneráveis também são atualizados. Para obter detalhes, consulte Mudanças de IC para itens descobertos.

Procedimento

1. Navegar até **Todos** > **Security Operations > Reconciliar itens descobertos incompatíveis**.
2. Na página Trabalhos em segundo plano, clique em **Criar trabalho de reconciliação**.
3. No formulário, preencha os campos.

Nota:
Você só pode editar o campo **Parâmetros**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de trabalho em segundo plano

Campo	Descrição
Número	Número do trabalho exclusivo.
Criado por	Usuário que criou o trabalho.
Parâmetros	Parâmetros para reconciliar os itens descobertos incompatíveis: ○ limit: o número máximo de itens descobertos a serem reconciliados. Se você não inserir um valor, 10.000 itens descobertos serão reconciliados. ○ firstDiscovereditem: primeiro item descoberto que deve ser reconciliado. Se você não inserir um valor, o processo de reconciliação será iniciado a partir do primeiro item descoberto.
Estado	Estado atual do trabalho em segundo plano.
Descrição do estado	Descrição do estado atual do trabalho em segundo plano.
Tipo de trabalho	Tipo de trabalho. O valor é **Reconciliar itens descobertos incompatíveis**.
Iniciada em	Hora em que o trabalho foi iniciado.
Finalizado às	Hora em que o trabalho foi concluído.
Duração do trabalho	Tempo total para concluir o trabalho.
Subestado	Subestado para o estado selecionado.
Anotações	Número de registros que foram processados.

4. Clique em **Enviar**.

Nota:

- Para parar de executar o trabalho, clique em **Cancelar**.
- Você não pode reconciliar ICs incompatíveis ou reaplicar as regras de pesquisa de IC enquanto estiver importando hosts ou itens vulneráveis.

Reaplicar regras de pesquisa de IC em itens descobertos selecionados

Reaplicar as regras de pesquisa de item de configuração (IC) em itens descobertos selecionados das ações de seleção de exibição de lista de itens descobertos. Se o IC mudar depois de reaplicar as regras, os itens descobertos serão atualizados com o novo IC e as detecções afetadas. Itens vulneráveis também são atualizados.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Para obter mais informações, consulte Mudanças de IC para itens descobertos.

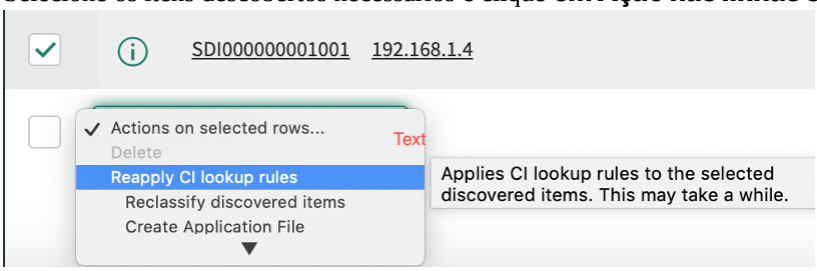
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre os conceitos de correspondência de IC e o CMDB, pesquisa de item descoberto, identificação baseada em regra e outras informações detalhadas sobre como funciona a correspondência de IC, consulte o artigo Correspondência de IC no Vulnerability Response [KB0998706] na Base de conhecimento HI.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **CMDB** > **Itens Descobertos**.
2. Selecione os itens descobertos necessários e clique **em Ação nas linhas selecionadas**.



3. Na lista, selecione **Reaplicar regras de pesquisa de IC**.

   As regras são reaplicadas nesses itens descobertos.

4. Clique em **Exibir status** na mensagem.

   O status é exibido no formulário de trabalho em segundo plano.

> **Nota:**
> No campo **Anotações**, não foi possível processar os itens descobertos porque um atributo de exceção com um valor diferente de zero indica que há um erro ou uma exceção ao reaplicar uma regra de pesquisa de IC. Verifique os logs do sistema para obter mais detalhes.

Etapas para ajudar a evitar registros duplicados ou órfãos após a execução de Vulnerability Response regras de pesquisa de IC

Tome medidas para ajudar a evitar registros duplicados ou órfãos resultantes da correspondência (itens de configuração (ICs)) no CMDB.

A importação de dados de vulnerabilidade pode sobrecarregar uma instância e podem ocorrer problemas de desempenho com recursos se as regras não forem construídas com cuidado. A lógica usada para iterar e executar a correspondência no CMDB pode resultar em longos tempos de processamento. O teste completo e a depuração de scripts de processamento nas regras ajudam a reduzir o potencial de problemas posteriormente no processo.

Como evitar registros duplicados ou órfãos

- Use pequenos subconjuntos de dados que são específicos à regra de pesquisa de IC que está sendo testada.
  - Defina todas as Regras de pesquisa de IC, exceto a que está sendo testada, como Inativas.
  - Analise os ICs importados para garantir que você esteja observando o comportamento esperado e que a correspondência esteja ocorrendo corretamente.
- Revisar ICs correspondentes

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Examine a contagem de ICs correspondentes versus não correspondentes. Certifique-se de que a porcentagem seja aceitável. Não olhe apenas para a primeira página, que provavelmente é a primeira inserida.
- Pesquise manualmente alguns ICs.
- Verifique se há algum problema de nomenclatura ou de campo (como pesquisar um domínio específico).

  Se parecer apropriado, adicione regras de correspondência adicionais.

- Revisar ICs incompatíveis
  - Navegue até a tabela ICs incompatíveis.
  - Agrupar por classe de item de configuração.
  - Revise todas as classes que não parecem corretas (certificados, placas de rede, imagens).
    - Descobrir por que eles não corresponderam ao IC correto?
    - A classe deve ser excluída?
    - A classe deve ser elevada a uma classe relacionada?
- Revise os estados de IC, como **Descontinuado**.
- Remover Dados de Teste
  - Depois de começar a observar o comportamento correto ou esperado na correspondência de IC, reinicie.
  - Reinicie: Excluindo os dados usados para teste: (consulte a seção **Excluindo dados de tabelas**)
    - Itens Descobertos
    - Itens vulneráveis
    - Tarefas de correção
  - Reexecução manual de todas as regras de Correspondência de IC.

Para obter mais informações sobre Regras de pesquisa de IC e Qualys, consulte o artigo KB0750656 .

Para obter mais informações sobre Regras de pesquisa de IC e Rapid7, consulte KB0818096 .

Excluindo dados de tabelas

Às vezes, você importou dados e percebeu que algo está errado. Se algo estiver errado em um ambiente de desenvolvimento ou desempenho, você poderá recriar a partir de um ambiente melhor, mas isso nem sempre é uma opção.

Nota:
Realizar essas ações requer experiência em ServiceNow.

Existem quatro opções para excluir dados de tabelas:

- Usando **Excluir todos os registros** na **configuração da tabela**.
- Configure o **limpador de tabela** navegando até **Limpezas automáticas** (sys_auto_flush.list) e criando um novo registro **de limpeza automática**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Truncar gs.truncateTable usando um script em segundo plano.

  Usar `truncateTable` requer a desativação do registro para a caixa de seleção de reversão nos scripts em segundo plano. Caso contrário, uma cópia da tabela e das tabelas em cascata relacionadas será criada, demorará muito e provavelmente falhará.

  Nota:
  Nunca use `truncateTable` em um ambiente de produção. Consulte seu representante do Suporte antes de executar grandes exclusões em ambientes de produção ou compartilhados.

Desduplicando itens de configuração existentes

Sempre que os itens de configuração (ICs) são atualizados por meio de uma tarefa de desduplicação, os itens descobertos (DIs) que estão relacionados a esses ICs também são atualizados. Os itens vulneráveis (IVs) e as detecções também são atualizados com o IC.

Para obter mais informações, consulte Mudanças de IC para itens descobertos.

Tópicos relacionados

Como corrigir uma tarefa de desduplicação

Resolver tarefas de correção

A flexibilidade inerente ao Vulnerability Response permite que você corrija vulnerabilidades de qualquer maneira que se adeque à sua organização de segurança.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Por Que e Quando Desempenhar Esta Tarefa

Depois de ser notificado de que uma solicitação de mudança foi resolvida, mova o estado da tarefa de correção para Resolvido e aguarde a próxima verificação. As novas verificações são acionadas automaticamente pela programação de importação de terceiros configurada no Assistente de configuração.

Nota:

Se a sincronização de estado estiver ativada, as tarefas de correção serão movidas automaticamente para o estado Resolvido depois que uma solicitação de mudança associada a uma tarefa de correção (VUL) for implementada e no estado Revisão. Consulte Change Management para Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Tarefas de correção** > **Atribuído a mim**.
2. Clique em um registro que esteja no estado Aberto.

   O estado Aberto indica que o registro ainda não foi trabalhado. O formulário exibe:

   - Informações da tarefa de correção
   - Detalhes da configuração de grupo
   - Anotações
   - Itens vulneráveis associados
   - ANSs de tarefas
   - Solicitações de Mudança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Realize sua análise do grupo.
4. Quando estiver pronto para começar a trabalhar no registro, escolha uma das opções a seguir.

Opção	Descrição
Se o item vulnerável representar um risco para o seu ambiente de TI, crie um registro CHG e escale o problema para a equipe do Change Management .	Atribua o grupo ao grupo ou indivíduo apropriado e clique em **Criar mudança**.
Se o item vulnerável representar um possível risco à segurança da sua organização, crie um registro de incidente de segurança e escale o problema para a equipe Security Incident Response.	Clique **em Criar incidente de segurança**. Este botão é exibido somente quando Security Incident Response está ativado. Um cálculo de impacto nos negócios é aplicado, o incidente é atribuído e o incidente de segurança é criado.

Depois de criar uma solicitação de mudança, o registro apropriado aparece na lista relacionada **Solicitações de mudança** no formulário Grupo de vulnerabilidades.

5. Se você determinar que o problema é de baixo risco e pode ser adiado, clique em **Solicitar exceção**.
Para obter instruções, consulte Adiar uma tarefa de correção.
6. Se você determinar que o problema pode ser encerrado imediatamente sem análise adicional, clique em **Fechar**.
Para obter instruções, consulte Fechar uma tarefa de correção.

Um trabalho programado de integração de terceiros atualiza e verifica automaticamente os registros em um intervalo definido. Os itens vulneráveis são verificados na próxima data e hora programadas. Como alternativa, você pode iniciar manualmente uma verificação de vulnerabilidade usando o link relacionado **Verificar vulnerabilidades**.

Se a verificação encontrar novamente a vulnerabilidade no item de configuração e não marcá-la como Corrigida, o item vulnerável retornará ao estado Sob investigação. Entre em contato com Operações de TI para reabrir a solicitação de mudança.

Se a verificação não encontrar a vulnerabilidade e retornar que o item vulnerável foi marcado como Corrigido, o item vulnerável fará a transição para o estado Encerrado-Corrigido e será encerrado durante a importação.

Somente quando todos os itens vulneráveis em uma tarefa estão no estado Encerrado-Corrigido, a tarefa de correção é encerrada automaticamente. Tarefas de correção com itens vulneráveis em estados Encerrado diferentes de Corrigido devem ser encerradas manualmente.

Adiar uma tarefa de correção

Se você determinar que o problema associado a uma tarefa de correção (VUL) é de prioridade baixa e pode ser adiado imediatamente sem análise adicional, você pode usar o recurso **Solicitar exceção**.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você pode adiar uma tarefa de correção de um registro de tarefa de correção nos espaços Vulnerability Response. Depois de enviar a solicitação, ela é enviada para aprovação. Consulte Solicitar uma exceção no Espaço de correção de problemas de TI.

Um trabalho programado é executado todos os dias para verificar se há tarefas de correção adiadas que atingiram a data de reabertura. No dia em que o adiamento da tarefa é definido para expirar, a tarefa é reaberta.

Nota:
Você pode mover manualmente solicitações de mudança e tarefas de correção pelos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que um CHG mudou seu estado, ou você adiciona um CHG ou remove-o de uma tarefa de correção , a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados de solicitação de mudança não movem automaticamente as tarefas de correção dos estados Encerrado ou Adiado.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Tarefas de correção**.
2. Abra um registro.
3. Clique **em Solicitar exceção**.
4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Até	Selecione a data em que o estado Adiar expira e a tarefa de correção é reativada. Depois que o registro for enviado, se as notificações por e-mail forem definidas, os membros do grupo Vulnerability Response receberão um e-mail quando a data de expiração estiver dentro de uma semana. Quando a data de adiamento expira, a tarefa de correção é definida novamente como **Aberta** e uma segunda notificação por e-mail é enviada.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Falso positivo ○ Correção indisponível ○ Risco aceito ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Clique em **Enviar**.
   O grupo está marcado em revisão. Um link relacionado **Reabrir** é exibido. A data e o motivo de reabertura aparecem nas anotações de trabalho na guia **Aprovações de mudança de estado**.

Solicitar uma extensão para uma tarefa de correção adiada

Solicite uma extensão para uma tarefa de correção adiada (VUL) antes que ela atinja a data de vencimento. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão nos espaços Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Tarefas de correção**.
2. Abra uma tarefa de correção adiada.
3. Selecione **Solicitar extensão**.
4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Prorrogar até	Selecione a data em que o estado Adiar expira e a tarefa de correção é reativada.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Na aprovação da solicitação, as mudanças na tarefa de correção também são revertidas para os itens vulneráveis, que fazem parte da tarefa de correção. No entanto, os itens vulneráveis devem estar no estado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

adiado e seus dados atuais até precedem a data até a atualização. Um e-mail também é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma tarefa de correção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Fechar uma tarefa de correção

Se você determinar que o problema associado a uma tarefa de correção pode ser encerrado imediatamente sem análise adicional, poderá usar o recurso **Fechar**.

Antes de Iniciar

Função necessária: administrador

Nos Vulnerability Response espaços, uma tarefa de correção passa pelos mesmos estados que um grupo de vulnerabilidades anterior tinha nas versões anteriores do Vulnerability Response. Quando todos os IVs em uma tarefa de correção são encerrados, a tarefa de correção muda para o estado Inativo.

Importante:
Você pode mover manualmente solicitações de mudança e tarefas de correção pelos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que um CHG mudou seu estado, ou você adiciona um CHG ou remove-o de uma tarefa de correção , a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados de solicitação de mudança não movem automaticamente as tarefas de correção dos estados Encerrado ou Adiado.

Procedimento

1. Abra o registro para o qual você deseja solicitar uma revisão.
2. Clique no botão **Fechar/Adiar**.
3. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Estado	Selecione um estado. As opções são: ○ Adiado ○ Encerrado
Até	Disponível somente no pop-up de estado **Adiar**. Selecione a data em que o estado **Adiar**expira e a tarefa de correção é reativada. Depois que o registro for enviado, se as notificações por e-mail forem definidas, os

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	membros do grupo Vulnerability Response receberão um e-mail quando a data de expiração estiver dentro de uma semana. Quando a data de adiamento expira, o item vulnerável é definido novamente como **Aberto** e uma segunda notificação por e-mail é enviada.
Motivo	Insira o motivo para encerrar o problema.
Informações adicionais	Insira outras informações relevantes.

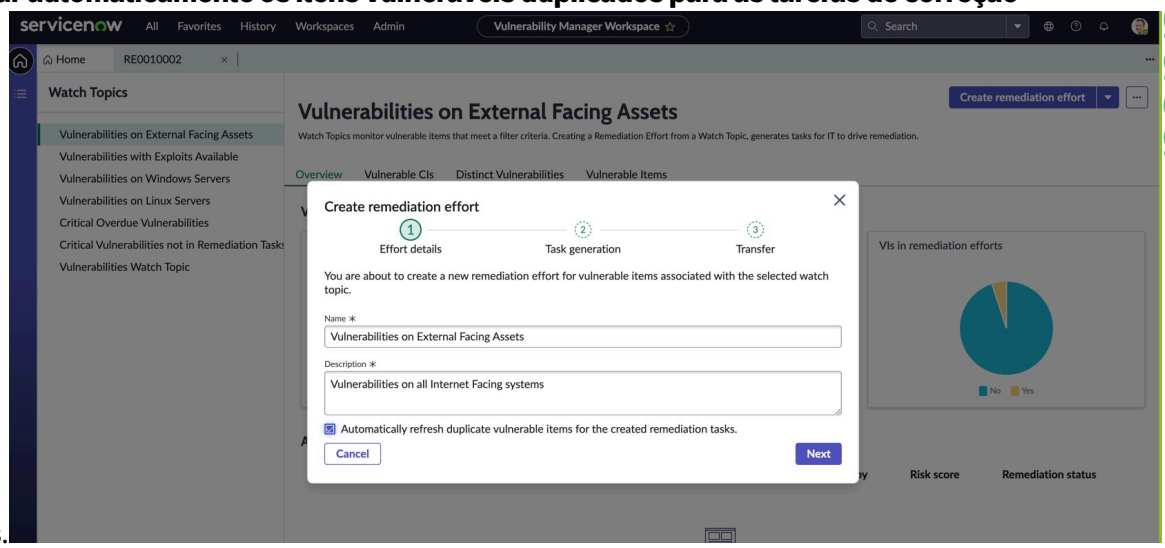
4. Clique em **Enviar**.
   O grupo está marcado como **Encerrado**.

Identificar itens vulneráveis duplicados de vários scanners

Se você estiver usando vários scanners no mesmo ativo para detectar vulnerabilidades, vários itens vulneráveis (IVs) poderão ser criados. Você pode identificar esses IVs duplicados para garantir que as vulnerabilidades duplicadas não sejam atribuídas aos responsáveis pela correção.

Essa resolução só será possível se as mesmas vulnerabilidades, como as mesmas CVEs (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns) forem detectadas. A combinação de vulnerabilidades depende dos scanners que estão sendo usados. Por exemplo, Qualys e Tenable têm seu próprio tipo de vulnerabilidade, ou seja, entradas de terceiros (TPEs), e outros scanners, como o Microsoft Defender para Endpoint, detectam vulnerabilidades com base em CVEs.

A partir da v 17.1, ao criar um esforço de correção, você pode atualizar automaticamente os itens vulneráveis duplicados nas tarefas de correção criadas. Para atualizar automaticamente os itens vulneráveis duplicados, você deve selecionar a opção **Atualizar automaticamente os itens vulneráveis duplicados para as tarefas de correção criadas**.



Mostrar IVs duplicados: identifica itens vulneráveis duplicados relatados por vários scanners no sistema. Você pode marcar o IV duplicado como Resolvido. Para obter mais informações, consulte Resolver vulnerabilidades duplicadas automaticamente. Entradas duplicadas são mostradas somente quando a combinação de vulnerabilidades é criada usando CVEs. Para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

obter mais informações, consulte Tarefa de correção do Vulnerability Response e estados de item vulnerável.

Possíveis duplicatas são identificadas para as seguintes combinações de vulnerabilidade:

Combinação de scanner	Tipo de vulnerabilidade
Scanner 1 e Scanner 2	CVE
Scanner 1 e Scanner 2	CVE e TPE

Resolver vulnerabilidades duplicadas automaticamente

A partir de Vulnerability Response (VR) v17.1, você pode resolver automaticamente quaisquer vulnerabilidades duplicadas em um ativo.

Quando um ativo é verificado com vários scanners, há uma chance de identificar a mesma vulnerabilidade como duplicatas pelos diferentes scanners. Por exemplo, se os scanners Qualys e Microsoft identificarem a mesma vulnerabilidade, você poderá optar por resolver automaticamente a duplicada.

Cenário de amostra

O VR cria um registro, VI1, para a vulnerabilidade 1 do scanner do Microsoft Defender for Endpoint. Um segundo registro, VI2, é criado a partir do scanner Qualys para a mesma vulnerabilidade. A equipe de correção aplica os patches que podem resolver os registros VI1 e VI2. Se você configurar a programação de verificação do Qualys além de um dia, o Microsoft Defender fornecerá as informações de vulnerabilidade corrigida e o VR fechará o registro VI1 como Encerrado/Corrigido.

Neste cenário, o registro VI2 ainda está no estado Aberto e o VR aguarda os resultados da verificação do Qualys. Nessa situação, os registros de IV do segundo scanner permanecem no estado Aberto mesmo se o patch for aplicado e o IV for confirmado como corrigido pelo outro scanner.

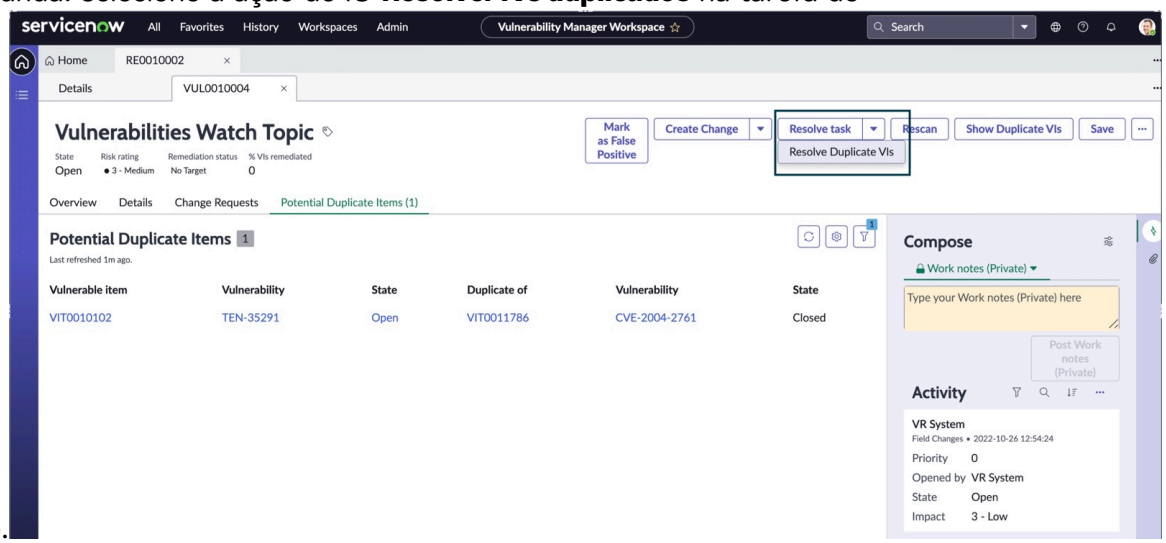
Para resolver essa situação, você pode considerar resolver o registro de vulnerabilidade duplicado com base na condição de que a vulnerabilidade foi encerrada pelo primeiro scanner.

Resolva vulnerabilidades das seguintes maneiras:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Sob demanda: selecione a ação de IU **Resolver IVs duplicados** na tarefa de correção.



- Automatizado: habilite a propriedade do sistema `sn_vul.auto_resolve_duplicate_vit` para resolver automaticamente itens vulneráveis duplicados. O trabalho programado diário "Atualizar e resolver VITs duplicados na tarefa de correção" atualiza automaticamente os itens duplicados.

Os IVs duplicados são marcados como resolvidos.

Nota:
O registro do item de vulnerabilidade resolvido será reaberto se o scanner o identificar como **Não corrigido**.

Criar e editar um grupo de classificação

Crie grupos para que as regras subjacentes deste grupo possam classificar os registros da tabela com base nas condições. As regras podem ser usadas para selecionar qualquer campo na tabela correspondente.

Antes de Iniciar

Função necessária: sn_vul.manage_classification_rule

Procedimento

1. Navegue até a tabela Propriedades do sistema.
2. Na propriedade do sistema *`sn_sec_cmn.classificationTables`*, adicione o nome da tabela para a qual você deseja criar o grupo de classificação.
3. Crie uma nova regra de negócios adicionando o seguinte snippet de código à regra de negócios na tabela definida no grupo:
   `var classificationCalc = new sn_vul.VulnerabilityCalculator(current,true,false,'sn_vul_classification_group','sn_vul_classification_rule'); classificaçãoCalc.calcular();`

   Nota:
   As regras de negócios são fornecidas para executar a classificação durante a ingestão dos itens descobertos e das tabelas de entrada de vulnerabilidade. Para outras tabelas, para que tenham as regras de classificação na ingestão, você deve adicionar as regras de negócio.

4. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de classificação**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. No menu de contexto Grupos de classificação, clique em **Novo**.
6. No formulário, preencha os campos.

Formulário Grupo de classificação de vulnerabilidade

Campo	Descrição
Nome	Nome do novo grupo de classificação.
Ativo	Opção para ativar o grupo.
Descrição	Descrição do novo grupo de classificação.
Tabela	Tabela baseada na qual as regras são executadas. **Nota:** O sistema básico do Vulnerability Response inclui grupos de classificação para itens descobertos e vulnerabilidades.

Criar e editar uma regra de classificação

Crie regras para classificar automaticamente as vulnerabilidades de entrada para as equipes corretas para correção.

Antes de Iniciar

Função necessária: sn_vul.manage_classification_rule

Por Que e Quando Desempenhar Esta Tarefa

Quando criadas, essas regras classificam as vulnerabilidades como pertencentes a uma plataforma ou a uma aplicação. Você pode configurar essas regras para substituir o valor de um campo específico na entrada da vulnerabilidade.

Use essas regras para mover o cálculo ascendente para a tabela Entrada de vulnerabilidades de terceiros para habilitar a reutilização do conteúdo.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de classificação**.
2. Para exibir um grupo de classificação, clique nesse grupo.
3. No menu de contexto Regras de classificação, clique em **Novo**.
4. No formulário, preencha os campos.

Formulário Regra de classificação de vulnerabilidade

Campo	Descrição
Nome	Nome da nova regra de classificação.
Ativo	Opção para ativar a regra.
Descrição	Descrição da nova regra de classificação.
Ordem de execução	Ordem na qual a regra deve ser executada.
Exibição avançada	Opção para exibir campos adicionais nas seções com guia.
Quando esta condição for atendida	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo de condição	Tipo de condição para a regra. Estas são as opções: ○ **Filtro**: condições básicas de filtro para determinar se a regra deve ser usada ou não. ○ Grupo de**filtros**: conjunto de várias condições que são usadas juntas. A regra é avaliada com base nas condições definidas no grupo de filtros. ○ **Script**: condição de script usada para determinar quando aplicar esta regra. Este campo é exibido somente quando a opção **de exibição Avançada** é selecionada.
Condição	Condição para a regra. Defina condições com base na coluna selecionada na coluna de entrada de vulnerabilidade necessária. Você pode adicionar várias condições para refinar a regra. Este campo é exibido somente quando **Filtro** é selecionado no campo **Tipo de condição**. **Nota:** Ao definir várias condições ou modelos, você pode selecionar somente a partir de uma tabela primária e secundária. Você não pode selecionar duas ou mais tabelas secundárias.
Grupo de filtros	Grupo de filtros. O grupo é definido quando um conjunto de condições é usado repetidamente em vários locais. Clique na pesquisa usando o ícone de lista (ícone de de lista) para selecionar o grupo de filtros. Para obter mais informações, consulte Criar e definir grupos de filtros no Security Operations. Este campo é exibido somente quando **Grupo de filtros** é selecionado no campo **Tipo de condição**.
Script	Script que é avaliado para determinar quando aplicar esta regra. Você pode escrever seu código e definir a resposta como verdadeira ou falsa. Este campo é exibido somente quando **Script** é selecionado no campo **Tipo de condição**
Definir estes valores	
Classificação	Classificação da regra. Para selecionar uma opção, clique no ícone de lâmpada (Ícone de). A lista exibe as opções de plataforma e aplicação. Como alternativa, você pode inserir sua própria classificação que não está na lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipo de classificação	Tipo de classificação. Este campo mostra a lista filtrada de tipos de classificação com base no valor selecionado para o campo **Classificação**.
Tipo de valor	Tipo do valor que é atribuído por usando esta regra. Estas são as opções: ○ **Modelo**: selecionar um modelo. Você pode usar um modelo necessário. ○ **Script**: selecione um script preexistente ou escreva seu próprio script personalizado. Este campo é exibido somente quando a opção **de exibição Avançada** é selecionada.
Modelo	Outra condição para a regra além dos campos **Classificação** e **Tipo** de classificação. Selecione uma combinação de campos e valores que você deseja definir quando a regra for avaliada. Este campo é exibido somente quando o **modelo** é selecionado no campo **Tipo de valor**.
Valor do script	Script para definir valores no registro atual. Este campo define quais valores definir nos campos nas entradas de vulnerabilidade. Este campo é exibido somente quando **Script** é selecionado no campo **Tipo de valor**.

5. Para criar a nova regra, clique em **Enviar**.

Example:
Use regras de classificação de VR para adicionar a lógica a tabelas ascendentes, como Vulnerabilidade e Itens descobertos, e calculá-la. Você pode reutilizar a saída várias vezes, melhorando assim o desempenho de regras, como regras de atribuição. Por exemplo, classifique a entrada de terceiros (TPE) como Java e reutilize a saída nas regras de atribuição várias vezes. Exemplo de regra de atribuição:

```
VI.TPE.Classfication Type
        | IS | Java
```

Aplicar uma regra a uma vulnerabilidade existente

Ao alterar uma regra de classificação, execute novamente todas as regras ativas em todas as entradas de vulnerabilidade. Você também pode retroajustar as vulnerabilidades existentes, aplicando as regras de classificação recém-criadas às vulnerabilidades existentes.

Antes de Iniciar
Função necessária: sn_vul.manage_classification_rule

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Regras de classificação de vulnerabilidade**.
2. Para selecionar uma regra, marque a caixa de seleção ao lado da regra.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique em **Aplicar mudanças**.
4. Clique **em Reaplicar**.

Desativar ou excluir uma regra de classificação

Desative ou exclua uma regra de classificação se ela não for mais necessária ou relevante.

Antes de Iniciar

Função necessária: sn_vul.manage_classification_rule

Por Que e Quando Desempenhar Esta Tarefa

Quando uma regra de classificação é desativada ou excluída, os dados que foram preenchidos nos campos **Classification** e **Classification_type** por essa regra excluída permanecem em suas respectivas tabelas.

Se você quiser limpar esses dados, crie uma regra com valores vazios nos campos **Classification** e **Classification_type** e reaplique o grupo. Depois que esta nova regra for reaplicada, as mudanças serão refletidas em todos os registros aos quais esta regra é aplicável, com base nas condições da regra.

Procedimento

1. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Regras de classificação de vulnerabilidade**.
2. Para selecionar a regra que você deseja excluir, clique na caixa de seleção ao lado da regra.
3. Para excluir a regra, siga um destes procedimentos:
   - Na lista Ação em linhas selecionadas, clique em **Excluir**.
   - Selecione a regra e clique no botão **Excluir**.
4. Clique em **Aplicar mudanças**.

Nota:
Se você não clicar neste botão, a regra continuará a residir no sistema. As vulnerabilidades referenciadas pela regra continuam a fazer referência a elas.

Gestão de mudanças tarefas para Vulnerability Response

A partir de tarefas de correção (RTs), crie solicitações de mudança, associe RTs a solicitações de mudança existentes ou divida tarefas de correção em novas tarefas com subconjuntos de itens vulneráveis (IV).

Crie e gerencie solicitações de mudança diretamente de uma tarefa de correção se um processo manual e controlado de qualquer tipo for necessário para modificação ou remoção de itens de configuração (ICs) compatíveis no seu CMDB. Criar e gerenciar solicitações de mudança diretamente de um registro ajuda a investigar e resolver vulnerabilidades rapidamente.

Consulte Change Management para Vulnerability Response para obter uma visão geral de como o gerenciamento de mudanças funciona com a aplicação Vulnerability Response e os requisitos do sistema.

Consulte os tópicos a seguir para saber como criar solicitações de mudança, associar tarefas de correção a solicitações de mudança existentes e dividir tarefas de correção. Consulte Sincronização de estado entre solicitações de mudança e tarefas de correção para obter informações sobre como os campos de estado em solicitações de mudança (CHG) resolvem automaticamente as tarefas de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar uma solicitação de mudança a partir de uma tarefa de correção

Como proprietário de correção de TI, crie uma solicitação de mudança (CHG) diretamente de uma tarefa de correção (VUL) para todos os itens vulneráveis do grupo. Crie uma solicitação de mudança com informações preenchidas previamente que incluam a solução preferencial para agilizar sua investigação de vulnerabilidades que exigem intervenção manual.

Antes de Iniciar

Funções necessárias: para criar uma solicitação de mudança: qualquer usuário com a função itil. A função sn_vul.remediation_owner também é atribuída automaticamente quando a função itil é atribuída a um usuário.

Função necessária: para aprovação de solicitações de mudança: usuários com funções itil, admin, sn_change_write, change_manager.

Por Que e Quando Desempenhar Esta Tarefa

Para obter informações sobre como criar uma solicitação de mudança nos espaços Vulnerability Response, consulte Criar uma solicitação de mudança no Espaço de correção de problemas de TI.

Para criar uma solicitação de mudança no ambiente clássico, siga as etapas listadas abaixo.

Você pode criar, aprovar, implementar, revisar e fechar solicitações de mudança diretamente de uma tarefa de correção. Você pode criar três tipos de solicitações de mudança com informações preenchidas previamente de uma tarefa de correção:

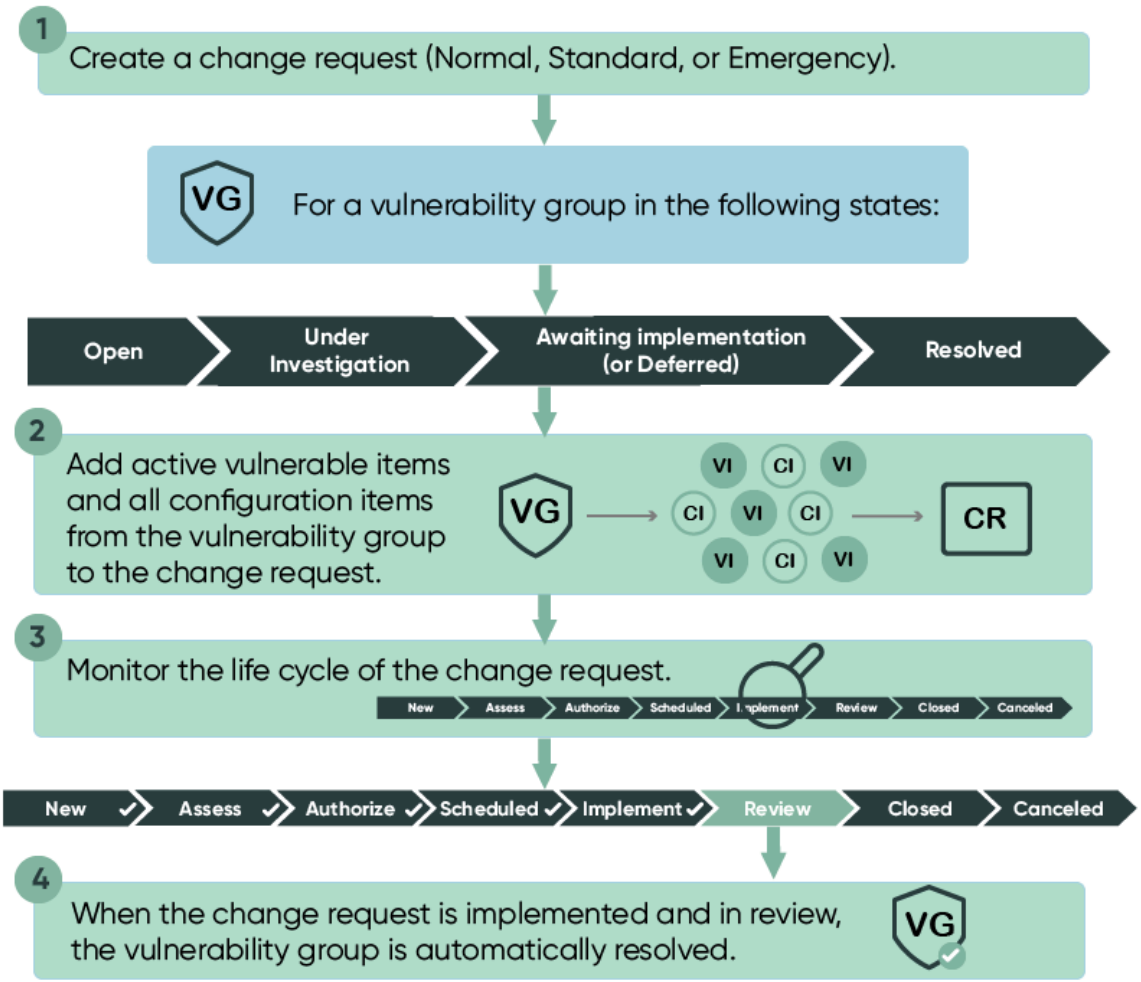
- Padrão. Uma mudança pré-autorizada de baixo risco, relativamente comum e que segue um procedimento especificado ou instrução de trabalho.
- Normal. As solicitações de mudança normais seguem um processo prescritivo que requer dois níveis de aprovação antes de ser implementado, revisado e encerrado.
- Emergência. Uma mudança para resolver um incidente grave.

A imagem a seguir ilustra o fluxo básico para criar uma solicitação de mudança a partir de uma VUL (tarefa de correção). As etapas detalhadas para este fluxo seguem a imagem.

O registro da tarefa de correção é conhecido como VUL nas seções a seguir. Em versões anteriores do Vulnerability Response, as tarefas de correção eram chamadas de grupos de vulnerabilidade (VG). Nas imagens a seguir, VG = tarefa de correção ou um registro VUL.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tradução automática

Nota:
Pontos principais sobre como criar novas solicitações de mudança:

- Você pode criar novas solicitações de mudança para qualquer tarefa de correção (VUL) em um estado diferente de Encerrado.
- Verifique se você tem um aprovador para solicitações de mudança diferente de Padrão (pré-aprovado) que você cria ou associa a um VUL. Isso agiliza a movimentação da VUL para a resolução. Para obter mais informações sobre como adicionar usuários, consulte Adicionar usuários ao grupo do Vulnerability Response.
- Antes que uma tarefa de correção possa ser resolvida, todas as tarefas em pelo menos um CHG associado ao VUL devem ser concluídas para que a solicitação de mudança possa ser implementada e movida para o estado Revisar.

Procedimento

1. Para criar uma solicitação de mudança completa a partir de um registro de tarefa de correção existente, navegue até **Todos** > **Vulnerability Response** > **Tarefas de correção** > **Atribuído aos Meus grupos**.
   A lista de tarefas de correção atribuídas ao seu grupo de atribuição será exibida.
2. **Opcional:** Navegar até **Todos** > **Vulnerability Response** > **Visão Geral da Correção** para exibir o painel Visão geral da correção e localizar uma VUL atribuída a você ou ao seu grupo de atribuição.
3. Como alternativa, na coluna Número, clique em uma tarefa de correção para abrir o registro e exibir os detalhes.

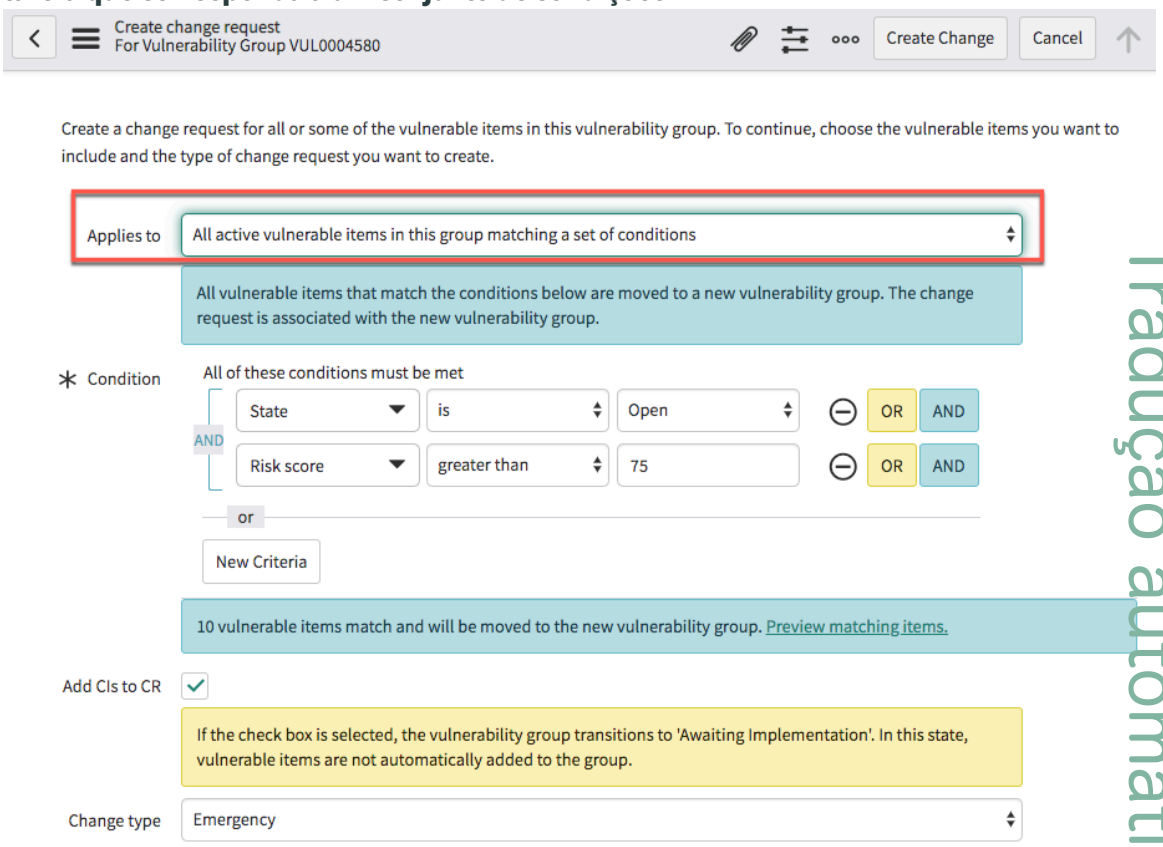
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O registro é exibido.

4. Com o registro VUL exibido para o qual você deseja criar a solicitação de mudança, no canto superior direito do registro, clique em **Criar mudança**.
   O formulário Criar solicitação de mudança é exibido.
5. Preencha os campos.

   a. Na lista de seleção do campo Aplica-se a, escolha um para continuar.

Criar formulário de solicitação de mudança para itens vulneráveis em uma tarefa que corresponda a um conjunto de condições



   b. **Opcional:** Se exibido no formulário, clique no link **Visualizar itens correspondentes** para obter uma lista dos IVs que correspondem aos seus critérios de filtro.
   A visualização da Lista de tarefas de correção é exibida. Você pode selecionar itens nesta lista de visualização e executar ações de IU neles. No entanto, essas ações também são realizadas no VUL. Por exemplo, se você excluir um IV da lista de visualização, esse IV também será excluído da VUL.

   c. Depois de concluir a visualização, feche a janela do navegador para retornar o formulário de solicitação de mudança.

   d. Na caixa de seleção Adicionar ICs ao CR, escolha um para continuar.

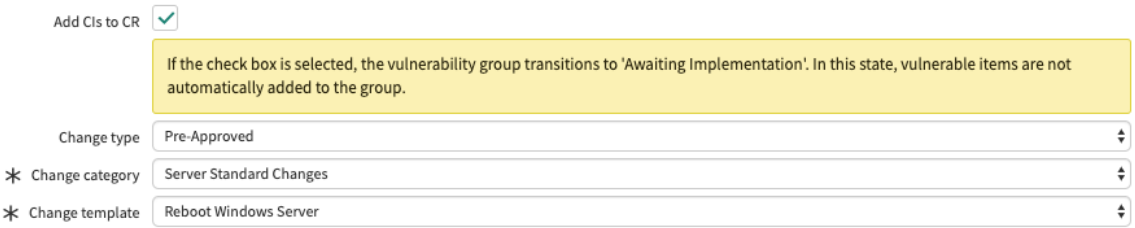
   e. Na lista de seleção do campo Tipo de mudança, escolha um para continuar.

      O recurso lê automaticamente os tipos de solicitações de mudança que você configura em seu catálogo no ITSM Change Management. Por exemplo, se você alterar o nome das solicitações de mudança padrão no ITSM de Padrão para Pré-aprovado, o novo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

nome será exibido automaticamente na lista de seleção Tipo de mudança em Criar solicitação de mudança de, conforme mostrado na figura a seguir.



Os campos na seção Visualização da solicitação de mudança do formulário são preenchidos previamente com informações do VUL. Se necessário, esses valores de campo podem ser editados. Por exemplo, revise os valores nos campos na figura a seguir:

Data de término planejada

Esta data (2019-10-10) é o mesmo valor exibido no campo Data de destino da correção do VUL. Este valor é derivado da data de meta de correção mais antiga dos itens vulneráveis que pertencem ao VUL. Se você estiver criando uma solicitação de mudança para um problema crítico que requer uma data de correção anterior, convém editar este valor e o valor no campo Prioridade.

Justificativa

Este campo exibe o número de ICs adicionados ao CHG. Se você quiser adicionar informações adicionais, talvez prefira editar este texto. Por exemplo, talvez você prefira adicionar uma anotação neste campo sobre o filtro usado para criar o novo VUL, por exemplo, `Pontuação de risco maior que 75`. Este texto pode ajudá-lo a localizar sua nova solicitação de mudança e grupo de vulnerabilidades.

Plano de implementação

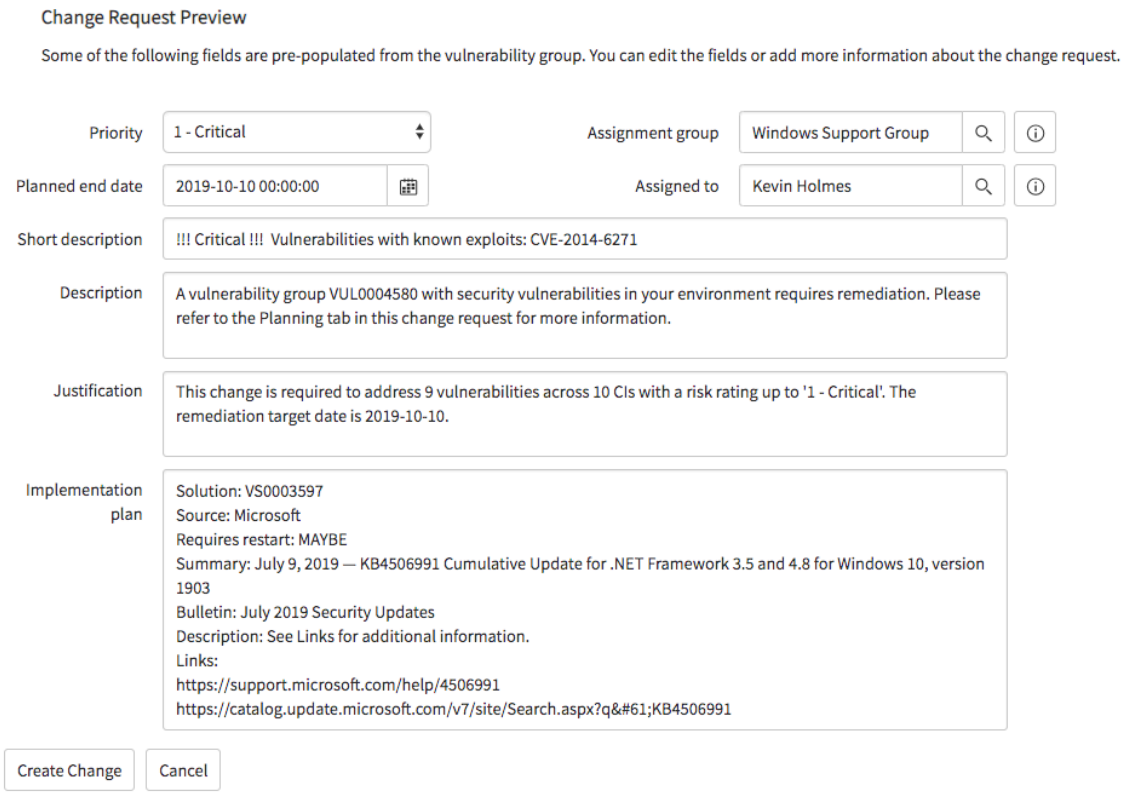
Este campo exibe a solução preferencial para a vulnerabilidade.

Grupo de atribuição e Atribuído a

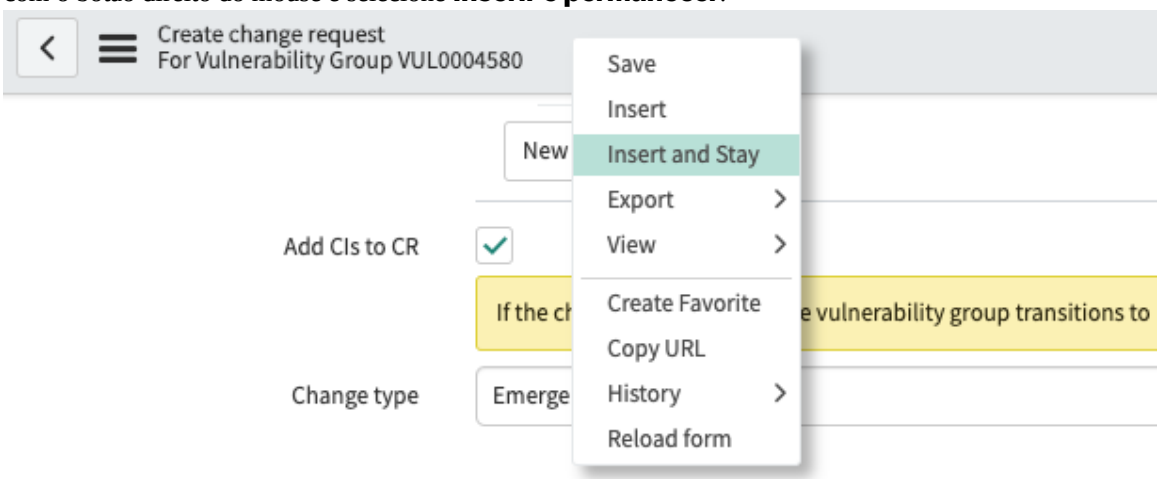
Edite esses campos para mudar o grupo de atribuição ou reatribua esta solicitação de mudança a um usuário em um dos seus grupos de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



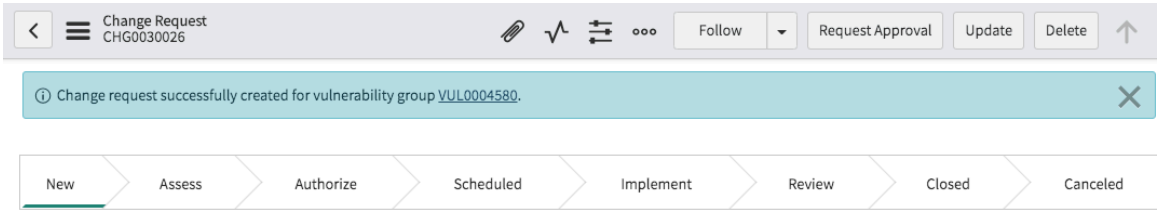
6. Continue a visualizar e editar os campos conforme necessário.
7. Para salvar suas mudanças e permanecer nesta página, na faixa cinza na parte superior do formulário, clique com o botão direito do mouse e selecione **Inserir e permanecer**.



8. Depois de concluir as edições, escolha uma para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:

Para uma tarefa de correção no estado Aberto com o Grupo de atribuição e os campos Atribuído a não atribuídos (vazios), o usuário conectado no momento é atribuído automaticamente à tarefa depois que você clica em **Criar mudança**. Além disso, a caixa de seleção Adicionar ICs ao CR deve estar marcada. Na parte superior da VUL, uma mensagem de confirmação azul é exibida que indica esta atribuição.

O que Fazer Depois

Monitore a solicitação de mudança e as tarefas de mudança para verificar se foram concluídas e se a solicitação de mudança foi implementada. Depois que este CHG for implementado e movido para o estado Revisar, se a sincronização de estado estiver habilitada, a VUL será movida automaticamente para Resolvido. Para obter mais informações sobre sincronização de estado, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

Associar uma tarefa de correção a uma solicitação de mudança existente

Como proprietário de correção de TI, evite criar solicitações de mudança duplicadas (CHG) enquanto trabalha para resolver suas tarefas de correção, associando uma tarefa de correção (VUL) a uma solicitação de mudança que já está disponível em sua instância.

Antes de Iniciar

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Função necessária: qualquer usuário com a função itil. A função sn_vul.remediation_owner também é atribuída automaticamente a um usuário quando a função itil é atribuída.

Por Que e Quando Desempenhar Esta Tarefa

Para obter mais informações sobre como associar uma tarefa de correção a uma solicitação de mudança existente, consulte Criar uma solicitação de mudança no Espaço de correção de problemas de TI.

O registro da tarefa de correção é conhecido como VUL nas seções a seguir. Em versões anteriores do Vulnerability Response, as tarefas de correção eram chamadas de grupos de vulnerabilidade (VG). Nas imagens a seguir, VG = tarefa de correção ou um registro VUL.

Para obter mais informações sobre como associar uma tarefa de correção a uma solicitação de mudança existente, consulte Criar uma solicitação de mudança no Espaço de correção de problemas de TI.

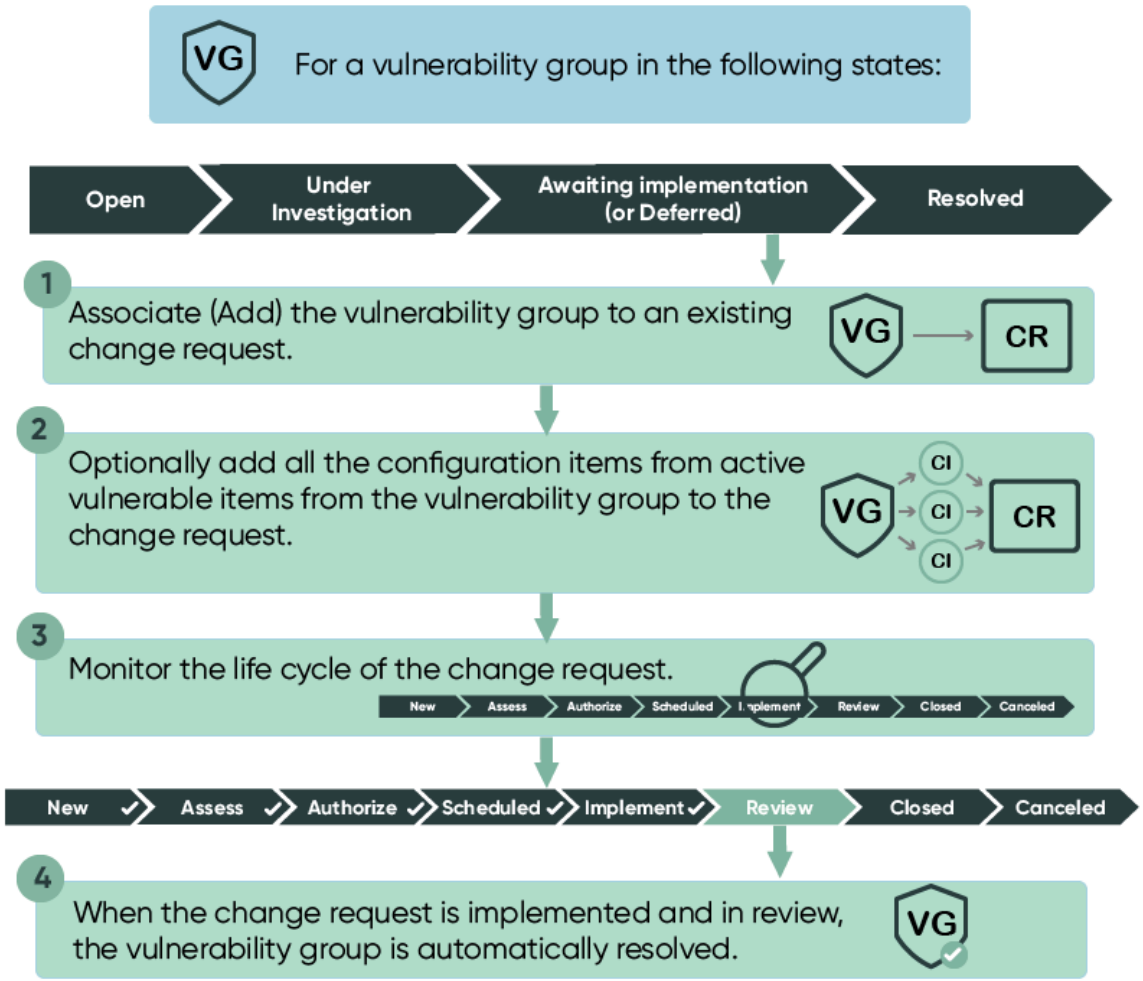
Como proprietário de correção, você pode associar tarefas de correção que são atribuídas a você ou ao seu grupo de atribuição a solicitações de mudança existentes diretamente dos registros da tarefa de correção. A imagem a seguir ilustra o fluxo básico para associar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

uma solicitação de mudança a um VUL (VG) existente. As etapas detalhadas para este fluxo seguem a imagem.

Fluxo de trabalho para associar uma tarefa de correção a uma solicitação de mudança existente



Nota:
Você pode associar uma solicitação de mudança existente a um VUL em qualquer estado (Aberto, Sob investigação, Aguardando implementação, Encerrado e Adiado). Quando você associa uma solicitação de mudança a um VUL existente, somente os IVs ativos são adicionados à solicitação de mudança.

Antes de começar, para evitar a criação de solicitações de mudança duplicadas, talvez você prefira exibir todas as solicitações de mudança existentes já associadas a uma VUL. Para rastrear facilmente o número de solicitações de mudança relacionadas a um VUL específico, consulte a coluna de contagem de CR na lista Tarefas de correção. Se não for exibido, clique no ícone de configurações (ícone de ⚙) no canto superior direito. Mova a coluna de contagem de CR de Disponível para Selecionado e clique em **OK**.

Para preencher automaticamente a nova coluna, para clientes com dados existentes nesta tabela, execute o trabalho programado: Preencher nova coluna de contagem de CR.

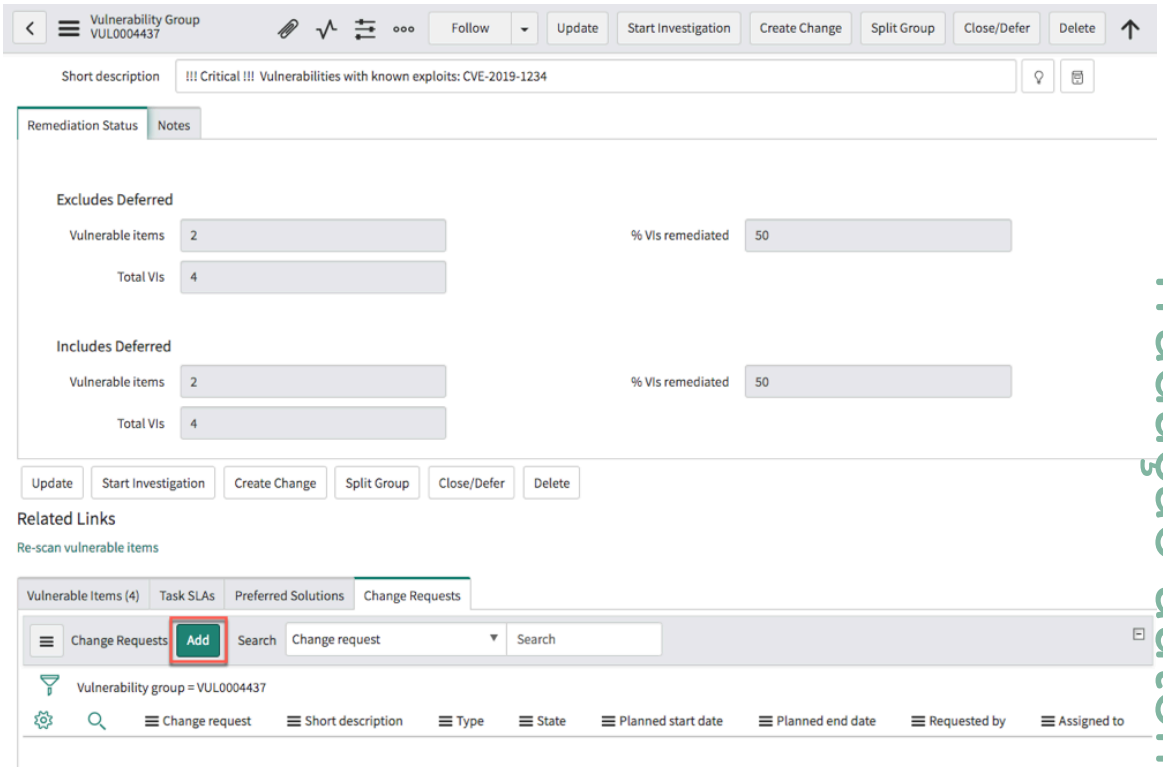
Procedimento

1. Para associar uma tarefa de correção a uma solicitação de mudança existente, navegue até **Todos** > **Vulnerability Response** > **Tarefas de correção**.
2. Localize a tarefa de correção com a qual você está trabalhando.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

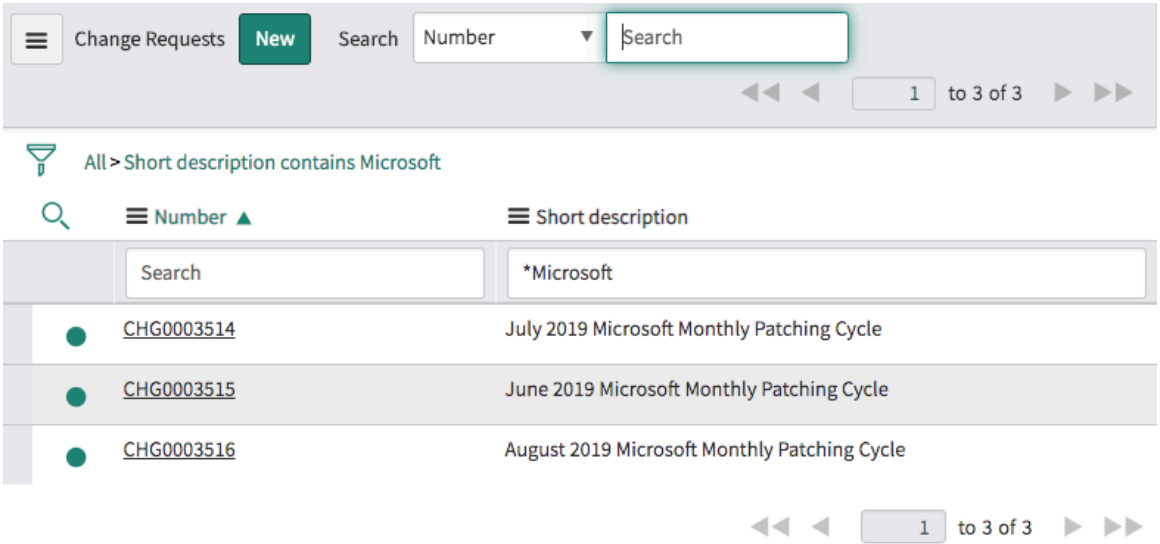
3. **Opcional:** Navegar até **Todos** > **Vulnerability Response** > **Visão Geral da Correção** para exibir o painel Visão geral da correção e localizar uma VUL atribuída a você ou ao seu grupo de atribuição.
4. Na coluna Número, clique em um registro VUL para abri-lo.
   O registro VUL é exibido.
5. Com o registro aberto exibido, se ainda não estiver em exibição, role até a lista relacionada Solicitações de mudança e selecione-a.
   Todas as solicitações de mudança associadas ao VUL são exibidas junto com o botão **Adicionar**. Na figura a seguir, não há solicitações de mudança já associadas a este VUL.



6. Para associar a VUL a um CHG existente, clique em **Adicionar**.
   O formulário Adicionar solicitação de mudança existente à Tarefa de correção é exibido.
7. No formulário, clique no ícone de pesquisa.
   Uma exibição de lista de solicitações de mudança existentes é exibida em uma nova janela, conforme mostrado na figura a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. Selecione um item na lista exibida ou, como alternativa, clique no filtro ( ) e insira condições para limitar os resultados da pesquisa.
9. Na caixa de seleção Adicionar ICs ao CR, escolha um para continuar.

Nota:
Esta caixa de seleção é exibida somente para solicitações de mudança existentes no estado Novo.

10. Com o número da solicitação de mudança que você deseja exibir no campo Pesquisar solicitação de mudança, clique em **Enviar**.
O VUL é exibido. Na parte superior do registro, a mensagem de confirmação azul é exibida indicando que a solicitação de mudança selecionada foi associada com sucesso ao VUL.

Nota:
Para uma VUL no estado Aberto com o Grupo de atribuição e Atribuído a campos não atribuídos (vazios), o usuário conectado no momento é atribuído automaticamente à VUL depois que você clica em **Adicionar**. Além disso, a caixa de seleção Adicionar ICs ao CR deve estar marcada. Na parte superior da VUL, uma mensagem de confirmação azul é exibida indicando que o usuário atual está atribuído.

O que Fazer Depois

Revise o registro VUL. Na coluna Solicitação de mudança na lista relacionada Solicitações de mudança, clique no link do novo CHG para exibir o registro de CR. No registro CHG aberto, você pode monitorar o estado da solicitação de mudança. Os itens de configuração (IC) afetados e as tarefas de correção são exibidos nas listas relacionadas aos ICs afetados e às tarefas de correção.

Dividir uma tarefa de correção

Como proprietário de correção de TI, a partir de uma tarefa de correção existente (VUL), identifique um subconjunto de itens vulneráveis (IV) que você deseja mover para um novo grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Nota:

Os casos de uso para dividir IVs de VULs existentes em novas tarefas de correção podem incluir os seguintes exemplos:

- Quando você deseja criar uma solicitação de mudança ou solicitações de mudança para uma tarefa de divisão.
- Quando você reatribui um grupo de divisão a outro usuário em seu grupo de atribuição.
- Quando você solicita um adiamento ou exceção para uma tarefa de divisão, porque você sabe que algumas vulnerabilidades em itens de configuração (IC) específicos não podem ser corrigidas em um determinado intervalo de tempo.

Função necessária: qualquer usuário com a função itil para dividir uma VUL.

Nota:

A função sn_vul.remediation_owner também é atribuída automaticamente quando a função itil é atribuída a um usuário.

Por Que e Quando Desempenhar Esta Tarefa

Para obter mais informações sobre como dividir tarefas de correção nos espaços Vulnerability Response, consulte Dividir uma tarefa de correção no Espaço de correção de problemas de TI.

Para dividir uma tarefa de correção no ambiente clássico ou para versões de Vulnerability Response.

Você pode dividir as tarefas de correção existentes com mais de um item vulnerável que esteja nos estados Aberto, Sob investigação ou Aguardando implementação. Ao criar um novo VUL com itens vulneráveis que correspondam a critérios específicos, você pode trabalhar com um grupo específico de itens vulneráveis sem afetar a tarefa de correção original.

Quando você especifica as condições dos itens vulneráveis que deseja mover para uma nova tarefa de correção com o construtor de condição, somente os IVs ativos que correspondem aos seus critérios são movidos para o novo grupo.

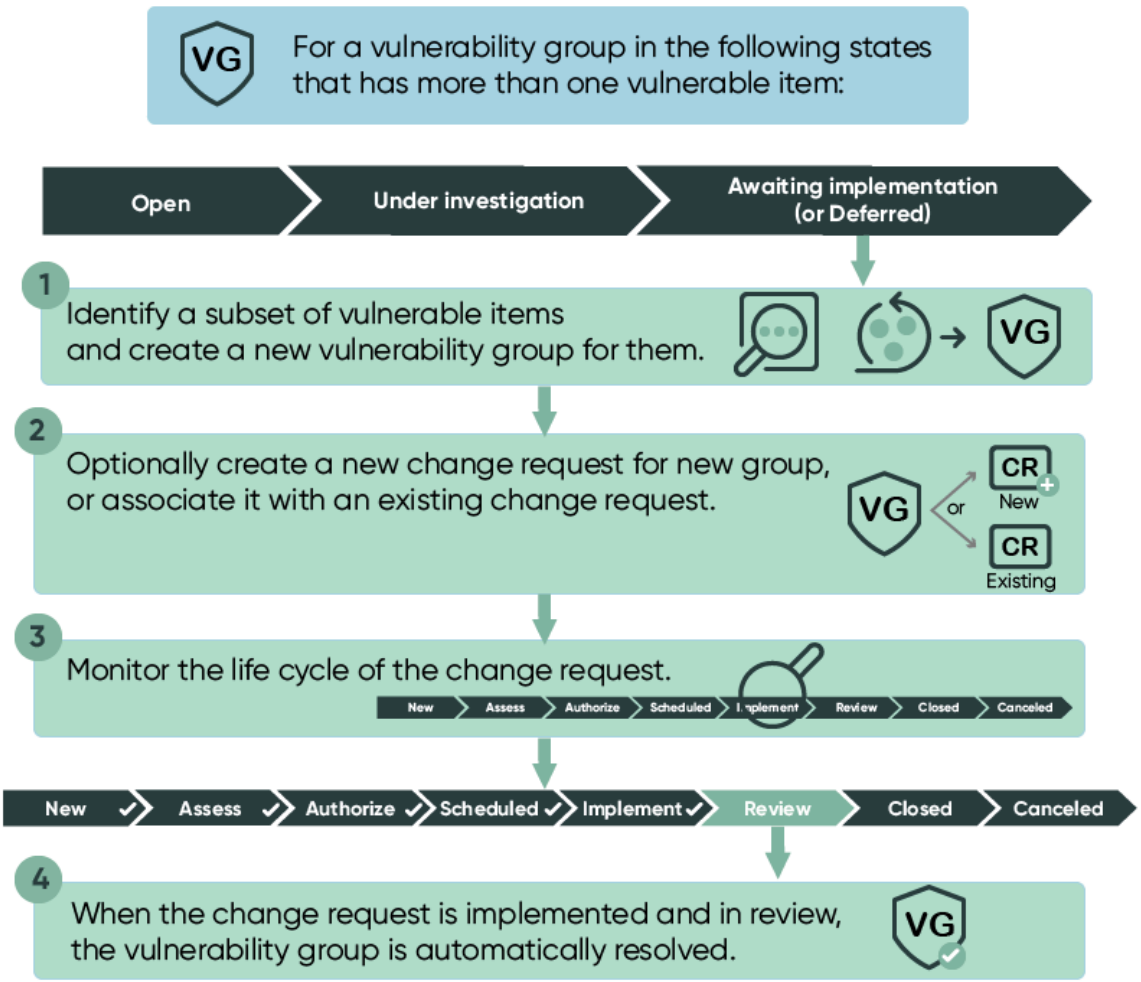
Você não precisa criar solicitações de mudança (CHG) ao dividir uma VUL. Você tem a opção de dividir uma VUL ao mesmo tempo em que cria uma solicitação de mudança ou pode dividir uma VUL sem criar uma solicitação de mudança. A imagem a seguir ilustra o fluxo básico para dividir um grupo de vulnerabilidades. As etapas detalhadas para este fluxo seguem a imagem.

O registro da tarefa de correção é conhecido como VUL nas seções a seguir. Em versões anteriores do Vulnerability Response, as tarefas de correção eram chamadas de grupos de vulnerabilidade (VG). Nas imagens a seguir, VG = tarefa de correção ou um registro VUL.

Tradução automática

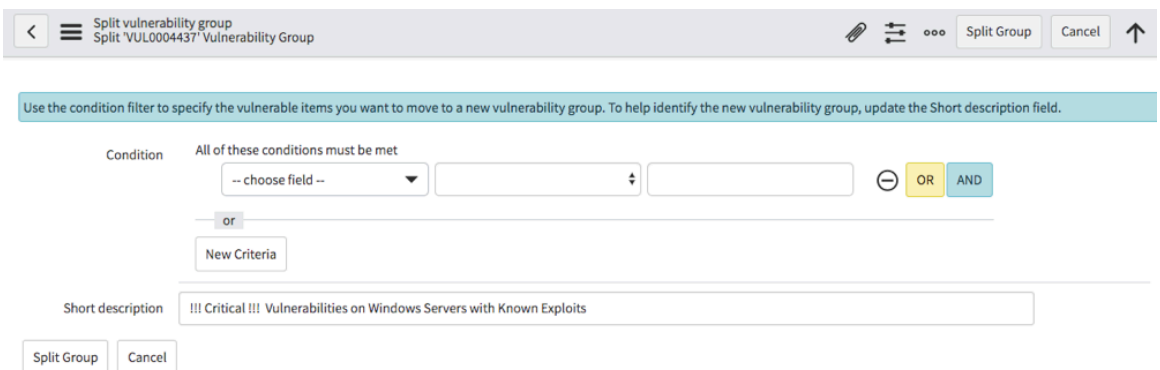
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho para dividir uma tarefa de correção



Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Tarefas de correção** > **Atribuído aos Meus grupos**.
   A lista de tarefas de correção é exibida.
2. Na coluna Número, clique em um registro para abri-lo.
   O registro é exibido.
3. No canto superior direito do VUL, clique em **Dividir tarefa**.
   O formulário Dividir tarefa de correção é exibido.



Tradução automática

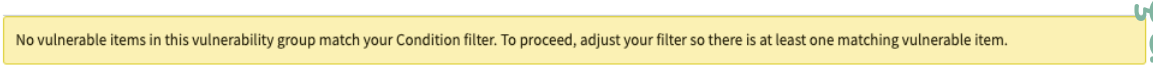
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Com o filtro de condição exibido, especifique as condições dos itens vulneráveis que você deseja mover para uma nova tarefa.
   Por exemplo, talvez você prefira filtrar somente itens vulneráveis que correspondam às seguintes condições:
   - Nos estados Aberto.
   - Pontuações de risco superiores a 80.
   - Itens de configuração que contêm "WINSV".
   - Localizado em San Diego.

   Por exemplo, para condições, você pode inserir:
   - Estado - é - Aberto
   - Pontuação de risco - é maior que ou é - 80
   - Item de configuração. Nome - contém - WINSV
   - Item de configuração. Local - é - San Diego

   Se os itens vulneráveis corresponderem ao seu filtro depois de inserir as condições, será exibida uma mensagem com o número de itens vulneráveis correspondentes.

   Nota:
   Se for exibida uma mensagem informando que nenhum item vulnerável corresponde ao seu filtro, ajuste as condições para que pelo menos um item vulnerável corresponda aos seus critérios de filtro.

5. **Opcional:** Ajuste o filtro conforme necessário.
6. **Opcional:** Para ajudá-lo a identificar o novo VUL depois que ele for criado, convém atualizar o campo Descrição resumida.
   Se editado, use o campo de descrição resumida como critério de pesquisa para o novo VUL para ajudá-lo a localizá-lo depois que ele for criado, por exemplo,LOCALIZADO EM SAN DIEGO.
7. **Opcional:** Para visualizar detalhes sobre os itens vulneráveis que correspondem aos seus critérios de filtro, siga estas etapas antes de clicar em **Dividir tarefa** para criar o novo VUL.
   Esses detalhes incluem solicitações de mudança existentes que já estão associadas a este subconjunto e VULs a esses itens vulneráveis. Exibir essas informações na visualização pode impedir a criação de VULs duplicados.

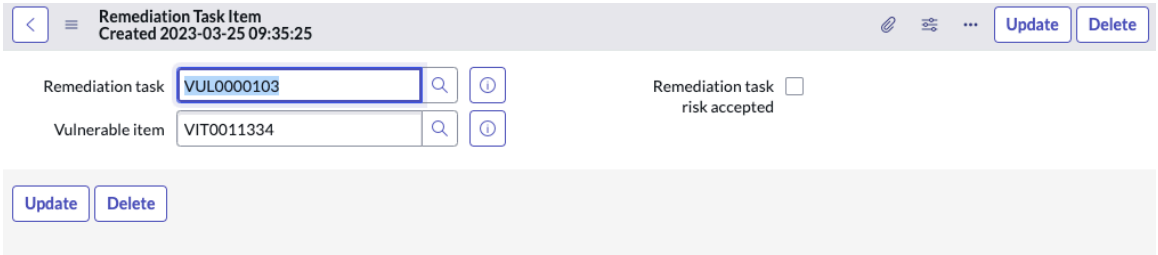
   a. Na mensagem de confirmação azul no formulário da tarefa de correção de divisão, clique em **Visualizar itens correspondentes**.
      A lista de itens da Tarefa de correção é exibida em uma nova janela no navegador com uma lista de itens vulneráveis que correspondem às suas condições.

   b. Na coluna Número, clique em um item para abrir o registro.

   c. No registro exibido, à direita do grupo de vulnerabilidades ou dos campos de item de vulnerabilidade, clique no ícone de informações do item vulnerável para exibir os registros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. Na caixa de diálogo exibida, clique em **Abrir registro**.
As informações sobre a data de destino da correção são exibidas. Na seção Listas relacionadas, clique em uma lista relacionada para exibir mais informações sobre o IV.

8. Quando estiver pronto para criar a nova VUL com os IVs que atendem às suas condições, feche a janela de visualização para retornar ao formulário de tarefa de divisão na outra janela e, na parte superior do formulário, clique em **Dividir tarefa**.

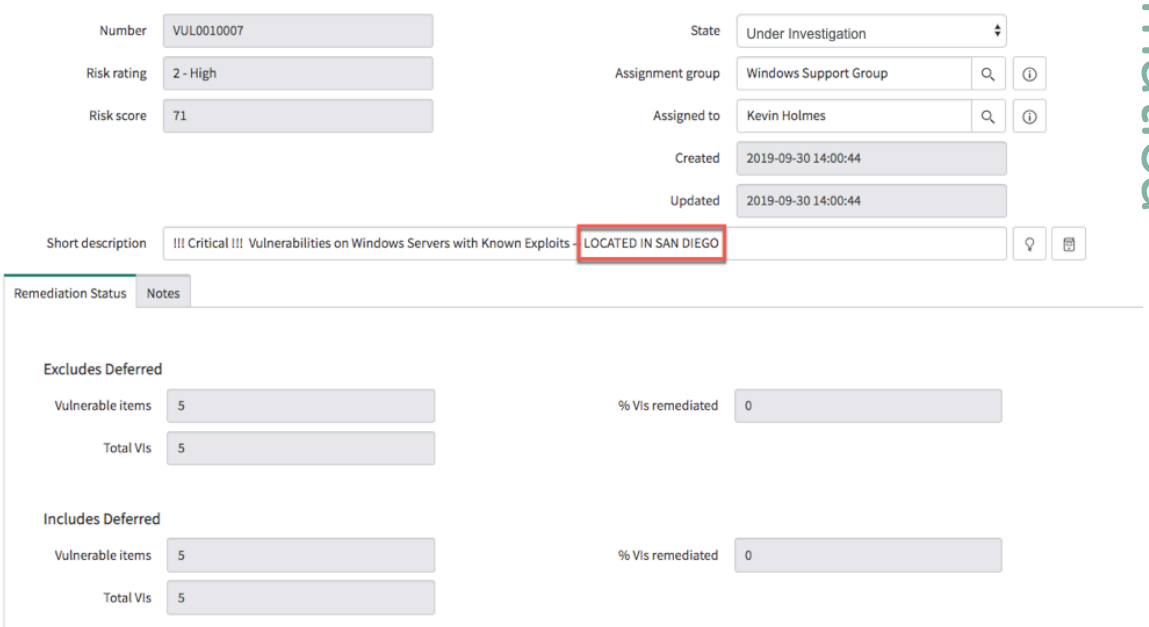
Nota:

Para menos de 200 IVs, a operação de divisão é feita de forma síncrona.

Para mais de 200 IVs, a operação de divisão é feita de forma assíncrona em segundo plano e pode levar alguns segundos para que os IVs apareçam no novo grupo.

Uma mensagem de confirmação é exibida e mostra todos os IVs ativos que foram movidos para o novo grupo. O novo número da tarefa de correção também é exibido. Se ainda não estiver em Sob investigação, o VUL será movido para Sob investigação. Verifique o campo Descrição resumida para o texto inserido para o novo VUL em (LOCALIZADO EM SAN DIEGO).

Os cálculos de acúmulo no novo grupo são realizados para calcular a nova Pontuação de risco, a Data de destino da correção e outros valores de campo.



Os itens vulneráveis, as soluções preferenciais e as solicitações de mudança são exibidos nas Listas relacionadas na parte inferior do registro. Processe e monitore esta nova tarefa como faria com qualquer tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

9. **Opcional:** Role até a lista relacionada **Anotações** e clique para selecioná-la.
   Confirme se o número de itens vulneráveis da tarefa de correção original foi movido para o novo grupo no fluxo de atividades.
10. **Opcional:** Na nova VUL, para selecionar e dividir os IVs da lista relacionada Itens vulneráveis mais uma vez, role até a parte inferior do registro do grupo de vulnerabilidades e, com os IVs que você deseja mover selecionados na coluna Item vulnerável dos Itens vulneráveis relacionados lista, na lista de seleção Ações nas linhas selecionadas, selecione **Dividir tarefa**.
    O formulário Dividir tarefa de correção é exibido.
11. Para dividir o grupo novamente e mover os itens selecionados para um novo grupo, clique em **Dividir tarefa**.
    Os IVs selecionados são movidos para outra tarefa de correção, a mensagem de confirmação é exibida e o novo grupo é exibido.
12. Escolha um para continuar sua investigação ou correção.

O que Fazer Depois

Monitore o estado da nova VUL para agilizar sua resolução.

Sincronização de estado entre solicitações de mudança e tarefas de correção

Há um relacionamento sincronizado entre os campos de estado das tarefas de correção (VULs) e os campos de estado das solicitações de mudança (CHG) no produto Vulnerability Response. Conforme uma solicitação de mudança passa por seu ciclo de vida, ela também muda o estado de todas as tarefas de correção relacionadas automaticamente.

Visão geral

O registro da tarefa de correção é conhecido como VUL nas seções a seguir. Em versões anteriores do Vulnerability Response, as tarefas de correção eram chamadas de grupos de vulnerabilidade (VG). Nas imagens a seguir, VG = tarefa de correção ou um registro VUL.

A sincronização de estado é habilitada por uma propriedade do sistema (sn_vul.cr_state_synch) por padrão em sua instância quando você baixa a aplicação Vulnerability Response.

Quando a sincronização de estado está habilitada, o campo Estado CHG muda o campo Estado da tarefa de correção automaticamente nos seguintes casos:

- Quando um novo CHG é criado para uma tarefa de correção (VUL), se não estiver em Aguardando implementação, o estado do VUL avança para Aguardando implementação.
- Quando um CHG existente é associado a uma VUL, se não estiver em Aguardando implementação, o estado da VUL avança para Aguardando implementação.
- Depois que as tarefas em um CHG são concluídas (Implementado) e o CHG é movido para o estado Revisar, a VUL avança para Resolvido.

Para obter mais informações e exemplos de sincronização de estado, consulte as seções a seguir.

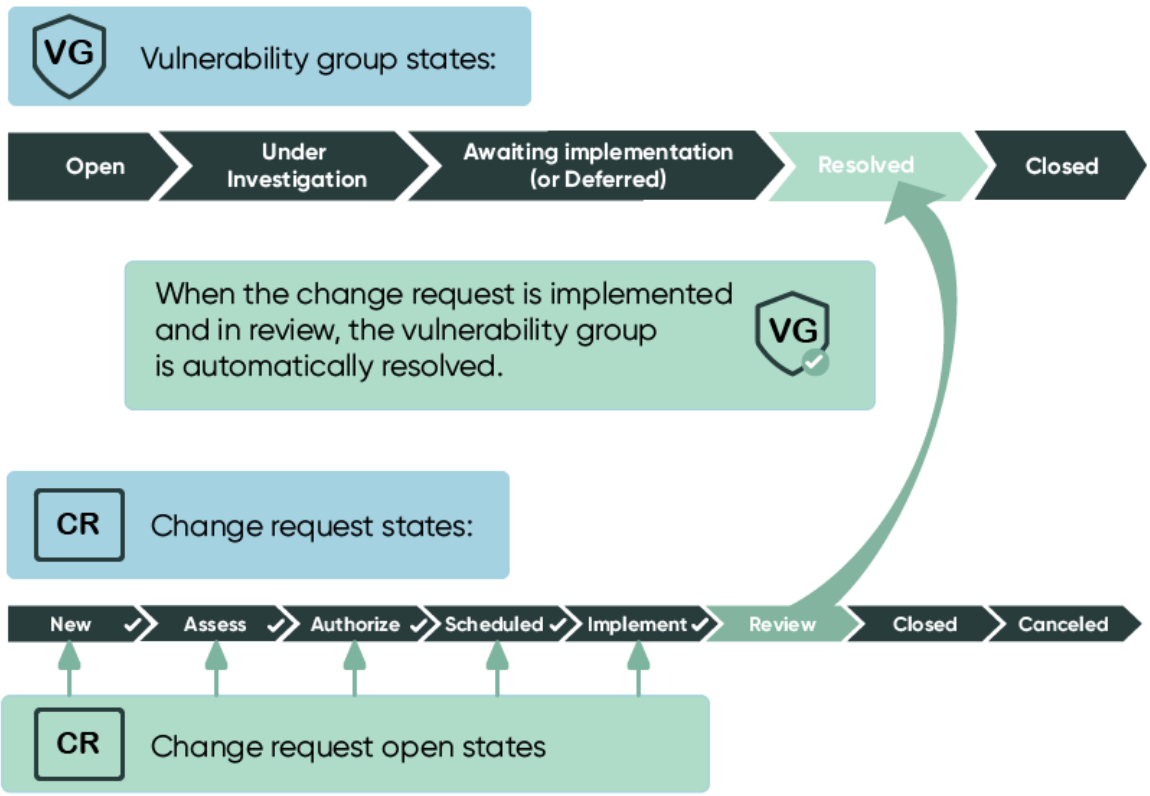
Nota:
Você ainda pode mover CHGs e VULs manualmente pelos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que um CHG mudou de estado, ou você adiciona um CHG ou o remove de um VUL, o estado A sincronização pode potencialmente substituir sua intervenção manual. No entanto, os estados das solicitações de mudança não movem automaticamente o VUL dos estados Encerrado ou Adiado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sincronização de estado de encaminhamento

A imagem a seguir ilustra como os estados CHG movem automaticamente os estados VUL em um ciclo de vida avançado, ou seja, de Aberto para Resolvido.



Você pode criar novas solicitações de mudança para qualquer tarefa de correção em um estado diferente de Encerrado. A sincronização de estado move automaticamente o VUL bidirecionalmente pelos estados Aberto, Sob investigação, Aguardando implementaçãoe Resolvido. Este movimento é baseado em determinados valores do campo de estado na solicitação de mudança. A sincronização de estado entre a solicitação de mudança e a tarefa de correção é invocada automaticamente, a menos que a caixa de seleção (Adicionar ICs ao CR) seja exibida em um formulário e você opte por desmarcar a caixa de seleção.

A VUL não avança para Resolvido quando um CHG está em seus estados abertos. Qualquer CHG em estados anteriores a Revisão em seu ciclo de vida, como Novo, Avaliar, Autorizar, Programado ou Implementar, conforme mostrado na figura anterior, são considerados estados abertos para o CHG. Estados abertos não movem o campo de estado no VUL, porque as investigações ou tarefas no CHG não são concluídas. A sincronização de estado é invocada quando um CHG é criado para, ou associado a, o VUL, ou o estado de um relacionamento existente muda no CHG. Os estados CHG concluídos são Revisão e Encerradocom sucesso. Quando um CHG é encerrado com sucesso, seus códigos encerrados são: Bem- sucedidoou Bem-sucedido com problemas. Nesse caso, o VUL avança para Resolvido.

Sincronização de estado para trás

Como um CHG é processado durante seu ciclo de vida, ele pode ser cancelado em algum momento. Nesse caso, se o CHG for Canceladoou Encerrado (com um código de encerramento Malsucedido), o VUL voltará automaticamente para Sob investigação. O VUL retorna para Sob investigaçãoporque não há nenhum plano ativo para corrigir a vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se uma VUL estiver em um estado Resolvido e você criar um novo CHG ou associá-lo a um CHG existente em um dos estados abertos iniciais, o VUL fará a transição automaticamente de volta para Aguardando implementação. O VUL retorna para este estado, pois agora há mais trabalho atribuído ao CHG.

VULs com mais de um CHG

Se uma VUL em Aguardando implementação tiver mais de um CHG associado a ela, a sincronização de estado será baseada no status do CHG no estado mais antigo de seu ciclo de vida. Por exemplo, uma VUL tem quatro CHGs associados a ela, CHG1, CHG2, CHG3 e CHG4, conforme mostrado na tabela a seguir.

Número CHG	Estado CHG
1	Implementar
2	Cancelado(a)
3	Encerrado (código de encerramento malsucedido)
4	Encerrado (código de encerramento bem- sucedido)

A sincronização de estado entre o CHG e o VUL, neste caso, é baseada no CHG1, que está no estado mais antigo dos quatro CHGs, (Implementar). Nesse caso, o VUL permanece em Aguardando implementação.

Em outro exemplo, se uma VUL estiver no estado Resolvido e tiver um CHG existente que foi implementado e está no estado Revisão, e um novo CHG for criado, o VUL voltará de Resolvido para Aguardando Implementação. A sincronização de estado é baseada no CHG no estado Novo, que é o CHG no estado mais antigo.

Número CHG	Estado CHG
1	Revisar
2	Novo

Além disso, quando as VULs têm mais de um CHG, o estado da VUL muda automaticamente nos seguintes casos:

- Quando um CHG avança para Revisão, se todos os outros CHGs associados ao VUL estiverem nos estados Revisão ou Encerrado (com um código de encerramento bem-sucedido), o VUL faz a transição automaticamente para Resolvido. Quaisquer outros CHGs relacionados que sejam cancelados ou encerrados sem sucesso serão ignorados.
- Quando um CHG é movido para Cancelado ouEncerrado (código de fechamento de Malsucedido), se todos os outros CHGs associados ao VUL estiverem no mesmo estado, o VUL fará a transição automaticamente de volta para Sob investigação .

Para obter mais informações sobre os estados da tarefa de correção e o que você pode fazer em cada estado, consulte Vulnerability Response tarefa de correção e estados de item vulnerável.

Avalie sua exposição a software vulnerável

Você pode fornecer as informações do fornecedor e do produto no módulo Avaliação de exposição para avaliar a exposição de dia zero (dia atual) de seus ativos a software vulnerável usando a aplicação Gestão de ativos de software ITSM.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Para obter mais informações sobre requisitos do sistema, consulte Configurar avaliação de exposição.

Exiba o módulo de avaliação de exposição de software e crie e edite registros de avaliação de exposição sob demanda para software vulnerável em sua instância Now Platform®.

Você gerencia as atividades de resposta de vulnerabilidade para uma grande operação responsável por muitos ativos. O Security Operations Center (SOC) em sua operação entra em contato com você sobre uma versão de software que eles aprenderam que é vulnerável. Você descobre que uma verificação de seus ativos foi concluída recentemente e não encontrou esta vulnerabilidade. A equipe de SOC descobriu esta vulnerabilidade por meio de uma fonte confiável fora do Banco de Dados de Vulnerabilidades Nacionais (NVD), Common Weakness Enumeration (CWE) ou de outras bibliotecas de terceiros em sua instância, e você acha que seu verificador de vulnerabilidades ainda não adicionou o plug-in para ele.

Você tem certeza de que os dados dessa vulnerabilidade serão atualizados no NVD e importados em breve para que o scanner possa detectá-la na próxima verificação. No entanto, como você está preocupado com o escopo de sua possível exposição, deseja determinar hoje se você tem ativos em sua rede que têm este software instalado.

Função necessária: administrador de vulnerabilidades (sn_vulnerability_write)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Tenha as seguintes informações disponíveis sobre o software vulnerável que você deseja avaliar:

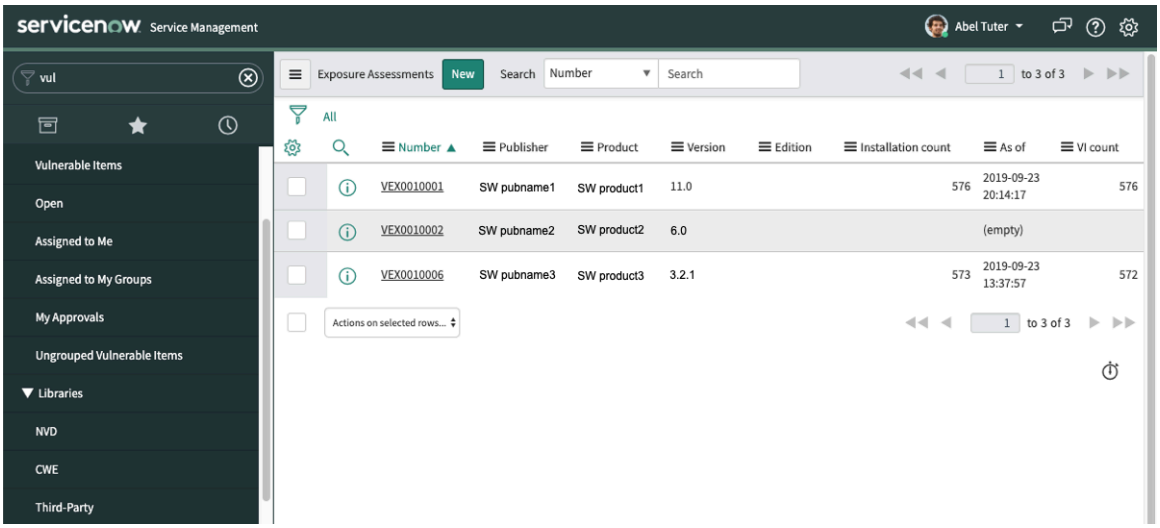
- Fornecedor
- Versão
- Produto
- Edição

Procedimento

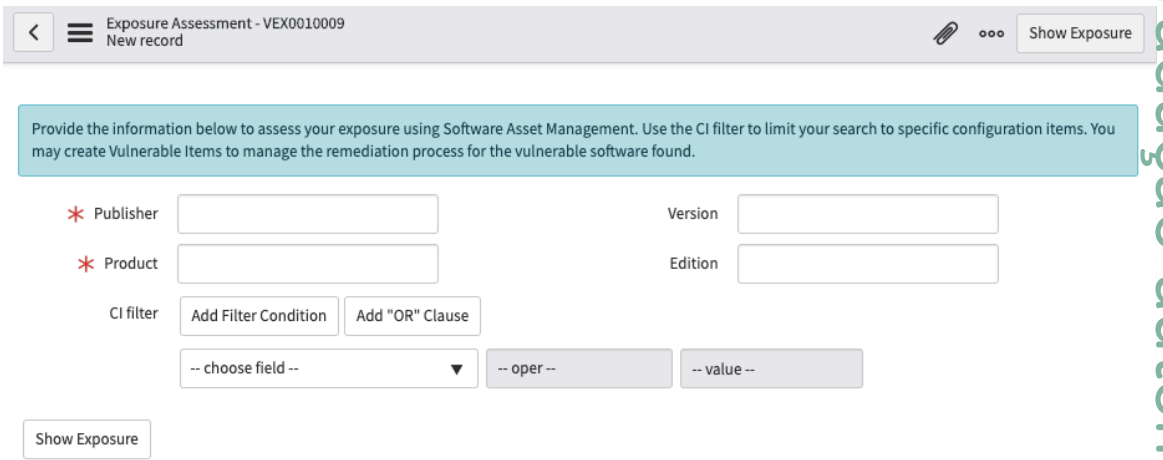
1. Para criar uma nova avaliação de exposição, navegue até **Todos** > **Vulnerability Response** > **Verificação de Vulnerabilidades** > **Avaliação de Exposição**.
   A lista Avaliações de exposição é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



2. Clique em **Nova**.
O formulário Avaliação de exposição é exibido.



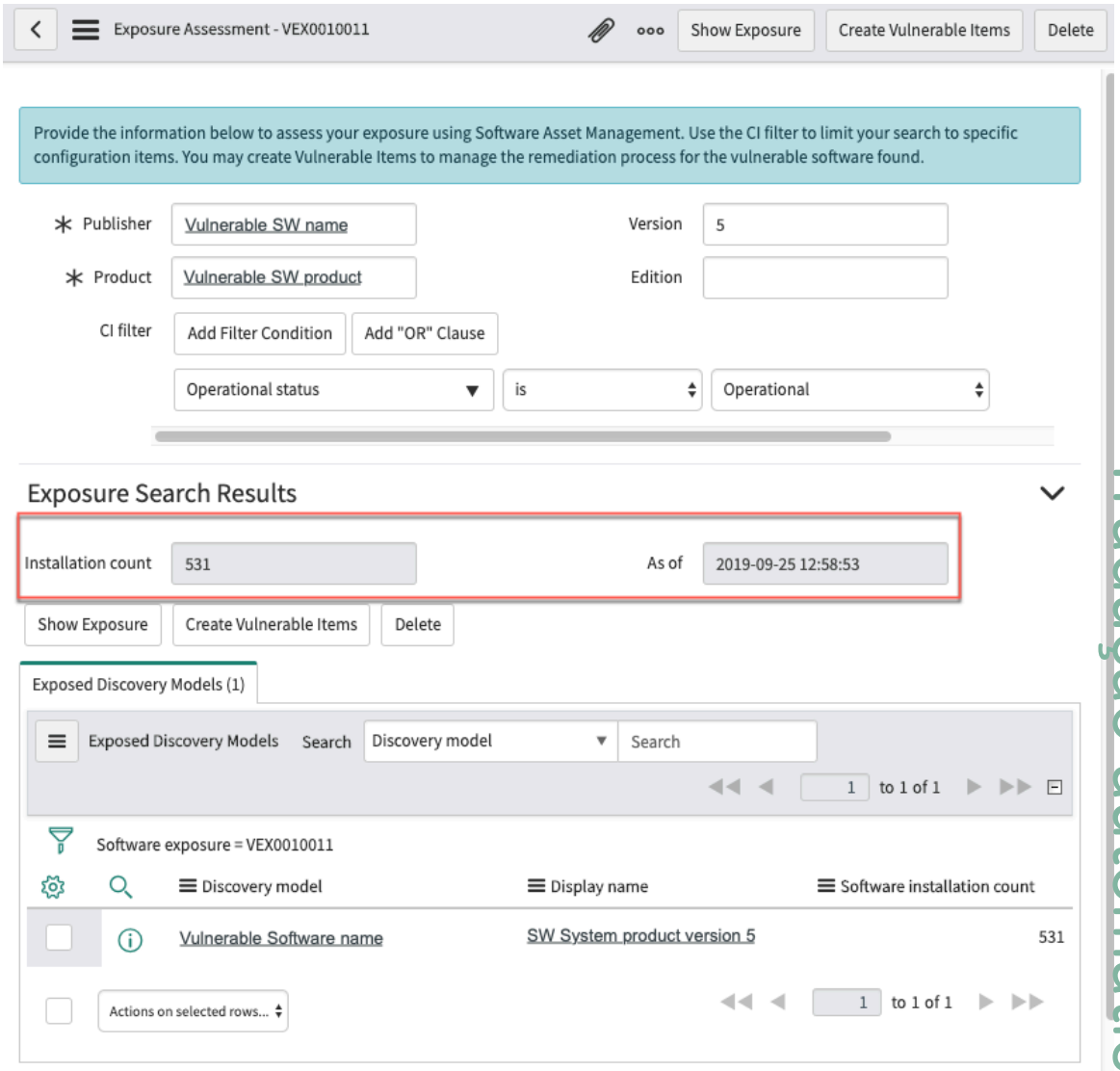
3. Preencha o formulário.

Campo	Descrição
Fornecedor	Nome do fornecedor do software.
(Opcional) Versão	Insira o número da versão para ajudar a restringir a pesquisa em seus ativos.
Produto	Nome do produto de software.
(Opcional) Edição	Insira a edição para ajudá-lo a restringir a pesquisa em seus ativos.
Filtro de IC	Use as listas de seleção do filtro Item de configuração (IC) para limitar sua pesquisa a itens de configuração específicos (ativos). Por exemplo, você pode enviar uma consulta somente para ativos ativos que podem ter este software instalado: `O status operacional é Operacional`

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique **em Mostrar exposição**.
   O registro de avaliação de exposição com seu modelo de descoberta e a contagem de instalação de software em seus ativos a partir da data específica é exibido.



5. Escolha um para continuar.

6. **Opcional:** Crie um item vulnerável para o resultado da pesquisa.

   Nota:
   Depois de criar itens vulneráveis, você não pode alterar os critérios de pesquisa para este registro de exposição.

7. Como alternativa, revise as condições do filtro e refine ainda mais os resultados da pesquisa.

8. Para criar itens vulneráveis, siga estas etapas:

   a. Clique **em Criar itens vulneráveis**.
      A caixa de diálogo Criar itens vulneráveis é exibida.

   b. Preencha os campos.

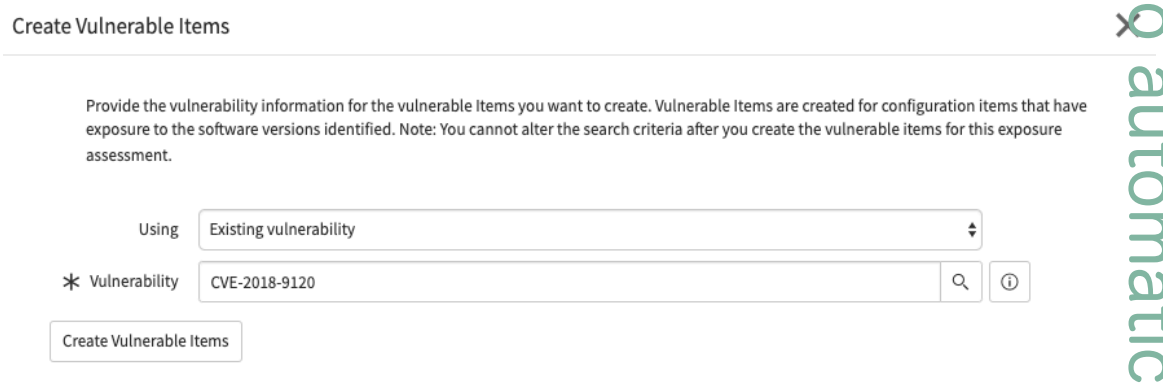
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

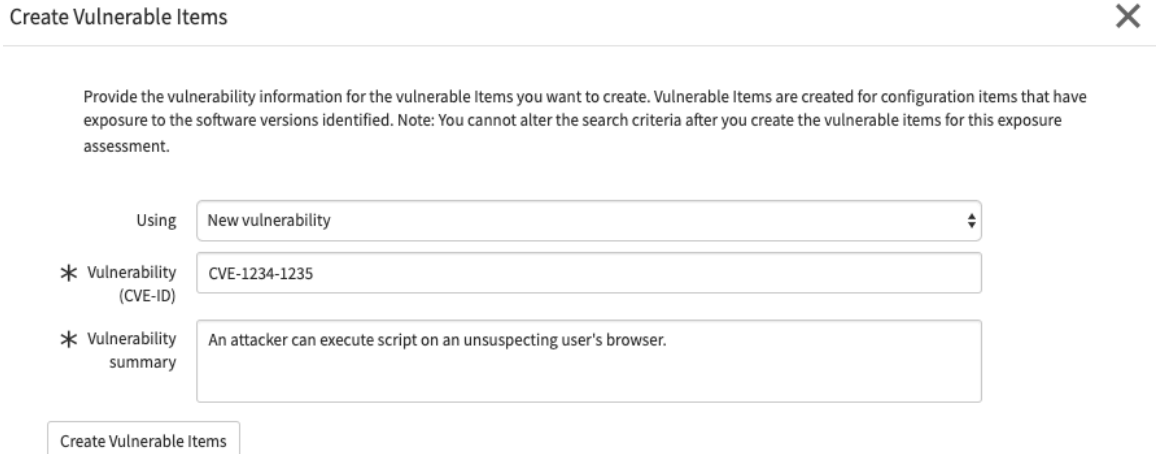
Campo	Descrição
Usando	Na lista de seleção, escolha um para continuar. ▪ **Vulnerabilidade existente**. À direita do campo Vulnerabilidade, clique no ícone de pesquisa. Na lista exibida, selecione o CVE-ID ou insira os critérios de pesquisa para localizar o CVE-ID existente, por exemplo, CVE 2018-9120. **Nota:** Pode ser um CVE-ID de um banco de dados de vulnerabilidades diferente do NVD. ▪ **Nova vulnerabilidade**. Insira o CVE-ID da sua nova vulnerabilidade no formato xxxx-xxxx, xxxx-xxxxx ou xxxx-xxxxxxx.
Resumo da vulnerabilidade (somente para nova vulnerabilidade)	Insira um resumo para a nova vulnerabilidade, por exemplo, Um invasor pode executar um script no navegador de um usuário desavisado.

As imagens a seguir mostram exemplos do formulário preenchido para uma vulnerabilidade existente e uma nova vulnerabilidade.

Vulnerabilidade Existente



Nova Vulnerabilidade



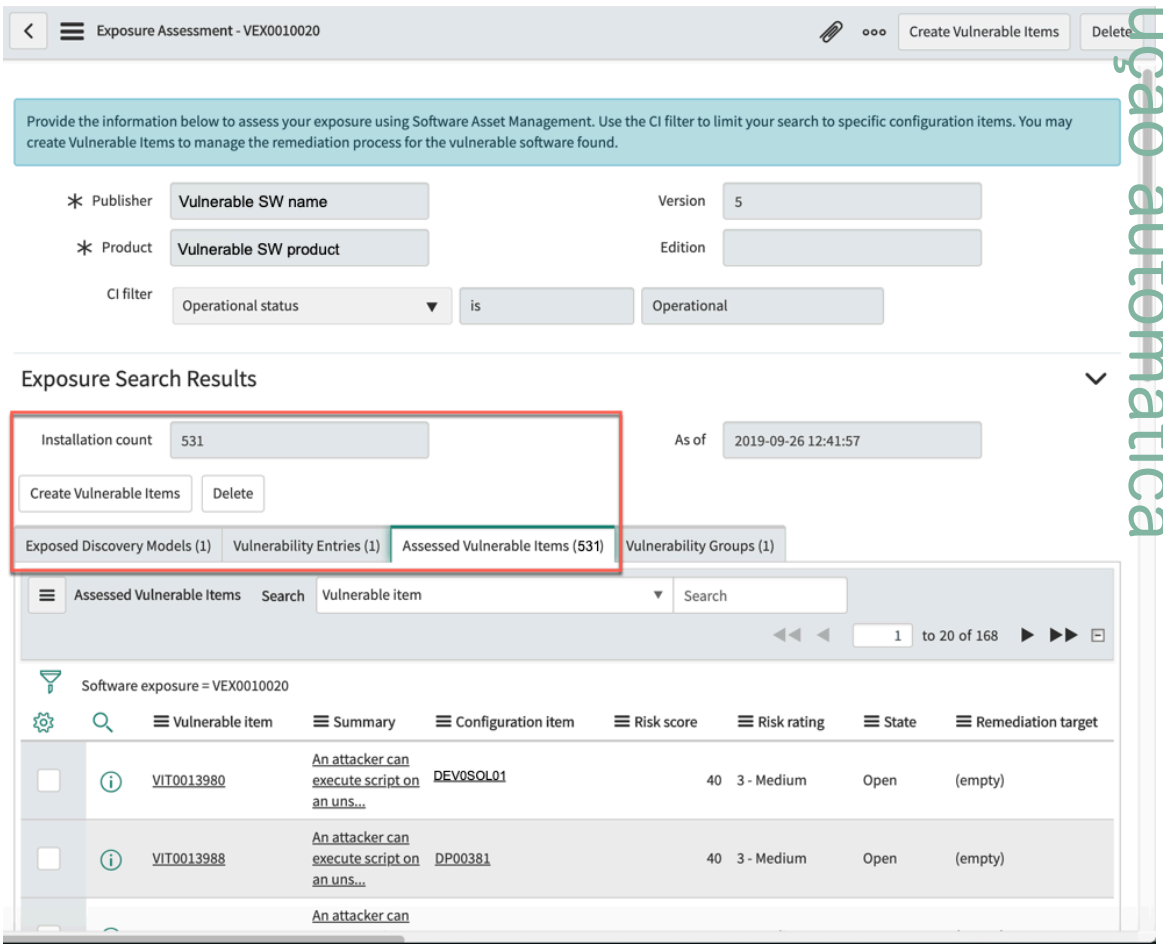
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Clique **em Criar itens vulneráveis**.
O registro de avaliação de exposição é exibido com uma mensagem de status que indica que os itens vulneráveis estão sendo criados.

d. Após alguns segundos, na parte superior do formulário, clique com o botão direito do mouse na faixa cinza para recarregar a página.
Os novos itens vulneráveis são exibidos conforme mostrado na figura a seguir na guia Itens vulneráveis avaliados (531). A nova tarefa de correção criada para esses itens vulneráveis é exibida na guia de tarefa de correção (1).

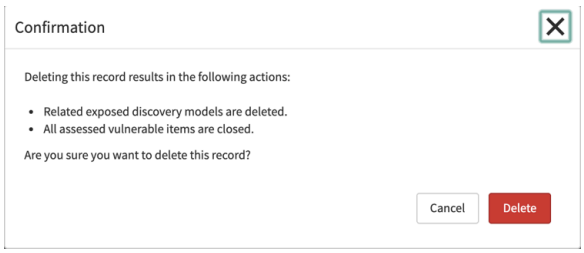
Nota:
Para este exemplo, uma tarefa de correção é criada de acordo com as regras e condições do grupo da regra de tarefa de correção chamada Vulnerabilidade. Esta regra de grupo é a regra de tarefa de correção padrão que é instalada com o produto Vulnerability Response na sua instância Now Platform®. Neste exemplo, as condições desta regra de grupo colocaram todos os itens vulneráveis em uma única tarefa de correção. Se você preferir criar mais de uma tarefa de correção para os itens vulneráveis que correspondem aos resultados da pesquisa de avaliação de exposição, talvez prefira configurar regras de tarefa de correção adicionais. Criar mais tarefas de correção pode ajudar a evitar a criação de tarefas de correção com um grande número de itens vulneráveis. Para obter mais informações sobre regras de tarefa de correção, consulte Vulnerability Response tarefas de correção e regras de tarefa visão geral e Criar ou editar Vulnerability Response regras de tarefa de correção.



9. Escolha um para continuar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Tarefas de correção	Com a guia Tarefas de correção selecionada, na coluna numérica, clique para abrir o registro e revisar e atribuir a tarefa de correção. Para obter mais informações sobre grupos de atribuição, consulte Creating groups .
Itens de vulnerabilidade avaliados	Com a guia Itens vulneráveis avaliados selecionada, na coluna Item vulnerável, clique para abrir os registros e revisar e atribuir itens vulneráveis individuais.
Excluir	Exclua o registro de avaliação de exposição. Uma caixa de diálogo de confirmação é exibida. **Nota:** Se você excluir o registro de exposição depois de criar itens de vulnerabilidade, todos os itens vulneráveis que você criar para este registro que não estejam relacionados a outro registro de exposição serão movidos automaticamente para o estado Encerrado. O motivo do fechamento é Cancelado.
	

O que Fazer Depois

Responda a quaisquer ameaças de dia zero (dia atual) com base em sua avaliação de exposição. Para obter mais informações sobre tarefas de correção e gerenciamento de mudanças para Vulnerability Response, consulte Vulnerability Response tarefas de correção e regras de tarefa visão geral e Change Management para Vulnerability Response.

Exibição de recomendações de atribuição

Um grupo de atribuição geralmente é alocado a um item vulnerável usando regras de atribuição. Essas regras são configuradas pelo administrador de vulnerabilidades para alocar os grupos de atribuição corretos que são baseados nos dados recebidos de scanners de terceiros.

Para obter mais informações, consulte Vulnerability Response visão geral de regras de atribuição. Se um grupo de atribuição correspondente não estiver disponível ou estiver incorreto, você poderá usar Recomendações de atribuição de vulnerabilidade para exibir grupos de atribuição alternativos.

Use Recomendações de atribuição de vulnerabilidade para fazer as seguintes ações:

- Solicitar recomendações do grupo de atribuição para um item vulnerável.
- Solicitar recomendações do grupo de atribuição para vários itens vulneráveis.
- Solicitar recomendações do grupo de atribuição para uma tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitar recomendações do grupo de atribuição para um item vulnerável

Solicite Recomendações de atribuição de vulnerabilidade para que você possa exibir as recomendações do grupo de atribuição. Você pode solicitar recomendações se um grupo de atribuição correspondente não estiver disponível ou estiver incorreto para um item vulnerável (IV).

Antes de Iniciar

Função necessária: sn_vul.remediation_owner

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Itens vulneráveis** e abrir um IV.
   O item deve estar no estado Aberto, Adiado, Sob investigação ou Aguardando implementação.
2. Clique no ícone de recomendação (ícone de) ao lado do campo **Grupo** de atribuição para obter sugestões de atribuição para esse IV.
3. Na caixa de diálogo Recomendações de grupo de atribuição, selecione uma recomendação baseada na pontuação de confiança.
   A pontuação de confiança prevê a relevância da correspondência para o IV. Para obter mais informações, consulte Soluções de aprendizado de máquina para Vulnerability Response.
4. Clique **em Atribuir**.

Resultado

O grupo selecionado aparece no campo **Grupo de atribuição** e o tipo de atribuição muda para Recomendação.

Solicitar recomendações do grupo de atribuição para vários itens vulneráveis

Use Recomendações de atribuição de vulnerabilidade para exibir as recomendações do grupo de atribuição para vários itens vulneráveis (IVs) usando uma edição em massa. Quando vários IVs são selecionados, uma previsão é realizada em uma amostra aleatória dos IVs selecionados.

Antes de Iniciar

Função necessária: sn_vul.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa

As recomendações e suas pontuações de confiança podem diferir um pouco entre as invocações, com base nas amostras obtidas dos IVs selecionados. A pontuação de confiança avalia se o sistema está confiante de que o grupo de atribuição recomendado é adequado para resolver a vulnerabilidade. Use a propriedade do sistema `assignment_recommendation_batchsize` para definir o tamanho do lote ao solicitar Recomendações de atribuição de vulnerabilidade para tarefas de correção (VULs) e IVs usando a opção de edição em massa. O valor padrão desta propriedade do sistema é definido para um desempenho de previsão ideal.

Nota:
Se você aumentar o valor padrão, o tempo de resposta para Recomendações de atribuição de vulnerabilidade nesses casos poderá mudar.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Item Vulnerável** e selecione vários IVs.
   Os itens devem estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. Clique **em Edição em massa**.
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de itens vulneráveis em massa

Campo	Descrição
Seleção de registro	Registros a serem selecionados para edição em massa.
Grupo de atribuição	Grupo de atribuição a ser definido para os itens vulneráveis selecionados. Para exibir os grupos de atribuição recomendados, clique no ícone de recomendação (ícone de) ao lado do campo. Selecione uma recomendação baseada na pontuação de confiança e clique em **Atribuir**.
Anotações de trabalho	Anotações a serem adicionadas.

4. Clique em **OK**.

Resultado

O grupo selecionado aparece no campo **Grupo de atribuição** e o tipo de atribuição muda para Recomendação para todos os IVs selecionados.

Solicitar recomendações do grupo de atribuição para uma tarefa de correção

Use Recomendações de atribuição de vulnerabilidade para exibir recomendações de grupo de atribuição para uma tarefa de correção (VUL).

Antes de Iniciar

Função necessária: sn_vul.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa

Use a propriedade do sistema `assignment_recommendation_batchsize` para definir o tamanho do lote ao solicitar Recomendações de atribuição de vulnerabilidade para VULs e itens vulneráveis (IVs) usando a opção de edição em massa. O valor padrão desta propriedade do sistema é definido para um desempenho de previsão ideal.

Nota:
Se você aumentar o valor padrão, o tempo de resposta para Recomendações de atribuição de vulnerabilidade nesses casos poderá mudar.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Tarefas de correção** e selecione uma VUL.
   O grupo deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. Clique no ícone de recomendação (ícone de) ao lado do campo **Grupo** de atribuição para as recomendações do grupo de atribuição da VUL selecionada.
   A caixa de diálogo Recomendações de grupo de atribuição exibe os grupos de atribuição recomendados com a pontuação de confiança média para todos os IVs nesse grupo.
3. Selecione uma recomendação na lista Grupo de atribuição com base na pontuação de confiança.
   A pontuação de confiança prevê a relevância da correspondência para o VUL selecionado.
4. Clique **em Atribuir**.
   O grupo selecionado aparece no campo **Grupo de atribuição**.
5. Salve a tarefa de correção com as informações atualizadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado
Todos os IVs com o mesmo grupo de atribuição que o VUL são atribuídos ao grupo de atribuição selecionado. O tipo de atribuição muda para Recomendação para o VUL, bem como todos os IVs modificados.

Solicitação e aprovação de uma exceção

Você pode solicitar o adiamento da correção de um item vulnerável ou tarefa de correção por um período especificado. Por exemplo, como proprietário de correção, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina. Os aprovadores que têm acesso podem aprovar solicitações de outros usuários.

Você pode solicitar exceções nos espaços Vulnerability Response. Consulte Solicitar uma exceção no Espaço de correção de problemas de TI.

- Solicitar uma exceção para um item vulnerável
- Solicitar uma exceção para uma tarefa de correção
- Solicitar uma exceção em massa

Você também pode solicitar exceções de política usando GRC: Policy and Compliance Management:

- Solicitar uma exceção usando GRC: Policy and Compliance Management
- Solicitar uma exceção em massa usando GRC: Policy and Compliance Management

Nota:

Notificações por e-mail são enviadas em todas as fases do gerenciamento de exceções, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma exceção é solicitada, o solicitante recebe um e-mail confirmando que a solicitação foi gerada. O aprovador também recebe um e-mail informando que uma exceção foi solicitada.

A partir da v21.0 de Vulnerability Response, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Solicitar uma exceção para um item vulnerável

Solicite uma exceção para um item vulnerável (IV) que não possa ser corrigido imediatamente. Por exemplo, como proprietário de correção, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Antes de Iniciar
Função necessária: sn_vul.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa
Você pode solicitar exceções nos espaços Vulnerability Response. Consulte Solicitar uma exceção no Espaço de correção de problemas de TI.

Você também pode solicitar exceções para IVs no ambiente clássico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

A partir da v21.0 de Vulnerability Response, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Vulnerability Response** > **Itens vulneráveis** > **Todos**.
2. Selecione o item para o qual você deseja solicitar uma exceção.
   O item selecionado deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
3. No formulário Item vulnerável, clique em **Solicitar exceção**.
4. Se Vulnerability Response for selecionado na tela Gestão de exceções, preencha os campos no formulário Solicitar exceção.

Formulário de Exceção de solicitação

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração selecionada no **Todos** > **Vulnerability Response** > **Administração** > **Gestão de exceção** tela. Quando a solicitação de exceção expira, o grupo é revertido para o estado Aberto. **Nota:** A partir da versão 18.0 do Vulnerability Response (VR), se um item vulnerável foi adiado para correção usando o recurso de gestão de exceções, caso ele seja reaberto pelo scanner, a data de adiamento definida na vulnerabilidade ainda persistirá. Para habilitar esta funcionalidade, defina o valor da propriedade do sistema `sn_vul.auto_defer_vit_in_active_exception_win` como verdadeiro. Além disso, a data adiada **até** persiste mesmo depois que o item vulnerável é encerrado ou a exceção expira. A função necessária é sn_vul.manage_exception_configuration para leitura e gravação.
Motivo	Motivo da solicitação. As opções são: ○ Risco aceito ○ Aguardando janela de manutenção ○ Correção indisponível

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Redução do controle no local ○ Outro Para ver como adicionar novas opções de motivo, consulte Definir mapeamento do motivo da política.
Informações adicionais	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo obrigatório deve ser atualizado pelo responsável pela correção.

5. Envie a solicitação de exceção clicando em **Solicitar aprovação**.

Resultado

O estado do item vulnerável muda para Em revisão. Use a guia **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

Solicitar uma exceção para uma tarefa de correção

Solicite uma exceção para adiar uma tarefa de correção por um período especificado se ela não puder ser resolvida imediatamente.

Antes de Iniciar

Você pode solicitar exceções nos espaços Vulnerability Response. Consulte Solicitar uma exceção no Espaço de correção de problemas de TI.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Função necessária: sn_vul.remediation_owner

Você também pode solicitar exceções para tarefas de correção no ambiente clássico.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Tarefas de correção** > **Todos**.
2. Selecione o grupo para o qual você deseja solicitar uma exceção.
   A tarefa selecionada deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
3. No registro da tarefa de correção (VUL), selecione **Solicitar exceção**.
4. No formulário, preencha os campos.

Formulário de Exceção de solicitação

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração da exceção definida na configuração.
Motivo	Justificativa para solicitar uma exceção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Informações adicionais	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

5. Clique em **Solicitar Aprovação**.

Solicitar uma exceção em massa

Use a opção de edição em massa para solicitar uma exceção para vários itens vulneráveis (IVs) em vez de selecionar cada item manualmente.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_analyst

Você pode solicitar exceções nos espaços Vulnerability Response. Consulte Solicitar uma exceção no Espaço de correção de problemas de TI.

Por Que e Quando Desempenhar Esta Tarefa

Quando vários IVs são selecionados, uma tarefa de correção (VUL) é formada com esses itens. Consulte Editar itens vulneráveis em massa no Vulnerability Response para obter mais informações sobre como editar vários IVs.

Procedimento

1. Navegar até **Vulnerability Response** > **Itens vulneráveis** > **Todos** e selecione os itens para os quais você deseja solicitar uma exceção.
   Os itens selecionados devem estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. Clique **em Edição em massa**.
3. No formulário, preencha os campos.

Formulário de edição em massa de item vulnerável

Campo	Descrição
Seleção de registro	Registros que você selecionou para uma edição em massa.
Estado	Estado do item vulnerável. Selecione o estado Adiado para solicitar uma exceção para os itens selecionados.
Motivo	Subestado para o Estado que você selecionou.
Descrição resumida	Nome da tarefa de correção que você está criando.
Até	Data de término que você especificar para sua solicitação de exceção.
Informações adicionais	Detalhes adicionais que você deseja mencionar para informar o aprovador sobre os motivos da sua solicitação.
Solução preferencial	Solução que é direcionada para corrigir todos os itens vulneráveis que você selecionou para uma edição em massa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Grupo de atribuição	Grupo de atribuição para o IV. Você pode selecionar um grupo manualmente ou usar Recomendações de atribuição se esse recurso estiver habilitado.
Anotações de trabalho	Anotações a serem adicionadas.

4. Clique em **OK**.
   Uma tarefa de correção é criada contendo os IVs que você selecionou. Esta tarefa de correção é enviada para aprovação.

Solicitar uma exceção usando GRC: Policy and Compliance Management

Solicite exceções de política usando o recurso de gestão de exceções de política GRCPolicy and Compliance Management na aplicação [] de dentro de Vulnerability Response.

Antes de Iniciar

Antes de usar a integração de exceção de política para solicitar exceções de política, você deve baixar a aplicação GRC: Policy and Compliance Management do ServiceNow Store.

Função necessária: sn_vul.remediation_owner

Você também pode solicitar exceções na IU clássica:

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Itens vulneráveis** (ou **Tarefas**de correção)>**Todos**e abra o item ou grupo para o qual você deseja solicitar uma exceção.
   O item ou grupo selecionado deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. No formulário selecionado, clique em **Solicitar exceção**.
3. No formulário, preencha os campos.

Formulário de Exceção de solicitação

Campo	Descrição
Política	Política de gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válido de	Data em que a exceção será iniciada. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até	Data em que a exceção de política expira e o estado do item ou grupo vulnerável muda de Adiado para Aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: O número de dias em que a exceção de política é válida não pode exceder a **Duração máxima da exceção (dias)** que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Criar uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo obrigatório deve ser preenchido pelo responsável pela correção.

4. Clique em **Enviar**.
   Para obter mais informações sobre a integração de exceção de política e a transferência entre o proprietário de correção e o gerente de conformidade, consulte Configuração opcional do Policy and Compliance Management .

Solicitar uma exceção em massa usando GRC: Policy and Compliance Management

Selecione um grupo de itens vulneráveis e envie uma exceção em massa.

Antes de Iniciar

Antes de usar a integração de exceção de política para solicitar exceções em massa, você deve baixar a aplicação GRC: Policy and Compliance Management do ServiceNow Store.

Nota:
Para usar este recurso, você deve atualizar o GRC: Policy and Compliance Management antes de atualizar o Vulnerability Response. Se você já atualizou Vulnerability Response antes de GRC: Policy and Compliance Managemente deseja usar este recurso, execute os procedimentos de atualização novamente na ordem correta.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Função necessária: sn_vul.remediation_owner

Você também pode solicitar exceções no ambiente clássico em Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Itens vulneráveis** > **Todos** e selecione os itens para os quais você deseja solicitar uma exceção.
   Os itens selecionados devem estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. Clique **em Edição em massa**.
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de edição em massa de item vulnerável

Campo	Descrição
Seleção de registro	Registros que você selecionou para uma edição em massa.
Estado	Estado do item vulnerável. Selecione o estado Adiado para solicitar uma exceção para os itens selecionados.
Descrição resumida	Nome da tarefa que você está criando.
Solução preferencial	Solução que você está direcionando para corrigir todos os itens vulneráveis selecionados para edição em massa.
Grupo de atribuição	Grupo de atribuição para o IV. Você pode selecionar um grupo manualmente ou usar Recomendações de atribuição se esse recurso estiver habilitado.
Anotações de trabalho	Anotações a serem adicionadas.

4. Clique em **OK**.
   Uma tarefa de correção é criada com os itens vulneráveis selecionados.
5. No formulário, preencha os campos.

Formulário de Exceção de solicitação

Campo	Descrição
Política	Política de gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle que estão associados à política que você selecionou. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válido de	Data em que a exceção será iniciada. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até	Data em que a exceção de política expira e o estado do item ou grupo vulnerável muda de Adiado para Aberto. **Nota:** O número de dias em que a exceção de política é válida não pode exceder a **Duração máxima da exceção (dias)** que você definiu para a política em GRC: Policy and Compliance Management. Para obter mais informações, consulte Criar uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo obrigatório deve ser preenchido pelo responsável pela correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Enviar**.
   Para obter mais informações sobre a integração de exceção de política e a transferência entre o proprietário de correção e o gerente de conformidade, consulte Configuração opcional do Policy and Compliance Management .

Aprovar uma solicitação de exceção no Vulnerability Response

Aprove solicitações de exceção para itens vulneráveis ou tarefas de correção que não possam ser corrigidas imediatamente. Você deve avaliar essas solicitações quanto ao risco e aprová-las para adiamento até que possam ser corrigidas.

Antes de Iniciar

Você pode aprovar solicitações de exceção e falso-positivo no espaço Vulnerability Response. Consulte Aprovar solicitações no Vulnerability Manager Workspace.

Função necessária: sn_vul.exception_approver

Você também pode aprovar solicitações de exceção no ambiente clássico.

Nota:

A partir da v21.0 de Vulnerability Response, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprove ou rejeite a solicitação com os comentários apropriados.

Trabalhando com uma regra de exceção

Você pode solicitar uma exceção para vulnerabilidades, itens vulneráveis (IVs) ou itens de configuração (ICs) que não podem ser corrigidos ou adiados imediatamente. Ao automatizar o processo de adiamento de IV, você pode adiar os IVs correspondentes com base na regra quando o sistema os identifica.

Você pode executar as seguintes tarefas para uma regra de exceção:

- Criar uma regra de exceção
- Aprovar uma solicitação de regra de exceção
- Ativação de uma regra de exceção
- Reabrir uma regra de exceção
- Atualizar uma regra de exceção aprovada
- Excluir uma regra de exceção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

A partir da v21.0 de Vulnerability Response, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Criar uma regra de exceção

Crie uma regra para solicitar automaticamente uma exceção para uma condição específica de um grupo de itens vulneráveis (IVs), como uma regra com uma condição que se baseia na severidade da vulnerabilidade desses IVs. Com esta regra, você pode adiar IVs novos e existentes automaticamente se eles corresponderem à condição de regra aprovada.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

A regra é aplicada da data "Válido a partir de" até a data "Válido até". A tarefa de correção (VUL) é criada quando a regra é aprovada. O método de agrupamento para este VUL é conhecido como regras de exceção. O VUL é criado no estado Adiado. Você não pode fechar, reabrir ou excluir este VUL. IVs novos e reabertos são adiados e adicionados a este VUL a partir da data "Válido a partir de" até o grupo expirar na data "Válido até".

Nota:

As notificações por e-mail são enviadas em todas as fases do fluxo de trabalho da regra de exceção. Esses e-mails fornecem o status e outros detalhes de uma solicitação. Por exemplo, quando uma regra de exceção é solicitada, o solicitante recebe um e-mail que confirma que a solicitação foi enviada.

Nota:

Se a regra for rejeitada, você poderá reabri-la no estado Rascunho, atualizá-la e reenviá-la para aprovação.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de exceção**.
2. Na página de novo registro da regra de exceção, clique em **Novo** para criar uma regra.
3. No formulário, preencha os campos.

Formulário Regra de exceção

Campo	Descrição
Nome	Nome da regra de exceção.
Válido de	Data a partir da qual esta regra está ativa para adiar os IVs.
Válido até	Data a partir da qual a tarefa de correção para de aceitar novos IVs.
Motivo	Motivo para criar esta regra de exceção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Grupo de atribuição	Grupo ao qual a tarefa de correção criada para rastrear os IVs adiados é atribuída.
Informações adicionais	Informações adicionais que o solicitante deseja fornecer ao aprovador. Essas informações são preenchidas no campo de descrição da tarefa de correção.
Condição	Condição de filtro para os IVs que podem ser definidos durante o processamento dos IVs.
Executar em dados existentes	Opção que permite executar esta regra em dados existentes na primeira vez em que esta regra é executada.
Fase do fluxo de trabalho	Status de aprovação atual da regra de exceção.
Estado	Estado da regra de exceção.
Ordem de execução	Ordem exclusiva para cada regra de exceção.
Adiado até	Data até quando as VULs e IVs são adiadas. Nesta data, a VUL criada é fechada, todos os IVs são movidos para fora do grupo e as regras do grupo são reaplicadas.

4. Adicione o grupo de atribuição ao criar a regra.
5. Envie o formulário para aprovação.
   O status da solicitação muda para Em revisão. Até que você envie a regra de exceção, ela permanecerá no estado Rascunho.

Aprovar uma solicitação de regra de exceção

Avalie as solicitações de regra de exceção dos usuários para que você possa aprovar ou rejeitar essas solicitações.

Antes de Iniciar

Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa

Os membros do grupo de usuários de nível 1 do aprovador de exceções podem aprovar as solicitações de regra de exceção de nível 1. Da mesma forma, os membros do grupo de usuários de nível 2 do aprovador de exceções podem aprovar as solicitações de regra de exceção de nível 2. Ambos os grupos de usuários herdam a função de aprovador de exceção por padrão.

Nota:

Se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Aprove ou rejeite a solicitação com e explique por que você aprovou ou rejeitou a solicitação.
   Depois que uma regra de exceção é aprovada, uma tarefa de correção (RT) é criada no estado Adiado por padrão. A partir da data "Válido a partir de", esta regra é executada em todos os IVs criados e também nos que são movidos do estado Encerrado para Aberto. Os IVs que correspondem às condições definidas são adicionados ao RT e adiados pelo período especificado.

   Nota:
   Se a regra for rejeitada, você poderá reabri-la no estado Rascunho, atualizá-la e reenviá-la para aprovação.

Ativação de uma regra de exceção

Uma regra é ativada na data "Válido a partir de". Após a ativação, ele automatiza o processo de exceção para itens vulneráveis (IVs).

A regra de exceção segue este ciclo de vida:

1. Os novos itens vulneráveis (IVs) que você cria ou reabre e que atendem à condição especificada são adiados. Se você habilitar a opção Executar nos dados existentes ao executar a regra de exceção pela primeira vez, todos os IVs ativos e não adiados que correspondem à condição da regra de exceção serão movidos para a tarefa de correção (RT) recém-criada e seu estado será alterado para Adiado.
2. Se um IV recém-criado corresponder à condição de regra de exceção, ele será movido para o RT adiado que está associado à regra e a regra de grupo não será executada nele.
3. Na data "Válido a partir de", os IVs existentes serão adicionados se você habilitar a opção Executar nos dados existentes.
4. O RT para de aceitar novos IVs quando a regra expira na data "Válido até". O RT permanece até a data "Adiado até".
5. A regra de exceção expira na data "Válido até".

Solicitar uma extensão para uma regra de exceção

Solicite uma extensão para uma regra de exceção adiada antes que ela atinja o adiado até a data de vencimento. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar
Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa
Você também pode solicitar uma extensão nos espaços Vulnerability Response. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no Espaço do gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Regras de exceção**.
2. Selecione uma regra de exceção aprovada.
3. Selecione **Solicitar extensão**.
4. Preencha os campos no formulário, conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Prorrogar até	Selecione a data até quando a regra de exceção deve ser estendida.
Motivo	Insira o motivo para adiar a regra de exceção. As opções incluem: ○ Risco aceito ○ Aguardando janela de manutenção ○ Correção indisponível ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Na aprovação da solicitação, os campos Adiado até, Motivo e Informações adicionais são atualizados na regra de exceção e nas tarefas de correção e itens vulneráveis associados. Um e-mail também é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.
- A partir da v21.0 de Vulnerability Response, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Reabrir uma regra de exceção

Reabra uma regra de exceção que foi rejeitada, mas você deseja reenviar. Reabrir a regra a move para o estado Rascunho.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode atualizar e reenviar a regra para aprovação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de exceção**.
2. Encontre a regra que você deseja reabrir e clique em **Reabrir**.
3. Atualize o formulário e reenvie-o para aprovação.

Atualizar uma regra de exceção aprovada

Cancele uma regra aprovada para poder atualizá-la. Por exemplo, antes de modificar datas ou adicionar uma condição a uma regra aprovada, você deve cancelá-la para que a tarefa de correção (VUL) seja excluída e os itens vulneráveis (IVs) sejam movidos para o estado Aberto.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

As regras de grupo são reaplicadas a esses IVs. Envie a regra depois de fazer as mudanças para que ela passe pelo processo de aprovação novamente.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de exceção**.
2. Abra a regra de exceção que você deseja cancelar e clique em **Cancelar**.
3. Na caixa de diálogo Cancelar regra, clique em **Cancelar regra**.
   A regra retorna para o estado Rascunho e a VUL associada é excluída. Os IVs relacionados são reabertos e as regras de grupo são aplicadas aos IVs individuais.

Excluir uma regra de exceção

Exclua uma regra de exceção que não seja mais necessária. Por exemplo, você pode excluir uma regra se não quiser adiar um item vulnerável (IV) durante a ingestão.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

A exclusão de uma regra cancela a tarefa de correção associada (VUL). Os IVs relacionados são reabertos e as regras de grupo são aplicadas aos IVs individuais.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Regras de exceção**.
2. Abra a regra de exceção que você deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo Excluir regra, clique em **Excluir regra** para excluir a regra selecionada.
   A tarefa de correção associada também é excluída. Os IVs relacionados são reabertos e as regras de grupo são aplicadas aos IVs individuais.

Marcar e aprovar um falso-positivo

Itens vulneráveis (IVs) e tarefas de correção (VULs) podem ser marcados como falsos positivos. Aprovadores com acesso de gravação podem aprovar essas solicitações de outros usuários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Marcar como falso-positivo
- Edição em massa para falso-positivo
- Aprovar um falso-positivo

Nota:

Notificações por e-mail são enviadas em todas as fases do fluxo de trabalho de falso-positivo, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando um IV ou tarefa de correção é marcado como falso positivo, o solicitante recebe um e-mail de confirmação. Simultaneamente, o aprovador recebe um e-mail informando que um IV ou tarefa de correção foi marcado como falso positivo.

A partir da v21.0 de Vulnerability Response, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Marcar como falso-positivo

Marque um item vulnerável (IV) ou tarefa de correção (VUL) como falso positivo se o aviso fornecido pelo scanner não for realmente um problema. Por exemplo, se um item de configuração foi desativado, mas o scanner ainda está levantando um problema relacionado a ele, marque-o como um falso positivo.

Antes de Iniciar

Função necessária: responsável pela correção

Você pode solicitar falsos positivos nos espaços Vulnerability Response. Consulte Solicitar um falso-positivo no Espaço de correção de problemas de TI.

Você também pode solicitar falsos positivos no ambiente clássico:

Procedimento

1. Navegar até **Vulnerability Response** > **Itens vulneráveis (ou Tarefas de correção)** > **Todos**.
2. Abra o IV ou VUL que você deseja marcar como falso-positivo e clique em **Marcar como falso-positivo**.
   O IV ou VUL deve estar em um estado **Aberto**.
3. No formulário de falso positivo, insira os detalhes em **Informações adicionais** e clique em **Solicitar aprovação**.
   A solicitação é enviada para aprovação e o Estado do IV ou VUL muda para **Em revisão**.

Edição em massa para falso-positivo

Use a edição em massa para marcar vários itens vulneráveis (IVs) como falso-positivos. Se vários IVs forem selecionados, uma tarefa de correção será formada com esses itens.

Antes de Iniciar

Função necessária: responsável pela correção

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

. Para solicitar um falso positivo dos espaços de vulnerabilidade Vulnerability Response, consulte Solicitar um falso-positivo no Espaço de correção de problemas de TI. Você também pode solicitar falsos positivos no ambiente clássico:

Procedimento

1. Navegar até **Vulnerability Response** > **Itens vulneráveis** > **Todos** e selecione os itens que você deseja marcar como falso-positivo.
   Os itens selecionados devem estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. Clique **em Edição em massa**.
3. No formulário, preencha os campos.

Formulário de edição em massa de item vulnerável

Campo	Descrição
Seleção de registro	Registros a serem selecionados para edição em massa.
Estado	Estado dos itens vulneráveis. Selecione Encerrado para marcar como falso positivo.
Motivo	Subestado para o estado que foi selecionado. Se você selecionou Encerrado como o Estado, selecione Falso-positivo aqui para marcar como falso-positivo.
Cancelar atribuição	Envie uma solicitação para limpar os campos Atribuído a e Grupo de atribuição.
Solução preferencial	Solução direcionada para corrigir todos os itens vulneráveis selecionados para edição em massa.
Grupo de atribuição	Grupo de atribuição para o IV. Selecione manualmente ou usando recomendações de atribuição se estiver habilitado.
Anotações de trabalho	Anotações a serem adicionadas.

4. Clique em **OK**.
   Uma nova tarefa de correção é criada contendo os IVs selecionados e essa tarefa é enviada para aprovação.

Aprovar um falso-positivo

Como aprovador de falso-positivo, você pode aprovar solicitações de falso-positivo de outros usuários.

Antes de Iniciar

Função necessária: sn_vul.false_positive_approver ou sn_vul.app_false_positive_aprovador

Você pode aprovar solicitações de exceção e falso-positivo no espaço Vulnerability Response. Consulte Aprovar solicitações no Vulnerability Manager Workspace.

Você também pode aprovar solicitações de exceção e falso-positivo no ambiente clássico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Vulnerabilidades** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprove ou rejeite a solicitação com os comentários apropriados.

Nota:
Um falso positivo pode ter um limite de tempo. Somente o aprovador pode definir a data de término.

Soluções de análise e relatório para Vulnerability Response

O monitoramento da correção de vulnerabilidades envolve a exibição de tendências, o gerenciamento de riscos e o monitoramento de grupos de atribuição. Você pode revisar problemas de alto risco, cargas de trabalho de grupo de atribuição, adiamentos e vulnerabilidades recorrentes. Vulnerability Response oferece ferramentas, relatórios e procedimentos para tornar esse processo mais produtivo e eficiente.

Visualizações de dados nos espaços Vulnerability Response

Os espaços Vulnerability Response incluem visualizações de dados que podem ajudar a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a severidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizadas conforme os dados de vulnerabilidade mudam. Consulte Espaço para gerentes de vulnerabilidades e Explorando o Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos que estão disponíveis.

Os analistas de vulnerabilidade também podem usar painéis padrão Vulnerability Response em **Todos** > **Vulnerability Response** > **Visão geral**.

A partir da versão 19.0 do Vulnerability Response, este painel também pode ser exibido na IU da nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique no ícone**Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Painéis no Vulnerability Manager Workspace e Painéis no IT Remediation Workspace.

Nota:
Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Vulnerability Response processo de correção

A maior parte da correção de vulnerabilidade é feita a partir do registro da tarefa de correção de dentro dos Vulnerability Response Espaços. A partir das tarefas de correção (RTs) no estado Sob investigação, você pode executar várias tarefas.

- Crie solicitações de mudança.
- Adicione anotações de trabalho e descrições de vulnerabilidades na tarefa de correção.
- Adie a tarefa de correção e os itens vulneráveis nela para uma data posterior.
- Feche a tarefa de correção.
- Rastreie novas obrigações de conformidade regulatória, que geralmente são sensíveis ao tempo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Faça login na sua instância Vulnerability Response.
- Revise os painéis e relatórios do Vulnerability Management e de terceiros para localizar áreas com problemas. Por exemplo, exiba painéis que mostram o envelhecimento da tarefa de correção (RT) por estados ou itens vulneráveis (IVs) de alto risco após a data de meta de correção.
- Revise o estado das tarefas de correção, em ordem de risco.
- Revise a priorização das tarefas ajustando as calculadoras de pontuação de risco se a pontuação de risco não estiver sendo calculada corretamente ou adiando IVs ou RTs, conforme necessário. Consulte Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade ou Adiar uma tarefa de correção para obter mais informações sobre essas opções.
- Analise os itens vulneráveis adiados prestes a reabrir e tome medidas adicionais conforme necessário. Se você quiser iniciar e rastrear atividades de mudança em seus ativos, tarefas de correção e itens vulneráveis correspondentes, para obter mais informações, consulte Change Management para Vulnerability Responsepara obter mais informações.
- Analise o feedback do IT Operations.

  Depois de ser notificado de que uma solicitação de mudança foi resolvida, aguarde a próxima verificação. As verificações são acionadas automaticamente pela programação de importação de terceiros configurada no Assistente de configuração.
- Após uma verificação, se o estado for Fixo, os itens vulneráveis serão fechados automaticamente durante a importação. O grupo é encerrado quando todos os itens vulneráveis do grupo são corrigidos.
- Após a verificação, se o estado não for Corrigido, o IV será movido automaticamente de volta para Sob investigação.
- Itens vulneráveis definidos como "Resolvidos" em sua instância, mas não transicionados para "Encerrado/Corrigido" pelas execuções de integração de terceiros serão reabertos se forem detectados durante novas verificações.

  Para Qualys detecções, se o scanner continuar a encontrar IVs que foram definidos como "Resolvido", mas não transicionados para "Encerrado/Corrigido" pelas verificações subsequentes, esses IVs retornam para "Aberto" quando a última data encontrada for posterior a Data de resolução.

  Para Rapid7 detecções, uma opção agora está disponível na página de configuração Rapid7 em sua instância para reabrir IVs resolvidos por idade. Se habilitado, os IVs definidos como "Resolvido", mas não transicionados para "Encerrado/Corrigido" pelas verificações subsequentes, retornam para "Aberto" após o número de dias inserido.

Solução de gerenciamento de vulnerabilidade Andamento da implantação

Métricas de implantação abrangentes para tarefas de correção e entradas de vulnerabilidade estão incluídas em Solução de gerenciamento de vulnerabilidade em **Status** de correção em vulnerabilidades, itens vulneráveis. Identifique facilmente qual tarefa de correção ou vulnerabilidade está atrasando o andamento da resolução. Detalhe como a vulnerabilidade é identificada ou quais aspectos dos ativos afetados podem estar causando o problema de correção. Atualize o status de suas métricas usando o link relacionado **Atualizar status** nos formulários de tarefa de vulnerabilidade, soluções e correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando os painéis padrão Vulnerability Response

O Vulnerability Response painel de visão geral (Gestão de vulnerabilidades) fornece uma visão executiva de vulnerabilidades e itens vulneráveis, ajudando o Administrador de vulnerabilidades a identificar áreas de preocupação rapidamente. O Vulnerability Response painel de correção (Correção de vulnerabilidade) permite que um especialista em correção se concentre nas tarefas de correção e nos itens vulneráveis que possui.

Visualizações de dados nos espaços Vulnerability Response

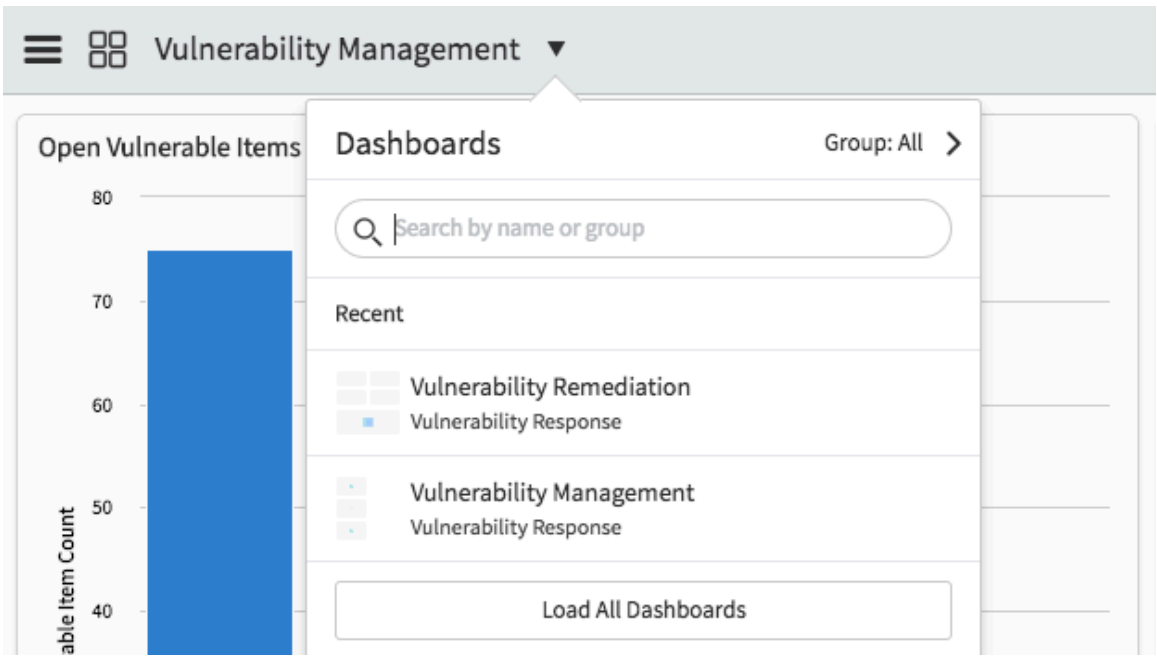
Os espaços Vulnerability Response incluem visualizações de dados que podem ajudar a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a severidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizadas conforme os dados de vulnerabilidade mudam. Consulte Vulnerability Response Espaços, Espaço para gerentes de vulnerabilidades e Explorando o Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos que estão disponíveis.

Os analistas de vulnerabilidade também podem usar painéis padrão Vulnerability Response.

Funções necessárias: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst e usuários com sn_vul.vulnerability_read (ou que herdam a função sn_vul.vulnerability_read) e pa_viewer.

Os painéis padrão Vulnerability Response no ambiente legado

Esses relatórios são incluídos como parte da aplicação Performance Analytics para Vulnerability Response e não exigem uma assinatura separada. Para abrir um, selecione a lista de seleção para expandi-la e escolha um painel. Como alternativa, insira o nome de um painel no campo de pesquisa.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Quando a aplicação Performance Analytics Content Pack for Vulnerability Response é instalada e ativada, o painel Vulnerability Management (PA) é exibido automaticamente no módulo Visão geral. Este painel contém relatórios que abrangem todas as fases do ciclo de vida de gestão de vulnerabilidades.

Para obter informações sobre os relatórios incluídos no Pacote de conteúdo do Performance Analytics para Vulnerability Response, consulte Painel do Vulnerability Management [PA].

Para obter informações sobre o painel do CISO e os relatórios de Cobertura de verificação, consulte Painel do Vulnerability Management do CISO.

Painel do Vulnerability Management

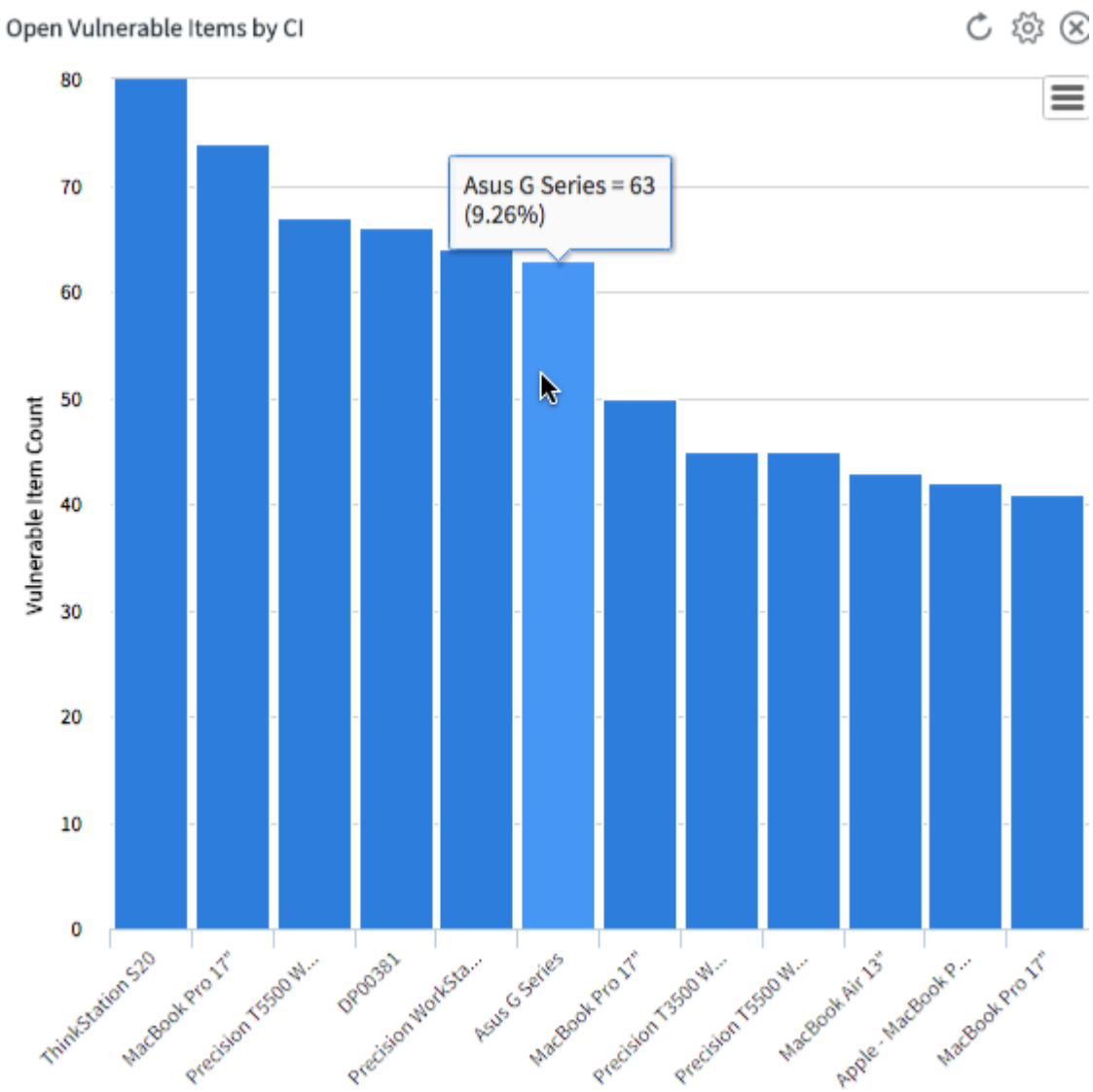
Em cada gráfico, você pode apontar para qualquer parte de um gráfico (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Nota:

Se painéis personalizados forem necessários, consulte Criar e usar painéis para obter mais informações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Relatórios de visão geral de vulnerabilidade

Nome	Visual	Descrição
Itens vulneráveis abertos por IC	Barra	Exibe o número de itens vulneráveis em aberto registrados para cada item de configuração (IC), do maior para o menor.
Itens vulneráveis por status da meta de correção	Barra	Exibe o número de itens vulneráveis que estão se aproximando da meta, em curso e na meta anterior. **Nota:** Itens no estado Adiado, Resolvido ou Encerrado não são incluídos.
Itens vulneráveis adiados que expiram esta semana	Gráfico	Exibe o número de itens vulneráveis adiados programados para serem reativados em sete dias.
Itens vulneráveis abertos por vulnerabilidade	Barra	Exibe o número de itens vulneráveis em aberto para cada vulnerabilidade, do maior para o menor.
Vulnerabilidades por modelo	Barra	Exibe o número de itens vulneráveis registrados para cada modelo (classe de IC), do mais para o menos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de visão geral de vulnerabilidade

Nome	Visual	Descrição
Vulnerabilidades por semana	Tendência	Exibe o número de entradas de vulnerabilidade registradas a cada semana.
Modelos mais vulneráveis	Donut	Exibe modelos (classes de IC) com os itens mais vulneráveis.
Vulnerabilidades por fornecedor	Barra	Exibe o número de itens vulneráveis registrados para cada fornecedor, do mais para o menos.
Vulnerabilidades por impacto	Barra	Exibe o número de entradas de vulnerabilidade para os tipos de rede afetados.
Fornecedores mais vulneráveis	Donut	Exibe fornecedores com os itens mais vulneráveis.
ICs mais vulneráveis	Donut	Exibe os ICs com os itens mais vulneráveis.
Vulnerabilidades por pontuação	Barra	Exibe o número de entradas de vulnerabilidade por pontuações de vulnerabilidade.
Itens vulneráveis reabertos	Lista	Lista os itens vulneráveis reabertos e sua idade.
ICs mais vulneráveis por classe	Donut	Exibe os ICs com os itens mais vulneráveis.
Idade do Item Vulnerável	Lista	Lista o número de dias desde a última abertura dos itens vulneráveis.
ICs com vulnerabilidade por data	Lista	Lista os itens de configuração que foram verificados nos últimos 30 dias.
ICs não verificados	Lista	Lista os itens de configuração que nunca foram verificados quanto a vulnerabilidades.

Painel de correção de vulnerabilidade

A partir da versão 19.0 do Vulnerability Response, este painel está disponível na IU da nova experiência.

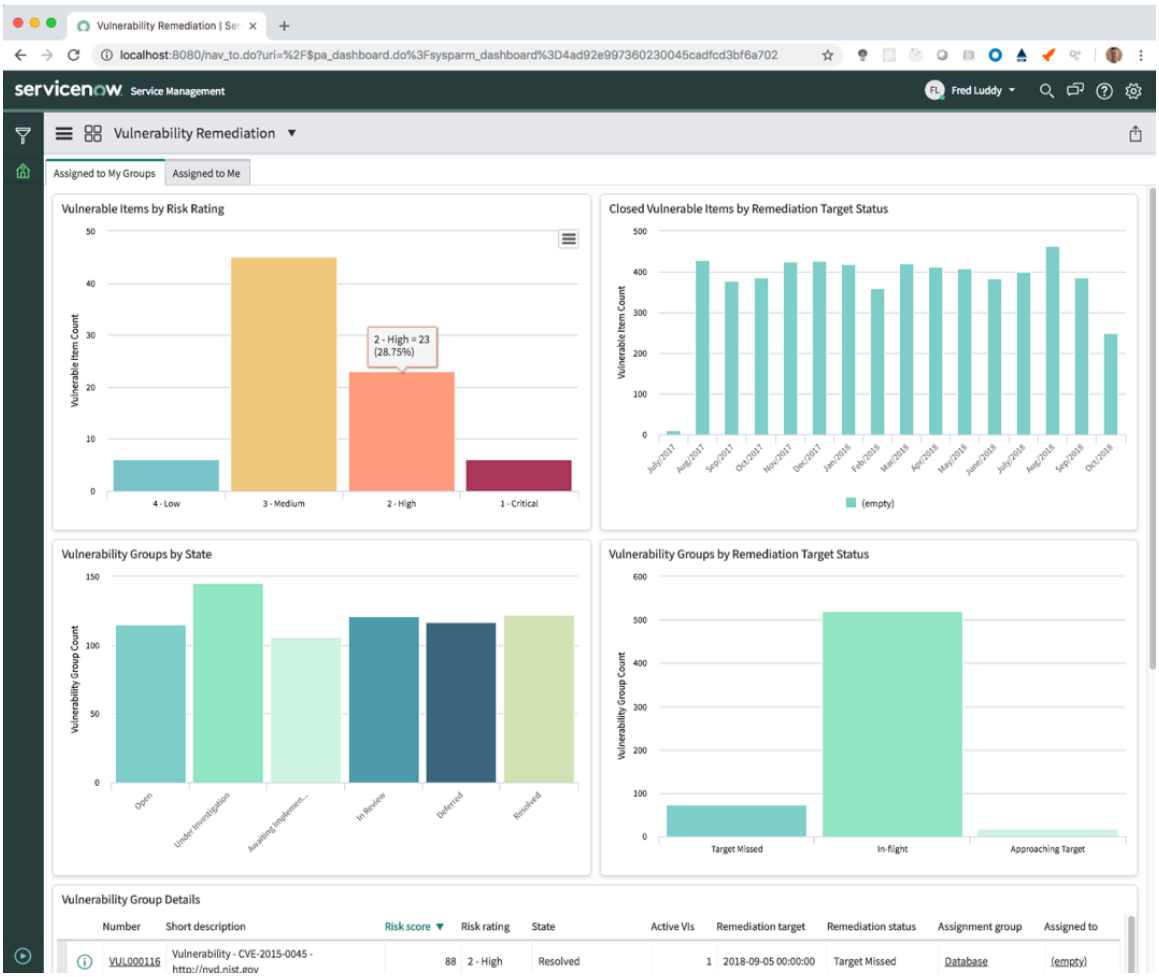
Nota:
Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

O painel do Vulnerability Remediation contém as seguintes guias: **Atribuído aos meus grupos**, **Atribuído a mim**e **Solicitado por mim**. As guias Atribuído aos Meus grupos e Atribuído a mim mostram os mesmos relatórios. A primeira guia relata os grupos de atribuição aos quais você pertence e a última por itens vulneráveis ou tarefas de correção que são atribuídas a você. A guia Solicitado por mim relata os falsos positivos e as exceções que você solicitou.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painel de correção de vulnerabilidade



Relatórios

Atribuído aos Meus grupos e Atribuído a mim

Nome	Visual	Descrição
Itens vulneráveis por classificação de risco	Barra de barra	Número de itens vulneráveis ativos, agrupados por classificação de risco no período selecionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atribuído aos Meus grupos e Atribuído a mim

Nome	Visual	Descrição
Itens vulneráveis encerrados por status da meta de correção	Barra de barra	Número de itens vulneráveis encerrados, agrupados por status de destino de correção no período selecionado.
Tarefas de correção por estado	Barra de barra	Número de tarefas de correção (RTs) ativas agrupadas por estado.
Tarefas de correção por status do destino de correção	Barra de barra	Número de RTs ativos agrupados por status de meta de correção. Este relatório exclui itens vulneráveis adiados.
Detalhes da tarefa de correção	Lista	Detalhes do registro da tarefa de correção em uma lista.

Solicitado por mim

Nome	Visual	Descrição
Status solicitações de falso-positivo e de exceção	Barra de barra	Número de solicitações ativas de você.
Tarefas de correção de falso-positivo e adiadas expirando	Barra de barra	Número de Tarefas de correção de falso-positivo (RTs) e adiadas, agrupadas por data Até.

Painel de aprovações de vulnerabilidade

O painel Aprovações de vulnerabilidade contém os seguintes relatórios para aprovadores de exceção e falso-positivos.

A partir da versão 19.0 do Vulnerability Response, este painel está disponível na IU da nova experiência.

Nota:
Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Nome	Visual	Descrição
Solicitações de falso-positivo e exceção por idade com minha aprovação pendente	Barra de barra	Número de aprovações pendentes para você, agrupadas por data de criação.
Minha aprovação, exceção rejeitada e solicitações de falso-positivo	Barra de barra	Número de solicitações de aprovação aprovadas ou rejeitadas, agrupadas por estado de aprovação.
Todas as Tarefas de correção por classificação de risco com aprovação pendente	Barra de barra	Número de tarefas de correção com aprovação pendente, agrupadas por classificação de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Visual	Descrição
Todas as solicitações de aprovação pendentes e de falso-positivo agrupadas por motivo	Barra de barra	Número de solicitações de aprovação pendentes agrupadas por motivo.

Soluções Análise da plataforma para Gestão de vulnerabilidades

Soluções Análise da plataforma contêm conteúdo pré-empacotado Performance Analytics e Relatórios para uso com outros produtos Now Platform. Esta Solução de análise e relatório permite que você rastreie o volume, o desempenho e o andamento das vulnerabilidades, desde a análise e detecção iniciais até a contenção ou correção. Você pode filtrar relatórios por grupo de atribuição, explorações, classificação de risco ou estado.

O pacote de conteúdo Performance Analytics para Vulnerability Response não é instalado automaticamente com a aplicação Vulnerability Response. Ele está disponível no ServiceNow Store como uma assinatura separada.

Performance Analytics para Vulnerability Response contém dois painéis:

- Painel do Vulnerability Management (PA)
- Painel do CISO (Chief Information Security Officer, diretor de segurança da informação) do Vulnerability Management

Funções necessárias, instalação e exibição dos painéis

As seguintes funções e tarefas estão associadas a esta Solução:

- Now Platform administrador (admin): instale e ative esta Solução de análise e relatório e faça as mudanças necessárias nas propriedades do sistema.
- Performance Analytics Administrador (pa_admin): revise os indicadores, detalhamentos, widgets e painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.

Para instalar esse aplicativo, consulte Instalar e configurar o aplicativo Performance Analytics for Vulnerability Response [PA].

Nota:
Configure e teste as Soluções de análise e relatório em uma instância de não produção antes de habilitá-las na produção.

As Soluções de análise e relatório fornecem todos os registros de configuração necessários para analisar as aplicações padrão. Personalize esses registros para uso em seu ambiente de produção. Para obter mais informações, consulte Configurar Soluções de análise e relatório .

Para exibir o painel de gestão de vulnerabilidades (PA), navegue até **Vulnerability Response** > **Visão geral** > **.**

Para exibir o painel Vulnerability Management CISO, navegue até **Vulnerability Response** > **Painel do CISO** > **.**

Termos-chave

Performance Analytics (PA)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solução que cria painéis de gestão, relatórios sobre KPIs e métricas e responde às principais perguntas de negócios para ajudar a aumentar a qualidade e reduzir custos.

Item vulnerável (IV)

Uma vulnerabilidade de segurança relatada por um scanner de vulnerabilidade de terceiros que está presente em um item de configuração (IC).

Tarefa de correção

As tarefas de correção são criadas e atribuídas automaticamente às equipes de TI com base no grupo associado aos itens vulneráveis em um esforço de correção. As equipes de TI e os proprietários de correção exibem as tarefas de correção no Espaço de correção de TI. Consulte Vulnerability Response Espaços para obter mais informações

.

Indicador de PA

Define uma medição de desempenho feita em intervalos regulares de um serviço de negócios, atividade ou comportamento organizacional, por exemplo, itens vulneráveis críticos e atrasados não adiados.

Origem do indicador de PA

Conjuntos de dados que filtram registros de uma tabela ou exibição de banco de dados, por exemplo, IV ativo.

Exibir visualizações de dados em tempo real

Para ver o que está acontecendo hoje com os itens mais críticos na sua aplicação Vulnerability Response, você pode exibir determinados relatórios no painel Vulnerability Management (PA) em tempo real. Exibir esses relatórios em tempo real ajuda a gerenciar seus itens vulneráveis (IVs) mais importantes e a corrigi-los rapidamente. Você pode exibir os seguintes relatórios em tempo real:

- Guia Visão geral – Itens vulneráveis por grupo de atribuição
- Guia ICs vulneráveis
  - Itens de configuração (ICs) vulneráveis sem proprietários
  - ICs desativados ou roubados com IVs ativos
- Guia Exceções
  - Itens vulneráveis adiados por motivo
  - Solicitações de postergação prestes a expirar
  - Itens vulneráveis adiados por gerente de CIO
- Guia Correção – Itens vulneráveis não atribuídos

Para obter mais informações, consulte Exibir relatórios do Performance Analytics para Vulnerability Response [PA] em tempo real.

Tópicos relacionados

Soluções de análise e relatório

Painel Vulnerability Management do CISO

Com o painel do Vulnerability Management CISO, exiba dados como KPIs (Key Performance Metrics) para correção de vulnerabilidades, veja os riscos mais altos, verifique a cobertura da verificação e saiba como reduzir riscos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Funções necessárias de Now Platform

- sn_vul.vulnerability_ciso para exibir o painel.
- sn_vul.ciso_write para editar o painel.

Ativação do painel do CISO

Para ativar o painel do CISO, você deve instalar o Performance Analytics para Vulnerability Response e ativar o trabalho do Performance Analytics correspondente. Para obter mais informações, consulte Soluções de análise e relatório para Vulnerability Response.

Casos de uso

Usuário	Uso do painel
Diretores de segurança da informação (CISOs)	Os diretores de segurança da informação (CISOs) podem usar o painel do CISO para obter informações sobre o programa de gestão de vulnerabilidades de suas organizações. O painel fornece dados para ajudá-los a identificar dados rapidamente como eles podem usar para reduzir as vulnerabilidades de seus ambientes.

Como usar o painel do CISO

Usuários executivos, como os diretores de segurança da informação (CISOs) em sua organização, podem exibir o painel do CISO para o Vulnerability Response para entender a eficácia do programa de gestão de vulnerabilidades. Você pode exibir o painel do CISO navegando até **Vulnerability Response** > **Painel do CISO**. Use os filtros de nível superior para filtrar relatórios por Classificação de risco, Faixa etária ou Voltado para a Internet. Alguns relatórios exibem dados de tendências ao longo de um período. Você pode exibir as tendências das métricas importantes regularmente, analisar o risco geral à segurança dos negócios e identificar as áreas que precisam de melhorias.

A partir da versão 19.0 do Vulnerability Response, este painel também pode ser exibido na IU da nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique no ícone**Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Painéis no Vulnerability Manager Workspace e Painéis no IT Remediation Workspace.

Nota:
Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Executando os trabalhos programados

Execute os trabalhos programados nesta ordem para atualizar os dados nos relatórios:

1. Atualizar tabelas do painel
2. [PA VR] Painel do CISO

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalhos programados para o painel do CISO

Nome do trabalho programado	Descrição
Atualizar tabelas do painel	Trabalho programado diariamente que você deve executar antes do trabalho do Painel do CISO [PA VR] para que possa coletar os dados do CISO. Ao executar este trabalho programado, você atualiza os relatórios de cobertura de verificação. As informações atualizadas incluem os itens de configuração operacional (ICs) verificados nos últimos 90 dias, suas classes e o número total de ICs operacionais que correspondem a essas classes. A execução deste trabalho programado também atualiza os relatórios na guia **Ações recomendadas**. **Nota:** Os ICs operacionais se referem aos ICs que têm um status operacional como Operacional.
[PA VR] Painel do CISO	Depois que o trabalho programado Atualizar tabelas do painel for concluído, execute esse trabalho programado para preencher todos os relatórios na guia **Visão geral do CISO**.

Guias do painel do CISO

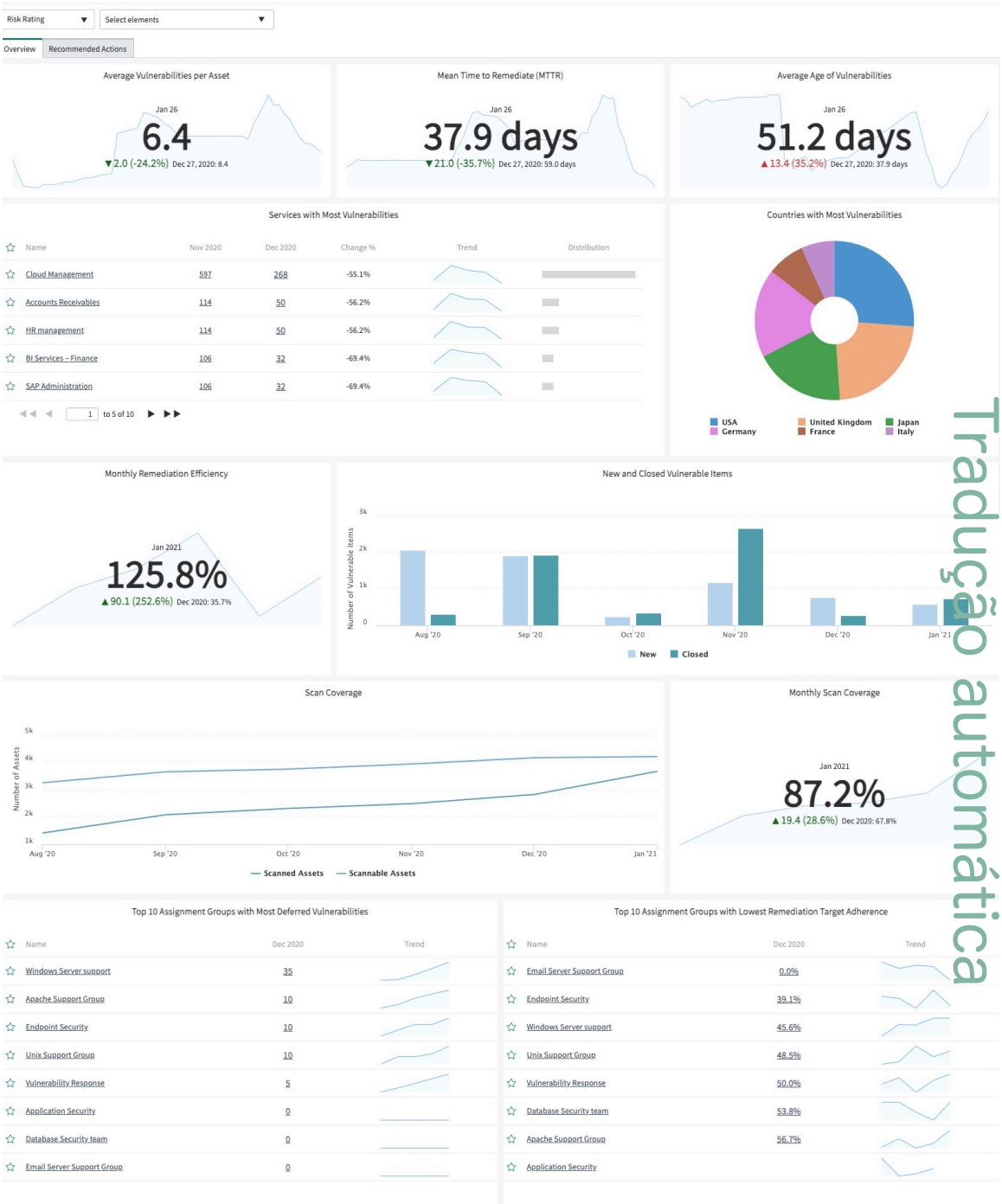
Este painel fornece informações sobre os riscos presentes no Vulnerability Management. Você pode exibir vulnerabilidades e seus dados relacionados por região, idade, serviços e outros detalhamentos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral

A guia Visão geral contém relatórios que fornecem uma visão geral da postura de segurança da sua organização.



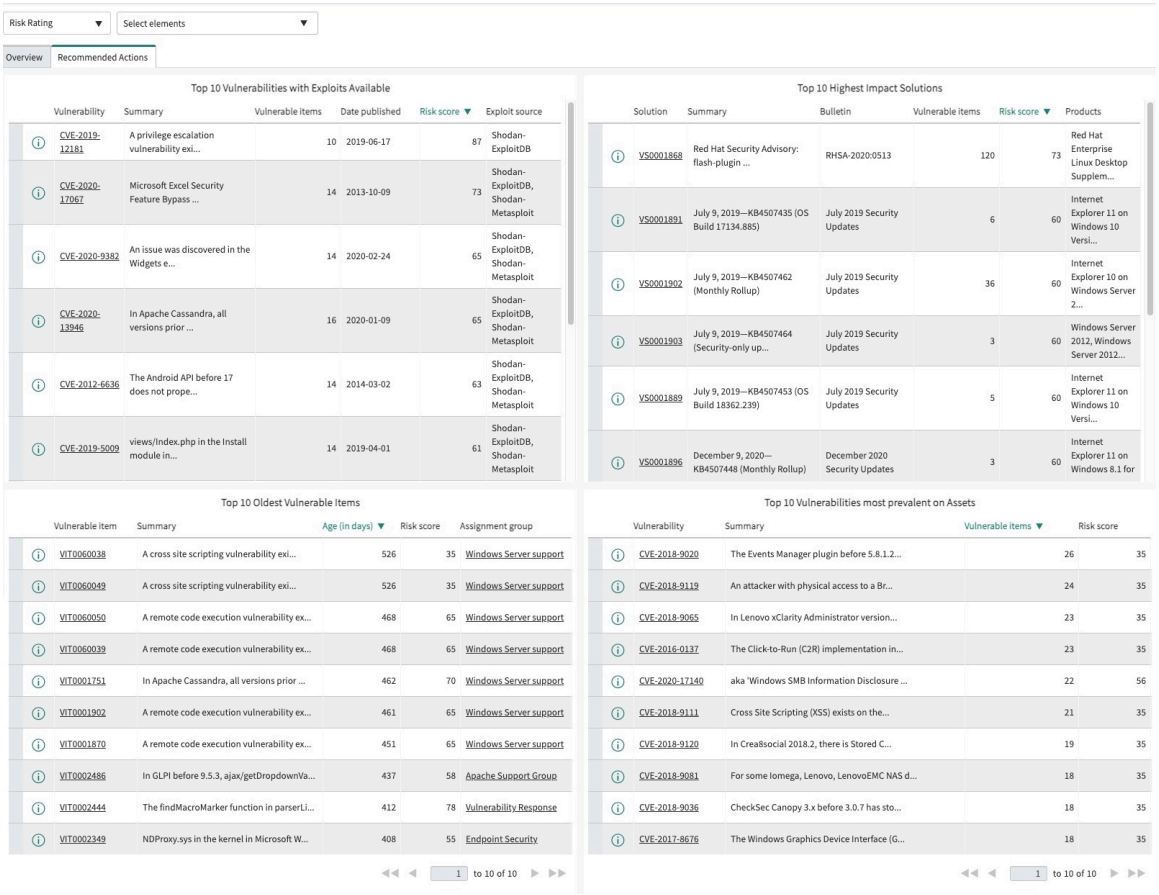
Nota:
O filtro de nível superior só pode ser usado para alguns relatórios.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Ações recomendadas

A guia Ações recomendadas contém relatórios que fornecem informações sobre vulnerabilidades exploráveis, obsoletas e prevalentes. Ele também contém soluções que recomendam ações para reduzir os riscos. Execute o trabalho programado **Atualizar tabelas do painel do CISO** para atualizar os relatórios nesta guia.



Indicadores

Para exibir os indicadores, navegue até **Performance Analytics** > **Indicadores**.

1. Na página Indicadores, pesquise o nome do indicador necessário na coluna Nome.
2. Clique no nome do indicador para abrir o registro e exibir seus detalhes.

Os indicadores do painel do CISO não coletam registros por padrão. Você pode optar por coletar registros marcando a caixa de seleção Coletar registros.

Duração total de itens vulneráveis encerrados

A duração total de IVs encerrados é medida diariamente em dias. O objetivo deste indicador é minimizar a pontuação.

Ativos verificáveis

Os ativos verificados são medidos diariamente em unidades numéricas. O objetivo deste indicador é maximizar a pontuação.

Serviços com mais vulnerabilidades

Serviços com a maioria das vulnerabilidades são medidos diariamente como unidade #. O objetivo deste indicador é minimizar a pontuação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerabilidades médias por ativo

[[Itens vulneráveis ativos]] / [[Itens de configuração vulneráveis ativos]

Itens vulneráveis encerrados

Os itens vulneráveis encerrados são medidos diariamente em unidades numéricas. O objetivo deste indicador é maximizar a pontuação.

Tempo médio de correção dos itens vulneráveis

[[Soma da duração de itens vulneráveis encerrados]]/[[Itens vulneráveis encerrados]]

Cobertura de verificação atual

Calcula a cobertura da verificação atual como porcentagem.

Ativos verificados

Os ativos verificados são medidos diariamente em unidades numéricas. O objetivo deste indicador é maximizar a pontuação.

Itens vulneráveis encerrados (meta atingida)

Os itens vulneráveis encerrados (meta atingida) são medidos diariamente como unidade #. O objetivo deste indicador é maximizar a pontuação.

Percentual de itens vulneráveis encerrados que cumpriram a meta

[[Itens vulneráveis encerrados (Meta atingida) / SOMA por mês]] / [[Itens vulneráveis encerrados / SOMA por mês]] *100

Itens vulneráveis ativos

Os itens vulneráveis ativos são medidos diariamente em unidades numéricas. O objetivo deste indicador é minimizar a pontuação.

Idade média dos itens vulneráveis

A idade média dos IVs ativos é medida diariamente em unidades Dias. O objetivo deste indicador é minimizar a pontuação.

Itens de configuração vulneráveis ativos

Os ICs vulneráveis ativos são medidos diariamente como unidade #. O objetivo deste indicador é minimizar a pontuação.

Eficiência de correção mensal

[Número de itens vulneráveis encerrados durante um mês] / [Número de itens vulneráveis novos ou reabertos no mesmo mês]

Novos itens vulneráveis

Novos itens vulneráveis são medidos diariamente em unidades numéricas. O objetivo deste indicador é minimizar a pontuação.

Itens vulneráveis com postergação

Os IVs adiados são medidos diariamente como unidade #. O objetivo deste indicador é minimizar a pontuação.

Detalhamentos

- Grupo de atribuição: aplica-se a alguns relatórios de IV.
- Classificação de risco: aplica-se a relatórios de IV.
- Faixa etária: aplica-se a relatórios de IV.
- Idade do fechamento: aplica-se a relatórios de IVs encerrados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Voltado para a Internet: indica se o IC pertence à classe de hardware e é voltado para a Internet.
- Região: o parâmetro de IC do CMDB usado é Location. Este local indica o país de origem do item de configuração.

Visualizações de dados

Nome	Tipo	Descrição
Vulnerabilidades médias por ativo	Pontuação	Número médio de itens vulneráveis ativos para cada item de configuração.
Tempo médio para correção (MTTR)	Pontuação	O tempo médio para corrigir (encerrar) um item vulnerável, exibido como uma média de 30 dias de execução. **Nota:** O valor da Idade do encerramento é calculado quando os dados são coletados. O valor é a diferença entre a data da última abertura e a data e hora do trabalho de coleta.
Idade média das vulnerabilidades	Pontuação	Idade média dos itens vulneráveis ativos em dias.
Serviços com mais vulnerabilidades	Lista e linha Ícone	Média mensal de itens vulneráveis ativos para serviços na empresa. **Nota:** Para obter informações sobre como definir as classificações de serviço que você deseja exibir nos relatórios do Vulnerability Response e nas listas relacionadas, consulte a guia Serviços no painel Vulnerability Management [PA].
Países com mais vulnerabilidades		10 principais países com o maior número de itens vulneráveis.
Eficiência de correção mensal	Pontuação	Percentual de itens vulneráveis encerrados dividido por novos itens vulneráveis no mês atual.
Itens vulneráveis novos e encerrados	Barra de barra	Número de novos itens vulneráveis importados e número de itens vulneráveis encerrados em um mês.
Cobertura de verificação	Linha de linha	Número de ativos verificados em comparação com o número total de ativos verificáveis, mostrado ao longo do tempo. As classes de IC incluídas no widget são especificadas no módulo Configuração de cobertura de verificação. Para obter informações sobre como configurar o módulo Cobertura de verificação, consulte Configurar os relatórios de Cobertura de verificação.
Cobertura de verificação mensal	Pontuação	Percentual de ativos verificados dividido pelo número total de ativos verificáveis para o mês atual.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
		Para obter informações sobre como configurar o módulo Cobertura de verificação, consulte Configurar os relatórios de Cobertura de verificação
10 principais grupos de atribuição com vulnerabilidades mais adiadas	Lista e linha Ícone	10 principais grupos de atribuição com o maior número de itens vulneráveis adiados, adiados com base na média mensal.
10 principais grupos de atribuição com menor adesão à meta de correção	Lista e linha Ícone	10 principais grupos de atribuição cujos itens vulneráveis têm a menor aderência às metas de correção.

Ações recomendadas

Nome	Tipo	Tabela de origem	Descrição
10 principais vulnerabilidades com explorações disponíveis	Lista	Item principal de vulnerabilidade [sn_vul_analytics_top_item]	Vulnerabilidades ativas com explorações disponíveis para todos os fornecedores de inteligência contra ameaças que usam a estrutura de exploração de VR.
10 principais soluções de maior impacto	Lista	Item principal de vulnerabilidade [sn_vul_analytics_top_item]	Soluções ou patches preferenciais com as pontuações de risco mais altas para itens vulneráveis ativos. Este relatório usa os recursos do Vulnerability Solution Management (VSM), que correlaciona patches da Microsoft e do Red Hat a vulnerabilidades no ambiente. O VSM ajuda a identificar a solução preferencial para vulnerabilidades.
10 principais itens vulneráveis mais antigos	Lista	Item principal de vulnerabilidade [sn_vul_analytics_top_item]	Itens vulneráveis ativos com a maior idade. Resolva esses itens para diminuir a idade média da vulnerabilidade na guia Visão geral.
10 principais vulnerabilidades mais prevalentes nos ativos	Lista	Item principal de vulnerabilidade [sn_vul_analytics_top_item]	Itens vulneráveis ativos disponíveis para o maior número de ativos.

Configurar os relatórios de cobertura de verificação

Permita que seus usuários executem relatórios de cobertura de verificação no painel do CISO. Com esses relatórios, os usuários podem ver qual é a cobertura de verificação da organização ao longo de um período.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

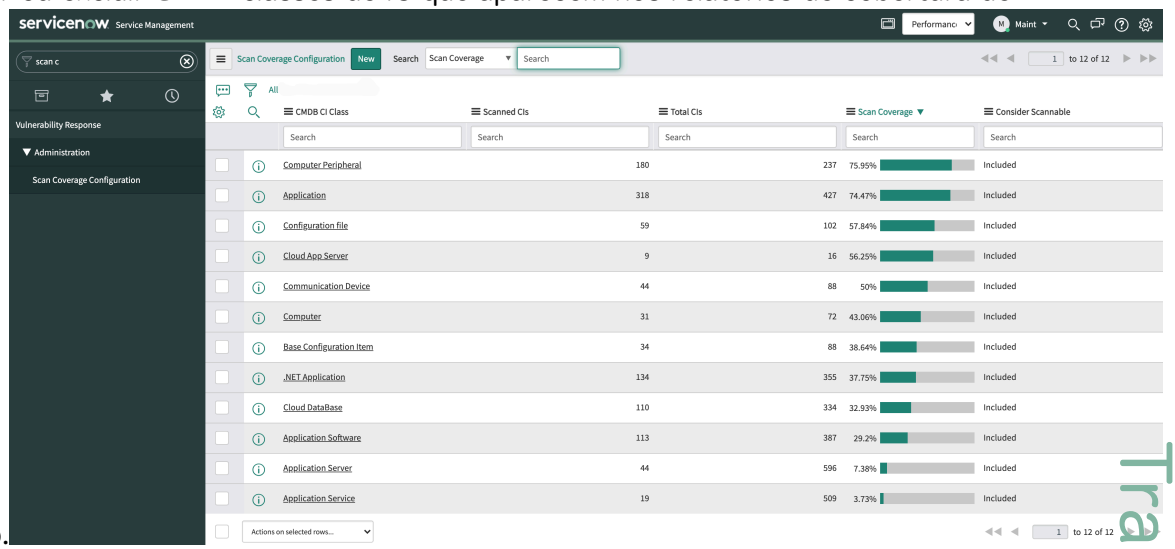
Por Que e Quando Desempenhar Esta Tarefa

A cobertura da verificação mostra o número de ativos que estão sendo verificados pelos scanners de vulnerabilidade para as várias classes nos últimos 90 dias. Esses ativos são

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

comparados ao número de ativos verificáveis no Configuration Management Database (CMDB). Por padrão, o módulo Configuração de cobertura de verificação inclui CMDB classes de IC, às quais pelo menos um ativo verificado foi correspondido. Você pode adicionar uma classe de IC de CMDB ao relatório Cobertura de verificação que é exibido no painel do CISO. Você pode incluir ou excluir CMDB classes de IC que aparecem nos relatórios de cobertura de verificação.



Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Configuração de cobertura de verificação**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Configuração de cobertura de verificação

Campo	Descrição
Classe de IC do CMDB	Classe de IC que deve ser adicionada ao relatório de cobertura de verificação no painel do CISO. **Nota:** Se uma classe de IC já existir no módulo Configuração de cobertura de verificação, ela não será incluída nesta lista.
Considerar verificável	Opção para definir se a classe de IC deve ser incluída ou não. Inclua uma classe de IC se quiser que seus dados sejam adicionados aos relatórios de cobertura de verificação. Se excluídos, os dados dessa classe de IC não serão adicionados.

4. Clique em **Enviar**.

Configurar os indicadores de PA para o painel do CISO

Monitore os indicadores CISO automatizados e formulados para que você possa gerenciar os dados de vulnerabilidade em sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Vulnerability Response tem indicadores automatizados e formulados.

Termos-chave

Indicador

Define uma medição de desempenho feita em intervalos regulares de um serviço de negócios, atividade ou comportamento organizacional. Um exemplo é um item vulnerável ativo.

Fonte do indicador

Conjuntos de dados que consistem em registros filtrados de uma tabela ou exibição de banco de dados para maior eficiência. Um exemplo é VI.Active (voltado para a Internet).

Detalhamentos

Os detalhamentos filtram e agrupam pontuações do indicador usando atributos qualitativos, como Prioridade, Categoria e Grupo de atribuição.

Trabalhos programados

Trabalhos programados são executados para preencher os dados de origem do indicador. O trabalho programado diário do painel CISO [PA VR] está desabilitado por padrão. Você deve ativá-lo para coletar pontuações do indicador para o painel do CISO.

Procedimento

1. Navegar até **Todos** > **Performance Analytics** > **Indicadores** e escolha uma das seguintes opções:
   - Indicadores Automatizados
   - Indicadores de Fórmula

   Para obter mais informações sobre indicadores, consulte Indicadores do Performance Analytics .
2. Na página Indicadores, pesquise o nome do indicador necessário na coluna Nome.
3. Clique no nome do indicador para abrir o registro e exibir seus detalhes.

   Os indicadores do painel do CISO não coletam registros por padrão. Você pode optar por coletar registros marcando a caixa de seleção **Coletar registros**.

   Nota:
   Ativar a coleta de registros em um indicador pode causar problemas de desempenho, como consumir muito mais tempo e memória, o que é necessário para executar o trabalho de coleta de dados.

   O número máximo de linhas que você pode buscar para uma origem de indicador é 1.000.000.

Painel de integridade do Vulnerability Response de SecOps

O painel Vulnerability Response Health é uma ferramenta projetada para capacitar as organizações com informações abrangentes sobre a implementação e o uso de suas aplicações Vulnerability Response.

A avaliação geral de integridade é determinada pela agregação de vários fatores críticos em configuração, implementação, integração, desempenho, dados e processo. Exiba o painel agregado de cada categoria para as seguintes aplicações:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Vulnerability Response
- Application Vulnerability Response
- Vulnerability Response do contêiner
- Conformidade de configuração

Instalando o SecOps Vulnerability Response Health Dashboard

Para instalar e configurar as aplicações SecOps Vulnerability Response Health Dashboard for Vulnerability Response em sua instância da Now Platform, navegue até ServiceNow® Store e ative o plug-in SecOps Health Analytics (sn_sec_analytics).

Funções necessárias de Now Platform

Funções necessárias: sn_sec_analytics.admin, sn_sec_analytics.read

Trabalho programado

Para exibir o trabalho programado, navegue até **Todos** > **Scheduler do Sistema** > **Trabalhos programados** > **Coletar métricas do painel de integridade**. O trabalho programado "Coletar métricas do painel de integridade" é executado diariamente às 00:00 horas. Ele gera os dados para o painel de Integridade do SecOps Vulnerability Response. Você também pode optar por executar o trabalho programado manualmente.

Casos de uso

Para obter exemplos de como as pessoas em sua organização usariam este painel, consulte estes casos de uso.

Usuário	Uso do painel
Administrador de vulnerabilidade	Ajuda a entender a pontuação de integridade das aplicações Vulnerability Response. Também é útil destacar as áreas que precisam de melhorias. O painel de integridade do Vulnerability Response lida somente com a implementação e a integridade do uso. Ele não ajuda no gerenciamento de vulnerabilidades ou ativos.
Administrador do suporte	Ajuda a identificar problemas de desempenho, personalização e configuração usando KPIs. Com base na integridade da aplicação, você pode executar uma análise extra ou fornecer uma recomendação aos usuários.
Parceiro de implementação	Ajuda a avaliar a integridade da implementação Vulnerability Response para configurações, complementos, personalizações e integrações e fornece recomendações de melhoria para os usuários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As guias do painel de integridade do SecOps Vulnerability Response

Para exibir o painel SecOps Vulnerability Response Health, navegue até **Integridade do Security Operations** > **Integridade do Vulnerability Response**. Cada cor no painel representa o seguinte:

- Verde: seguro
- Amarelo: aviso
- Vermelho: Crítico

Guia Resumo

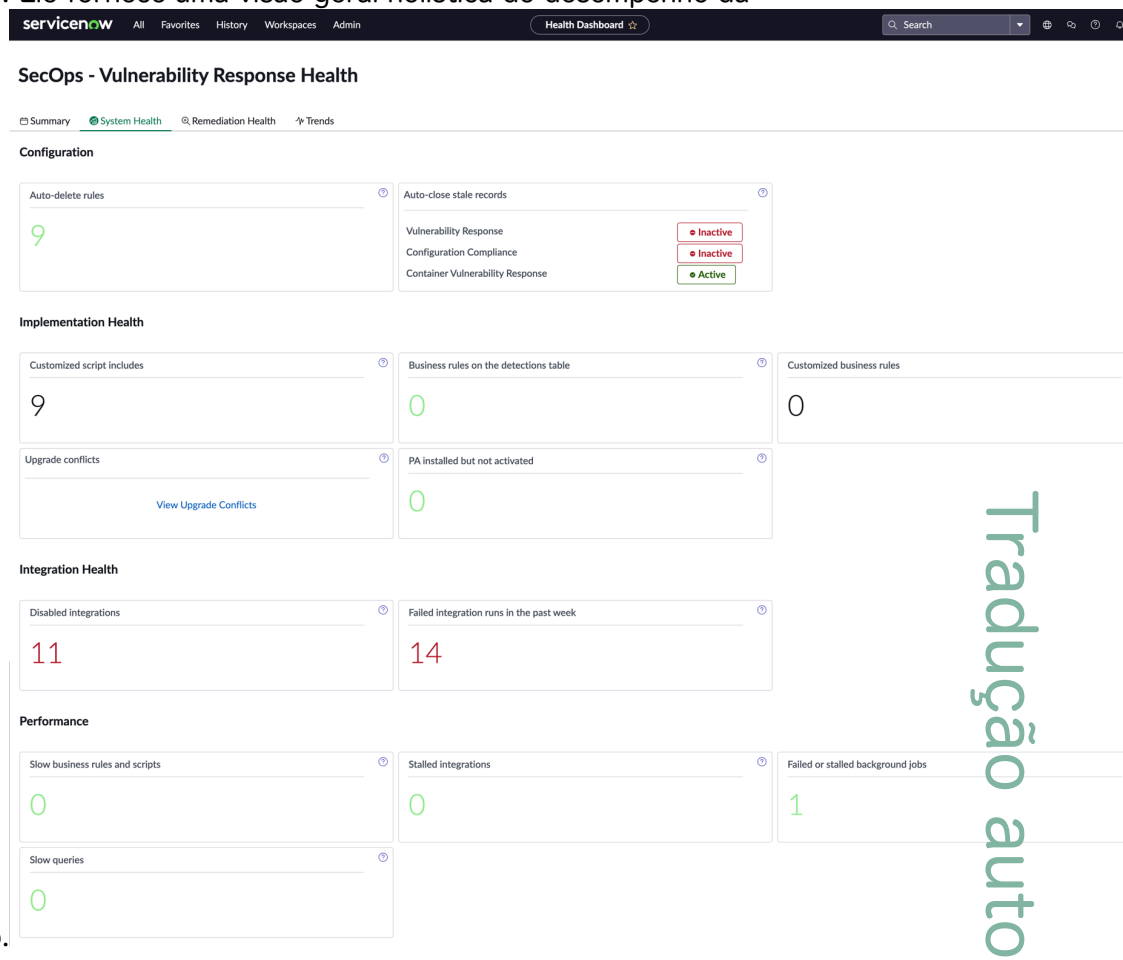
Este painel comunica a pontuação de integridade geral para a integridade de configuração e correção das aplicações de VR.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Integridade do sistema

Este painel exibe a configuração e a integridade da integração da sua implementação. Ele fornece uma visão geral holística do desempenho da implementação.

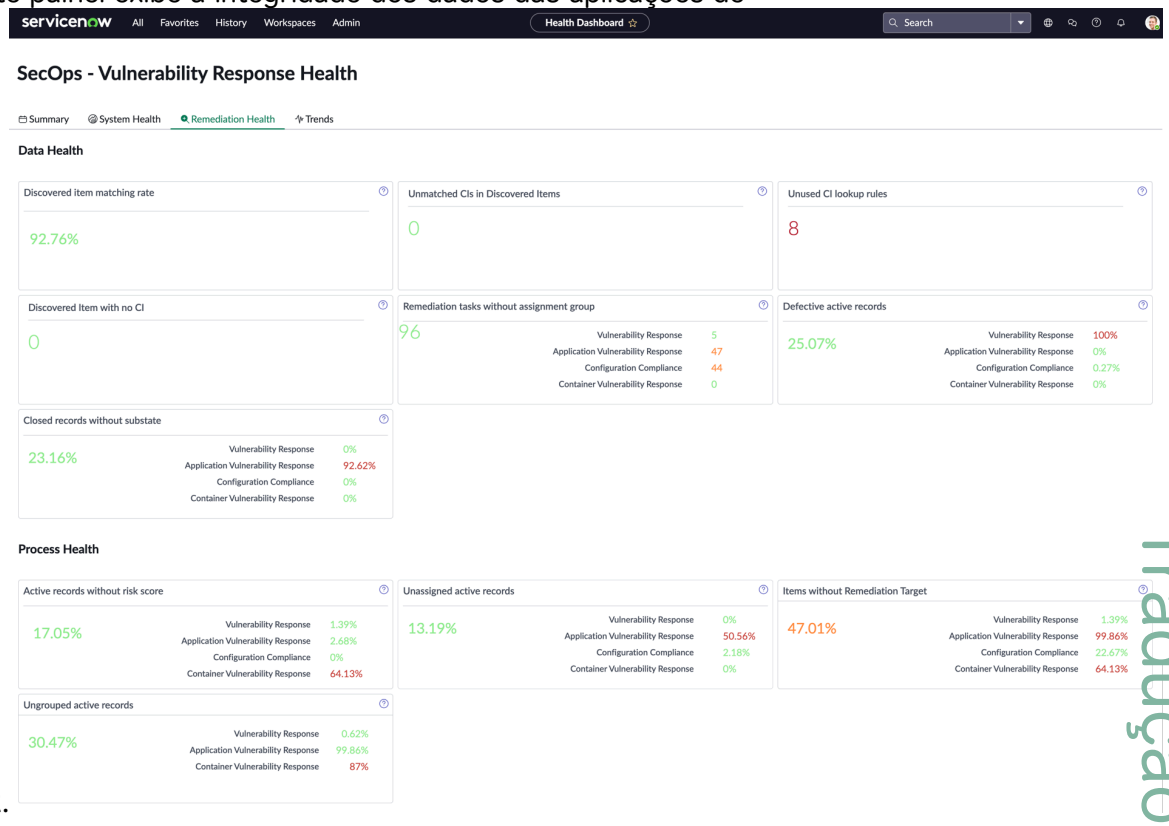


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

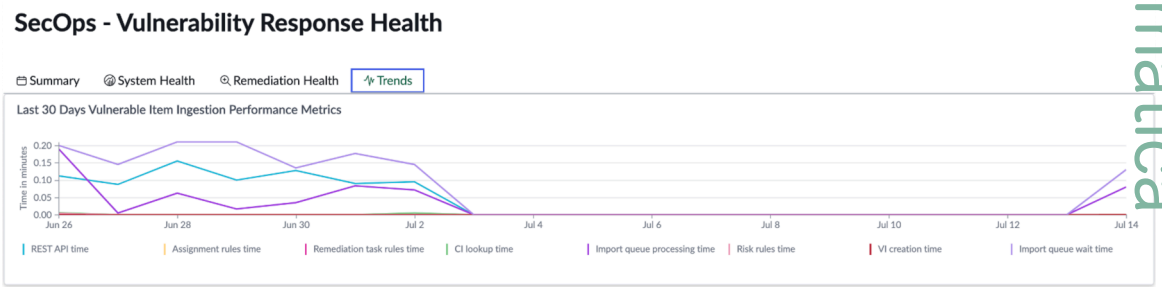
Guia Integridade de correção

Este painel exibe a integridade dos dados das aplicações de VR.



Guia Tendências

Este painel exibe as tendências das métricas de desempenho de ingestão de item vulnerável nos últimos 30 dias para as aplicações de VR.



Relatórios

Nota:
Os valores de limite fazem parte do sistema de base. Você pode configurar os valores com base em seus requisitos.

Resumo

Título	Descrição
Integridade geral	Pontuação de integridade geral das aplicações de VR. Para obter mais informações, consulte os relatórios das métricas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resumo

Título	Descrição
Configuração	Integridade geral da configuração das aplicações de VR.
Integridade da implementação	Integridade geral da implementação das aplicações de VR.
Integridade da integração	Integridade geral da integração das aplicações de VR.
Desempenho	Pontuação geral de integridade do desempenho das aplicações de VR.
Integridade de dados	Integridade geral dos dados das aplicações de VR.
Integridade do processo	Pontuação geral de integridade do processo das aplicações de VR.

Integridade do Sistema

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
Configuração				
Regras de exclusão automática	Exibe o número de regras de exclusão automática habilitadas.	Revise e resolva as regras de exclusão automática inativas.	3	1
Fechar automaticamente registros obsoletos	Fecha detecções obsoletas automaticamente. Para obter mais informações, consulte o tópico "Fechar automaticamente detecções obsoletas no Vulnerability Response" em docs.servicenow.com.	Reduza o volume de detecções obsoletas. Habilite esta opção para fechar as detecções obsoletas que não são fechadas pelos scanners.	3	1
Integridade da implementação				
Inclusões de script personalizadas	Número de "inclusões de script" personalizadas.	Minimize "inclusões de script" personalizadas para facilitar as atualizações.	10	12
Regras de negócio na tabela de detecções	Número de regras de negócios personalizadas na tabela de detecção.	Minimize as regras de negócios para facilitar os upgrades.	4	8

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integridade do Sistema

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
Regras de negócios personalizadas	Número de regras de negócios personalizadas antes da criação de registros no CMDB.	Use as regras de negócios padrão em registros.	5	8
Conflitos de upgrade	Conflitos como regras de negócios e scripts identificados em um upgrade.	Revise e resolva os conflitos de atualização.	10	15
PA instalado, mas não ativado	Indica se o painel do Performance Analytics não está habilitado.	Ative o painel do PA.	10	15
Integridade da integração				
Integrações desabilitadas	Número de integrações que foram desabilitadas.	Revise e habilite as integrações necessárias.	6	9
Execuções de integração com falha na última semana	Número de execuções de integração que não foram bem-sucedidas na última semana.	Revise e resolva a causa das execuções de integração com falha.	9	12
Desempenho				
Regras de negócios e scripts lentos	Regras de negócios e scripts com tempo médio de execução maior que 10 ms e contagem de execução maior que 10.000.	Revise e resolva as regras de negócios de execução lenta.	10	15
Integrações paradas	Número de integrações que expiraram antes da conclusão.	Revise e resolva a causa das integrações paradas.	10	15
Trabalhos em segundo plano com falha ou parados	Trabalhos em segundo plano expirados ou com falha na última semana.	Revise e resolva a causa dos trabalhos com falha.	5	10
Consultas lentas	Consultas cujo tempo médio de execução é maior que 10 ms e a contagem de	Revise e resolva as regras de negócios de execução lenta.	10	15

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integridade do Sistema

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
	execução é maior que 10.000.			

Integridade da correção

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
Integridade de dados				
Taxa de correspondência de item descoberto	Número de itens descobertos correspondentes aos ICs existentes.	Analise a integridade do seu CMDB e a lógica das regras de pesquisa de IC.	50	20
ICs incompatíveis em itens descobertos	Itens descobertos em estado incompatível.	Analise a integridade do seu CMDB e a lógica das regras de pesquisa de IC.	9	12
Regras de pesquisa de IC não utilizadas	Regras de pesquisa de IC que não estão associadas a nenhum item descoberto.	Altere o status das regras de pesquisa de IC não utilizadas para inativo.	4	6
Item descoberto sem IC	Item descoberto sem item de configuração.	Revise e reaplique as regras de pesquisa de IC.	9	12
Registros ativos com defeito	Registros sem um item de configuração ou vulnerabilidade.	Desative os ICs usando a opção CMDB CI Lifecycle Management. **Nota:** A exclusão de ICs diretamente pode resultar em VITs órfãos.	40	60
Tarefas de correção sem grupo de atribuição	Tarefas de correção ativas cujo grupo de atribuição ainda não foi atribuído.	Atribua tarefas de correção a um grupo de atribuição e revise as regras de atribuição existentes.	40	60

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integridade da correção

Título	Descrição	Considerações para melhorar o desempenho	Ponto de aviso do limite	Ponto crítico do limite
Registros encerrados sem subestado	Registros que são encerrados sem um subestado.	Forneça informações no campo Motivo ao fechar os registros.	40	50
Integridade do processo				
Registros ativos sem pontuação de risco	Registros ativos com uma pontuação de risco de 0 ou sem pontuação de risco atribuída.	Revise e resolva as regras de risco.	40	60
Registros ativos não atribuídos	Registros sem um grupo de atribuição.	Atribua um grupo aos registros e revise as regras de atribuição existentes.	30	50
Itens sem meta de correção	Itens sem data de meta de correção.	Revise e resolva as regras de destino de correção. Essas regras devem incluir todos os registros.	30	50
Registros ativos desagrupados	Registros que não estão incluídos em uma regra de tarefa de correção.	Revise as regras de tarefa de correção.	40	60

Tendências

Título	Descrição
Métricas de desempenho de ingestão de item vulnerável nos últimos 30 dias	Tempo médio para ingerir itens vulneráveis e processar várias regras nos últimos 30 dias.

Tradução automática

Modificando os valores de limite

Você pode modificar os valores de limite dos dados do painel de Integridade de VR do SecOps com base em suas preferências.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Integridade do Security Operations** > **Configuração** > **Métricas**.
2. Na página Dados do painel de integridade, abra o registro que você deseja modificar.
3. Atualize o registro e salve.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Painel Vulnerability Management (PA)

Rastreie o volume, o desempenho e o progresso das vulnerabilidades, desde a análise e detecção iniciais até a contenção ou correção. Você pode filtrar relatórios por grupo de atribuição, explorações, classificação de risco ou estado, por exemplo. Obtenha rapidamente informações sobre sua exposição à vulnerabilidade e quais serviços de negócios são afetados.

Funções necessárias de Now Platform

Função necessária: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst e usuários com sn_vul.vulnerability_read (ou que herdam a função sn_vul.vulnerability_read) e pa_viewer.

Casos de uso

Para obter exemplos de como diferentes pessoas de sua organização podem usar este painel, consulte estes casos de uso.

Usuário	Uso do painel
Gerentes de TI, analistas de TI, responsáveis pela correção de vulnerabilidades	Ajude sua organização a lidar com o aumento de incidentes de segurança devido a vulnerabilidades exploradas, determinando com eficiência quais itens vulneráveis apresentam mais risco. Esses painéis fornecem uma exibição gráfica da atividade do item vulnerável e ajudam a projetar planos de correção e andamento do status. Você pode se concentrar nos KPIs associados aos ativos afetados críticos e às vulnerabilidades de alta visibilidade.

Para exibir o painel Vulnerability Management (PA), navegue até **Vulnerability Response** > **Visão geral**.

Consulte relatórios que mostram dados de tendências ao longo do tempo. Relatórios com dados em tempo real estão listados abaixo. Exiba tendências de métricas importantes em uma programação regular para analisar seus processos de negócios gerais e identificar áreas de melhoria.

Para obter mais informações sobre como exibir seus relatórios de PA com pontuações em tempo real, consulte Exibir relatórios do Performance Analytics para Vulnerability Response [PA] em tempo real.

Tradução automática

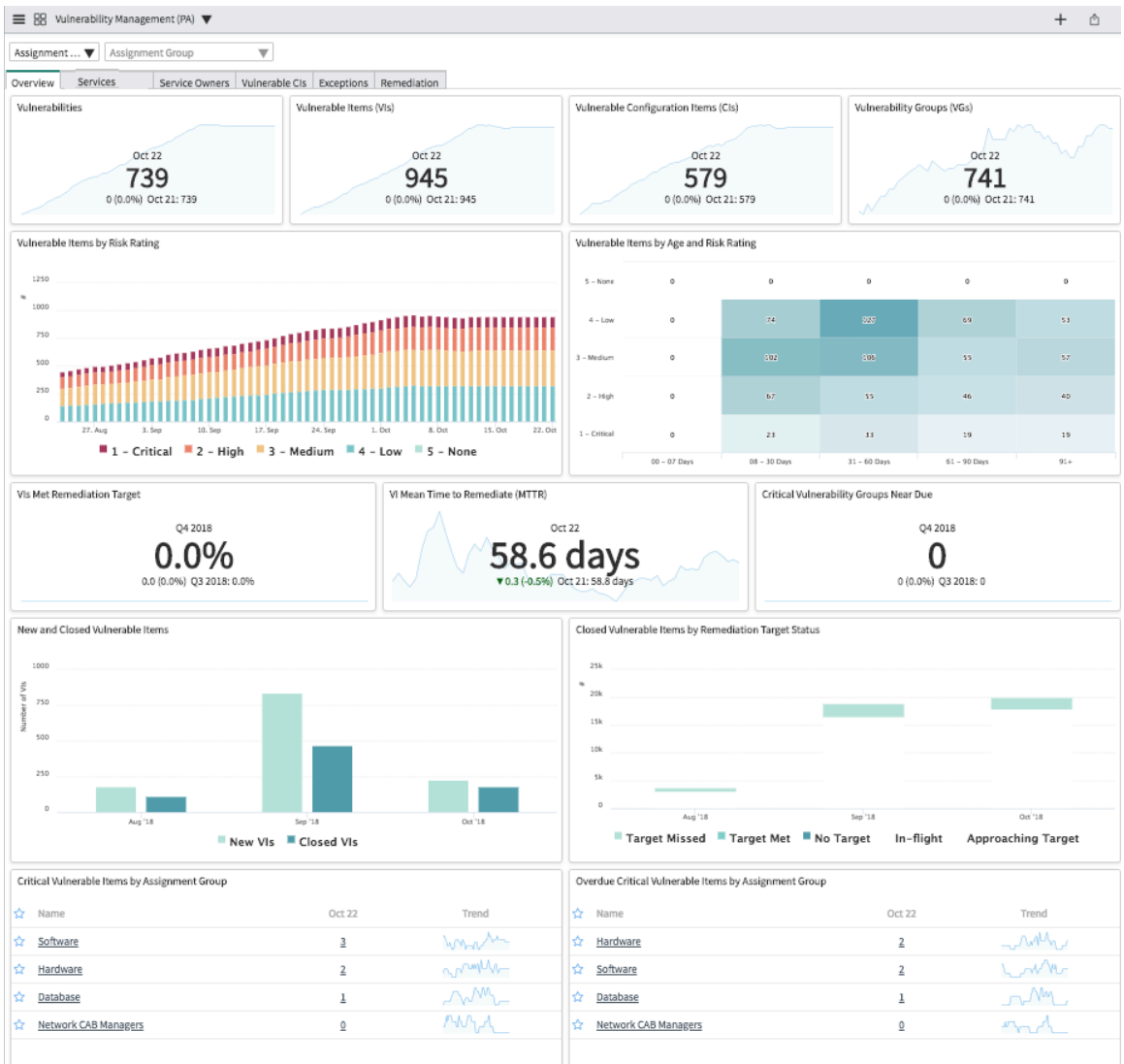
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As guias do painel do Vulnerability Management [PA]

Guia Visão geral

Este painel comunica os KPIs de risco de vulnerabilidade e predominância, ativos afetados, cumprimento da meta de correção e andamento da correção.

Na guia Visão geral, você pode exibir o relatório Itens vulneráveis críticos por grupo de atribuição que é executado com base no trabalho programado.



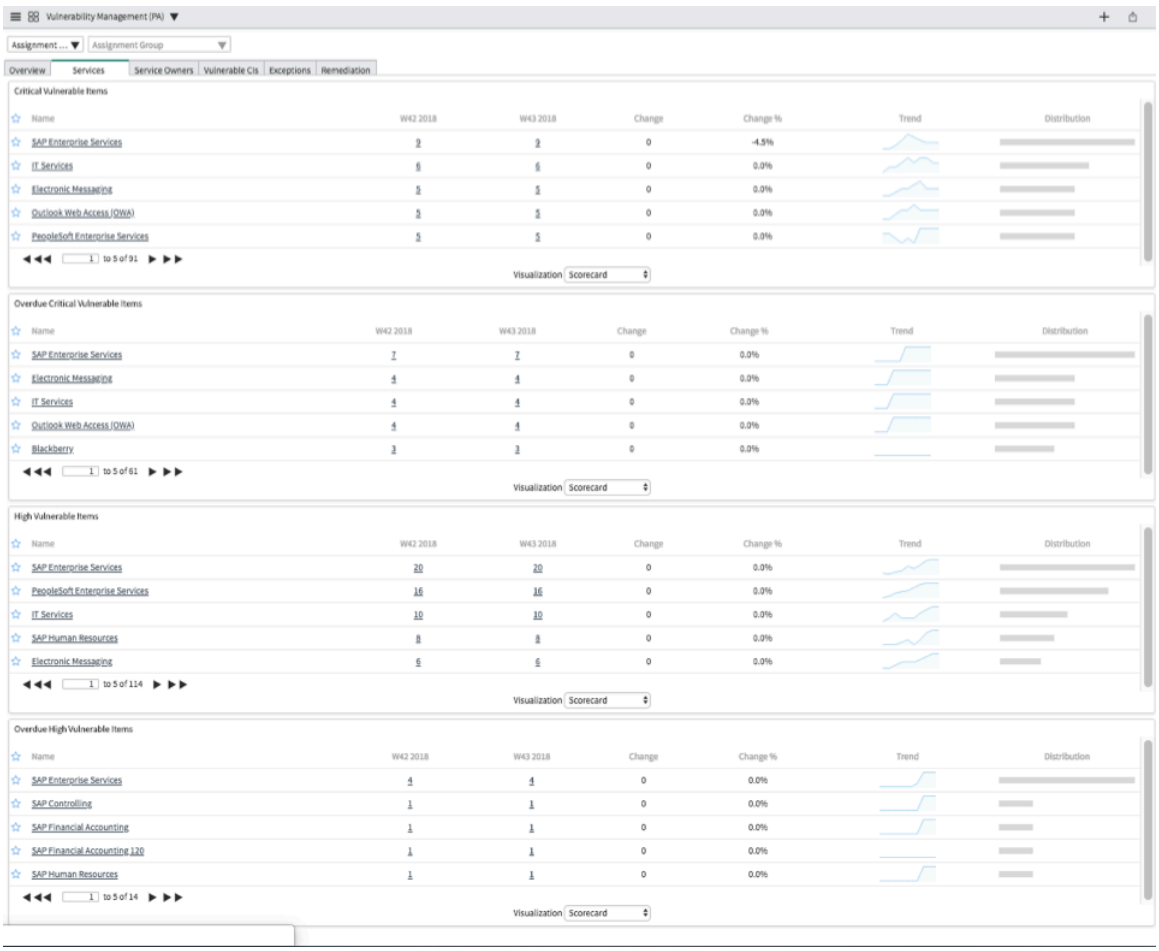
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Serviços de negócios

Este painel expõe o risco de vulnerabilidade no nível de serviço de negócios. Compartilhar essas informações em toda a organização pode ajudar os gerentes de serviço a corrigir vulnerabilidades de forma rápida e proativa e direcionar a organização para um modelo de responsabilidade compartilhada de segurança da informação.

Você pode mudar a classe de serviço para serviços técnicos ou de aplicações usando a propriedade do sistema `sn_vul.service_classifications`.

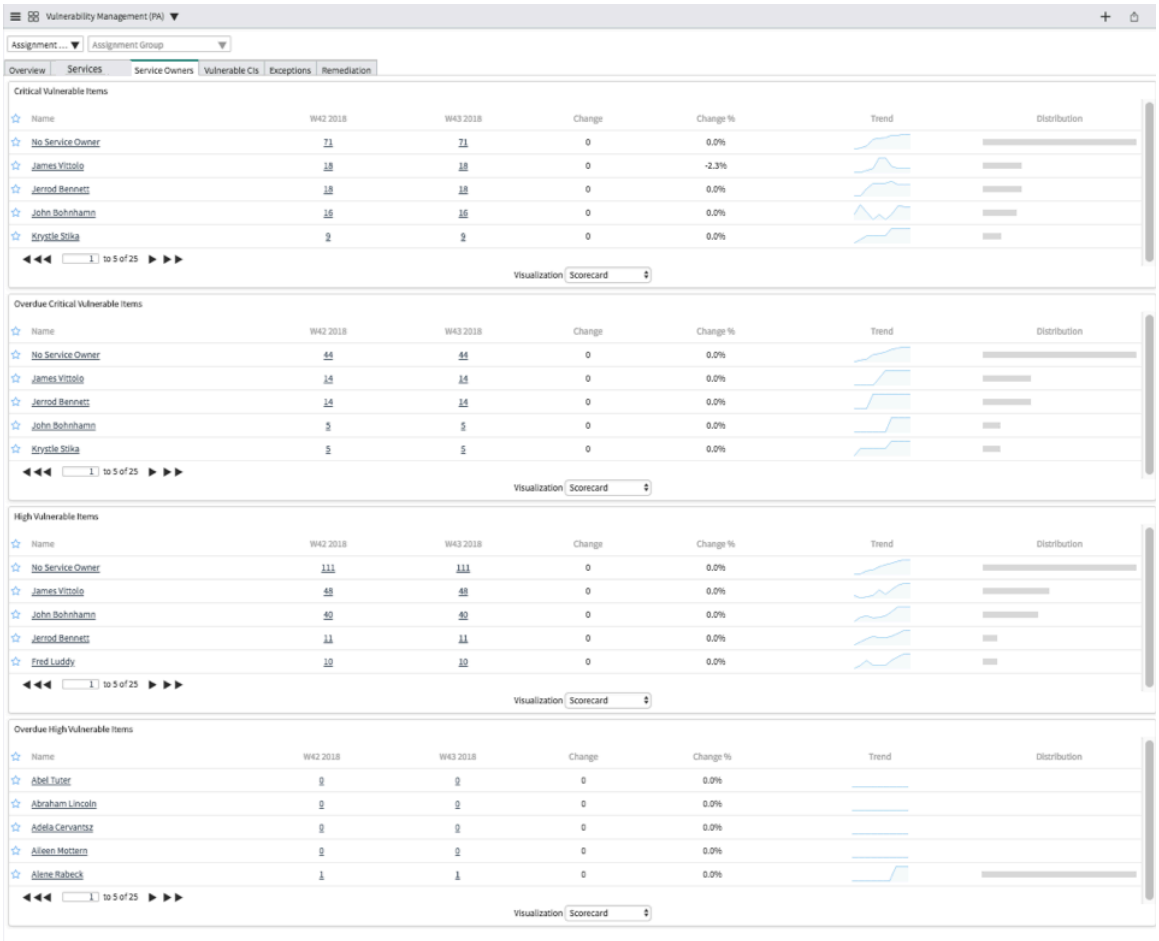


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Responsáveis pelo serviço

Este painel agrega o risco de vulnerabilidade do nível de serviço de negócios para os proprietários de serviço - os executivos responsáveis por esses serviços de negócios. Ele mostra quais executivos estão presumindo o maior risco de vulnerabilidade e quais podem precisar de mais ajuda para incentivar atividades de correção imediata.



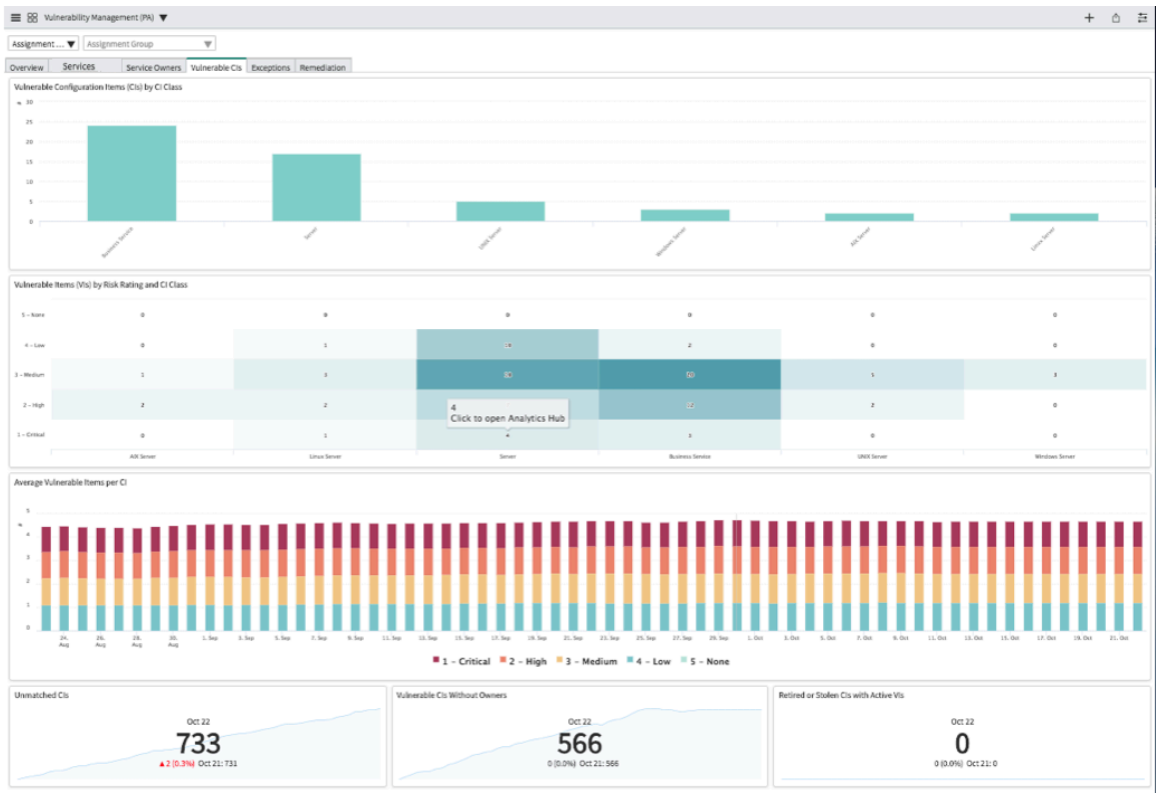
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia ICs vulneráveis

Este painel mostra o escopo e a composição de ICs com vulnerabilidades ativas e quais categorias de ICs precisam de mais atenção. Identifique ativos desativados com itens vulneráveis ativos e confirme se os ativos foram desativados. Exiba o número de ICs vulneráveis que não têm informações de propriedade, para que você possa identificar proativamente os proprietários desses ativos antes que uma vulnerabilidade crítica afete esses sistemas.

Na guia ICs vulneráveis, você pode exibir os relatórios de ICs vulneráveis sem proprietários e ICs descontinuados ou roubados com IVs ativos em tempo real.



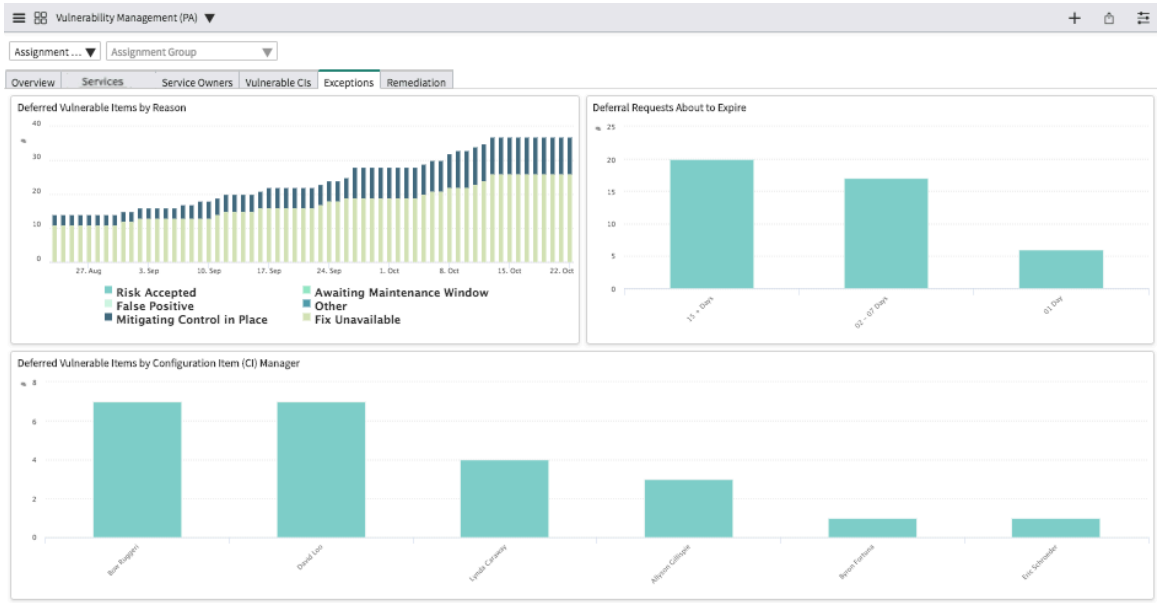
Guia Exceções

Este painel ajuda a entender onde sua organização está se arriscando devido a adiamentos potencialmente excessivos e a considerar as opções de correção.

Você pode exibir relatórios de itens vulneráveis adiados por motivo, solicitações de adiamento expirando, exceções para itens vulneráveis críticos por grupo de atribuição e solicitações de exceção por solicitante.

Tradução automática

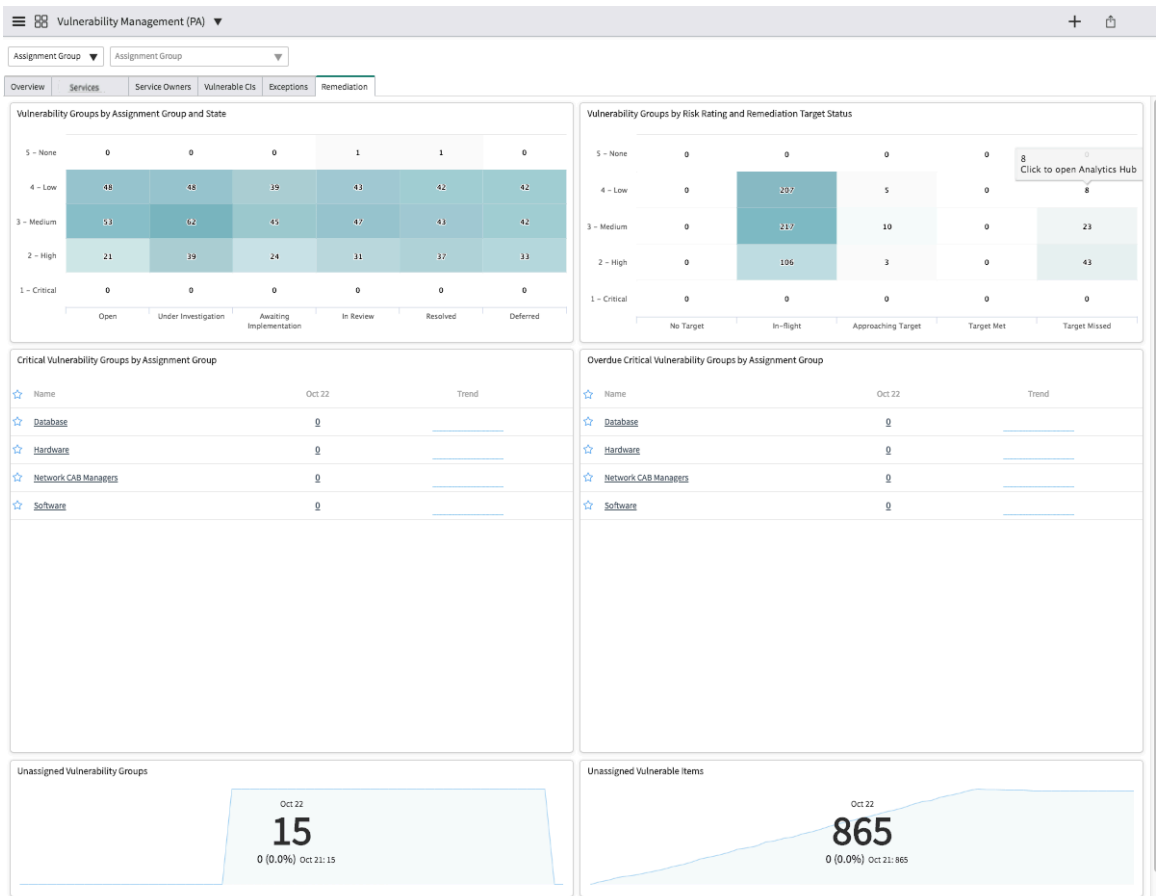
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Guia Correção

Este painel ajuda a entender o andamento das suas ações de correção e quais equipes de suporte precisam de mais assistência para concluí-las.

Na guia Correção, você pode exibir o relatório de itens vulneráveis não atribuídos em tempo real.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Indicadores

Indicadores do Vulnerability Response

Há vários indicadores usados para medir e rastrear o andamento da correção de vulnerabilidade na aplicação Vulnerability Response.

A opção de coletar registros para os indicadores está desabilitada por padrão para a aplicação Vulnerability Response. Esta opção está desabilitada para que determinados relatórios possam ser exibidos em tempo real. As informações de tendências usadas por esses indicadores ainda estarão disponíveis se você preferir habilitar a coleta de registros manualmente e exibir os registros que compõem as pontuações.

Vulnerabilidades distintas

Vulnerabilidades distintas com count_active_vi > 0. O objetivo é minimizar.

Itens vulneráveis críticos que estão atrasados e sem postergação

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Percentual de meta de correção atingida de itens vulneráveis

([[Itens vulneráveis encerrados > Meta de correção = Meta atingida]] / [[Itens vulneráveis encerrados]]) * 100. O objetivo é maximizar.

Itens vulneráveis não atribuídos

Todos os Itens vulneráveis ativos nos quais o Grupo de atribuição e os campos Atribuído a estão vazios. O objetivo é minimizar.

Itens vulneráveis críticos (serviços)

É a contagem na fonte de dados IVs ativos (serviços), que está usando a tabela: sn_vul_analytics_business_services_vi. O objetivo é minimizar.

Itens de alta vulnerabilidade atrasados (serviços)

É a contagem na fonte de dados IVs ativos (serviços), que está usando a tabela: sn_vul_analytics_business_services_vi. O objetivo é minimizar.

Tarefas de correção não atribuídas

Todas as tarefas de correção ativas em que os campos Grupo de atribuição e Atribuído a estão vazios. O objetivo é minimizar.

Itens vulneráveis críticos

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Novos itens vulneráveis

É a contagem na fonte de dados VI.New, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Itens de configuração vulneráveis

É a contagem distinta na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Soma da duração de itens vulneráveis encerrados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

É a soma na fonte de dados VI.Closed, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Tarefas de correção sem postergação

É a contagem na fonte de dados VG.Active, que está usando a tabela: sn_vul_vulnerability. O objetivo é minimizar.

Tempo médio de correção do item vulnerável

[[Soma da duração de itens vulneráveis encerrados]]/[[Itens vulneráveis encerrados]]

Itens vulneráveis críticos atrasados (serviços)

É a contagem na fonte de dados IVs ativos (serviços), que está usando a tabela: sn_vul_analytics_business_services_vi. O objetivo é minimizar.

Itens de configuração desativados

É a contagem distinta na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Solicitações de postergação

É a contagem na fonte de dados Solicitações de postergação ativas, que está usando a tabela: sn_vul_change_approval. O objetivo é minimizar.

Itens vulneráveis por itens de configuração

É a contagem na fonte de dados ICs com IVs ativos, que está usando a tabela: sn_vul_analytics_vi_ci_class. O objetivo é minimizar.

Itens vulneráveis encerrados

Os itens vulneráveis encerrados são medidos diariamente em unidades numéricas. O objetivo é maximizar.

Itens de configuração incompatíveis

Lista os hosts descobertos por scanners de vulnerabilidade de terceiros que não correspondem a nenhum IC existente no CMDB.

Tarefas de correção crítica que estão atrasadas e sem postergação

É a contagem na fonte de dados VG.Active, que está usando a tabela: sn_vul_vulnerability. O objetivo é minimizar.

Itens de configuração vulneráveis sem grupo de suporte

É a contagem na fonte de dados VI.Open, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Tarefas de correção crítica sem postergação

É a contagem na fonte de dados VG.Active, que está usando a tabela: sn_vul_vulnerability. O objetivo é minimizar.

Itens vulneráveis com postergação

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Itens de alta vulnerabilidade (serviços)

É a contagem na fonte de dados IVs ativos (serviços), que está usando a tabela: sn_vul_analytics_business_services_vi. O objetivo é minimizar.

Itens de configuração distintos com itens vulneráveis ativos

É a contagem distinta na fonte de dados ICs com IVs ativos, que está usando a tabela: sn_vul_analytics_vi_ci_class. O objetivo é minimizar.

Número médio de itens vulneráveis por item de configuração

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

[[Itens vulneráveis ativos]] / [[ICs vulneráveis]]. O objetivo é minimizar.

Tarefas de correção

É a contagem na fonte de dados VG.Active, que está usando a tabela: sn_vul_vulnerability. O objetivo é minimizar.

Itens vulneráveis críticos com postergação

É a contagem na fonte de dados VI.Active, que está usando a tabela: sn_vul_vulnerable_item. O objetivo é minimizar.

Solicitações de postergação (criadas)

É a contagem na fonte de dados Closed.Requests, que está usando a tabela: sn_vul_change_approval. O objetivo é minimizar.

Detalhamentos

Os seguintes nomes de detalhamento se aplicam aos indicadores no painel:

- Idade
- Momento do fechamento
- Grupo de atribuição
- Classe do IC
- Gerenciador de IA
- Idade do Adiamento
- Motivo do Adiamento
- Solicitantes da exceção
- Explorar Vetor de Ataque
- Explorar Itens Existentes
- Explorar Nível de Habilidade
- Regra de destino de correção
- Status do Destino de Correção
- Status da Meta de Correção (Encerrado)
- Pontuação de risco
- Serviço
- Importância do Serviço
- Proprietário de serviço
- Gravidade
- Estado

Fonte de detalhamento

- Grupo de atribuição: aplica-se a relatórios IV ou e RT
- Exploração existente: aplica-se a relatórios de IV.
- Explorar vetor de ataque: aplica-se a relatórios de IV.
- Explorar nível de habilidade: aplica-se a relatórios de IV.
- Status do destino de correção: aplica-se a relatórios IV e RT.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Classificação de risco: aplica-se a relatórios IV e RT.
- Estado: aplica-se a relatórios IV e RT.

Visualizações de dados

Título	Tipo	Descrição
Vulnerabilidades	Pontuação	Número de vulnerabilidades associadas a um ou mais itens vulneráveis ativos.
Itens vulneráveis (IVs)	Pontuação	Número de itens vulneráveis ativos (não encerrados).
Itens de configuração (ICs) vulneráveis	Pontuação	Número de itens de configuração (ICs) associados a um ou mais itens vulneráveis ativos.
Tarefas de correção	Pontuação	Número de tarefas de correção ativas (não encerradas).
Itens vulneráveis por classificação de risco	Barra de barra	Número de itens vulneráveis ativos, agrupados por classificação de risco no período selecionado.
Itens vulneráveis por idade e classificação de risco	Mapa térmico	Número de itens vulneráveis ativos agrupados por classificação de risco e idade (em dias).
Meta de Correção Atendida de IVs	Pontuação	Porcentagem de itens vulneráveis encerrados que atingiram suas datas de destino de correção nos trimestres atuais e anteriores. As metas de correção são calculadas a partir da data da última abertura mais o número de dias (medidos como incrementos de 24 horas).
Tempo médio de correção (MTTR) dos IVs	Pontuação	O tempo médio para corrigir (encerrar) um item vulnerável, exibido como uma média de 30 dias de execução. **Nota:** O valor da Idade do encerramento é calculado quando os dados são coletados. O valor é a diferença entre a data last_opened e a data e hora do trabalho de coleta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título	Tipo	Descrição
Tarefas de correção críticas próximas ao vencimento	Pontuação	Número de tarefas de correção ativas se aproximando da data de meta de correção. A data de destino de correção de uma tarefa de correção é definida como a data de vencimento mais próxima que pertença a um item vulnerável ativo no grupo. As metas de correção são calculadas a partir da data da última abertura mais o número de dias (medidos como incrementos de 24 horas). Este relatório exclui tarefas de correção adiadas.
Itens vulneráveis novos e encerrados	Barra de barra	Número de itens vulneráveis novos e encerrados no período selecionado. **Nota:** O valor da Idade do encerramento é calculado quando os dados são coletados. O valor é a diferença entre a data last_opened e a data e hora do trabalho de coleta.
Itens vulneráveis encerrados por status da meta de correção	Barra de barra	Número de itens vulneráveis encerrados, agrupados por status de destino de correção no período selecionado. **Nota:** O valor da Idade do encerramento é calculado quando os dados são coletados. O valor é a diferença entre a data last_opened e a data e hora do trabalho de coleta.
Itens vulneráveis críticos por grupo de atribuição	Lista e linha Ícone	Número de itens vulneráveis ativos, com uma classificação de risco crítica, agrupados por grupo de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título	Tipo	Descrição
Itens vulneráveis críticos e atrasados por grupo de atribuição	Lista e linha Ícone	Número de itens vulneráveis ativos com uma classificação de risco crítica e suas datas de destino de correção, agrupadas por grupo de atribuição. As metas de correção são calculadas a partir da data da última abertura mais o número de dias (medidos como incrementos de 24 horas). Este relatório exclui itens vulneráveis adiados.

Serviços de negócio

Nome	Tipo	Descrição
Itens vulneráveis críticos	Lista, linha e barra de distribuição Ícone de de de	Número de itens vulneráveis ativos com uma classificação de risco crítica, agrupados por serviço de negócios. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação.
Itens vulneráveis críticos que estão atrasados	Lista, linha e barra de distribuição Ícone de de de	Número de itens vulneráveis ativos com uma classificação de risco crítica e suas datas de destino de correção, agrupadas por serviço de negócios. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação. Este relatório exclui itens vulneráveis adiados.
Itens de alta vulnerabilidade	Lista, linha e barra de distribuição Ícone de de de	Número de itens vulneráveis ativos com uma classificação de alto risco, agrupados por serviço de negócios. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Serviços de negócio

Nome	Tipo	Descrição
		A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação.
Itens de alta vulnerabilidade atrasados	Lista, linha e barra de distribuição Ícone de de de	Número de itens vulneráveis ativos com uma classificação alta de risco e suas datas de destino de correção, agrupados por serviço de negócios. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação. Este relatório exclui itens vulneráveis adiados.

Responsáveis pelo serviço

Nome	Tipo	Descrição
Itens vulneráveis críticos	Lista, linha e barra de distribuição Ícone de de de	Número de itens vulneráveis ativos com uma classificação de risco crítica, agrupados por responsável pelo serviço de negócio. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação.
Itens vulneráveis críticos que estão atrasados	Lista, linha e barra de distribuição Ícone de de de	Número de itens vulneráveis ativos com uma classificação de risco crítica e suas datas de destino de correção, agrupados por responsável pelo serviço de negócio. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação. Este relatório exclui itens vulneráveis adiados.
Itens de alta vulnerabilidade	Lista, linha e barra de distribuição Ícone de de de	Número de itens vulneráveis ativos com uma classificação de alto risco, agrupados por responsável pelo serviço de negócios.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Responsáveis pelo serviço

Nome	Tipo	Descrição
		Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação.
Itens de alta vulnerabilidade atrasados	Lista, linha e barra de distribuição Ícone de de de	Número de itens vulneráveis ativos com uma classificação alta de risco e suas datas de destino de correção, agrupados por responsável pelo serviço de negócios. Exibe uma média semanal da semana atual e anterior, a diferença entre as duas semanas (em contagem e porcentagem) e uma tendência. A barra de distribuição exibe a diferença entre todos os valores na página atual do cartão de pontuação. Este relatório exclui itens vulneráveis adiados.

ICs Vulneráveis

Nome	Tipo	Descrição
Itens de configuração (ICs) vulneráveis por classe de IC	Barra de barra	Números de itens de configuração com vulnerabilidades ativas, agrupados por classe de IC no CMDB.
Itens vulneráveis (VIs) pela Classe de IC	Mapa de Árvore Mapa de	Número de IVs ativos divididos por classe de IC.
Média de Itens vulneráveis por IC	Barra de barra	Número médio de itens vulneráveis que pertencem a um item de configuração, agrupados conforme a classificação de risco.
ICs incompatíveis	Pontuação	Número de itens de configuração importados que não correspondem a nenhum IC existente no CMDB.
ICS vulneráveis sem grupo de suporte	Pontuação	Número de itens de configuração vulneráveis que não têm um grupo de suporte atribuído.
ICs desativados ou roubados com IVs ativos	Pontuação	Número de itens de configuração marcados como Desativados ou **Roubados** no **CMDB** que têm itens vulneráveis ativos.

Exceções

Nome	Tipo	Descrição
Itens vulneráveis adiados por motivo	Barra de barra	Número de itens vulneráveis adiados, agrupados por motivo de adiamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exceções

Nome	Tipo	Descrição
Solicitações de postergação prestes a expirar	Barra de barra	Número de solicitações de adiamento associadas a tarefas de correção ou itens vulneráveis que estão prestes a ser reabertos para revisão. Eles são agrupados pelo número de dias restantes até a reabertura. Se as notificações por e-mail forem definidas, um e-mail será enviado.
Itens vulneráveis adiados por gerenciador de item de configuração (IC)	Barra de barra	Número de itens vulneráveis adiados agrupados pelo gerente para o item de configuração associado.

Correção

Nome	Tipo	Descrição
Tarefas de correção por classificação de risco e estado	Mapa térmico	Número de tarefas de correção ativas agrupadas por classificação de risco e estado.
Tarefas de correção por classificação de risco e status do destino de correção	Mapa térmico	Número de tarefas ativas agrupadas por classificação de risco e status de meta de correção. Este relatório exclui itens vulneráveis adiados.
Tarefas de correção críticas por grupo de atribuição	Lista e linha Ícone	Número de tarefas de correção ativas com uma classificação de risco crítica agrupadas por grupo de atribuição. Este relatório exclui tarefas de correção adiadas.
Tarefas de correção críticas em atraso por grupo de atribuição	Lista e linha Ícone	Número de tarefas de correção ativas com uma classificação de risco crítica e suas datas de destino de correção, agrupadas por grupo de atribuição. Este relatório exclui tarefas de correção adiadas.
Tarefas de correção não atribuídas	Pontuação	Número de tarefas de correção ativas sem um designado ou grupo de atribuição.
Itens vulneráveis não atribuídos	Pontuação	Número de itens vulneráveis ativos sem um designado ou grupo de atribuição.

Exibir Performance Analytics para Vulnerability Response [PA] relatórios em tempo real

Para gerenciar seus itens vulneráveis (IVs) mais importantes e ajudá-lo a corrigi-los rapidamente, exiba relatórios sob demanda, em tempo real, no painel Vulnerability Management (PA). A aplicação Performance Analytics para Vulnerability Response está disponível com uma assinatura separada do ServiceNow Store.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Para obter mais informações sobre os relatórios de Performance Analytics para Vulnerability Response, consulte Painel do Vulnerability Management [PA].

Para obter mais informações sobre a configuração e a instalação da aplicação Performance Analytics para Vulnerability Response, consulte Instalar e configurar a aplicação Performance Analytics para Vulnerability Response [PA].

Se não for exibido, para exibir o painel, navegue até **Vulnerability Response** > **Visão geral**. Na parte superior do painel, as guias de relatório são exibidas.

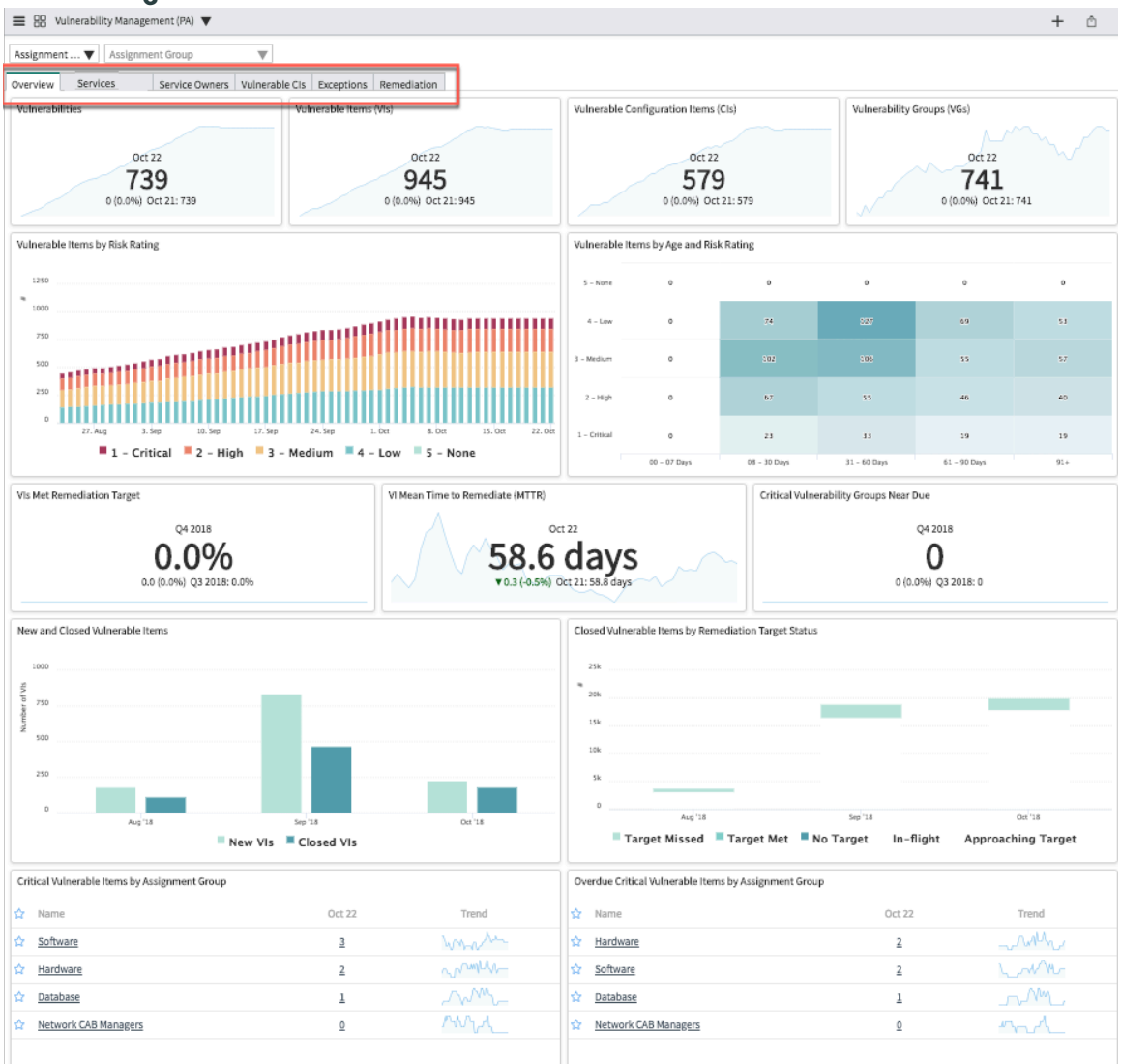
A partir da versão 19.0 do Vulnerability Response, este painel também pode ser exibido na IU da nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique no ícone**Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Painéis no Vulnerability Manager Workspace e Painéis no IT Remediation Workspace.

Nota:
Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Visão geral



Exiba os relatórios a seguir nas guias do painel Vulnerability Management (PA) em tempo real.

- Guia Visão geral
  - Itens vulneráveis críticos por grupo de atribuição
- Guia ICs vulneráveis:
  - ICs vulneráveis sem proprietários
  - ICs desativados ou roubados com IVs ativos
- Guia Exceções:
  - Itens vulneráveis adiados por motivo
  - Solicitações de postergação prestes a expirar
  - Itens vulneráveis adiados por gerente de CIO
- Guia Correção:
  - Itens vulneráveis não atribuídos

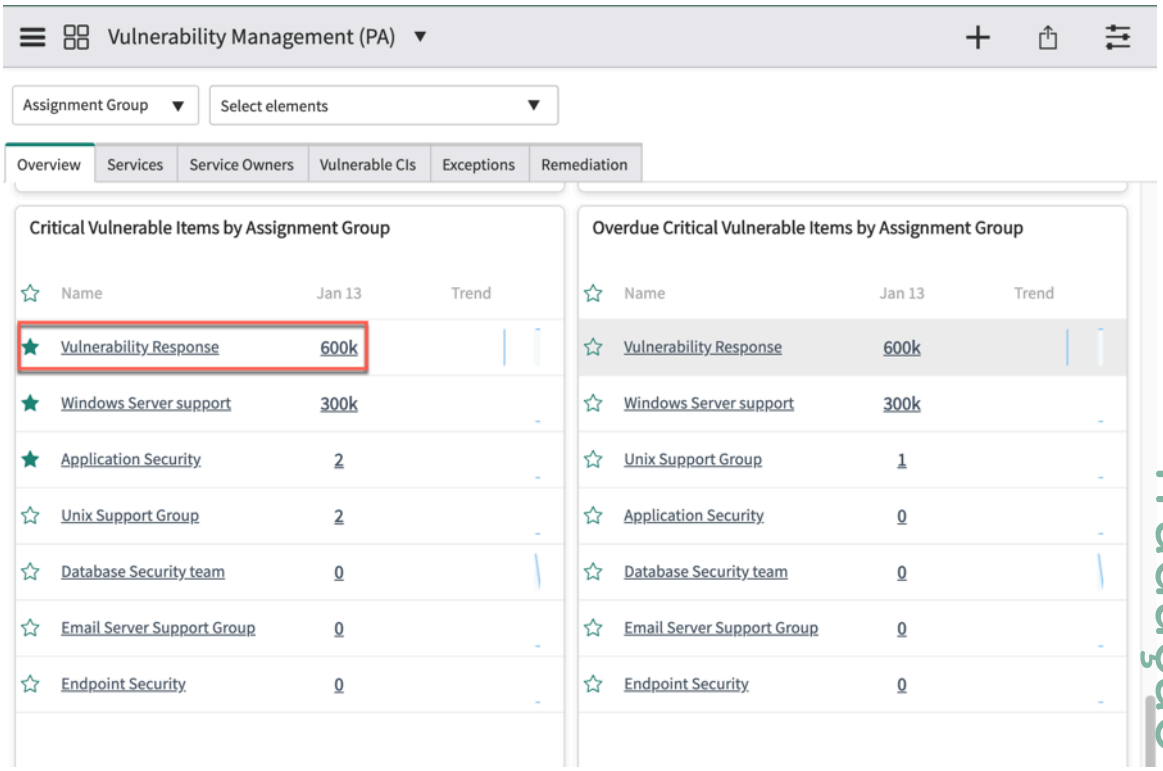
Para exibir pontuações em tempo real, com uma das guias selecionadas que contém relatórios em tempo real, siga estas etapas:

Tradução automática

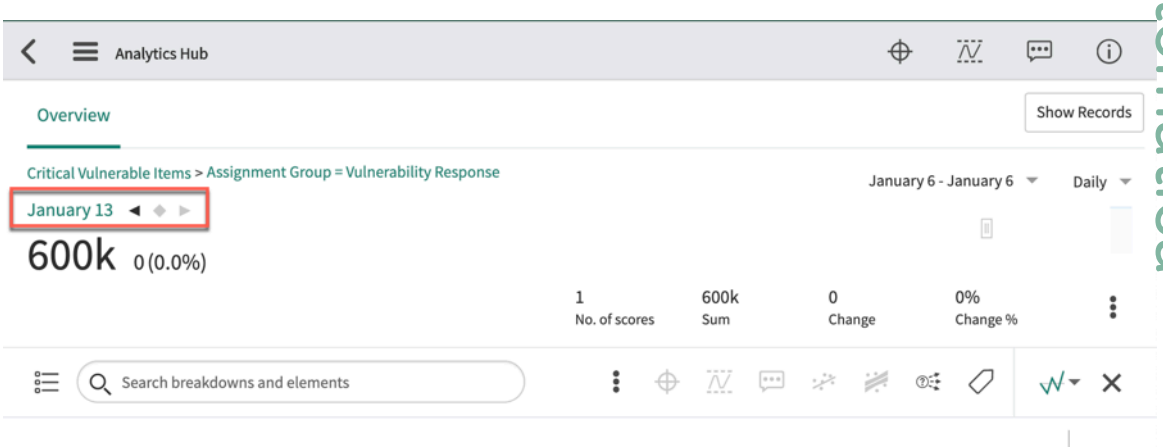
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. No relatório, por exemplo, Itens vulneráveis críticos por grupo de atribuição, clique em um dos links exibidos.



2. No registro exibido, clique na data.

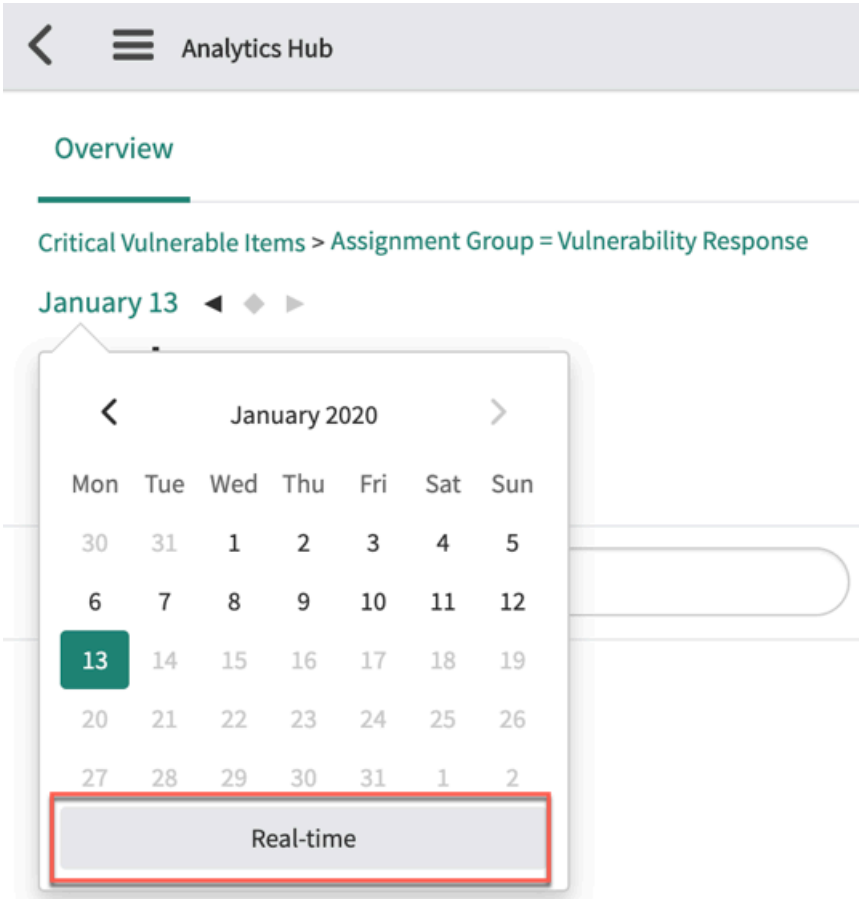


3. No calendário exibido, clique em Tempo real.

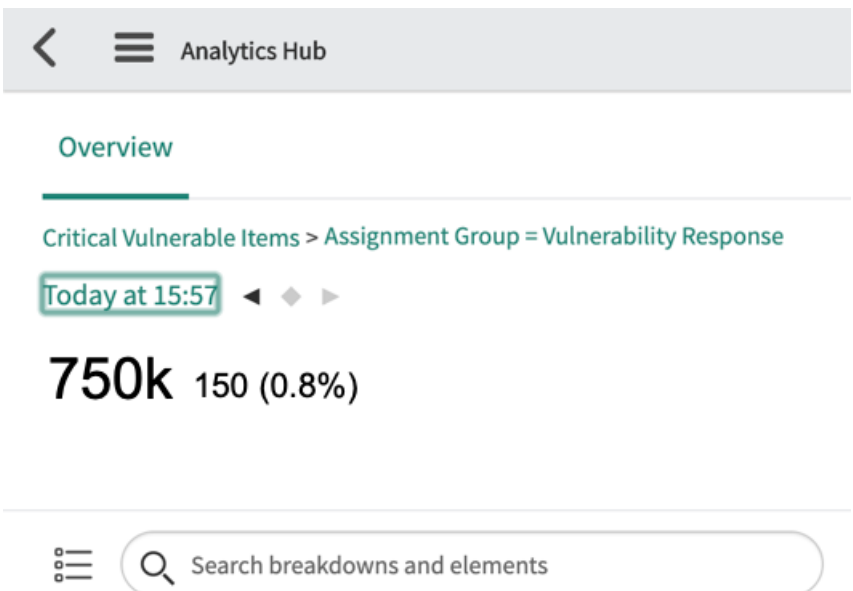
   Se um relatório não oferecer suporte a uma pontuação em tempo real, o botão Tempo real não será exibido no calendário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Pode levar alguns minutos para que o valor seja atualizado. A data atual, os registros, o número de novos registros desde o último relatório e a mudança percentual do último relatório também são exibidos.



4. **Opcional:** Para exibir os registros que compõem o relatório, com o relatório em tempo real exibido, no canto superior direito, clique em **Mostrar registros**.
   Uma lista de registros que compõem a pontuação é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir os Performance Analytics indicadores para Vulnerability Response [PA]

Exiba indicadores Performance Analytics automatizados e formulados que representam os dados de vulnerabilidade em sua instância.

Antes de Iniciar

A opção de coletar registros dos indicadores está inativa por padrão para a aplicação Performance Analytics - Content Pack Vulnerability Response. Esta opção está desabilitada para que determinados relatórios possam ser exibidos em tempo real. As informações de tendências usadas por esses indicadores ainda estarão disponíveis se você preferir habilitar a coleta de registros manualmente e exibir os registros que compõem as pontuações.

Nota:
Ativar a coleta de registros em um indicador pode afetar seu desempenho e aumentar consideravelmente o tempo e a memória necessários para executar o trabalho de coleta de dados.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) ou pa.viewer

Por Que e Quando Desempenhar Esta Tarefa

Vulnerability Response tem indicadores automatizados e formulados.

Termos-chave

Indicador de PA

Define uma medição de desempenho feita em intervalos regulares de um serviço de negócios, atividade ou comportamento organizacional, por exemplo, itens vulneráveis críticos e atrasados não adiados.

Origem do indicador de PA

Conjuntos de dados que filtram registros de uma tabela ou exibição de banco de dados, por exemplo, IV ativo.

Coletar registros

Quando habilitado, armazena registros na memória e fornece acesso ao Hub de análise.

Detalhamentos

Filtro de detalhamentos e registros coletados por grupo. Os detalhamentos podem aumentar o uso da memória, especialmente à medida que o número e a diversidade aumentam.

Exclusões de detalhamento

As exclusões removem determinados detalhamentos, o que pode reduzir o consumo de memória.

Procedimento

1. Para obter indicadores automatizados, navegue até **Performance Analytics** > **Indicadores** > **Indicadores Automatizados**.
2. Para obter indicadores formulados, navegue até **Performance Analytics** > **Indicadores de Fórmula**.

   Para obter informações detalhadas sobre indicadores, consulte Indicadores do Performance Analytics .
3. Em qualquer um dos casos, pesquise em **Aplicação** > **Performance Analytics**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

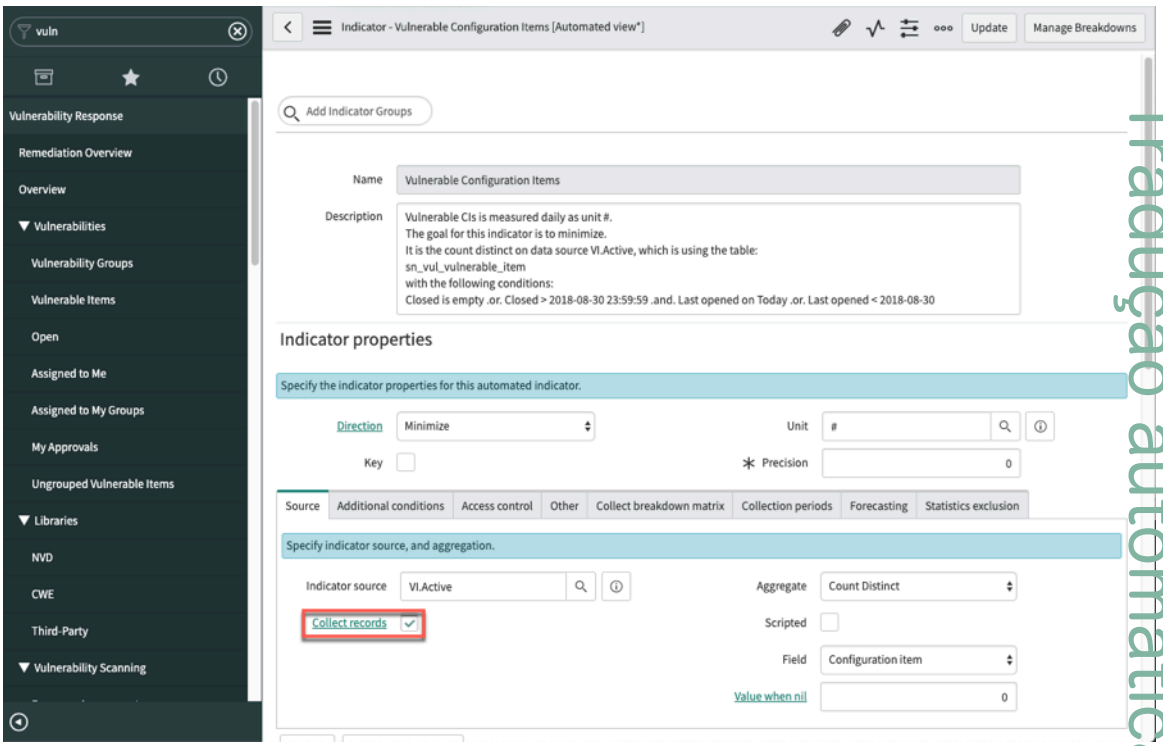
Nota:

Se não estiver na exibição padrão, adicione a coluna **Aplicação** usando o ícone de) no canto superior esquerdo da página. A coluna Aplicação é exibida no menu suspenso Pesquisar.

4. **Opcional:** Para habilitar Coletar registros em um indicador do Performance Analytics para Vulnerability Response, siga estas etapas:

   a. Com a lista de indicadores automatizados exibida, na coluna Nome, clique no indicador para o qual você deseja habilitar a coleta de registros.
   O registro do indicador é exibido.

   b. Na seção Propriedades do indicador com a guia Origem selecionada, marque a caixa de seleção Coletar registros.



Tradução automática

   c. Escolha um para continuar.

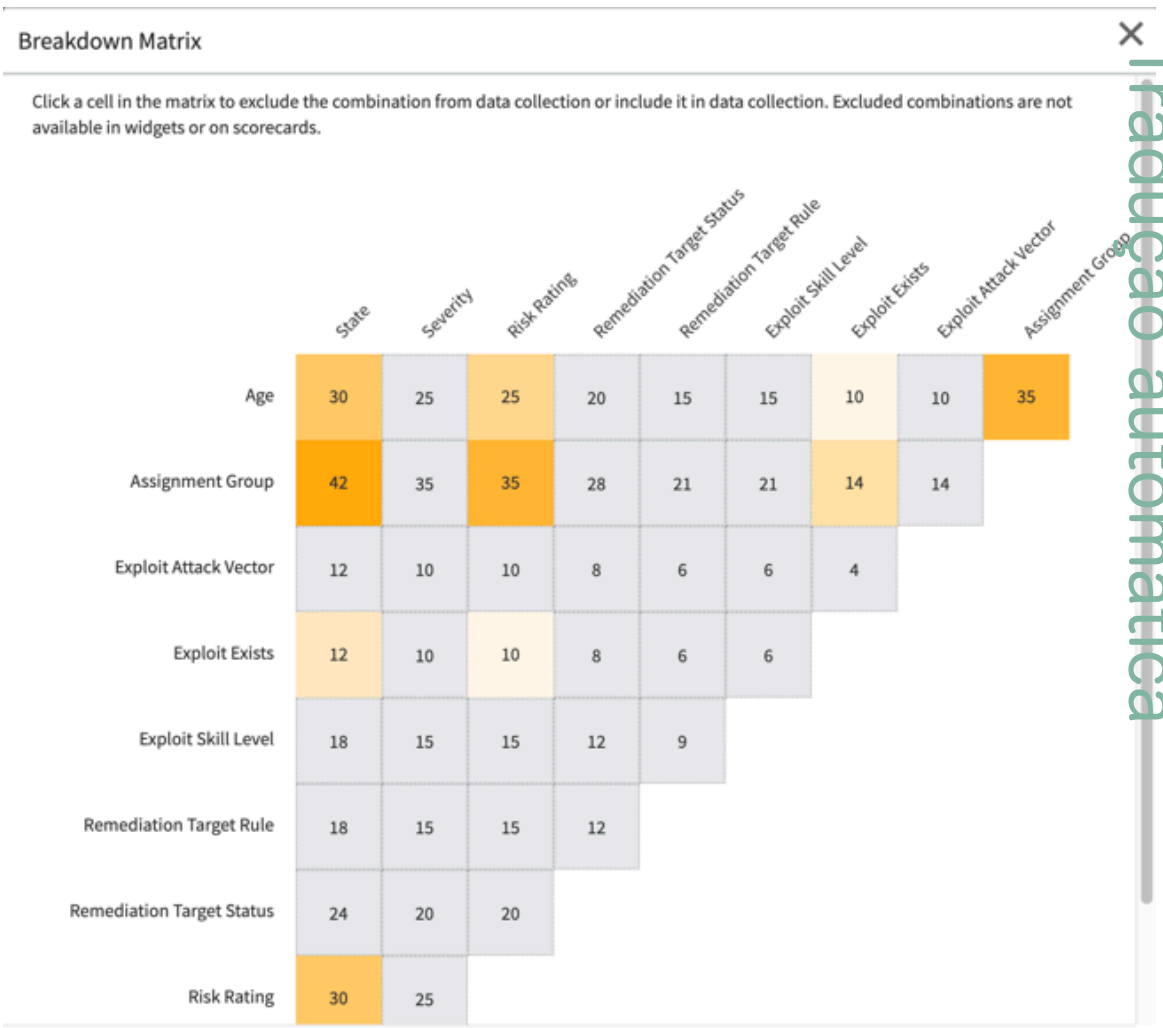
Opção	Descrição
Atualizar	Salve suas edições e retorne à lista de Indicadores.
Gerenciar Detalhamentos **Nota:** Se você optar por reativar os detalhamentos de segundo nível, poderá aumentar significativamente o consumo de memória e tornar mais lento o trabalho de coleta de dados.	Reative os detalhamentos de segundo nível para os indicadores listados ou edite os detalhamentos de outros indicadores. (Optional) Para obter mais informações sobre os detalhamentos do Performance Analytics, consulte Detalhamentos do Performance Analytics .

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Por padrão, as exclusões de detalhamento de segundo nível foram aplicadas aos seguintes indicadores: ▪ Itens de configuração vulneráveis ▪ ICs descontinuados ▪ IVs adiados	

d. Clique **em Gerenciar Detalhamentos**.

e. No formulário exibido, clique em **Configurar matriz de detalhamento**.
O formulário Matriz de detalhamento é exibido. As combinações excluídas são selecionadas e exibidas com cores, conforme mostrado na figura a seguir.



f. Para remover a exclusão e reativar uma combinação excluída, clique em uma célula selecionada.

g. No canto superior direito do formulário, clique em **Fechar** para retornar o formulário Gerenciar detalhamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

h. Clique na seta de voltar para retornar ao registro do indicador.

i. Clique em **Atualizar** para salvar suas edições e retornar à lista de Indicadores.

Vulnerability Response informações de referência

Os tópicos a seguir fornecem links, informações de referência, solução de problemas e artigos de conhecimento, além de dados de campo nos formulários e registros encontrados em Vulnerability Response.

Listados abaixo estão alguns links para outros recursos que podem ser úteis, começando com um link para os links da base de conhecimento para o artigo de suporte e solução de problemas VR/CC na Base de conhecimento HI.

- Links da base de conhecimento para suporte e solução de problemas VR/CC
- Para obter mais informações sobre aplicações e compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e mudanças de esquema de versão .
- Vídeos do Security Operations
- Desenvolver treinamento
- Desenvolver documentação
- Trabalhe com um especialista em implementação para alcançar os resultados de negócios desejados com a Central de sucesso do cliente .
- Faça um curso do Vulnerability Response para adquirir conhecimento e obter ROI mais rapidamente. Para se inscrever, consulte Treinamento e certificação da ServiceNow .
- Localizar componentes instalados com uma aplicação
- Orquestração do Vulnerability Response
- Dicas para escrever integrações
- Faça ou responda perguntas na comunidade do Security Operations
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Check-list de implementação da aplicação Vulnerability Response

Esta check-list lista as etapas necessárias para uma implementação básica da aplicação Vulnerability Response em sua instância Now Platform®. Quando você tiver concluído essas tarefas, o sistema de base estará pronto para operação e verificação.

Antes de Iniciar

Funções necessárias: admin para baixar e ativar aplicações e atribuir funções, sn_vul.vulnerability_admin para configurar Vulnerability Response.

Procedimento

1. Considere criar e imprimir um PDF desta check-list para que você possa marcar as tarefas conforme as conclui.

2. Para gerar um PDF, clique no ícone **Salvar como PDF** ( ) na parte superior do tópico e clique em Tópico selecionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerability Response tarefas de check-list de implementação básica para administrador

Item	Descrição
☐	Como um usuário com a função de administrador, verifique se você obteve todos os direitos e baixou (**Instale**) as seguintes aplicações da ServiceNow® Store na sua instância Now Platform : ○ Vulnerability Response ○ Vulnerability Response Integração com o NIST National Vulnerability Database ○ Qualys Integração para Security Operations **a.** Para verificar se as aplicações estão disponíveis em sua instância, navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e pesquise por [sn_vul], [sn_vul_nvd] e [sn_vul_qualys]. **b.** Se você não conseguir localizar as aplicações, consulte Security Operations e o ServiceNow Store para obter mais informações sobre como obter o direito e baixar as aplicações.
☐	Como um usuário com a função de administrador, navegue **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Instalação de aplicação de integração** e ative (**Instale**) a aplicação Vulnerability Response junto com suas dependências na sua instância Now Platform. **Nota:** Durante a instalação da aplicação Vulnerability Response, você tem a opção de instalar dados de demonstração. Os dados de demonstração serão necessários se você quiser executar testes automatizados para confirmar se a instância funciona após a instalação. Execute testes somente em instâncias de desenvolvimento, teste e outras que não sejam de produção para evitar corrupção e indisponibilidade de dados. Se dados de demonstração ou contas de demonstração forem criados, todos os dados de demonstração deverão ser removidos antes de usar a instância em produção ou não produção. O Assistente de configuração para Vulnerability Response é instalado automaticamente junto com a aplicação. O Assistente de configuração é necessário para configurar a aplicação Vulnerability Response. Além disso, ele é usado para instalar e configurar a aplicação Qualys Integration for Security Operations usada neste exemplo, bem como outras aplicações que oferecem suporte e são compatíveis com Vulnerability Response. Para obter mais informações sobre como instalar a aplicação Vulnerability Response, consulte Como instalar Vulnerability Response.
☐	Como um usuário com a função de administrador, no Assistente de configuração, navegue até **Todos** > **Grupos e Usuários do Vulnerability Response** e atribua usuários com as funções de persona Vulnerability Response necessárias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	a. No Assistente de configuração, exiba os usuários existentes e todas as funções que já estão atribuídas, clicando no link **do módulo Administração de usuários**. **b.** Na lista, clique em um nome de usuário para abrir o registro e clique na lista relacionada **Funções**. Todas as funções atribuídas a este usuário são exibidas. **c.** Navegar de volta para **Grupos e Usuários do Vulnerability Response** no Assistente de configuração e siga as instruções para atribuir a função sn_vul.vulnerability_admin. **Nota:** A função sn_vul.vulnerability_admin é necessária para continuar com a configuração. Como alternativa, você pode continuar com a configuração como um usuário com a função de administrador. (Opcional) Você também pode atribuir as funções de Gerente de item de configuração (IC) [sn_vul.ci_manager] e de Aprovador de exceção [sn_vul.exception_approver], mas essas personas não são necessárias para as tarefas de configuração restantes. Para obter mais informações sobre como atribuir funções de persona usando o Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre usuários e atribuição de funções a usuários e grupos, consulte Administração de usuários.
☐	**a.** Navegar até **Todos** > **Administração** > **Integrações** e verifique se a **Integração abrangente do CWE 2000** está ativada e execute o trabalho programado para importar dados. **b.** Como um usuário com a função de administrador, navegue até **Aplicações do sistema** > **Todas as aplicações disponíveis** e ative (**Instalar**) a aplicação Vulnerability Response Integration with NVD. Execute as integrações de NVD e CWE como parte de sua configuração inicial de Vulnerability Response e antes de importar dados de vulnerabilidade para sua instância com um produto de scanner de terceiros. Consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros e Configurar e executar o trabalho programado para atualizar registros CWE para obter mais informações sobre como instalar, configurar e exibir as bibliotecas NVD e CWE.
☐	Como um usuário com a função de administrador, navegue **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Instalação de aplicação de integração** e ative a aplicação Qualys Integration for Security Operations. Antes de instalar e executar um produto de scanner de terceiros como Qualys que tenha uma biblioteca, você deve primeiro instalar e executar as integrações de NVD e CWE para ingerir dados de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	Para obter mais informações, consulte Instalar Vulnerability Response aplicações de terceiros usando o Assistente de configuração.
☐	(Opcional) Como um usuário com a função de administrador, se você instalou dados de demonstração com a aplicação Vulnerability Response, poderá executar o Vulnerability Response ATF Test Suite para verificar as aplicações instaladas com sucesso. **Nota:** Execute testes somente em instâncias de desenvolvimento, teste e outras que não sejam de produção para evitar corrupção e indisponibilidade de dados. Para obter mais informações, consulte Executar o pacote de testes do Automated Test Framework (ATF) para Vulnerability Response. Para obter mais informações sobre testes automatizados, consulte ATF (Automated Test Framework).

3. Continue com a configuração das aplicações iniciando na seção Configurações do Vulnerability Response.

Analisar essas configurações ajuda a entender como Vulnerability Response funciona conforme você continua a configurar seu ambiente. Para a integração do scanner usada neste exemplo, é necessário editar as configurações.

Os conceitos usados neste exemplo de configuração para o produto Qualys se aplicam a outros aplicativos do scanner.

Suas Qualys credenciais são necessárias para configurar a aplicação. Verifique se você tem nomes de conta, senhas e outras informações de serviço exigidas pelos produtos Qualys para que você tenha acesso a eles.

Funções necessárias: sn_vul.vulnerability_admin ou, alternativamente, admin.

Vulnerability Response tarefas de check-list de implementação básica para administrador de vulnerabilidades

Tarefa	Descrição
☐	Revise as Regras de atribuição de vulnerabilidade. As regras de atribuição atribuem automaticamente itens vulneráveis (IVs) ao grupo de atribuição apropriado. Para obter mais informações, consulte Vulnerability Response visão geral de regras de atribuição. Para obter mais informações sobre como configurar Vulnerability Response usando o Assistente de configuração, consulte Configuração de Vulnerability Response usando o Assistente de configuração.
☐	Revise as regras de tarefa de correção. As regras de tarefa de correção agrupam automaticamente os itens vulneráveis (IVs) conforme eles são importados com base em

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	determinadas condições. Para obter mais informações, consulte Vulnerability Response tarefas de correção e regras de tarefa visão geral.
☐	Revise as calculadoras de risco. As calculadoras de risco pontuam itens vulneráveis para priorização. Você pode configurar calculadoras para incorporar características do item de configuração (IC), explorar a disponibilidade e a severidade da vulnerabilidade relatada pelo fornecedor de avaliação de vulnerabilidade (scanner). Para obter mais informações, consulte Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade.
☐	Revise as Regras de destino de correção. As Regras de destino de correção definem linhas do tempo de correção para IVs e tarefas de correção. Para obter mais informações, consulte Vulnerability Response regras de destino de correção.
☐	Na seção Configuração de integração, revise as configurações da aplicação Qualys e defina e programe suas importações de dados. **a.** Clique **em Integrações de scanner**. **b.** Na página Aplicações instaladas, clique em **Editar**. **c.** Insira suas credenciais e clique em **Avançar**. **d.** Leia as descrições da configuração da base de conhecimento. **e.** Revise a página Configuração de detecção de host para Configurações de importação, Regras de pesquisa de IC e Programações de importação. **f.** Quando estiver satisfeito com as configurações nesta página, clique em **Executar agora** para importar dados. Clique no link **Exibir detalhes** exibido para exibir o status de execução da integração de vulnerabilidade. **g.** (Opcional) Continue editando as definições de configuração. **h.** Clique em **Concluir** para concluir a instalação e a configuração no Assistente de configuração. Para obter mais informações sobre como configurar a aplicação Qualys, consulte Configurar o Qualys Vulnerability Integration usando o Assistente de configuração.

O que Fazer Depois

Parabéns! Você instalou com sucesso a aplicação Vulnerability Response e a configurou junto com uma aplicação de scanner usando o Assistente de configuração. O sistema de base agora está pronto para operação.

Para baixar, instalar e configurar outras aplicações para Vulnerability Response, siga as mesmas etapas e conceitos que você concluiu para a check-list anterior. Consulte os tópicos específicos fornecidos para cada aplicação para obter mais informações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre as aplicações compatíveis disponíveis que estão disponíveis para você em ServiceNow Store para Vulnerability Response, consulte Instalação de Vulnerability Response e aplicações compatíveis.

Para obter mais informações sobre como usar Vulnerability Response, consulte Explorando a aplicação Vulnerability Response.

Vulnerability Response estados da tarefa de correção

As integrações de terceiros importam dados de detecção de item vulnerável que criam novos itens de vulnerabilidade (IVs) ou atualizam IVs existentes. Os estados de detecção atualizam os estados de IV, desde que sejam Aberto ou Fechado. Para obter mais informações, consulte a seção "Detecções, Tarefas de correção e itens vulneráveis".

Com Change Management para Vulnerability Response, há um relacionamento sincronizado entre os campos de estado das tarefas de correção e os campos de estado das solicitações de mudança (CHG) no produto Vulnerability Response. Conforme uma solicitação de mudança passa por seu ciclo de vida, ela também muda o estado de todas as tarefas de correção relacionadas automaticamente. Depois que uma solicitação de mudança é implementada, a tarefa de correção é resolvida automaticamente. Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

A tabela a seguir lista os estados da tarefa de correção e as ações que você pode executar em uma tarefa de correção no respectivo estado:

Estados da tarefa de correção

Estado	Descrição
Em aberto	Estado após a criação. A partir deste estado, você pode: **Mostrar IVs duplicados** Identifique IVs duplicados relatados por vários scanners no sistema. Você pode marcar o IV duplicado como Resolvido ou Encerrado. Entradas duplicadas são mostradas somente quando a combinação de vulnerabilidades é criada usando Vulnerabilidades e exposições comuns (CVE). Para obter mais informações, consulte Vulnerability Response tarefa de correção e estados de item vulnerável. **Iniciar Investigação** Atribua esta tarefa de correção a uma pessoa ou grupo para começar a investigar. **Marcar como falso positivo** Marque um item ou grupo como falso positivo se o scanner relatar que existe uma vulnerabilidade no sistema, mas na realidade não há nenhuma vulnerabilidade. **Exceção de Solicitação** Solicite uma exceção, uma data de reabertura (até), um motivo e, opcionalmente, forneça informações adicionais. Adia a correção do item ou grupo até a data em que uma exceção é solicitada. **Resolver** Marque como Resolvido para mover o item ou grupo para um estado resolvido. **Criar Mudança**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados da tarefa de correção

Estado	Descrição
	Crie uma solicitação de mudança ou associe uma tarefa de correção a uma solicitação de mudança existente. Para obter mais informações, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção e Associar uma tarefa de correção a uma solicitação de mudança existente. **Dividir tarefa de correção** Para uma tarefa de correção com mais de um item vulnerável, use um conjunto de condições para filtrar um subconjunto de itens vulneráveis e dividir uma tarefa de correção. Os itens selecionados são movidos automaticamente para uma nova tarefa de correção. Para obter mais informações, consulte Dividir uma tarefa de correção no Espaço de correção de problemas de TI. **Adiar** Selecione o estado Adiado, uma data de reabertura, um motivo e, opcionalmente, forneça informações adicionais. Adia o estado da tarefa de correção até a data de reabertura. **Fechar** Selecione o estado Encerrado, selecione um motivo e forneça informações adicionais. Fecha o grupo. **Excluir** Confirmar a exclusão. Remove o grupo.
Sob Investigação	Acionado pelo botão **Iniciar investigação**. A partir deste estado, você pode: **Criar um incidente de segurança** Para obter mais informações, consulte Criar um incidente de segurança. **Criar Mudança** Crie uma solicitação de mudança ou associe uma tarefa de correção a uma solicitação de mudança existente. Para obter mais informações, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção e Associar uma tarefa de correção a uma solicitação de mudança existente. **Dividir tarefa** Para uma tarefa de correção com mais de um item vulnerável, use um conjunto de condições para filtrar um subconjunto de itens vulneráveis e dividir uma tarefa de correção. Os itens selecionados são movidos automaticamente para uma nova tarefa de correção. Para obter mais informações, consulte Dividir uma tarefa de correção. **Criar uma solicitação de mudança** Para obter mais informações, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção. **Aguardando Implementação** Muda o estado para Aguardando implementação. Este estado indica que as tarefas de correção foram encaminhadas para fora de um Vulnerability Response. **Adiar**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados da tarefa de correção

Estado	Descrição
	Selecione o estado Adiado, uma data de reabertura, um motivo e, opcionalmente, forneça informações adicionais. Adia o estado da tarefa de correção até a data de reabertura. **Fechar** Selecione o estado Encerrado, selecione um motivo e forneça informações adicionais. Fecha a tarefa de correção. **Excluir** Confirmar a exclusão. Remove a tarefa de correção.
Adiado	Acionado pelo botão **Solicitar exceção**. Como parte do fluxo de trabalho de aprovação, o estado Adiado é Em revisão e não pode ser fechado até ser aprovado. A partir deste estado, você pode: **Criar Mudança** Crie uma solicitação de mudança ou associe uma tarefa de correção a uma solicitação de mudança existente. Para obter mais informações, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção e Associar uma tarefa de correção a uma solicitação de mudança existente. **Dividir tarefa** Para uma tarefa de correção com mais de um item vulnerável, use um conjunto de condições para filtrar um subconjunto de itens vulneráveis e dividir um grupo de vulnerabilidades. Os itens selecionados são movidos automaticamente para um novo VG. Consulte Dividir uma tarefa de correção. **Criar um incidente de segurança** Para obter mais informações, consulte Criar um incidente de segurança. **Reabrir** Faça a transição de volta para um estado Aberto. **Excluir** Confirmar a exclusão. Remove a tarefa de correção. **Fechar** Selecione o estado Encerrado, selecione um motivo e forneça informações adicionais. Fecha a tarefa de correção. As informações de adiamento aparecem na guia **Fechar/Adiar**. Na data de adiamento, o grupo é reaberto para correção.
Aguardando Implementação	Acionado pelo botão **Aguardando implementação**. A partir deste estado, você pode: **Criar um incidente de segurança** Para obter mais informações, consulte Criar um incidente de segurança. **Criar Mudança**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados da tarefa de correção

Estado	Descrição
	Crie uma solicitação de mudança ou associe uma tarefa de correção a uma solicitação de mudança existente. Para obter mais informações, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção e Associar uma tarefa de correção a uma solicitação de mudança existente. **Dividir tarefa** Para uma tarefa de correção com mais de um item vulnerável, use um conjunto de condições para filtrar um subconjunto de itens vulneráveis e dividir um grupo de vulnerabilidades. Os itens selecionados são movidos automaticamente para uma nova tarefa de correção. Para obter mais informações, consulte Dividir uma tarefa de correção. **Criar uma solicitação de mudança** Para obter mais informações, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção. **Adiar** Selecione o estado Adiado, uma data de reabertura, um motivo e, opcionalmente, forneça informações adicionais. Adia o estado da tarefa de correção até a data de reabertura. **Fechar** Selecione o estado Encerrado, selecione um motivo e forneça informações adicionais. Fecha a tarefa de correção. **Resolver** Adicione anotações. O estado se torna Resolvido. As anotações aparecem na guia **Resolução**. **Excluir** Confirmar a exclusão. Remove a tarefa de correção.
Resolvido	Acionado a partir do botão **Resolver**. A partir deste estado, você pode: **Criar um incidente de segurança** Para obter mais informações, consulte Criar um incidente de segurança. **Criar Mudança** Crie uma solicitação de mudança ou associe um grupo de vulnerabilidades a uma solicitação de mudança existente. Para obter mais informações, consulte Criar uma solicitação de mudança a partir de uma tarefa de correção e Associar uma tarefa de correção a uma solicitação de mudança existente. **Reabrir** Faça a transição de volta para um estado Aberto. **Fechar** Selecione o estado Encerrado, selecione um motivo e forneça informações adicionais. Fecha o grupo. **Excluir** Confirmar a exclusão. Remove a tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados da tarefa de correção

Estado	Descrição
	As anotações aparecem na guia **Anotações**. As informações de resolução aparecem na guia **Resolução**.
Encerrado	Acionado a partir do botão **Fechar**. A partir deste estado, você pode: **Criar um incidente de segurança** Para obter mais informações, consulte Criar um incidente de segurança. **Reabrir** Faça a transição de volta para um estado Aberto. **Excluir** Confirmar a exclusão. Remove a tarefa de correção. As informações de fechamento aparecem na guia **Fechar/Adiar**.

- O proprietário de correção só pode marcar um item vulnerável ou tarefa de correção como resolvido. Com base na confirmação do scanner, este item resolvido ou tarefa de correção pode ser marcado como Encerrado ou reaberto.
- Enquanto a opção Fechar está disponível somente para o analista de vulnerabilidade, Excluir está disponível para o administrador quando há vários itens vulneráveis criados manualmente e eles precisam ser fechados ou excluídos.
- Se você determinar que os itens são de baixo risco, aguardando uma janela de mudança ou um patch, poderá mudar a tarefa de correção para o estado Adiar por um período definido ou fechar imediatamente o grupo. Você pode solicitar uma exceção usando a opção Solicitar exceção.

  Nota:
  Quando as tarefas de correção são adiadas ou encerradas, você pode especificar resoluções para definir melhor os motivos para isso.

- Quando um IV é reaberto, manual ou automaticamente, acontece o seguinte:
  - O estado do IV muda para Aberto. O estado da tarefa de correção original não é atualizado.
  - O IV é reavaliado e colocado em uma tarefa de correção nova ou existente que se baseia nas Regras de tarefa de correção ativas.

  Isso preserva o histórico e permite correções adicionais.

- Quando você cria uma tarefa de correção automaticamente, manualmente, divide uma tarefa de correção ou atualiza um IV, os campos **Estado**, **Motivo**e **Até** são avaliados para tarefas de correção novas e antigas.
  - Se todos os IVs em uma tarefa de correção forem adiados e tiverem o mesmo motivo, o estado da tarefa de correção será alterado para adiado e o motivo dos IVs será atribuído a uma tarefa de correção. Se os IVs diferirem no motivo, o motivo da tarefa de correção será alterado para **Nenhum**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A data **Até** mais próxima de todos os IVs é atualizada no campo **Até** da tarefa de correção.
- Se você reabrir qualquer IV, o estado da tarefa de correção mudará para **Aberto**.

Esta avaliação é feita pelo trabalho programado *`Rollup vulnerability item values to vulnerability and group`*, que é executado a cada 15 minutos.

Detecções, tarefas de correção e estados de item vulnerável

As integrações de terceiros recuperam os dados de detecção de item vulnerável. As detecções são ocorrências distintas de vulnerabilidades, conforme relatado pelos scanners.

Os dados de detecção são emparelhados com itens vulneráveis (IVs, VITs) e o estado do IV é atualizado com base no estado das detecções. Se um IV não for encontrado, um novo será criado. As detecções são abertas ou encerradas somente pelos dados encontrados diretamente por um scanner.

Se todas as detecções de um item vulnerável forem encerradas, esse item vulnerável será encerrado. No registro IV, o estado é Encerrado/Corrigido. Quando todos os IVs são encerrados para uma tarefa de correção, a tarefa de correção é encerrada. Caso contrário, o fluxo de estado permanecerá o mesmo.

Os IVs encerrados com um subestado fixo ou obsoleto serão reabertos se uma nova detecção for criada e os IVs puderem ser correspondidos com a nova vulnerabilidade.

A partir da versão 20.0 do Vulnerability Response, se a detecção for Obsoleta e o IV associado estiver no estado Encerrado, o estado do IV não fará a transição para Encerrado - Obsoleto. Isso evita que o IV seja reaberto quando uma nova detecção é identificada para que você possa evitar passar por todo o processo de aprovação e solicitação de falso-positivo. Para reverter esse comportamento, desmarque a caixa de seleção **Ignorar detecções obsoletas para IVs encerrados** no formulário Configuração de fechamento automático. Para obter mais informações, consulte Encerrar automaticamente detecções obsoletas no Vulnerability Response.

De acordo com a inclusão de script, *`DetectionBase`*, método *`_shouldReOpenVI()`*, se o IV foi encerrado anteriormente com um subestado de Fixo, Obsoleto ou IC desativado, ele será reaberto e a detecção será mapeada para o VIT existente.

Por exemplo, digamos que a data de encerramento de um IV seja posterior à última data encontrada de uma detecção. Você esperaria que esses registros de IV permanecessem fechados. No entanto, se você observar que um IV encerrado anteriormente foi reaberto, isso significa que o IV foi encerrado por uma detecção anterior e a vulnerabilidade foi encontrada novamente em uma verificação posterior. Quando é encontrada uma nova detecção que corresponde ao VIT encerrado que tem a mesma vulnerabilidade no item de configuração do IV, o IV é reaberto.

Tarefas de correção e estados de item vulnerável

Tarefas de correção e estados de itens vulneráveis podem afetar um ao outro. Na maioria das vezes, um estado de tarefa de correção atualiza o estado do item vulnerável, com o estado de tarefa de precedência mais alta usado para atualizar os itens vulneráveis no grupo.

A precedência de estado é a seguinte.

Adiado > **Resolvido** > **Aguardando implementação** > **Sob investigação** > **Aberto**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Quando um grupo de itens vulneráveis está em uma tarefa de correção e não é alterado em um nível individual, eles têm o mesmo estado da tarefa de correção.
- Quando a tarefa de correção passa do estado Aberto para Aguardando implementação, todos os IVs na tarefa de correção são movidos para o estado Aguardando implementação.
- Quando a tarefa de correção é adiada, o IV também é adiado. A partir da versão 16.5, você pode rastrear o número de vezes que um item vulnerável, item vulnerável de aplicação, item vulnerável de contêiner ou uma tarefa de correção é adiado. O trabalho programado, `set deferral counts`, é executado diariamente para publicar contagens dos registros que são adiados mais de uma vez na coluna Contagem de adiamento nos módulos Vários adiamentos para VR, AVR e CVR. Todas as contagens de IVs associadas a uma tarefa de correção serão coletadas e publicadas se uma tarefa de correção for adiada mais de uma vez.

Itens vulneráveis atualizados somente por tarefas de correção

Os itens correspondem ao estado da tarefa de correção, se não tiverem sido atualizados individualmente, com estas exceções:

- Se o estado da tarefa de correção mudar para Encerrado e sua resolução para Cancelado ou Corrigido com exceção, o item não será afetado e assumirá o estado de qualquer outra tarefa de correção que o contenha. Se o item vulnerável não estiver em nenhuma outra tarefa de correção, ele será revertido para o estado Aberto.
- Se o estado do item vulnerável for Encerrado/Corrigido (atualizado por uma verificação ou importação), quando a tarefa de correção mudar seu estado, o item vulnerável permanecerá no estado Encerrado/Corrigido. Esta condição é verdadeira, independentemente do estado da tarefa de correção.

Itens vulneráveis em estados definidos individualmente

Itens vulneráveis, em um estado atualizado no item, como os itens encerrados ou adiados individualmente, não correspondem ao estado da tarefa de correção automaticamente. Em vez disso, ele compara seu estado com todos os grupos associados para encontrar o estado com a precedência mais alta a ser aplicada.

Nota:
O estado Encerrado/Corrigido é um caso especial. Para os itens vulneráveis definidos com o estado Encerrado/Corrigido, se todos os itens vulneráveis em uma tarefa de correção estiverem definidos como Encerrado/Corrigido (por exemplo, quando um verificador descobre que todas as vulnerabilidades foram corrigidas), a tarefa de correção será marcada automaticamente como Encerrado/Corrigido.

Tarefas de correção contêm campos de atribuição vazios

Se o estado dos IVs em uma tarefa de correção mudar de Resolvido para Aberto, o estado da tarefa de correção também será atualizado de Resolvido para Sob investigação.

No entanto, se os campos **Atribuído a** e **Grupo de atribuição** na tarefa de correção estiverem vazios, a tarefa de correção permanecerá no estado Resolvido e não será movida para Sob investigação.

O grupo de atribuição de itens vulneráveis nem sempre é atualizado quando a tarefa de correção é atualizada

Se o grupo de atribuição de um IV no estado Aberto for atualizado manualmente, ele não será atualizado novamente quando o grupo de atribuição para sua tarefa de correção for atualizado. Essas informações não são substituídas porque o grupo de atribuição do IV foi atualizado intencionalmente e pode fazer parte de outra tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estado da tarefa de correção para itens vulneráveis (IVs) em vários grupos

Quando um IV está em várias tarefas de correção (grupo nas tabelas a seguir) e seu próprio estado não foi definido, o estado do grupo de precedência mais alta determina o estado desse IV, conforme mostrado na tabela a seguir.

Exemplos de estados de item vulnerável

Estado de tarefas de correção	Estado do item vulnerável
Grupo A: **Em aberto** > **Sob Investigação** Grupo B: **Aberto**	**Sob Investigação** Quando o Grupo A está Sob investigação e o Grupo B está Aberto, o IV muda para Sob investigação. Após a pesquisa, entre o Grupo A e o Grupo B, o Grupo A tem o estado com a precedência mais alta.
Grupo A: **sob investigação** Grupo B: **Em aberto** > **Sob Investigação**	**Sob Investigação** Quando o Grupo B estiver Sob investigação e o Grupo A estiver Sob investigação, o IV permanecerá como Sob investigação. Após a pesquisa, entre o Grupo A e o Grupo B, eles têm o estado com a mesma precedência.
Grupo A: **sob investigação** Grupo B: **Sob Investigação** > **Aguardando Implementação**	**Aguardando Implementação** Quando o Grupo B está Aguardando Implementação e o Grupo A está Sob Investigação, o IV muda para Aguardando Implementação. Após a pesquisa, entre o Grupo A e o Grupo B, o Grupo B tem o estado com a precedência mais alta.
Grupo A: **Sob Investigação** > **Adiado** Grupo B: **Aguardando Implementação**	**Adiado** Quando o Grupo A é Adiado e o Grupo B é Aguardando Implementação, o IV muda para Adiado. Após a pesquisa, entre o Grupo A e o Grupo B, o Grupo A tem o estado com a precedência mais alta.

Casos especiais de item vulnerável em vários grupos

Estado da tarefa de correção	Estado do item vulnerável
Grupo A: **Sob Investigação** Grupo B: **Aguardando Implementação** > **Encerrado (corrigido ou cancelado)**	**Sob Investigação** Quando o Grupo B é Encerrado/Corrigido ou Encerrado/Cancelado e o Grupo A está Sob investigação, o IV muda de Aguardando implementação (anteriormente a precedência mais alta) para Sob investigação (atualmente a precedência mais alta).
Grupo A: qualquer estado	Se o status de origem do item vulnerável for Corrigido (atualizado por uma verificação ou importação), quando

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Casos especiais de item vulnerável em vários grupos

Estado da tarefa de correção	Estado do item vulnerável
Grupo B: qualquer estado	o grupo mudar seu estado, o item vulnerável mudará seu estado para Encerrado/Corrigido. Esta condição é verdadeira, independentemente do estado dos outros grupos associados. A pesquisa de item vulnerável para o estado do grupo não ocorre.

Quando um estado de IV é definido individualmente, seu estado é considerado ao avaliar a precedência, como em qualquer outra tarefa de correção. Quando um IV pertence a mais de uma tarefa de correção, a tabela a seguir lista as atualizações feitas.

Estado de item vulnerável definido individualmente casos especiais

Estado do item de vulnerabilidade em um grupo	Estado final do item vulnerável
Estado do Grupo A: **Sob Investigação** Estado do Grupo B: **Sob Investigação** > **Aguardando Implementação** Estado do IV original: **Sob Investigação** > **(definido no IV)**	**Aguardando Implementação** Quando o Grupo B é movido para Aguardando Implementação e o Grupo A permanece Sob Investigação, o IV muda para Aguardando Implementação (a precedência mais alta).
Grupo A: **Sob Investigação** Grupo B: **Sob Investigação** > **Aguardando Implementação** Estado do IV original: **Adiado** > **(definido no IV)**	**Adiado** Quando o Grupo B é movido para Aguardando Implementação e o Grupo A permanece Sob Investigação, o IV permanece no estado Adiado (a precedência mais alta).

A tabela a seguir mostra que quando duas tarefas de correção com itens vulneráveis comuns são adiadas, o estado é adiado até a data mais recente.

Casos especiais de estado adiado de item vulnerável

Estado do item de vulnerabilidade em um grupo	Estado final do item vulnerável
Estado do Grupo A: **Em revisão (até 10 de abril)** Estado do Grupo B: **Sob Investigação** > **Em revisão (até 30 de abril)** Estado do IV original: **Em revisão (até 10 de abril)** > **(definido no IV)**	**Adiado (até 30 de abril)** Quando o Grupo B é movido para Adiado (até Abr-30) e o Grupo A permanece Adiado (até Abr-10), o IV muda do estado Adiado (até Abr-05) para Adiado (até Abr-30).
Grupo A: **Em revisão (até 15 de julho)** Grupo B: **Sob Investigação** > **Em revisão (até 10 de julho** Estado do IV original: **Adiado** > **(até 15 de julho)**	**Adiado (até 15 de julho)** Quando o Grupo B é movido para Adiado (até jul-10) e o Grupo A permanece Adiado (Jul-15), o IV permanece em Adiado (até jul-15).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações adicionais para Domain Separation

Para uma execução e resultados precisos, as precauções e configurações a seguir são necessárias para a separação de domínio em Vulnerability Response, Application Vulnerability Response, Vulnerability Response contêinere Configuration Compliance.

Não modifique a lógica de negócios e os processos no domínio global para evitar problemas para que todas as mudanças mais recentes sejam atualizadas para cada atualização. Duplique todas as lógicas de negócios e processos em cada domínio separadamente e certifique-se de que eles estejam inativos no domínio global. Caso contrário, as lógicas de negócios e os processos no domínio global terão precedência sobre o domínio secundário. Suponha que você tenha criado uma regra de risco em um domínio secundário e o domínio global também tenha uma regra de risco semelhante. A regra do domínio global terá precedência sobre a regra do domínio secundário.

Reavaliação de calculadoras e regras

Antes da v20.0, quando você reaplica calculadoras ou regras, o sinalizador de `reexecução` é definido como verdadeiro e uma regra de negócios é acionada para executar um trabalho de programação que reaplica as calculadoras e as regras. A partir da v20.0, você não precisa depender do sinalizador de `reexecução`. Quando você clica no botão **Reaplicar calculadora**, um trabalho em segundo plano é acionado que reaplica as calculadoras e as regras. Isso permite que você crie calculadoras e regras para todos os domínios.

Configurações para calculadoras de acúmulo

Em um domínio, apenas uma calculadora de acúmulo deve estar ativa para uma tabela. Por exemplo, considere a tabela Tarefa de correção, *`sn_vul_vulnerability`* com a calculadora de acúmulo, **Acúmulo de tarefa** de correção no domínio global. Se você duplicar esta calculadora de acúmulo alterando os pesos da mesma tabela no mesmo domínio, haverá discrepâncias nos cálculos de acúmulo. Portanto, certifique-se de ativar apenas uma calculadora de acúmulo se houver duas ou mais calculadoras de acúmulo para uma tabela no mesmo domínio.

Campos de formulário de Itens descobertos

Os ativos são correspondidos automaticamente aos itens de configuração (ICs) no Configuration Management Database (CMDB) quando são importados usando as Regras de pesquisa de IC. Registros de ICs incompatíveis são criados automaticamente durante as importações de integração de vulnerabilidade de terceiros e incluídos nos Itens descobertos. No entanto, para ativos de nuvem que não estão presentes em CMDB CI, o registro é criado na classe de recurso de nuvem.

Campos de Itens Descobertos

As informações nesses registros são ingeridas dos registros de terceiros e classificadas durante a importação.

Campo	Descrição
Número	Identificador atribuído ao registro.
Item de Configuração	Item de configuração que é importado da integração de origem de terceiros. A partir da v12.0, o item de configuração é o IC mais recente da lista de ICs após filtrar os desativados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Classe	Classe atribuída ao IC durante a importação por Vulnerability Response.
Fonte	Origem que é importada da integração de origem de terceiros.
Regra de correspondência de IC	A regra de correspondência de IC que foi usada para criar o item.
V18.0: tipo de correspondência para DI	Tipo correspondente usado para criar o item descoberto. As opções são: • Criado por VR • Criado por IRE • Correspondido por pesquisa de IC • Correspondido por IRE Essas informações estão disponíveis somente para dados preenchidos para Vulnerability Response v18.0 e posterior. Nos dados existentes, esta coluna não contém nenhum valor. **Nota:** Se você reaplicar as regras de pesquisa de IC, alguns ICs em DIs poderão ser atualizados, resultando no preenchimento desta coluna.
Outros ICs correspondentes	Lista dos outros itens de configuração que correspondem à regra de pesquisa de IC.
Estado	Estado do IC determinado durante a importação. As opções são: • **Correspondido**: um item de configuração correspondente foi encontrado no CMDB. • **Incompatível**: nenhuma correspondência foi encontrada no CMDB. Um registro de espaço reservado é criado.
Criado em	Data em que o registro do item descoberto foi criado.
Atualizado em	Data em que o registro do item descoberto foi atualizado.
Atualizado por	Usuário que atualizou os dados.
Marcador de host	Marcadores de host atribuídos a este item descoberto durante a importação. Você pode ter até 31 marcadores de host por item descoberto.
Nome de domínio totalmente qualificado	Dados associados a este IC encontrados no CMDB.
Endereço MAC	Dados associados a este IC encontrados no CMDB.
Sistema operacional	Sistema operacional associado a este IC.
NetBIOS	NetBIOS importado da integração de origem de terceiros.
Endereço IP	Dados associados a este IC encontrados no CMDB.
Dados de origem	Dados mais recentes associados a este IC da origem.
V16: dados de origem iniciais	Dados iniciais associados a este IC da origem.
V16: reavaliar IC	Recebe dados do scanner. Se houver dados atualizados, o valor será definido como verdadeiro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Os valores dos dados de origem são recalculados de acordo com os dados de origem mais recentes. Quando os dados atualizados são recuperados do scanner, os dados de origem são atualizados. O valor de dados de origem existente é movido para o campo de dados de origem inicial. Para reavaliar os itens descobertos, ative o trabalho programado Reaplicar regras de pesquisa de IC nos itens descobertos alterados.
Agente existe	Indica verdadeirose o agente estiver instalado no ativo. Se os valores hostUID e UUID na coluna Dados de origem estiverem vazios, este valor será preenchido como verdadeiro. **Nota:** Este campo aparece a partir da v19.0 de Vulnerability Response.

A partir da versão 18.0 de Vulnerability Response, Qualys, Tenable para Vulnerability Response e Rapid7 os scanners podem receber os seguintes metadados adicionais para ativos em nuvem.

Campo	Descrição
Provedor de serviços em nuvem	Nome do provedor de serviços de nuvem que oferece serviços de computação em nuvem. Por exemplo, Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).
Região da nuvem	Local onde o recurso foi hospedado.
Conta de nuvem	Conta fornecida por provedores de serviços em nuvem, como AWS, GCPe assim por diante, para acessar serviços de computação em nuvem.
Tipo de recurso de nuvem	Tipos de ativos presentes na nuvem, como a máquina Amazon Elastic Compute Cloud (EC2), AWS buckets S3 e assim por diante.
ID do recurso	Identificador exclusivo que é atribuído a um recurso em um ambiente de computação em nuvem. Este ID é usado para identificar e gerenciar o recurso.
Nome do recurso	Nome definido pelo usuário usado para identificar e gerenciar um recurso em um ambiente de computação em nuvem.
Imagem	A imagem de máquina virtual ou uma imagem de servidor é uma máquina virtual pré-configurada que contém um sistema operacional, aplicativos e outros softwares. Por exemplo, Amazon Machine Image.

Uma nova regra de pesquisa de IC, "ID de recurso de nuvem", foi introduzida para corresponder aos ICs de nuvem com base nos metadados de nuvem.

Vulnerability Response campos de formulário de vulnerabilidade

As vulnerabilidades são criadas automaticamente quando os registros são baixados do National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) ou integrações de terceiros e armazenados em **Bibliotecas** em Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de entrada do NVD

Os campos importados nesta tabela são somente leitura. Itens vulneráveis (IVs), Software vulnerável e Referências de vulnerabilidade são associados automaticamente e as entradas podem ser adicionadas manualmente.

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Pontuação de risco	(Oculto quando não há IVs associados à vulnerabilidade) **Pontuação de risco** quantificada que separa itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade. **Nota:** Esta **classificação de risco** base não é igual à **classificação de risco do registro da solução.**
Pontuação de risco	(Oculto quando não há IVs associados à vulnerabilidade) Valor calculado de risco que o item vulnerável representa para o seu ambiente. **Nota:** Esta **pontuação de risco** base não é igual à **pontuação de risco do registro da solução.** Para obter mais informações, consulte Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade.
Gravidade	Grau normalizado de severidade desta vulnerabilidade. Mapas de severidade são fornecidos para NVD e com ServiceNow integrações de terceiros. Para obter mais informações sobre como criar ou ajustar mapas de severidade, consulte Criar um mapa de severidade Vulnerability Response.
Explorar itens existentes	Sim, se pelo menos uma exploração estiver associada a esta vulnerabilidade.
Nível de habilidade Exploit	Nível de habilidade mais baixo necessário para explorar esta vulnerabilidade.
Vetor de ataque Exploit	Vetor de ataque mais vulnerável das explorações para esta vulnerabilidade. Disponível quando o NVD do SAM está habilitado.
IVs ativos	(Oculto quando não há IVs associados à vulnerabilidade) Número de itens vulneráveis associados a esta vulnerabilidade, não no estado Encerrado. Se não houver IVs ativos para esta vulnerabilidade, a **Classificação** de **risco e a Pontuação** de risco não serão exibidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Entrada de CWE	Referência ao elemento de Enumeração de Pontos Fracos Comuns no qual esta vulnerabilidade melhor se encaixa.
Data de publicação	Data em que a vulnerabilidade foi publicada.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez.
Resumo	Descrição da vulnerabilidade.
Informações sobre ameaças (começando com Vulnerability Response versão 20.0)	Inteligência contra ameaças fornecida por Qualys. Com esses dados, você pode entender os motivos, os destinos e os comportamentos de ataque de um agente da ameaça.
Detalhes da Vulnerabilidade	
CVSS v2	Dados do CVSS v2 importados
CVSS v3	Dados do CVSS v3 importados, não disponíveis antes de 2015.
Solução preferencial	(Oculto quando não há IVs associados à vulnerabilidade) Solução da substituição mais alta na cadeia, derivada das soluções referenciadas na vulnerabilidade. Se houver mais de uma substituição mais alta na cadeia, nenhum valor será definido. Qualquer valor definido manualmente pode ser substituído nas importações subsequentes. A definição manual deste valor deve ser feita no item vulnerável.
Exploração CISA (Esta guia está disponível somente quando a aplicação CISA está instalada.)	
Data de vencimento da CISA	Prazo para resolver a vulnerabilidade.
Data adicionada	Data em que a vulnerabilidade foi adicionada ao catálogo CISA.
Produto	Produto no qual a vulnerabilidade foi identificada.
Fornecedor/projeto	Fornecedor associado à vulnerabilidade identificada.
Ransomware conhecido A partir da v21.0 de Vulnerability Response.	Selecionado quando o campo **Conhecido por ser usado em campanhas de ransomware** é ingerido do catálogo de vulnerabilidades exploradas conhecidas (KEVs) da CISA. O sinalizador é definido no nível de vulnerabilidades e exposições comuns (CVE) e acumulado para a entrada de terceiros (TPE).
Status da Correção (Oculto quando não há IVs associados à vulnerabilidade)	
Exclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
% IVs corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Inclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade.
% IVs corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade.
Links relacionados	
Antes da v13.0: forçar importação de vulnerabilidade de software **Nota:** Removido em v13.0	(Obsoleto) Recalcula o mapeamento do produto com Gestão de ativos de software ITSM com base nas informações do NVD. Atualiza a biblioteca de software vulnerável.
Atualizar status	Exibe a data e a hora da última atualização. Atualiza o seguinte: • Estado de tarefas de correção • Pontuação e classificação de risco • Métricas como IVs ativos, total de IVs da seção Status de correção
Listas relacionadas	
Itens vulneráveis	(Oculto quando não há IVs associados à vulnerabilidade) Itens vulneráveis associados a esta vulnerabilidade.
Referências de vulnerabilidade	Informações sobre a vulnerabilidade de fontes externas, citadas pelo NVD.
Explorações	Explorações associadas a esta vulnerabilidade.
Soluções	(Oculto quando não há IVs associados à vulnerabilidade) Todas as Solução de gerenciamento de vulnerabilidade soluções de integração associadas a esta vulnerabilidade.
Pontos fracos	Dados de **vulnerabilidade** importados associados a um CVE (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns).
Software Vulnerável	(Oculto quando o software está associado ao CVE) Dados de enumeração de plataforma comum (CPE) associados à vulnerabilidade.
Kits de Malware de Vulnerabilidade	Malware importado de várias origens de scanner para uma vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de entrada de vulnerabilidade do CWE

Os campos importados nesta tabela são somente leitura.

Campo	Descrição
CWE-Identificador	Identificador desta entrada de vulnerabilidade. Este identificador é usado para categorias e pontos fracos e é exclusivo entre os dois conjuntos de dados.
Nome	Nome descritivo atribuído a este CWE-ID.
Probabilidade de exploração	Qual a probabilidade de o ponto fraco ser explorado, em uma escala qualitativa. Um dos seguintes: • Baixa • Média • Alto(a)
10 principais posições da OWASP	A posição numérica desta vulnerabilidade na lista das 10 principais da OWASP.
SANS para a posição 25	A posição numérica desta vulnerabilidade na lista das 25 principais da SAN.
Classe	Tipo de fraqueza
Status	Um dos seguintes: • Incompleto • Rascunho • Estável • Preterido • descontinuado • Instável
Subtração	Um dos seguintes: • Variante • Classe • Base • Composto
Atualizado em	Última vez em que o registro foi atualizado na instância.
Áreas funcionais	Lista de áreas funcionais afetadas. Por exemplo, **Processamento de arquivos**. Preenchido somente para pontos fracos do 24/862.
Recursos afetados	Lista de recursos afetados. Por exemplo, **Arquivo** ou **Diretório**. Preenchido somente para pontos fracos 51/863.
URL	Artigo da base de conhecimento associado a esta vulnerabilidade.
Descrição	Descrição da vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Execução de integração	A execução de integração em que este CWE foi importado.
Seções	
Detalhes adicionais	Descrições do conceito de software que explicam melhor o ponto fraco. Inclui: • Descrição estendida • Detalhes do plano de fundo • Anotações
Métodos de detecção	Detalhes sobre como você pode detectar esse ponto fraco em uma aplicação.
Modos de introdução	As fases em que o ponto fraco é introduzido, por exemplo, **Implementação**, **Arquitetura e Design**e assim por diante.
Exemplos demonstrativos	Exemplos de código do ponto fraco com descrições de acompanhamento.
Mitigações potenciais	Detalhes sobre como evitar o ponto fraco, incluindo em que fase do ciclo de vida da aplicação ele ocorre e a eficácia da mitigação.
Listas relacionadas	
Relacionamentos	CWEs associados a esta vulnerabilidade. Lista os relacionamentos entre este CWE e outros. Pode incluir primário/secundário, segue/precede, obrigatório por/requer (para pontos fracos compostos), CanAlsoBe, PeerOf, MemberOf .
Exemplos observados	Alguns CVEs que são representativos desse ponto fraco.
Consequências Comuns	Consequências de uma exploração bem-sucedida, em termos de escopo e impacto. Por exemplo: Escopo: confidencialidade Impacto: ler dados da aplicação
Associações	Associações do CWE com esta vulnerabilidade.
Plataformas aplicáveis	Plataformas associadas a esta vulnerabilidade.
Entradas de vulnerabilidade da aplicação	Outras entradas de vulnerabilidade da aplicação associadas a uma.
Referências externas	Informações sobre a vulnerabilidade de fontes externas.

Campos de entrada de vulnerabilidade de terceiros

Os campos importados nesta tabela são somente leitura.

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Versão 16.0: CVEs	Várias vulnerabilidades e exposições comuns (CVEs) associadas a esta vulnerabilidade de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Fonte	Origem da vulnerabilidade, seja um scanner ou um teste físico.
Pontuação de risco	**Pontuação de risco** quantificada que separa os itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade. **Nota:** Esta **classificação de risco** base não é igual à **classificação de risco**do registro da solução
Pontuação de risco	Valor calculado de risco que o item vulnerável representa para o seu ambiente, com base na pontuação de risco. **Nota:** Esta **pontuação de risco** base não é igual à **pontuação de risco do registro da solução.** Para obter mais informações, consulte Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade.
Gravidade	Grau normalizado de severidade desta vulnerabilidade. Mapas de severidade são fornecidos para NVD e com ServiceNow integrações de terceiros. Para obter mais informações sobre como criar ou ajustar mapas de severidade, consulte Criar um mapa de severidade Vulnerability Response.
Explorar itens existentes	Sim, se pelo menos uma exploração estiver associada a esta vulnerabilidade.
Nível de habilidade Exploit	Nível de habilidade mais baixo necessário para explorar esta vulnerabilidade.
Vetor de ataque Exploit	Vetor de ataque mais vulnerável das explorações para esta vulnerabilidade.
IVs ativos	Número de itens vulneráveis associados a esta vulnerabilidade, não no estado Encerrado.
Categoria	Classificação fornecida pela integração de terceiros. Auxilia na atribuição.
Tipo de correção	Tipos de ações de correção. • Patch • Mudança de configuração • Mudança de Configuração e Patch • Contramedida
Entrada de CWE	Referência ao elemento de Enumeração de Pontos Fracos Comuns no qual esta vulnerabilidade melhor se encaixa.
PCI	Quando a caixa de seleção está marcada, a vulnerabilidade é sinalizada como risco significativo de exposição de informações de pagamento.
Gravidade de PCI	Nível de risco de exposição de informações de pagamento. [Somente Qualys.]
Data de publicação	Data em que a vulnerabilidade foi publicada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez.
Resumo	Descrição da vulnerabilidade.
Detalhes da Vulnerabilidade	
CVSS v2	Dados do CVSS v2 importados
CVSS v3	Dados do CVSS v3 importados, não disponíveis antes de 2015.
Ameaça	Descrição da ameaça desta vulnerabilidade.
Solução preferencial	Solução da substituição mais alta na cadeia, derivada das soluções referenciadas na vulnerabilidade. Se houver mais de uma substituição mais alta na cadeia, nenhum valor será definido. Qualquer valor definido manualmente pode ser substituído nas importações subsequentes. A definição manual deste valor deve ser feita no item vulnerável.
Anotações de correção	Descrição da solução de correção extraída do fornecedor.
Status da Correção	
Exclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
% IVs corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Inclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade.
% IVs corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade.
Links relacionados	
Atualizar status	Exibe a data e a hora da última atualização. Atualiza o seguinte: • Estado de tarefas de correção • Pontuação e classificação de risco • Métricas como IVs ativos, total de IVs da seção Status de correção
Listas relacionadas	
Itens vulneráveis	Itens vulneráveis associados a esta vulnerabilidade.
Referências de vulnerabilidade	Informações sobre a vulnerabilidade de fontes externas, citadas pelo NVD.
CVEs	Registro de enumeração de vulnerabilidade comum (CVE) associado a esta vulnerabilidade.
Categorias	Categorias associadas a esta vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Explorações	Explorações associadas a esta vulnerabilidade.
Kits de Malware de Vulnerabilidade	Kits de malware associados a esta vulnerabilidade.
Soluções (Rapid7)	Informações da solução das integrações da solução Rapid7. Exibido quando disponível.
Estruturas de Exploração	Explorar estruturas associadas a esta vulnerabilidade.
Soluções	Solução de gerenciamento de vulnerabilidade soluções associadas a esta vulnerabilidade.
Exploração CISA	
CISA existe	A exploração CISA existe para a tabela de entrada de vulnerabilidades de terceiros.
Data de vencimento da CISA	Prazo para resolver a vulnerabilidade.

Campos de formulário de tarefa de correção

Usando tarefas de correção, o analista pode monitorar o andamento e conduzir o processo de mediação com mais eficiência.

Os campos importados nesta tabela são somente leitura.

Campos de tarefa de correção

Campo	Descrição
Número	O número do item vulnerável (IV) gerado automaticamente para este registro.
Pontuação de risco	Acúmulo de pontuações de risco de item vulnerável separadas em intervalos: Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade. **Nota:** Esta **classificação de risco** base não é igual à **classificação de risco do registro da solução.**
Pontuação de risco	Acúmulo das pontuações de risco de todos os itens vulneráveis associados a esta tarefa de correção. Quantidade de risco que os itens vulneráveis, coletivamente, representam para o seu ambiente. **Nota:** Esta **pontuação de risco** base não é igual à **pontuação de risco do registro da solução.**
Destino de correção	Data em que os itens vulneráveis devem ser corrigidos, desde a primeira identificação. Para obter mais informações sobre destinos de correção, consulte Vulnerability Response regras de destino de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

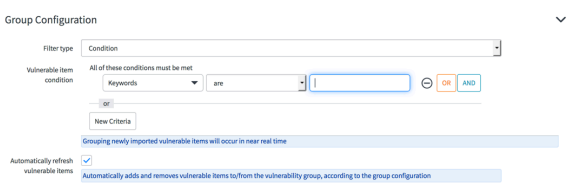
Campos de tarefa de correção

Campo	Descrição
Status da Correção	Status da correção da tarefa. É determinado pelo item vulnerável com a data de vencimento mais próxima. Para grupos abertos, os estados incluem: • Em andamento • Perto da meta • Meta não atingida Para grupos fechados, os estados incluem: • Nenhuma Meta • Meta atingida • Meta não atingida Para datas de destino de correção calculadas, se a tarefa for encerrada, o status geral de correção de todos os itens vulneráveis encerrados será mostrado na tarefa. Eles determinam se a tarefa atendeu à data ou não. O status de correção de uma tarefa encerrada será **Sem meta** se nenhum de seus itens encerrados tiver uma data de meta de correção. Será **Meta** não atingida se algum dos itens encerrados não tiver atingido a data de destino. É **Meta** atingida se pelo menos um IV encerrado atendeu sua meta e nenhum dos outros a errou.
Estado	Status de andamento da tarefa. Os estados incluem: • Em aberto • Sob Investigação • Aguardando Implementação • Adiado • Em Revisão • Resolvido • Encerrado Para obter mais informações sobre os estados, consulte Vulnerability Response tarefa de correção e estados de item vulnerável.
Até a data para redução de risco	Data em que os controles compensatórios aplicados à tarefa de correção expiram. **Nota:** Este campo é exibido somente quando o valor está disponível.
Grupo de atribuição	Grupo selecionado para trabalhar nesta tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

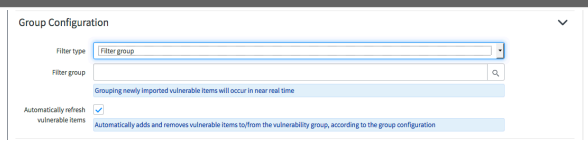
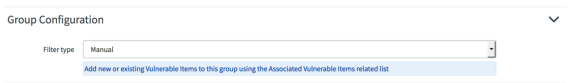
Campos de tarefa de correção

Campo	Descrição
Atribuído a	Indivíduo do grupo de atribuição selecionado que trabalha nesta vulnerabilidade.
Criado em	Data em que esta tarefa de correção foi criada.
Atualizado em	Data em que esta tarefa de correção foi atualizada pela última vez.
Vulnerabilidade	Vulnerabilidade aplicável à tarefa. (Visível quando o grupo é formado com base em uma única vulnerabilidade.)
Descrição resumida	Breve descrição desta tarefa de correção.
Em revisão (visível quando o RT está no estado Em revisão)	
Solicitados por	Indivíduo que solicitou o adiamento.
Motivo desejado	Motivo do adiamento.
Estado desejado	O estado solicitado do aprovador.
Subestado desejado	O motivo solicitado pelo aprovador.
Adiamento(visível quando a tarefa está no estado Adiado)	
Adiado por	Indivíduo que adiou a tarefa.
Adiar expiração	Data em que o adiamento expira.
Motivo para adiar	Motivo do adiamento.
Resolução (visível quando o RT está no estado Resolvido)	
Resolvido por	Indivíduo que resolveu a tarefa de correção.
Data de resolução	Data em que a tarefa de correção foi resolvida.
Anotações de resolução	Informações adicionais.
Encerrar (visível quando o RT está no estado Encerrado)	
Encerrado por	Indivíduo que resolveu a tarefa de correção.
Encerrado	Data em que a tarefa de correção foi encerrada.
Anotações de encerramento	Informações adicionais.
Configuração de grupo (visível em todos os estados)	
Tipo de filtro	Tipo de filtragem usada para selecionar vulnerabilidades para o grupo: **Condição**  **Nota:** Atualiza uma vez por hora. **Grupo de filtros**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de tarefa de correção

Campo	Descrição
	 **Nota:** Atualiza uma vez por hora. **Manual** 
Status da Correção	
Exclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos nesta tarefa. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número total de itens vulneráveis nesta tarefa. Esta contagem exclui itens vulneráveis adiados.
% IVs corrigidos	Percentual concluído para correção de itens vulneráveis nesta tarefa. Esta contagem exclui itens vulneráveis adiados.
Inclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos nesta tarefa.
Total de IVs	Número total de itens vulneráveis nesta tarefa.
% IVs corrigidos	Percentual concluído para correção de itens vulneráveis nesta tarefa.
Anotações (visíveis em todos os estados)	
Descrição	Descrição do grupo ou das ações de correção.
Comentários adicionais	Informações adicionais.
Atividades	Anotações do sistema.
Links relacionados	
Examinar Itens Vulneráveis Novamente	Aciona uma nova verificação dos itens vulneráveis para determinar se eles foram corrigidos.
Status da atualização	Exibe a data e a hora da última atualização. Agrega o seguinte dos IVs na tarefa: • Estado de tarefas de correção • Pontuações de risco e classificações de risco • Data de destino da correção e status (se aplicável) • Métricas como IVs ativos, total de IVs da seção Status de correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de tarefa de correção

Campo	Descrição
Listas relacionadas	
Itens vulneráveis	Itens vulneráveis nesta tarefa.
ANSs de tarefas	SLAs de plataforma associados a esta tarefa.
Soluções Preferenciais	Soluções preferenciais dos itens vulneráveis nesta tarefa.
Solicitações de Mudança	Solicitações de mudança associadas a esta tarefa.
Aprovações Solicitadas	(Visível quando a tarefa está no estado Em revisão.) Lista de aprovadores. Depois que o adiamento for aprovado, a tarefa de correção será movida para o estado Adiado.

Campos de formulário de configuração de questionário

Você pode definir um questionário distinto para uma coleção distinta de vulnerabilidades ou tarefas de correção filtrando as vulnerabilidades ou tarefas de correção respectivamente na seção Configuração do questionário de VR do formulário Configurações para gestão de exceções de VR.

O formulário Configuração do questionário aparece quando você seleciona o botão **Novo** na seção Configuração do questionário de VR das Configurações do formulário Gestão de exceções de VR.

Campos de formulário de configuração de questionário

Campo	Descrição
Nome	Nome do questionário.
Regra de aprovação	Regra de aprovação para a qual o questionário é aplicável. • **Solicitação de exceção para grupos de vulnerabilidade** • **Solicitação de exceção para itens vulneráveis** • **Falso positivo para grupos de vulnerabilidade** • **Falso positivo para itens vulneráveis** • **Questionário para controles de compensação para grupos vulneráveis** para solicitações de redução de risco da tarefa de correção. • **Questionário para controles de compensação de itens** vulneráveis para solicitações de redução de risco do item vulnerável.
Descrição	Descrição resumida da configuração do questionário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de formulário de configuração de questionário

Campo	Descrição
Ordem	O questionário com a ordem mais baixa aparece durante as solicitações.
Ativo	Habilitado por padrão, o que significa que o questionário está em uso.
Tabela	Tabela para a qual a regra de aprovação é aplicável. • Item vulnerável [sn_vul_vulnerable_item] para as regras de aprovação relacionadas a itens vulneráveis. • Tarefa de correção [sn_vul_vulnerability] para as regras de aprovação relacionadas às tarefas de correção.
Condição	Condição para os registros para os quais o questionário deve aparecer. Você pode aplicar a condição em todos os campos de um item vulnerável e tarefa de correção, exceto **Motivo**.
Questionário	Questionário que deve aparecer quando o responsável pela correção estiver solicitando exceção, falso positivo ou redução de risco.

Tópicos relacionados

Configurar Gestão de exceções para Vulnerability Response

Configurar questionário para redução de risco

Vulnerability Response campos de formulário de item vulnerável

Itens vulneráveis são criados automaticamente durante as importações de integração de vulnerabilidade de terceiros.

Campos de item vulnerável

Se você habilitou a verificação de vulnerabilidades do SAM NVD, os registros serão comparados ao software em seu Configuration Management Database (CMDB) e as correspondências serão encontradas com software vulnerável ou itens de configuração (ICs).

Campo	Descrição
Selecione marcador de segurança	Marcador desegurança para adicionar metadados ao registro ou identificar quem deve ter acesso a este registro de incidente de segurança. Este campo é exibido somente depois que o item vulnerável foi salvo.
Número	Número de item vulnerável gerado automaticamente para este registro.
Fonte	Scanner que encontrou este item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Pontuação de risco	**Pontuação de risco** quantificada que separa itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade. **Nota:** Esta **classificação de risco** base não é igual à **classificação de risco do registro da solução.**
Pontuação de risco	Valor calculado de risco que o item vulnerável representa para o seu ambiente. **Nota:** Essa **pontuação de risco** base não é igual à **pontuação de risco do registro da solução.** Para obter mais informações, consulte Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade.
Vulnerabilidade	ID da vulnerabilidade associada a este item vulnerável.
Item de configuração	Ativo afetado.
Estado	O padrão deste campo é **Aberto**, mas você pode alterá-lo para **Sob investigação** se a vulnerabilidade estiver pronta para correção imediata.
Até a data para redução de risco	Data em que os controles compensatórios aplicados ao item vulnerável expiram. **Nota:** Este campo é exibido somente quando o valor da pontuação de risco original está disponível.
Grupo de atribuição	Grupo selecionado para trabalhar nesta tarefa de correção.
Atribuído a	Indivíduo do grupo de atribuição selecionado que trabalha nesta vulnerabilidade.
Criado em	Data em que este item vulnerável foi criado em sua instância.
Aberto pela última vez	Data em que o item vulnerável foi aberto mais recentemente em sua instância. Inicialmente, é a mesma que a data de criação do item vulnerável. No entanto, se ele foi fechado e reaberto, a data da última abertura conterá a data e a hora da reabertura.
Atualizado em	Data da última verificação.
Vulnerabilidade	
Resumo	Descrição da vulnerabilidade.
Gravidade	Grau normalizado de severidade desta vulnerabilidade. Mapas de severidade são fornecidos para NVD e com ServiceNow integrações de terceiros. Para obter mais informações sobre como criar ou ajustar mapas de severidade, consulte Criar um mapa de severidade Vulnerability Response.
Pontuação de vulnerabilidade (v3)	Pontuação do CVSS v3.
Pontuação de vulnerabilidade (v2)	Pontuação do CVSS v2.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Explorar itens existentes	Sim, se pelo menos uma exploração estiver associada às vulnerabilidades associadas a este item vulnerável.
Vetor de ataque Exploit	Vetor de ataque mais vulnerável das explorações para as vulnerabilidades associadas a este item vulnerável.
Nível de habilidade Exploit	Nível de habilidade mais baixo necessário para explorar as vulnerabilidades associadas a este item vulnerável.
Data de publicação	Data em que a vulnerabilidade foi publicada.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez.
Ameaça	Informações relevantes sobre a ameaça. Extraído do registro de entrada vulnerável. **Nota:** Todas as mudanças feitas aqui atualizam o registro de entrada vulnerável.
Anotações de correção	Solução relevante para a ameaça, extraída do registro de entrada vulnerável.
Etapas de Correção Disponível somente com Solução de gerenciamento de vulnerabilidade.	
Solução preferencial	Solução preferencial importada do registro de vulnerabilidade. **Nota:** Quaisquer mudanças manuais feitas aqui não mudam o registro de vulnerabilidade e permanecem inalteradas no IV nas importações subsequentes.
Resumo	Resumo importado do registro da solução.
Detecção inicial	
Nome DNS	Nome do serviço de nomes de domínio. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Nome NetBIOS	Nome do NetBIOS. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Endereço IP	Endereço IPv4 ou IPv6. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Porta	Endereço da porta
Protocolo	Nome do protocolo.
SSL	Se a criptografia SSL é usada ou não.
Detecções	
Status	Estado da detecção.
Primeiro encontrado	Data em que a origem de terceiros encontrou pela primeira vez a detecção neste ativo.
Último encontrado	Data em que a origem de terceiros encontrou a detecção neste ativo.
Nome DNS	Nome do serviço de nomes de domínio. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome NetBIOS	Nome do NetBIOS. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Endereço IP	Endereço IPv4 ou IPv6. Se um IC não for fornecido, este campo será usado para pesquisar um IC correspondente, se houver.
Porta	Endereço da porta
Protocolo	Nome do protocolo.
SSL	Se a criptografia SSL é usada ou não.
Horas encontradas	Número de vezes que esta vulnerabilidade foi detectada neste ativo pela origem de terceiros.
Execução de integração	Execução de integração que importou a detecção.
Fechar Disponível depois que o item vulnerável foi corrigido e encerrado. Os itens nesta seção são somente leitura.	
Encerrado por	Quem encerrou o item vulnerável.
Encerrado	Data em que o item vulnerável foi encerrado.
Anotações de encerramento	Informações incluídas no fechamento.
Momento do fechamento	Período após o qual o IV foi encerrado. Se o IV for reaberto, o valor do campo Idade encerrada será definido como zero.
Anotações	
Comentários adicionais/Anotações de trabalho	Qualquer informação relevante. Marque a caixa de seleção para adicionar Comentários adicionais. A partir da Vulnerability Response v20.0, você pode adicionar anotações de trabalho na seção Anotações para um item vulnerável adiado.
Atividade	Aparece somente quando uma anotação de trabalho foi criada.
Links relacionados	
Calcular Pontuação de Risco	Quando as calculadoras de **Gravidade da Vulnerabilidade** ou de **Pontuação de Risco** estão habilitadas, o campo **Pontuação de Risco** é atualizado.

A seguir estão as listas relacionadas a itens vulneráveis.

Lista relacionada	Descrição
Tarefas de correção	Tarefas associadas a este item vulnerável.
Tarefas que afetam	Tarefas associadas a este item vulnerável.
Endereços IP associados	Disponível se a aplicação Vulnerability Integration Qualys Vulnerability Integration estiver instalada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista relacionada	Descrição
	Endereços IP encontrados durante a desduplicação.
Serviços afetados	Serviços de negócios afetados por este item vulnerável. Mostrado quando essas informações estão disponíveis no registro do cmdb. Essas informações podem ser inseridas manualmente ou usando a aplicação ServiceNow® Mapeamento de serviços. Consulte Service Mapping para obter mais informações. Se um IC afetado associado ao item vulnerável for adicionado ou atualizado, as informações nesta lista relacionada serão atualizadas automaticamente quando o registro for salvo.
Tíquetes de Qualys	Qualys informações de integração de tíquete associadas a este item vulnerável.

Campos de formulário de solução

As soluções são criadas automaticamente quando os registros são baixados de integrações de soluções de terceiros e armazenados em **Soluções** em Vulnerability Response.

Campos de entrada de integração da solução

Os campos importados nesta tabela são somente leitura.

Campo	Descrição
Número	Identificador atribuído à solução.
Fonte	Origem da solução.
Identificador da origem	Identificador de origem para esta solução.
Pontuação de risco	Separa a **pontuação de risco** do registro da solução em intervalos de Crítico a Nenhum. Para obter mais informações sobre a **classificação de risco**da solução , consulte Solução de gerenciamento de vulnerabilidade. **Nota:** **A classificação de risco** da solução não é igual à **classificação**de risco do **item vulnerável**, **da entrada de vulnerabilidade de terceiros** e **da tarefa**de correção.
Pontuação de risco	Cálculo ponderado com base na **pontuação de risco** e na contagem de itens vulneráveis com esta solução como a **solução preferencial**. Para obter mais informações sobre a pontuação de risco da solução, consulte Solução de gerenciamento de vulnerabilidade. **Nota:** **A pontuação de risco** do registro de solução não é igual à pontuação de risco do **item vulnerável**, **da entrada de vulnerabilidade de terceiros**e das **tarefas** de **correção**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Disponível quando o NVD do SAM está habilitado, mas se não houver itens vulneráveis (IV) ativos associados a uma vulnerabilidade, a **pontuação de risco** da solução será definida como zero.
Maior substituição	Indica que nenhuma solução o substitui.
Tipo de solução	Que tipo de solução é. As opções são: • Solução alternativa • Mitigação • Correção do Fornecedor • Patch • Acúmulo • Direito • Não Corrigirá • Nenhum disponível
Requer reinicialização	Reinicialização necessária. As opções são: • Sim • Não • Talvez
Data de publicação	Data em que a vulnerabilidade foi publicada por origem.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez por origem.
Resumo	Resumo de correção da solução.
Informativo	Boletim de segurança associado à solução.
Categorias dos Produtos	Categorias de produto às quais a solução se aplica.
Produtos	Produtos aos quais a solução se aplica.
Detalhes da solução	
Descrição	Se nenhum conteúdo estiver disponível na origem da solução, você será direcionado para outra seção ou solução relevante para obter mais informações.
Links	Recursos de internet importados associados à solução.
Detalhes da Vulnerabilidade	
Anotações sobre vulnerabilidade	Resumo de vulnerabilidades corrigidas pela solução.
Status da Correção	
Metas da solução preferencial	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Status de correção para itens vulneráveis e seus itens de configuração exclusivos (ICs), para os quais esta é a solução preferencial. **Nota:** Um IC exclusivo é contado apenas uma vez, independentemente de quantos IVs ele esteja associado.	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número de itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção. Esta contagem exclui itens vulneráveis adiados.
Percentual de IVs corrigidos	Percentual concluído para correção de item vulnerável (IV). Aplica-se a IVs para os quais esta solução é a preferencial. Esta contagem exclui IVs adiados.
ICs Restantes	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos para os quais esta solução é a preferencial para correção. Esta contagem exclui os ICs de itens vulneráveis adiados.
Total de ICs	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção. Esta contagem exclui os ICs de itens vulneráveis adiados.
Percentual de ICs corrigidos	Percentual concluído de ICs exclusivos corrigidos (o que significa que todos os IVs desse IC e desta solução foram corrigidos). Determinado pelo número de ICs corrigidos sobre o total de ICs exclusivos associados a itens vulneráveis com a solução preferencial. Esta contagem exclui os ICs de itens vulneráveis adiados.
Metas da solução preferencial (inclui adiada) Status de correção para itens vulneráveis e seus ICs exclusivos, incluindo adiados, para os quais esta é a solução preferencial.	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é a preferencial para correção.
Total de IVs	Número de itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção.
Percentual de IVs corrigidos	Percentual concluído para correção de item vulnerável (IV). Aplica-se a IVs para os quais esta solução é a preferencial.
ICs Restantes	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos para os quais esta solução é a preferencial para correção.
Total de ICs	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos e encerrados para os quais esta solução é a preferencial para correção.
Percentual de ICs corrigidos	Percentual concluído de ICs exclusivos corrigidos (o que significa que todos os IVs desse IC e desta solução foram corrigidos). Determinado pelo número de ICs corrigidos sobre o total de ICs exclusivos associados a itens vulneráveis com a solução preferencial. Esta contagem exclui os ICs de itens vulneráveis adiados.
Possíveis Metas da Solução Status de correção de itens vulneráveis e seus ICs exclusivos, com uma vulnerabilidade relacionada a esta solução.	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é uma possível solução para correção. Esta contagem exclui itens vulneráveis adiados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
ICs Restantes	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos para os quais esta solução é uma possível solução para correção. Esta contagem exclui itens vulneráveis adiados.
Possíveis destinos da solução (inclui adiados) Status de correção de itens vulneráveis e seus ICs exclusivos, incluindo adiados, com uma vulnerabilidade que pode ser corrigida por esta solução, incluindo contagens de soluções preferenciais.	
Itens vulneráveis	Número de itens vulneráveis ativos (não encerrados) para os quais esta solução é uma possível solução para correção.
ICs Restantes	Número de ICs exclusivos associados a um ou mais itens vulneráveis ativos para os quais esta solução é uma possível solução para correção.
Anotações	
Anotações internas	Campo editável fornecido para o especialista em correção.
Links relacionados	
Atualizar status	Data e hora da última atualização do status de correção. Atualiza o seguinte: • Estado de tarefas de correção • Pontuação e classificação de risco • Métricas da seção Status de correção
Listas relacionadas	
Itens vulneráveis	Itens vulneráveis associados a esta solução como a solução preferencial para correção.
Vulnerabilidades de Terceiros	Vulnerabilidades de terceiros associadas a esta solução.
CVEs	Vulnerabilidades comuns de vulnerabilidade e exposição (CVE) associadas a esta solução.
Tarefas de correção	Tarefas de correção que contêm itens vulneráveis relacionados a esta solução preferencial para correção.
Soluções Anteriores	Soluções anteriores que resolvem uma ou mais vulnerabilidades desta solução.
Soluções Substitutas	Soluções posteriores que resolvem todas as vulnerabilidades desta solução. Esta lista está vazia quando a caixa **de substituição mais alta** está marcada.

Configurações de fluxo de trabalho de aprovação para solicitação de cancelamento de atribuição

Você pode projetar o fluxo de trabalho de aprovação para a remoção de atribuições de itens vulneráveis (IVs, VITs), tarefas de correção, itens vulneráveis da aplicação (AVITs) e itens vulneráveis de contêiner (CVITs) para você e seu grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

VIT, tarefa de correção, AVIT e CVIT têm uma regra de aprovação padrão cada. Cada regra de aprovação tem uma configuração de aprovação padrão. Cada configuração de aprovação tem um nível de aprovador padrão. As regras de aprovação para VITs, tarefa de correção, AVIT e CVIT são habilitadas por padrão. Como administrador, você pode executar as seguintes ações navegando até **Todos** > **Vulnerability Response** > **Minhas aprovações** > **Regras de aprovação** e selecionando a regra de aprovação apropriada.

- habilitar ou desabilitar uma regra de aprovação.
- criar e atualizar uma configuração de aprovação.
- defina condições para itens vulneráveis e tarefas de correção aos quais as regras de aprovação se aplicam.
- crie e atualize vários níveis de aprovador.

A tabela a seguir mostra as regras de aprovação padrão, as configurações de aprovação e os níveis de aprovador para um VIT, tarefa de correção, AVIT e CVIT que são enviados com o sistema de base.

Regras de aprovação padrão, configurações de aprovação e níveis de aprovador

Tipo	Regra de aprovação	Configuração de aprovação	Níveis de aprovação
VIT ou VI	Solicitação de mudança do campo de item vulnerável	Solicitação de mudança do campo de item vulnerável	Solicitação de cancelamento de atribuição de nível 1 para IV
Tarefa de correção	Solicitação de mudança do campo Grupo de vulnerabilidade	Solicitação de mudança de campo de vulnerabilidade	Nível 1: não atribuir solicitação para VG
AVIT	Solicitação de mudança do campo de item vulnerável da aplicação	Solicitação de mudança de campo de vulnerabilidade da aplicação	Desatribuir item de vulnerabilidade da aplicação
CVIT	Aprovação para gestão de contêiner	Configuração padrão Cancelar atribuição de CVIT	Nível de aprovação de desatribuição de CVIT – 1

Para obter mais informações sobre como aprovar solicitações de desatribuição, consulte Aprovar uma solicitação de cancelamento de atribuição no Vulnerability Response.

Vulnerability Response exemplos de regra de tarefa de correção

Exemplos de regras de tarefa de correção usando vulnerabilidade e risco, ou impacto, ou item de configuração (IC).

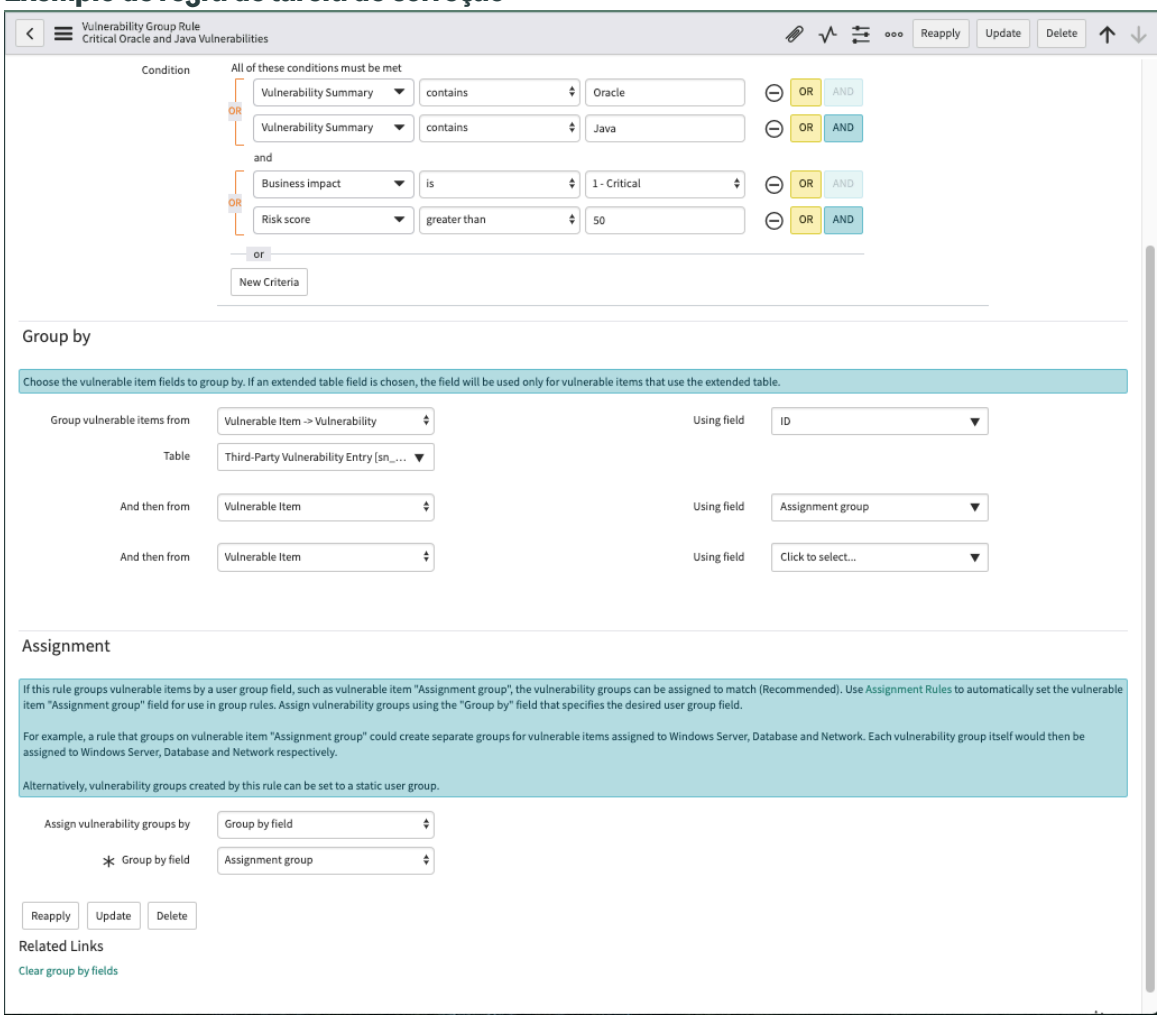
Regra de tarefa de correção para agrupar itens vulneráveis Java e Oracle de alto risco

Este exemplo mostra um passo a passo da regra que agrupa itens vulneráveis Java e Oracle por vulnerabilidade e os atribui aos respectivos grupos de suporte.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de regra de tarefa de correção



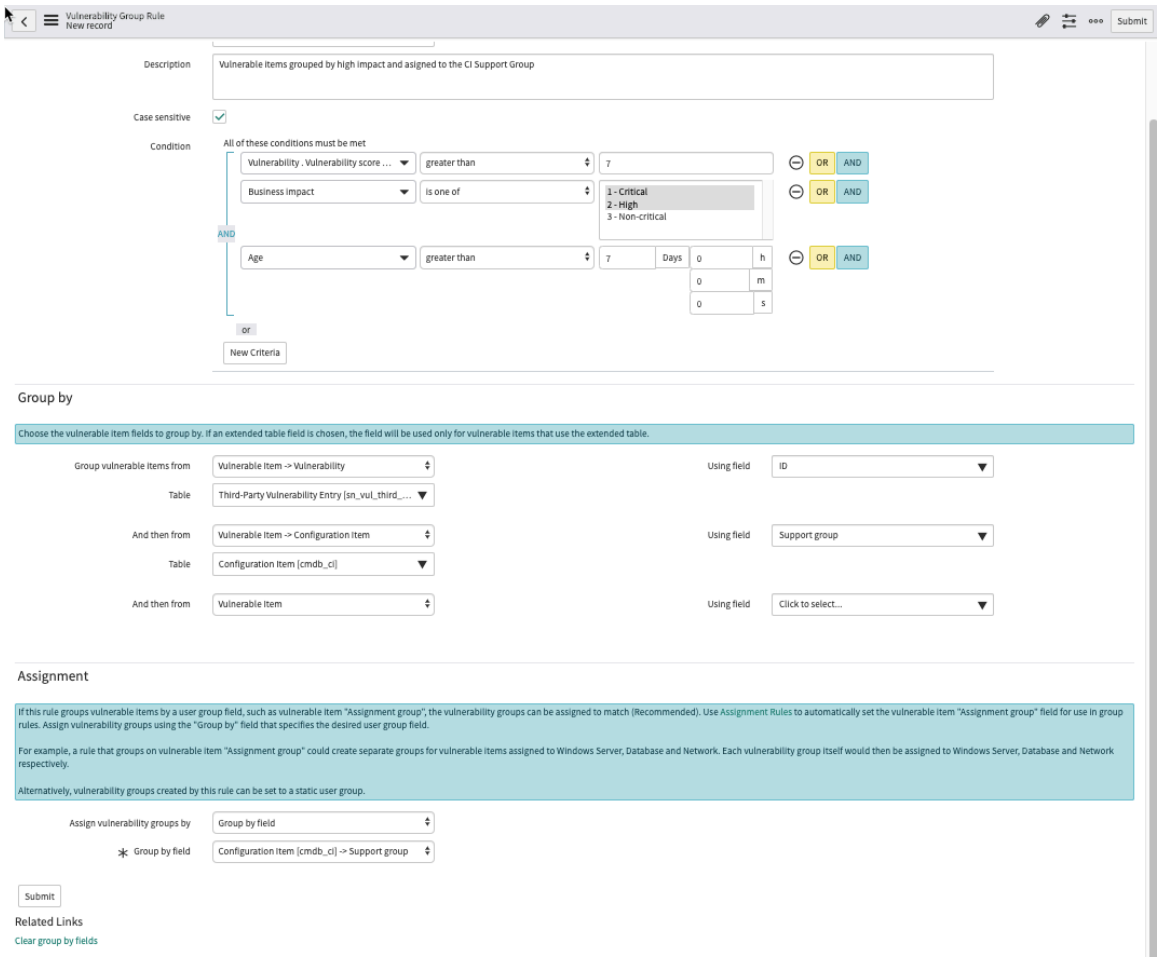
Clique com o botão direito do mouse no cabeçalho para **Salvar**.

Regra de tarefa de correção para agrupar todos os itens vulneráveis de alto impacto por vulnerabilidade e grupo de suporte de IC

Este exemplo mostra as configurações do campo de formulário para uma regra de grupo para itens vulneráveis de alto impacto que os atribui ao grupo de suporte de IC.

Tradução automática

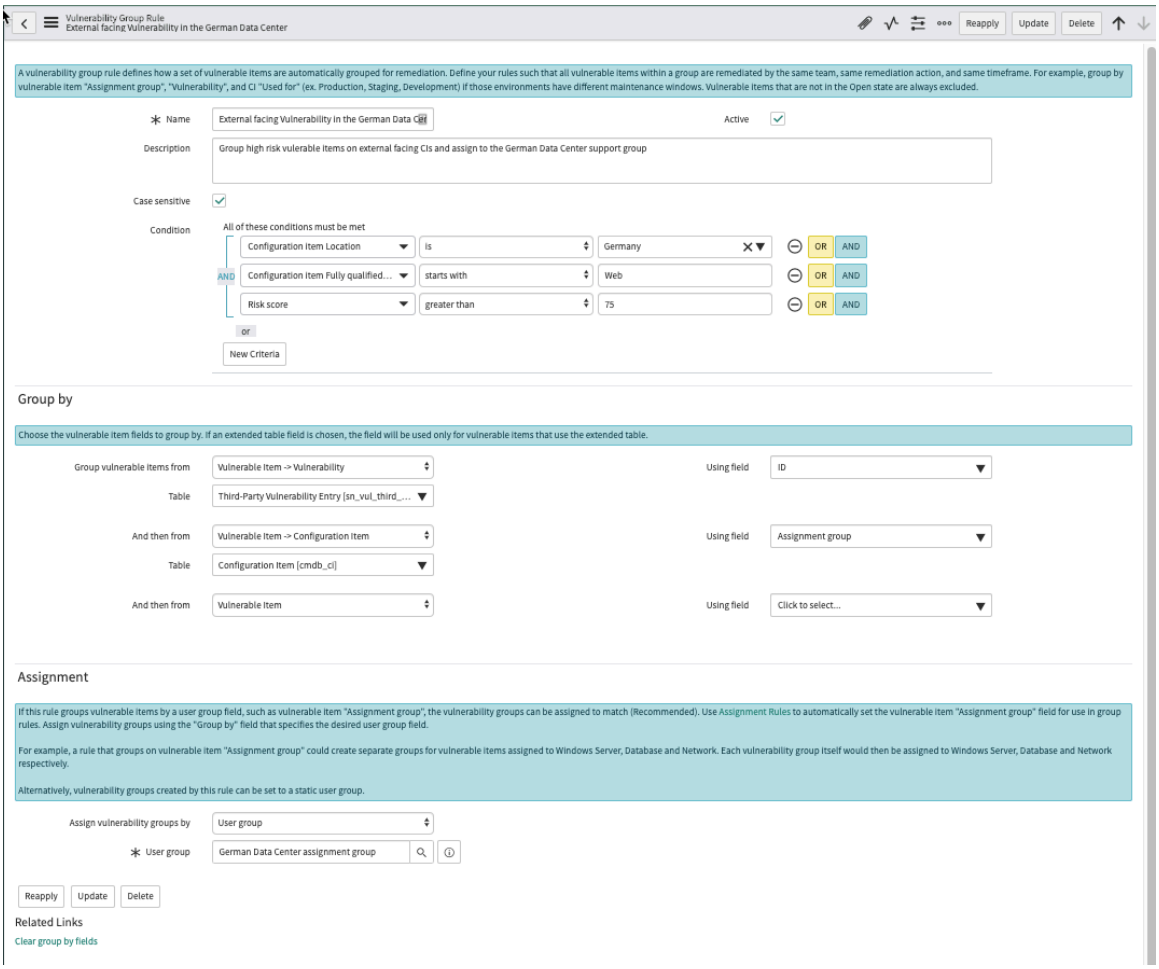
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Regra de tarefa de correção para agrupar todas as vulnerabilidades de alto risco em um IC externo em um datacenter alemão

Este exemplo mostra as configurações de campo de formulário para uma regra de grupo para vulnerabilidades de alto risco em ICs externos em um datacenter alemão. Eles são atribuídos ao grupo de atribuição de datacenter alemão.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exemplo de cálculo de pontuação de risco para Vulnerability Response

Você pode determinar as calculadoras de pontuação de risco para gerar pontuações de risco que usam os dados de vulnerabilidade e ativo exclusivos da sua organização.

Exemplo de determinação de pontuações de calculadoras de regra de risco

O exemplo a seguir demonstra como as pontuações das calculadoras de regra de risco são determinadas.

Suponha que uma calculadora de regra de risco esteja configurada com os campos nesta tabela:

Campo	Ponderação	Detalhamento de peso
Vulnerabilidade.Severidade	50	Padrão: 20 1 - Crítico: 100 2 - Alto: 80 3 - Média: 60 4 - Baixo: 40 5 - Nenhum: 20

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Ponderação	Detalhamento de peso
Vulnerabilidade.Existem exploração	50	Padrão: 50 Sim: 100 Nº: 0

Além disso, suponha que os itens vulneráveis mostrados nesta tabela estejam presentes no sistema:

ID	Gravidade da vulnerabilidade	Existe exploração de vulnerabilidade
VIT00001	1 - Crítica	1 - Sim
VIT00002	2 - Alta	1 - Sim
VIT00003	3 – Médio	2 – Não
VIT00004	4 - Baixa	2 – Não
VIT00005	5 - Nenhum	2 – Não

O cálculo da pontuação de risco para os itens vulneráveis é calculado com base na fórmula:

`Pontuação de risco = (S(gravidade) * FV (gravidade). + W(existe exploração) * FV(existência de exploração)) / 100`

em que **W** é o peso e **FV** é a porcentagem de peso do valor do campo.

A pontuação de risco resultante para esses itens vulneráveis é descrita nesta tabela:

ID	Gravidade da vulnerabilidade (50%)	Existe exploração de vulnerabilidade (50%)	Pontuação de risco resultante
VIT00001	1 – Crítico (50% x 100)	1 – Sim (50% x 100)	100
VIT00002	2 – Alto (50% x 80)	1 – Sim (50% x 100)	90
VIT00003	3 – Média (50% x 60)	2 – Não (50% x 0)	30
VIT00004	4 – Baixo (50% x 40)	2 – Não (50% x 0)	20
VIT00005	5 - Nenhum (50% x 20)	2 – Não (50% x 0)	10

Nota:
Para VIT00005, como o valor da severidade está vazio, a ponderação padrão é aplicada.

Se a porcentagem de ponderação for alterada para um dos valores de campo, consulte esta tabela para obter os resultados:

Campo	Ponderação	Detalhamento de peso
Vulnerabilidade.Severidade	50	• Padrão: 20 • 1 - Crítico: 100 • **2 - Alto: 70**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Ponderação	Detalhamento de peso
		*valor revisado • 3 - Média: 60 • 4 - Baixo: 40
Vulnerabilidade.Existem exploração	50	• Padrão: 50 • Sim: 100 • Nº: 0

A pontuação de risco dos itens vulneráveis após a reaplicação da calculadora é mostrada nesta tabela:

ID	Gravidade da vulnerabilidade (50%)	Existe exploração de vulnerabilidade (50%)	Pontuação de risco resultante
VIT00001	1 – Crítico (50% x 100)	1 – Sim (50% x 100)	100
VIT00002	**2 – Alto (50% x 70)** *valor revisado	1 – Sim (50% x 100)	**85** *valor revisado
VIT00003	3 – Média (50% x 60)	2 – Não (50% x 0)	30
VIT00004	4 – Baixo (50% x 40)	2 – Não (50% x 0)	20
VIT00005	5 - Nenhum (50% x 20)	2 – Não (50% x 0)	10

Tratamento de erros para detecções

Os erros são registrados ao criar detecções ou criar e atualizar itens vulneráveis, ao processar os anexos. Se um processo de integração de vulnerabilidade falhar, os erros serão registrados na guia "Log de integrações de vulnerabilidade".

Esses erros são registrados em log, com uma das seguintes categorias.

Campo	Descrição
Criação de VI	Erro ao criar ou atualizar a detecção.
Detecção	Erro ao criar uma detecção.

Experiência de dispositivos móveis Vulnerability Response

Como proprietário de correção, você pode acessar a aplicação Vulnerability Response (VR) em sua instância Now Platform® com seu dispositivo móvel Android ou iOS.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerability Response

Para se familiarizar com os conceitos de resposta de vulnerabilidade e como este produto pode ajudar sua organização, consulte Noções básicas sobre Vulnerability Response.

Nota:
Antes de instalar o Aplicativo Vulnerability Response Mobile mobile, familiarize-se com o Mobile Agent .

Visão geral

Como um usuário com a função de proprietário de correção (sn_vul.remediation_owner), o Aplicativo Vulnerability Response Mobile permite que você exiba e pesquise vulnerabilidades, tarefas de correção e atribuições em sua instância Now Platform diretamente do seu dispositivo móvel Android ou iOS.

Você será notificado quando tarefas de correção (RTs) ou IVs forem atribuídos a você ou ao seu grupo de atribuição. Esta aplicação oferece ao proprietário de correção a flexibilidade de reatribuir, editar campos e iniciar a correção sem estar vinculado à área de trabalho.

Você tem acesso a vulnerabilidades, itens de vulnerabilidade, módulos e todas as soluções. Você pode executar as seguintes tarefas no seu dispositivo móvel:

- Exibir e atualizar tarefas de correção.
- Exibir solicitações de mudança.
- Reatribua uma tarefa de correção ou item de vulnerabilidade a outro membro de um grupo de atribuição.
- Exiba notificações quando uma tarefa de correção crítica for atribuída a você ou a um de seus grupos de atribuição.
- Edite um subconjunto de campos em registros de tarefa de correção.
- Pesquise tarefas de correção que correspondam a critérios de pesquisa específicos.

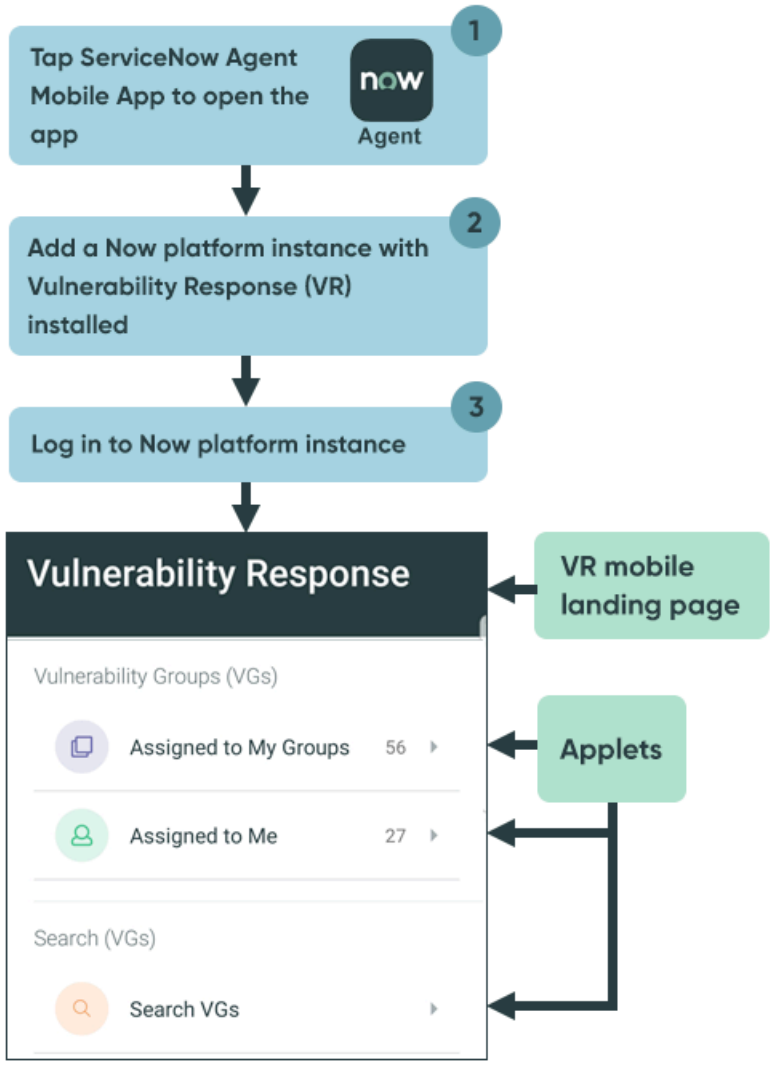
A figura a seguir ilustra como você faz login na instância Now Platform do seu dispositivo móvel e a tela inicial do Aplicativo Vulnerability Response Mobile que é exibida após o login.

Para obter instruções passo a passo sobre como configurar sua instância Now Platform e instalar o Aplicativo Vulnerability Response Mobile, consulte Configurar check-list para o Aplicativo Vulnerability Response Mobile. Para obter instruções sobre como fazer login, consulte Faça login no Aplicativo Vulnerability Response Mobile.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicativo Vulnerability Response Mobile



Aplicações

Aplicações são os ServiceNow componentes de software, como Security Incident Response (SIR), Vulnerability Response (VR), Governança, risco e conformidade (GRC) e outros produtos ServiceNow que fornecem recursos e funcionalidades específicos em sua instância Now Platform. Depois de instalar os aplicativos principais que têm aplicativos para celular na sua instância Now Platform, esses aplicativos são exibidos como ícones na parte inferior do seu dispositivo móvel.

Ícone do Vulnerability Response no dispositivo móvel

Pastas

Cada aplicação ServiceNow® mobile contém pastas que separam os applets por categorias. Na imagem anterior, tarefas de correção e pesquisa (VGs) são as pastas para o Aplicativo Vulnerability Response Mobile.

Applets

Applets são as diferentes opções da aplicação. Na imagem anterior, os ícones em Tarefas de correção e Pesquisa (VGs) são os applets disponíveis para Aplicativo Vulnerability Response Mobile.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Consulte os tópicos a seguir para obter mais informações sobre os applets do Aplicativo Vulnerability Response Mobile.

Configurar check-list para o Aplicativo Vulnerability Response Mobile

A check-list a seguir inclui as tarefas de configuração que você deve concluir na instância Now Platform® e no dispositivo móvel antes de usar o Aplicativo Vulnerability Response Mobile.

Antes de Iniciar

Mais informações seguem cada etapa na coluna à direita. Tempo estimado para concluir esta tarefa: 15 a 20 minutos.

Funções necessárias: admin, sn_vul.remediation_owner

Você configurou com sucesso seu dispositivo móvel para Aplicativo Vulnerability Response Mobile. A próxima etapa é fazer login no Aplicativo Vulnerability Response Mobile e adicionar uma instância Now Platform ao seu dispositivo móvel.

Procedimento

1. Como opção, imprima esta check-list e use-a como guia nas tarefas necessárias para instalar o Aplicativo Vulnerability Response Mobile.
2. Verifique se cada item da lista está concluído para que você possa fazer login em Aplicativo Vulnerability Response Mobile e adicionar uma instância Now Platform.

Check-list móvel

Item	Descrição
☐	Como um usuário com a função de administrador, verifique se você tem a aplicação principal Vulnerability Response instalada em uma instância Now Platform. Esta é a instância Now Platform que você exibe no seu dispositivo móvel. **Nota:** A aplicação principal Vulnerability Response e a instância Now Platform devem ser da mesma versão da família. **a.** Para verificar se a aplicação principal está instalada na sua instância, navegue até Plug- **ins** e pesquise por Vulnerability Response. **b.** Se a aplicação principal Vulnerability Response ainda não estiver instalada, clique em **Instalar** para instalá-la. Para obter mais informações sobre como instalar a aplicação principal Vulnerability Response, consulte Como instalar Vulnerability Response. Para obter mais informações sobre como obter a aplicação principal Vulnerability Response no ServiceNow Store, obter direito, instalar aplicações principais e ativar dependências, consulte Security Operations e o ServiceNow Store.
☐	Como um usuário com a função de administrador, verifique se você tem o Aplicativo Vulnerability Response Mobile instalado na instância Now Platform que deseja exibir no seu dispositivo móvel.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	Nota: As instâncias Aplicativo Vulnerability Response Mobile e Now Platform devem ser da mesma versão da família. As aplicações Aplicativo Vulnerability Response Mobile e Vulnerability Response devem ser compatíveis. Para obter mais informações sobre a compatibilidade da aplicação Vulnerability Response, consulte Vulnerability Response e Matriz de compatibilidade do Configuration Compliance. Baixe e instale o Aplicativo Vulnerability Response Mobile do ServiceNow Store na sua instância Now Platform. Quando você instala o Aplicativo Vulnerability Response Mobile, suas dependências, com.glide.sg e com.glide.sg.agent_native_client, também são instaladas. Para verificar se essas dependências estão instaladas: **a.** Navegar até **Todos** > **Plug-ins**. **b.** Pesquise os IDs de plug-in (com.glide.sg e com.glide.sg.agent_native_client). **c.** Se eles não estiverem ativados, ative esses plug-ins. Esses plug-ins são necessários para o Aplicativo Vulnerability Response Mobile. Para obter mais informações sobre como obter a aplicação Aplicativo Vulnerability Response Mobile no ServiceNow Store, obter direito, instalar aplicações e ativar dependências, consulte Security Operations e o ServiceNow Store.
☐	Como um usuário com a função de administrador, na sua instância Now Platform, verifique se você atribuiu usuários móveis com as funções Now Platform necessárias. **a.** Para exibir as funções atribuídas a um usuário, navegue até **Todos** > **Administração** > **Usuários**. **b.** Selecione o nome de usuário seguido pela lista relacionada de funções. Todas as funções atribuídas a este usuário serão exibidas. **c.** Verifique se um usuário está atribuído ou atribua um usuário com a função de biblioteca de infraestrutura de TI (itil). Usuários com a função itil podem criar, abrir, atualizar e fechar solicitações de mudança e tarefas de correção. Somente usuários com a função itil podem ter tarefas atribuídas a eles. **d.** Verifique se um usuário está atribuído ou atribua um usuário com a função de proprietário de correção (sn_vul.remediation_owner). Usuários com a função sn_vul.remediation_owner podem ler registros de vulnerabilidade e solução. Esta função é adicionada automaticamente quando você atribui a função itil. **e.** Verifique se você criou todos os grupos de atribuição necessários e atribuiu usuários móveis a esses grupos. **Nota:** Se você tiver um grande número de usuários para o aplicativo para celular, como alternativa, poderá atribuir a função sn_vul.remediation_owner a um grupo. Cada usuário adicionado ao grupo herda esta função.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	Para obter mais informações sobre regras de atribuição e grupos, consulte Vulnerability Response visão geral de regras de atribuição. Para obter mais informações sobre usuários e atribuição de funções a usuários e grupos, consulte Administração de usuários .
☐	Como um usuário com a função de proprietário de correção (sn_vul.remediation_owner), baixe o aplicativo Agent ServiceNow® mais atual no seu dispositivo móvel. O aplicativo Agent mais atual está disponível na Apple iOS App Store e na Google Play Store.
☐	Como um usuário com a função sn_vul.remediation_owner, verifique se as notificações estão habilitadas no seu dispositivo móvel e na sua instância Now Platform. As notificações informam quando tarefas de correção críticas são atribuídas a você ou ao seu grupo de atribuição. Para ajudá-lo com a correção oportuna, depois de habilitar as notificações, clique em uma notificação no Aplicativo Vulnerability Response Mobile e navegue diretamente para o registro. Para habilitar notificações na sua instância Now Platform para que elas sejam exibidas no seu dispositivo móvel, siga estas etapas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Item	Descrição
	a. Verifique se você baixou e instalou o Aplicativo Vulnerability Response Mobile na sua instância Now Platform. **b.** Em Configurações do sistema na sua instância Now Platform, em Notificações, verifique se você habilitou o **Aplicativo para celular da ServiceNow**. Para obter mais informações sobre como definir notificações, consulte Notification preferences . Now Platform As notificações do também são exibidas na tela de mensagens do seu dispositivo móvel. Verifique se as notificações também estão habilitadas nas configurações do seu dispositivo móvel.

Faça login no Aplicativo Vulnerability Response Mobile

Abra o aplicativo Vulnerability Response Mobile e adicione uma instância da Now Platform com Vulnerability Response ao seu dispositivo móvel.

Antes de Iniciar

Verifique se você concluiu as etapas de configuração descritas em Configurar check-list para o Aplicativo Vulnerability Response Mobile.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

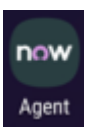
Função necessária: responsável pela correção (sn_vul.remediation_owner)

Por Que e Quando Desempenhar Esta Tarefa

Tempo para concluir esta tarefa: 5 a 7 minutos.

Procedimento

1. No seu dispositivo móvel, toque no aplicativo **ServiceNow Agent**.



Se você ainda não estiver conectado a uma instância Now Platform, a tela Instâncias será exibida.

2. Se a instância Now Platform com a aplicação principal Vulnerability Response ainda não tiver sido adicionada ao seu dispositivo móvel, siga estas etapas para adicioná-la.

a. Na tela Instâncias exibida, toque no ícone de).
Uma tela é exibida solicitando que você insira e salve um endereço de uma instância Now Platform.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

b. Preencha os campos.

c. Tocar em **Salvar e fazer login**

3. Na tela de login ServiceNow exibida, insira o Nome de usuário e a Senha da instância Now Platform que você deseja adicionar e toque em **Login**.
   A tela inicial do Vulnerability Response é exibida. Você fez login com sucesso em Aplicativo Vulnerability Response Mobile !
4. Depois de fazer login, verifique se as notificações estão habilitadas no Aplicativo Vulnerability Response Mobile.

   a. Na tela inicial na parte inferior, toque em **Notificação**.

   b. Na tela Notificações, toque em **Habilitar notificações** se não estiver habilitado.
   As notificações do Now Platform são exibidas na tela Notificações no Aplicativo Vulnerability Response Mobile.

5. Depois de fazer login em uma instância no seu dispositivo móvel, é a instância padrão Now Platform no dispositivo.
   Se você quiser exibir outro Now Platform no dispositivo, deverá sair da instância padrão. Para sair:

   a. Toque no ícone **Configurações**.

   b. Toque **em Logout**.
   A tela Instâncias é exibida com todas as instâncias Now Platform que você adicionou ao dispositivo móvel.

   c. Opcional: Toque em outra instância para fazer login nela ou, como alternativa, siga as etapas anteriores para adicionar outra instância.

Resultado
Se a tela de instâncias do Aplicativo Vulnerability Response Mobile não for exibida depois de tocar no aplicativo **ServiceNow Agent** no seu dispositivo, verifique se o **ServiceNow Agent** é permitido como um aplicativo confiável no seu dispositivo. Para permitir o acesso como um aplicativo confiável, navegue até as configurações e gerenciamento geral de dispositivos no seu dispositivo e toque na opção (aplicativo de confiança etc.) para permitir o acesso.

Se uma mensagem de erro for exibida depois de inserir suas credenciais na tela de login, verifique se o nome de usuário e a senha da instância Now Platform estão corretos.

Se você tiver problemas para exibir a tela inicial, verifique sua conexão de rede.

Se você não conseguir exibir a tela Instâncias depois de tocar no aplicativo **ServiceNow Agent**, tente desinstalá-lo do seu dispositivo. Verifique se você tem a versão mais atual do app na App Store da Apple iOS ou na Play Store Google e tente reinstalá-lo.

Exibir, atribuir e editar tarefas de correção com o Aplicativo Vulnerability Response Mobile

Exiba, atribua ou edite os campos nos registros de tarefa de correção (RT) atribuídos ao seu grupo. Navegue pelas vulnerabilidades, itens de vulnerabilidade e registros de soluções e listas relacionadas para exibir soluções, métricas de implantação e itens a serem resolvidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

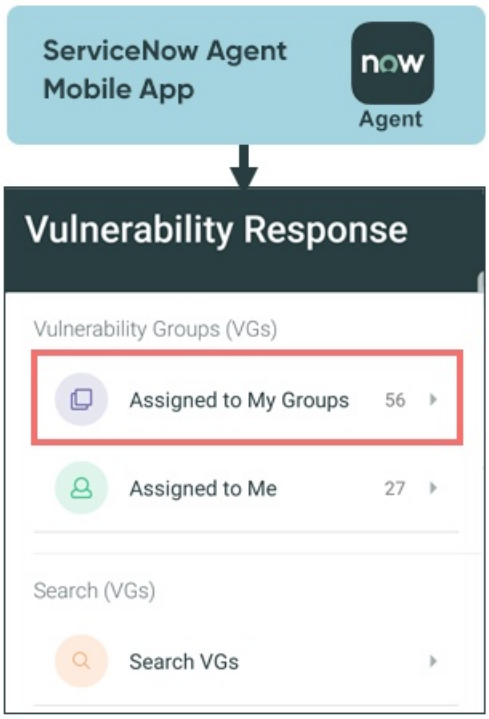
Função necessária: responsável pela correção (sn_vul.remediation_owner)

Por Que e Quando Desempenhar Esta Tarefa

Atribua registros RT (VUL) a você ou reatribua-os a outro membro do seu grupo. Como alternativa, exiba os detalhes dos registros de tarefa de correção ativos, itens vulneráveis (IV), vulnerabilidades de NVD e soluções antes da edição, atribuição ou correção. Tempo para concluir esta tarefa: 5 a 10 minutos.

Procedimento

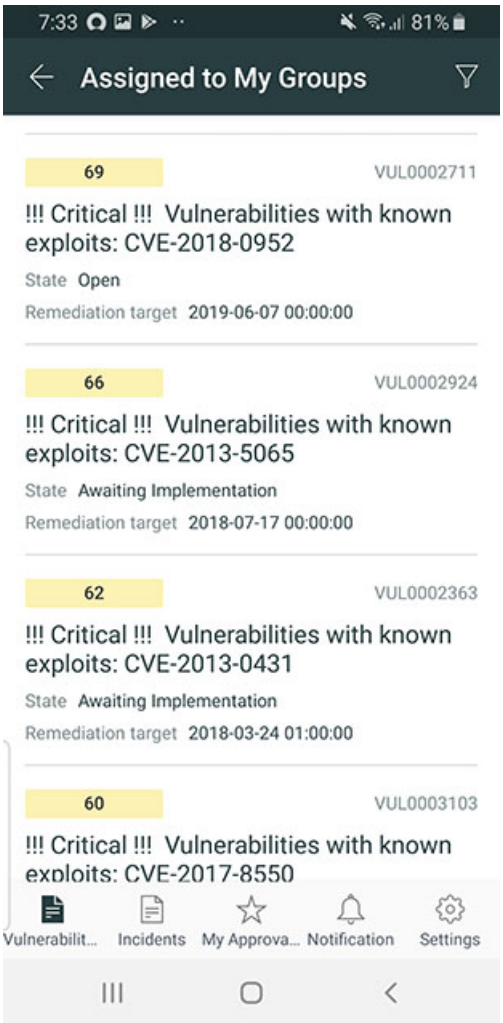
1. Se você não estiver conectado à sua instância Now Platform no seu dispositivo móvel, consulte Faça login no Aplicativo Vulnerability Response Mobilepara obter mais informações.
2. Com a tela inicial do Vulnerability Response exibida, toque **em Atribuído a Meus grupos**.
   Se você sair de Aplicativo Vulnerability Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



A lista de registros abertos atribuídos ao seu grupo é exibida.

Tradução automática

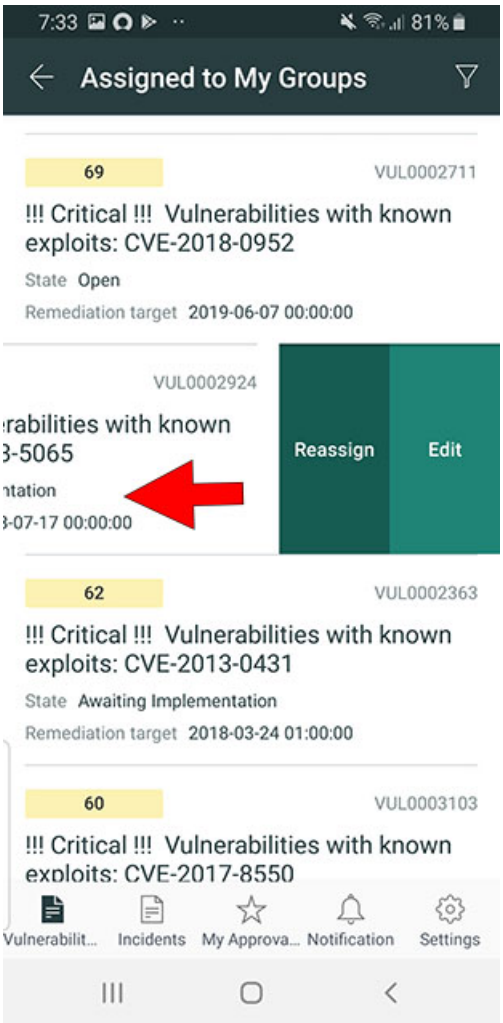
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. **Opcional:** Consulte Pesquisar tarefas de correção com o Aplicativo Vulnerability Response Mobile para pesquisar registros que correspondam a critérios específicos.
4. Como alternativa, com o ícone de filtro (ícone de) exibido, defina filtros para limitar o número de registros na lista.
   A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condição no Now Platform.
5. Para reatribuir ou editar um registro diretamente da lista, com a lista de registros abertos exibida, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



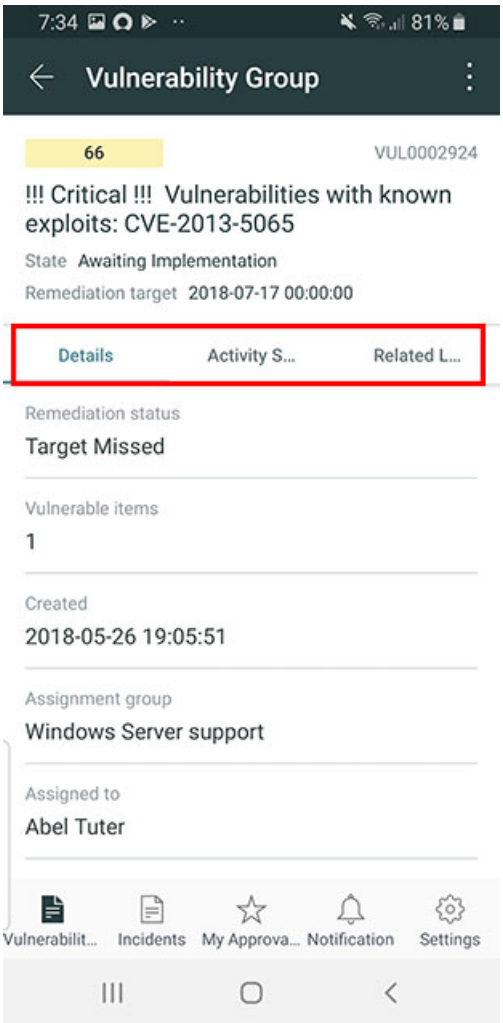
6. Escolha um no menu exibido para continuar.

7. Como alternativa, para exibir os detalhes de um registro de vulnerabilidade aberto e ver mais registros associados e listas relacionadas, com a tela Atribuído aos Meus grupos exibida, toque em um registro na lista.

8. No registro de tarefa de correção em aberto exibido, escolha uma opção na tabela a seguir para exibir as anotações de trabalho ou as listas relacionadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

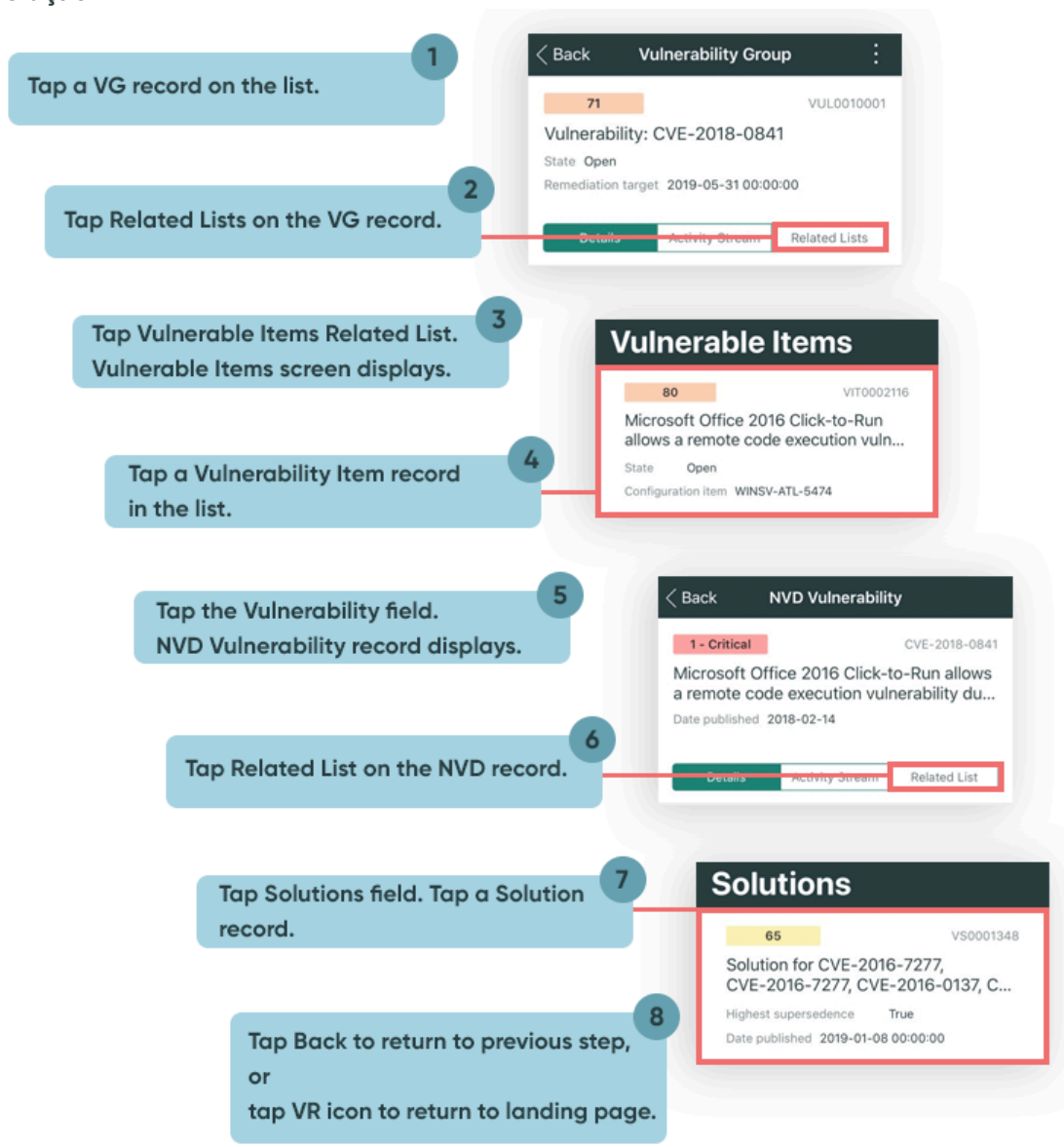


A imagem a seguir ilustra o caminho de navegação do registro da tarefa de correção até o registro da solução preferencial para a vulnerabilidade selecionada. Navegue pelos registros e listas relacionadas para exibir soluções, métricas de implantação e itens a serem resolvidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caminho de navegação da tarefa de correção por meio de um registro de solução



Tradução automática

9. Depois de revisar, editar ou corrigir, escolha um para continuar.

Exibir, reatribuir e editar tarefas de correção atribuídas a você com o Aplicativo Vulnerability Response Mobile

Exiba, atribua ou edite os campos nos registros de tarefas de correção que são atribuídos a você. Navegue pelos registros e listas relacionadas para exibir soluções, métricas de implantação e itens a serem resolvidos.

Antes de Iniciar

Função necessária: responsável pela correção (sn_vul.remediation_owner)

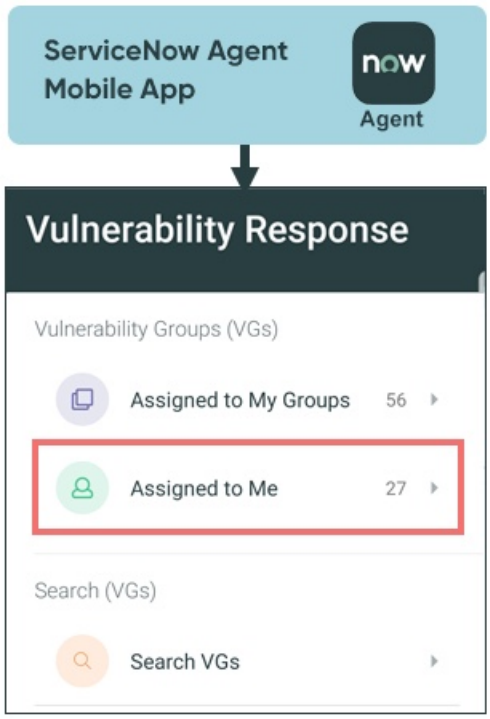
Por Que e Quando Desempenhar Esta Tarefa

Reatribuir ou editar registros atribuídos a você. Exiba os detalhes de registros de tarefas de correção ativas, registros de itens vulneráveis (IV), vulnerabilidades e soluções antes da edição, atribuição ou correção. Tempo para concluir esta tarefa: 5 a 10 minutos.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

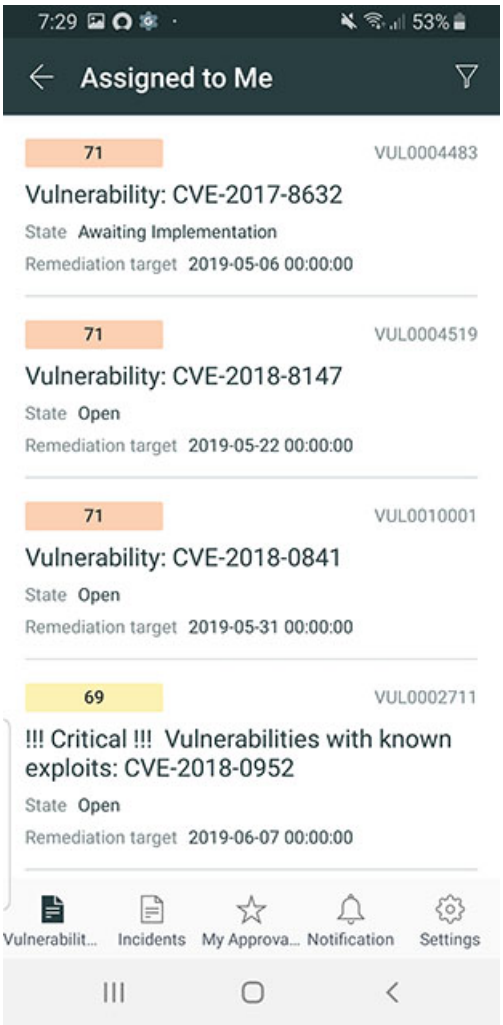
1. Se você não estiver conectado à sua instância Now Platform no seu dispositivo móvel, consulte Faça login no Aplicativo Vulnerability Response Mobilepara obter mais informações.
2. Com a tela inicial do **Vulnerability Response** exibida, toque **em Atribuído a mim**.
   Se você sair de Aplicativo Vulnerability Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



A lista de registros de tarefa de correção atribuídos a você é exibida.

Tradução automática

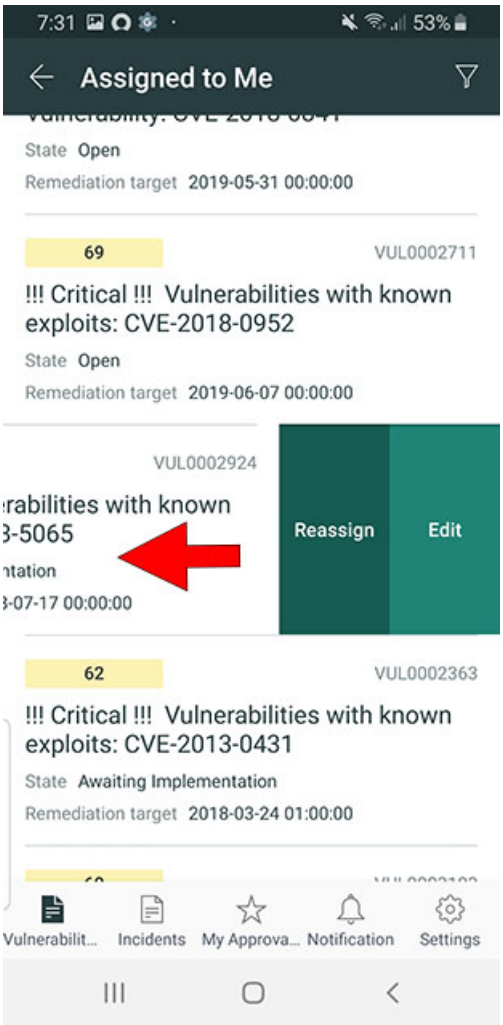
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. **Opcional:** Consulte Pesquisar tarefas de correção com o Aplicativo Vulnerability Response Mobile para pesquisar registros que correspondam a critérios específicos.
4. Como alternativa, com o ícone de filtro (ícone de) exibido, defina filtros para limitar o número de registros na lista.
   A filtragem de registros em telas no aplicativo para celular funciona como a filtragem com um construtor de condição no Now Platform.
5. Para reatribuir ou editar o registro diretamente da lista, com a tela Atribuído a mim exibida, deslize para a esquerda em um registro para abrir o menu.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



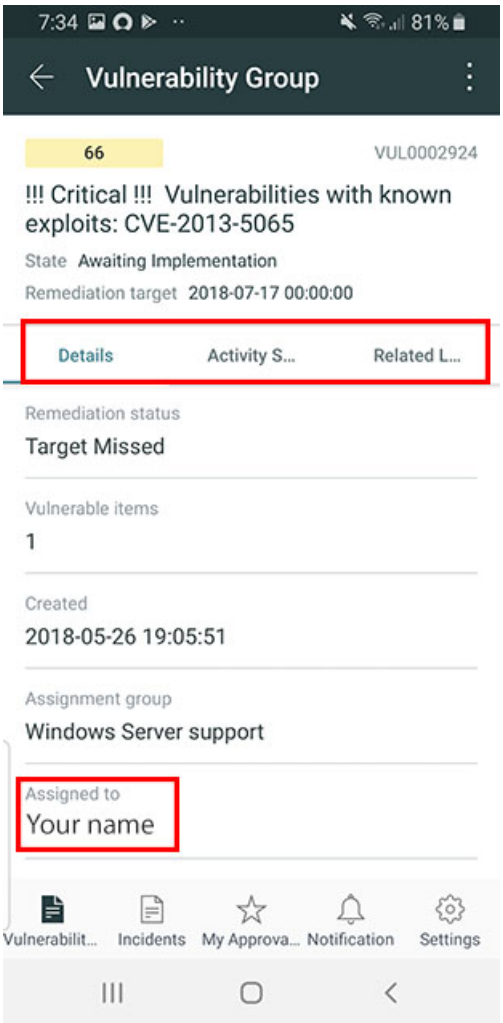
6. Escolha um para continuar.

7. Como alternativa, para exibir os detalhes de um registro aberto e ver mais registros associados e listas relacionadas, com a tela Atribuído a mim exibida, toque em um registro na lista.

8. No registro de tarefa de correção em aberto exibido, escolha uma opção na tabela a seguir para exibir as anotações de trabalho ou as listas relacionadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A imagem a seguir ilustra o caminho de navegação do registro da tarefa de correção até o registro da solução preferencial para a vulnerabilidade selecionada. Navegue pelos registros e listas relacionadas para exibir soluções, métricas de implantação e itens a serem resolvidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caminho de navegação do RT por meio de um registro de solução

Tradução automática

9. Escolha um para continuar.

Pesquisar tarefas de correção com o Aplicativo Vulnerability Response Mobile

Pesquise tarefas de correção que correspondam aos critérios de pesquisa específicos selecionados.

Antes de Iniciar

Função necessária: responsável pela correção (sn_vul.remediation_owner)

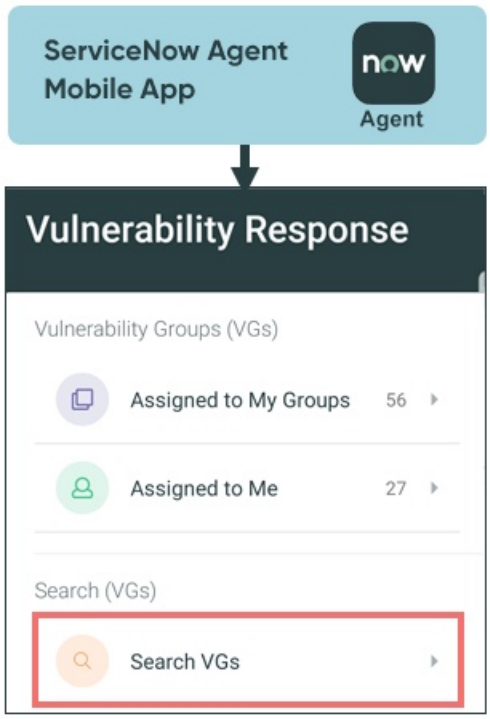
Por Que e Quando Desempenhar Esta Tarefa

Tempo para concluir esta tarefa: 5 a 7 minutos.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Se você não estiver conectado à sua instância Now Platform no seu dispositivo móvel, consulte Faça login no Aplicativo Vulnerability Response Mobilepara obter mais informações.
2. Com a tela inicial do **Vulnerability Response** exibida, toque **em Pesquisar RTs**.
   Se você sair de Aplicativo Vulnerability Response Mobile depois de fazer login, toque no aplicativo Now Agent a qualquer momento para retornar à última tela exibida.



3. Na tela Pesquisar exibida, toque nos campos e preencha o formulário com os critérios de pesquisa desejados.

   Siga as instruções após a tabela para editar os critérios de pesquisa, limpar os critérios de pesquisa ou enviar uma pesquisa.

Tocar neste campo	Para adicionar uma entrada em Android dispositivos	Para adicionar uma entrada em iOS dispositivos
Número	Toque na tela e insira um número de RT, por exemplo, (VUL0002372). Esse número é exibido no canto superior direito do registro de RT. Toque no ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTs. Toque no ícone fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTs.	Insira um número RT, por exemplo, (VUL0002372). Esse número é exibido no canto superior direito do registro RT. Toque em **Concluído** para retornar à tela Pesquisar RTs. No campo expandido, toque em **Cancelar** para limpar a entrada e retornar à tela Pesquisar RTs.
Pontuação de risco	Toque em um ou mais itens seguidos pelo ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTs.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** para retornar à tela Pesquisar RTs.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tocar neste campo	Para adicionar uma entrada em Android dispositivos	Para adicionar uma entrada em iOS dispositivos
	Toque no ícone fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTs.	No campo expandido, toque em **Cancelar** para limpar a entrada e retornar à tela Pesquisar RTs.
Status da Correção	Toque em um ou mais itens seguidos pelo ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTs. Toque no ícone fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTs.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** para retornar à tela Pesquisar RTs. No campo expandido, toque em **Cancelar** para limpar a entrada e retornar à tela Pesquisar RTs.
Estado	Toque em um ou mais itens seguidos pelo ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTs. Toque no ícone fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTs.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** para retornar à tela Pesquisar RTs. No campo expandido, toque em **Cancelar** para limpar a entrada e retornar à tela Pesquisar RTs.
Motivo	Toque em um ou mais itens seguidos pelo ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTs. Toque no ícone fechar (X) para cancelar sua entrada e retornar ao campo Pesquisar RTs.	Para adicionar uma entrada, toque em um ou mais itens ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Toque em **Concluído** para retornar à tela Pesquisar RTs. No campo expandido, toque em **Cancelar** para limpar a entrada e retornar à tela Pesquisar RTs.
Grupo de atribuição	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor para os campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor para os campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.
Atribuído a	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor para os campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.	Selecione um na lista ou toque no ícone de pesquisa e digite uma entrada no campo de pesquisa. Para limpar um valor para os campos Grupo de atribuição e Atribuído a, sem entrada, selecione **Nenhum**.
Descrição resumida	Toque na tela e insira o texto. O recurso reconhece cadeias de caracteres de texto	Na tela, insira o texto. O recurso reconhece cadeias de caracteres de texto

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tocar neste campo	Para adicionar uma entrada em Android dispositivos	Para adicionar uma entrada em iOS dispositivos
	e cadeias de caracteres parciais neste campo, mas caracteres curinga (*) não são aceitos. Letras maiúsculas não são necessárias. Toque no ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTs.	e cadeias de caracteres parciais neste campo, mas caracteres curinga (*) não são aceitos. Letras maiúsculas não são necessárias. Toque em **Concluído** para retornar à tela Pesquisar RTs. No campo expandido, toque em **Cancelar** para limpar a entrada e retornar à tela Pesquisar RTs.
Descrição	Toque na tela e insira o texto. O recurso reconhece cadeias de caracteres de texto e cadeias de caracteres parciais neste campo, mas caracteres curinga (*) não são aceitos. Letras maiúsculas não são necessárias. Toque no ícone de marca de seleção para adicionar sua entrada e retornar à tela Pesquisar RTs.	Na tela, insira o texto. O recurso reconhece cadeias de caracteres de texto e cadeias de caracteres parciais neste campo, mas caracteres curinga (*) não são aceitos. Letras maiúsculas não são necessárias. Toque em **Concluído** para retornar à tela Pesquisar RTs. No campo expandido, toque em **Cancelar** para limpar a entrada e retornar à tela SearchRTs.

Para dispositivos Android, com a tela Pesquisar RTs exibida e todos os seus critérios inseridos, escolha um para continuar.

4. Para dispositivos iOS, com a tela Pesquisar RTs exibida, escolha um para continuar.

5. **Opcional:** Se sua pesquisa retornar vários registros, você poderá Filtrar registros com o Aplicativo Vulnerability Response Mobile para refinar os resultados da pesquisa.

Filtrar registros com o Aplicativo Vulnerability Response Mobile

Defina filtros adicionais para limitar o número de registros exibidos em uma tela. A filtragem de registros no aplicativo para celular funciona como a filtragem com um construtor de condições na Now Platform.

Antes de Iniciar

Função necessária: responsável pela correção (sn_vul.remediation_owner)

Por Que e Quando Desempenhar Esta Tarefa

Tempo para concluir esta tarefa: 5 minutos.

Procedimento

1. Para refinar ainda mais os resultados da pesquisa ou para inserir critérios de filtro adicionais em qualquer lista de registros exibida, toque no ícone de filtro (ícone de).
2. Com a tela Filtros exibida, toque em um campo para expandi-lo.
   Um campo comum para inserir critérios de pesquisa para registros de tarefa de correção é o campo Estado.
3. Entre as opções exibidas, toque na caixa de seleção ou em um item para o seu filtro.
   Para muitos dos filtros, você pode selecionar mais de uma opção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Toque no ícone Voltar (ícone Back) ou em **FINALIZADO** para salvar suas mudanças em um campo.
   Os critérios escolhidos são exibidos na tela Filtros. O número de registros que correspondem aos seus critérios também é exibido na parte superior da tela. Toque em **REDEFINIR** para remover filtros e restaurar a configuração padrão.
5. **Opcional:** Repita as etapas 1 a 4 com a tela Filtros exibida para continuar definindo seus critérios de filtro.
6. Toque no ícone de interseção (ícone de) para criar condições E.
7. Como alternativa, toque no ícone de interseção (ícone de) para criar condições OU.
8. Depois de adicionar todos os critérios desejados, com a tela Filtros exibida, toque em **FINALIZADO**.
   Na tela, somente os registros que correspondem aos seus critérios de filtro são exibidos.

Tópicos relacionados

Pesquisar tarefas de correção com o Aplicativo Vulnerability Response Mobile

Orquestração do Vulnerability Response

Com Orquestração do Vulnerability Response fluxos de trabalho e atividades, você pode interagir e recuperar dados de sistemas e ambientes baseados em Windows ou UNIX usando a orquestração de fluxo de trabalho. Ao aprimorar os dados, você pode encurtar o ciclo de vida de correção.

Para obter mais informações sobre como editar fluxos de trabalho ou criar fluxos de trabalho personalizados, consulte Exploring Flow Designer .

Orquestração do Vulnerability Response fluxos de trabalho e atividades

Vários fluxos de trabalho estão incluídos com Orquestração do Vulnerability Response. Fluxos de trabalho e atividades automatizam e agilizam seus processos. Use fluxos de trabalho e atividades para criar registros de verificação, verificar itens vulneráveis, criar registros de verificação e muito mais.

Vulnerability Response - Fluxo de trabalho de verificação de vulnerabilidade

Automatize as verificações de vulnerabilidades para um ou vários itens vulneráveis usando o fluxo de trabalho **Vulnerability Response - Scan Vulnerability** incluído no sistema de base.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho **Vulnerability Response - Scan Vulnerability** cria um registro de verificação para a vulnerabilidade ou o grupo de vulnerabilidades a partir do qual foi invocado.

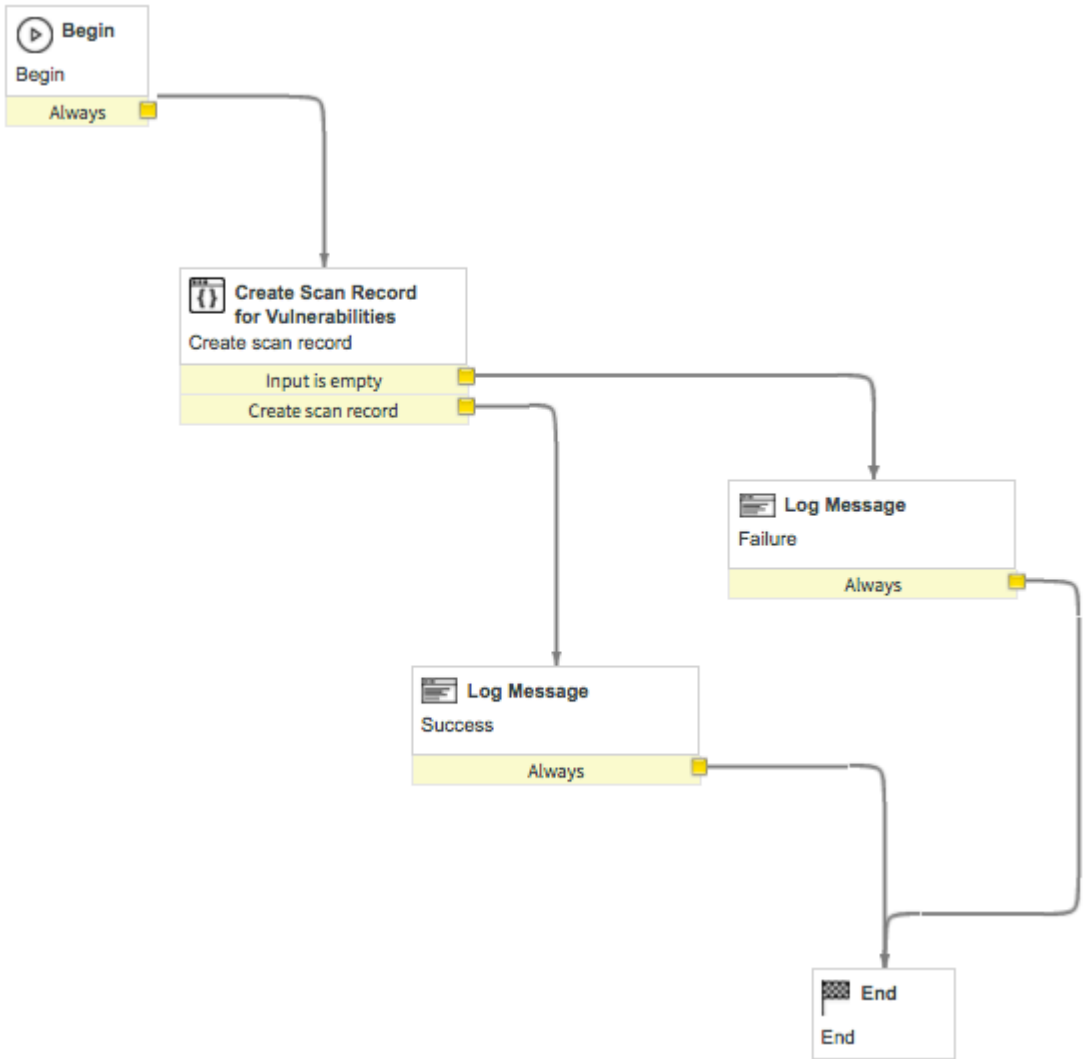
Nota:
É uma prática recomendada verificar novamente as vulnerabilidades ou os itens vulneráveis após a correção, quando um patch de vulnerabilidade é aplicado aos registros afetados. Você pode executar a nova verificação usando o método descrito ou pode automatizar as novas verificações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As atividades de fluxo de trabalho incluem Variáveis para a atividade Criar registro de verificação para vulnerabilidades

Vulnerability Response - Fluxo de trabalho de verificação de vulnerabilidade



Fluxo de trabalho de vulnerabilidade de verificação

O **Vulnerability Response** > **Vulnerabilidade de verificação** O fluxo de trabalho verifica novamente uma tarefa de correção.

Antes de Iniciar

Função necessária: none

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho é acionado pela nova verificação do **grupo vulnerável** durante uma ação **Fechar/Ignorar**.

As atividades do processo de fluxo de trabalho incluem:

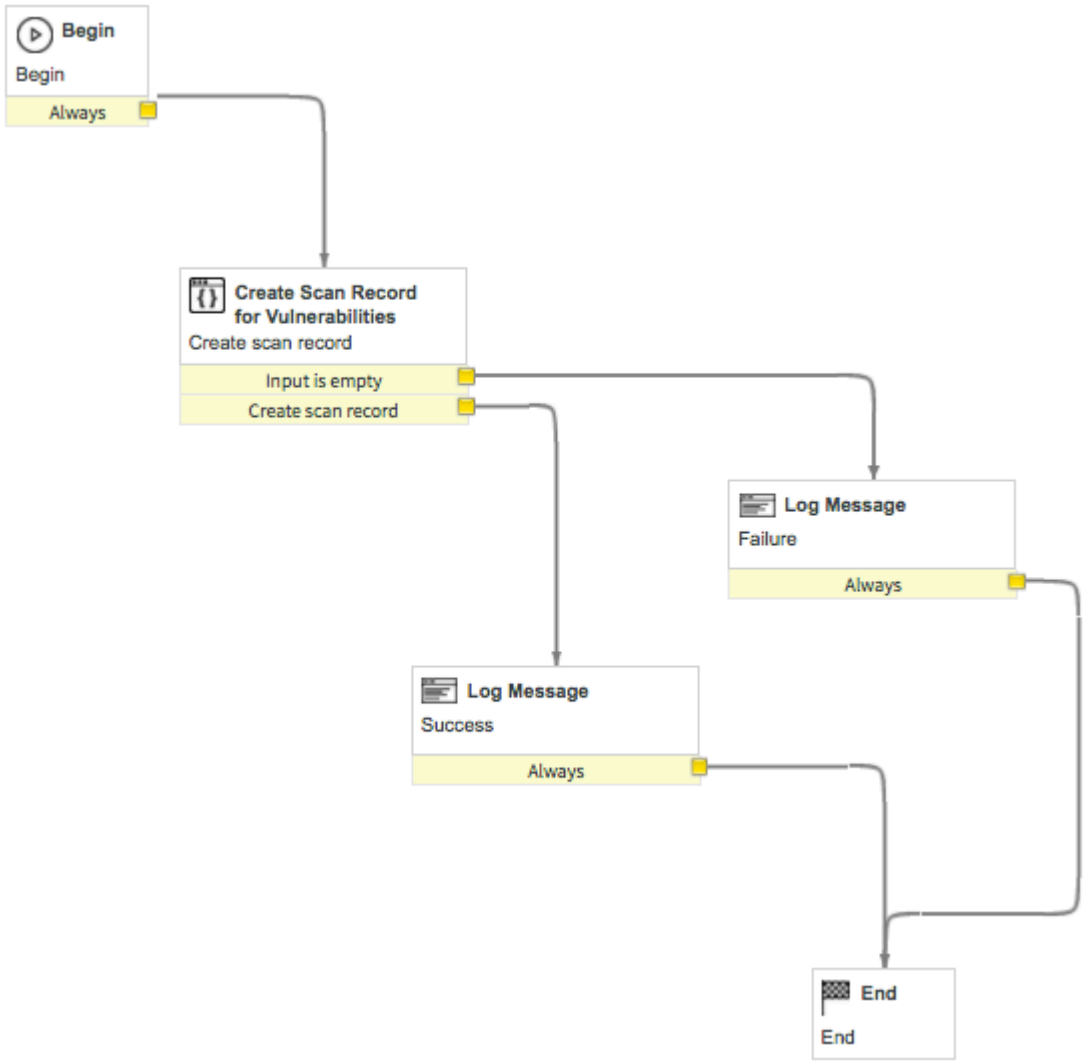
Variáveis para a atividade Criar registro de verificação para vulnerabilidades

Mensagem de log

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de verificação de vulnerabilidade



Tradução automática

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Tarefas de correção**.
2. Abra um registro de tarefa (VUL).
3. Clique em **Fechar**.
4. Escolha **Encerrado** para o **Estado desejado**.
5. Escolha **Fixo** para o **Subestado**.
6. Escolha **Aguardar confirmação da próxima verificação** para **Fechar agora?**
   Para a tarefa de correção e os itens vulneráveis, o **Estado** muda para **Confirmação pendente**, o **Subestado** muda para **Fixo**e uma nova verificação é executada.

Vulnerability Response - Fluxo de trabalho de verificação de itens vulneráveis

Automatize verificações de vulnerabilidades para um ou vários itens vulneráveis usando o fluxo de trabalho **Vulnerability Response - Verificar itens vulneráveis** incluído no sistema de base.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

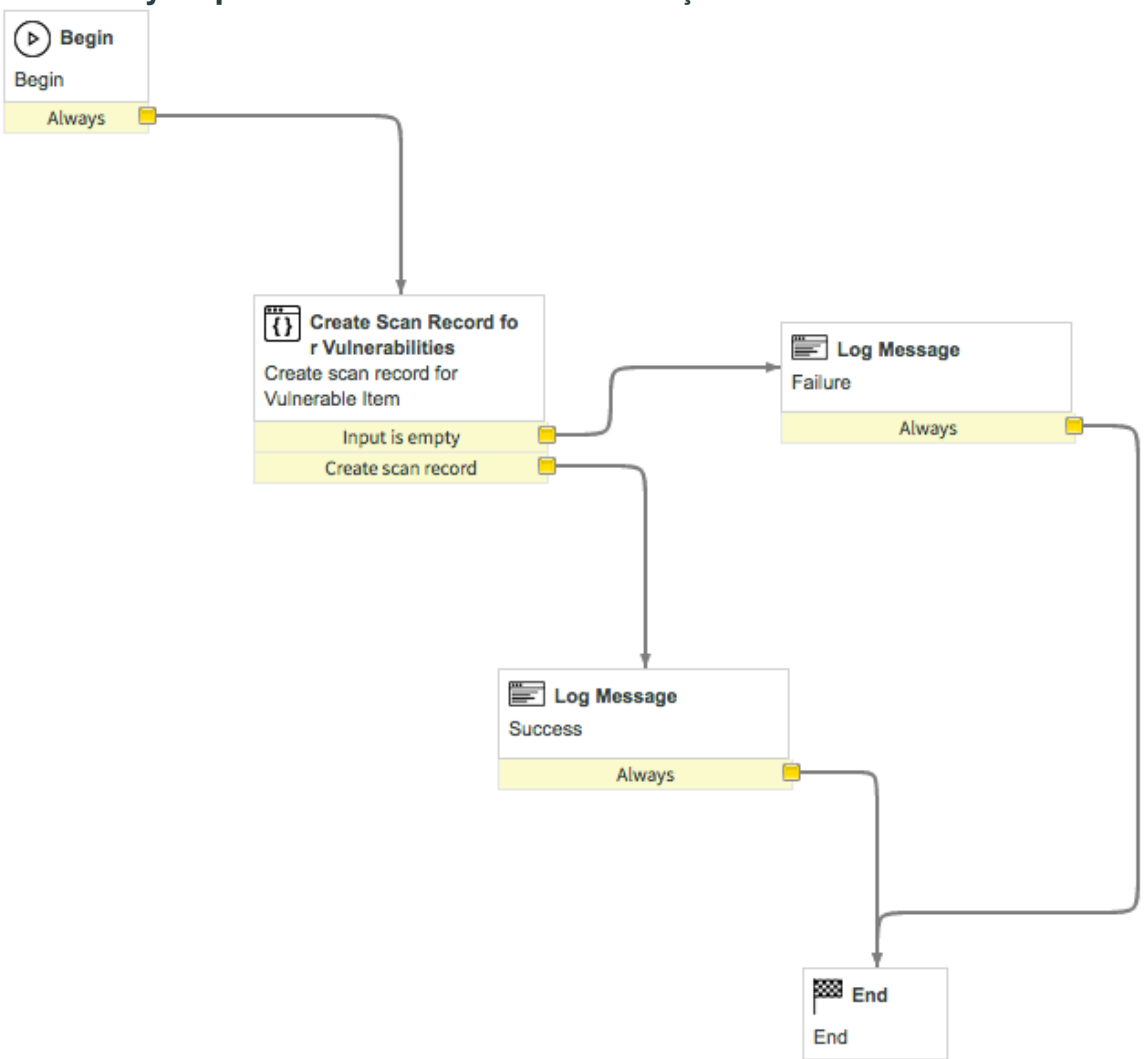
Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho **Vulnerability Response - Verificar itens vulneráveis** cria um registro de verificação para o item vulnerável ou grupo de itens do qual foi invocado.

Nota:
É uma prática recomendada verificar novamente as vulnerabilidades ou os itens vulneráveis após a correção quando um patch de vulnerabilidade for aplicado aos registros afetados. Você pode executar a nova verificação usando o método descrito ou pode automatizar as novas verificações.

As atividades do processo de fluxo de trabalho incluem: Variáveis para a atividade Criar registro de verificação para vulnerabilidades

Vulnerability Response - Fluxo de trabalho de verificação de itens vulneráveis



Fluxo de trabalho do item de vulnerabilidade de verificação

O**Resposta vulnerável** > **Item de vulnerabilidade de verificação** O fluxo de trabalho verifica novamente um item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: none

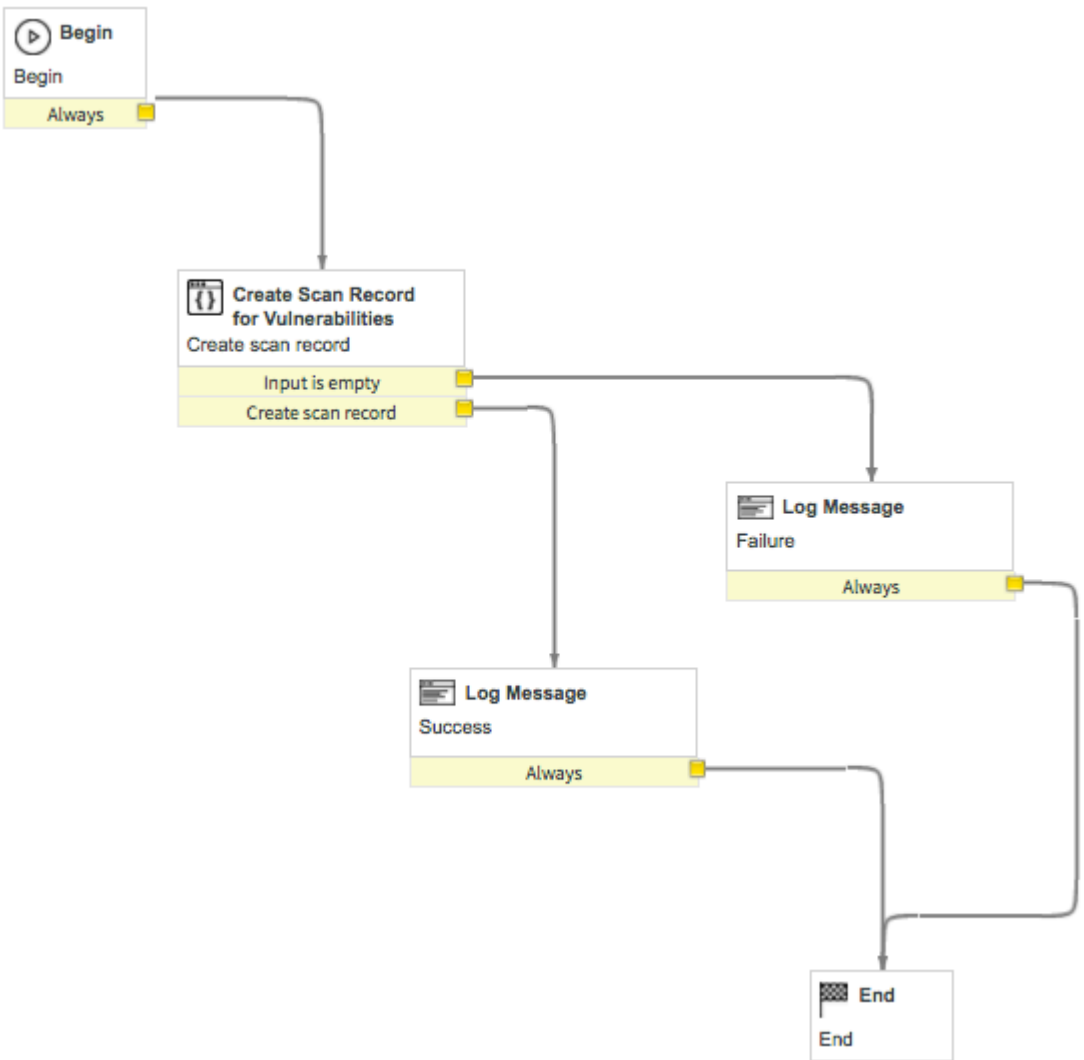
Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado pela **vulnerabilidade**de nova verificação durante uma ação **Fechar/Ignorar**.

As atividades do processo de fluxo de trabalho incluem:

Variáveis para a atividade Criar registro de verificação para vulnerabilidades

Mensagem de log

Fluxo de trabalho de verificação de vulnerabilidade



Tradução automática

Procedimento

1. Navegar até **Vulnerabilidade** > **Vulnerabilidades** > **Itens vulneráveis**.
2. Abra um item de vulnerabilidade.
3. Clique **em Fechar/Ignorar**.
4. Escolha **Encerrado**para o **Estado desejado**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Escolha **Fixo** para o **Subestado**.
   O **Estado** do grupo muda para **Confirmação pendente**, o **Subestado** muda para **Fixo**e uma nova verificação é executada.

Orquestração do Vulnerability Response atividades de fluxo de trabalho

Orquestração do Vulnerability Response As atividades permitem que os usuários determinem se uma vulnerabilidade foi vista antes em outros incidentes de segurança ou em outros sistemas usando a orquestração de fluxo de trabalho.

Variáveis para a atividade Criar registro de verificação para vulnerabilidades

As verificações de vulnerabilidade para um ou vários itens vulneráveis podem ser executadas usando a atividade de fluxo de trabalho **Criar registro de verificação para vulnerabilidades** incluída no sistema de base. Quando a entrada é passada para a atividade, ela cria um registro de verificação.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
taskids [cadeia de caracteres]	Uma cadeia de caracteres de sysIds separados por vírgulas que define as entradas esperadas. Este campo é obrigatório.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado da verificação [booliano]	Retorna Verdadeiro se a entrada não estiver vazia. Um registro de verificação é criado para os taskIds.

Application Vulnerability Response

O recurso Application Vulnerability Response (AVR) da aplicação ServiceNow® Vulnerability Response importa itens vulneráveis da aplicação (IVAs) e, de acordo com as regras, permite que você corrija vulnerabilidades da aplicação. Vulnerability Response está disponível por assinatura separada.

A partir do AVR v19.0, alguns nomes de tabela e coluna principais foram atualizados. Como resultado, você verá referências aos nomes mais antigos e mais recentes na documentação. Para obter a lista completa de termos atualizados, consulte Exibição de produto do Application Vulnerability Response.

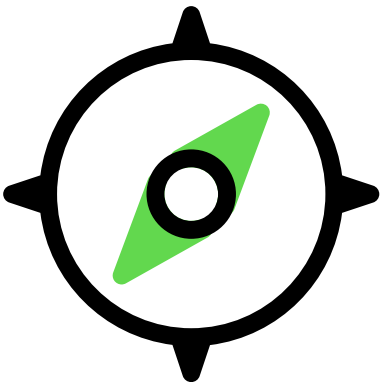
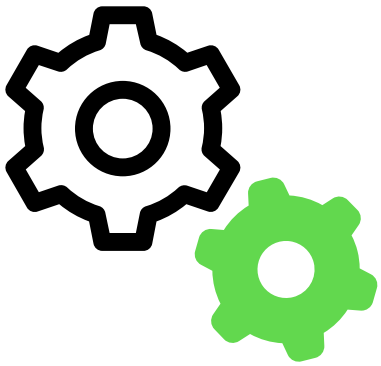
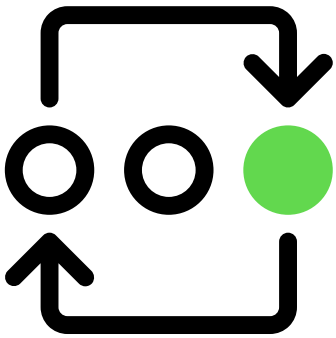
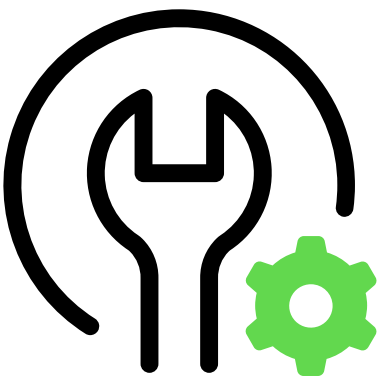
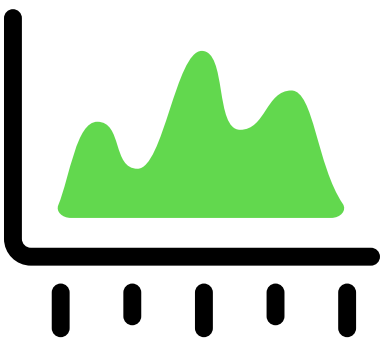
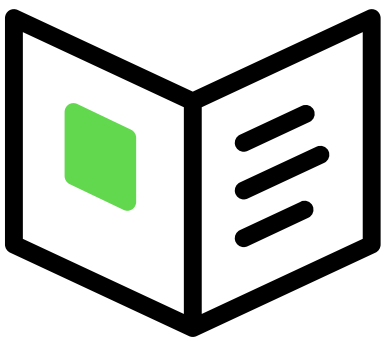
A partir da v19.0 de Vulnerability Response, você pode ingerir dados de vulnerabilidade da Análise de composição de software (SCA) e da Lista de materiais de software (SBOM) para ajudá-lo a identificar pontos fracos em seus aplicativos de software. Para obter mais informações, consulte Explorar o Lista de materiais de software e Veracode Vulnerability Integration.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A partir da versão 18.0 do Vulnerability Response, é possível monitorar e corrigir AVIs no Vulnerability Manager Workspace e no IT Remediation Workspace, respectivamente. Para obter mais informações, consulte Explorando o Vulnerability Manager Workspace e Explorando o Espaço de correção de problemas de TI.

Application Vulnerability Response

Explorar	Configurar	Integrar
		
Saiba mais sobre os conceitos e recursos do Application Vulnerability Response.	Configure o Application Vulnerability Response.	Estenda o Application Vulnerability Response integrando-o a outros aplicativos.
Corrigir	**Análise e relatório**	**Referência**
		
Saiba como corrigir vulnerabilidades da aplicação.	Exibir análise do Application Vulnerability Response	Veja os detalhes sobre os componentes do Application Vulnerability Response, como campos, tabelas e propriedades.

Explorar o Application Vulnerability Response

Vulnerabilidades de aplicação são vulnerabilidades em suas aplicações de software personalizadas que são verificadas durante todo o ciclo de vida de desenvolvimento da aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral de Application Vulnerability Response e versões disponíveis

Application Vulnerability Response (AVR) é a parte da aplicação Vulnerability Response que processa vulnerabilidades da aplicação.

Versões disponíveis

Versão de lançamento	Notas de versão
Vulnerability Response v21.0 Vulnerability Response v20.0 Vulnerability Response v19.0 Vulnerability Response v18.2 Vulnerability Response v18.0	Application Vulnerability Response release notes Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Como ele funciona

Os dados de vulnerabilidade são importados de fontes internas e externas, como Common Weakness Enumeration (CWE) ou integrações de terceiros. Depois que os dados são importados, eles são comparados aos dados da aplicação na aplicação Configuration Management Database (CMDB) e processados na aplicação Application Vulnerability Response. Se houver uma correspondência entre os dados de vulnerabilidade da aplicação importados e os dados no seu CMDB, um item vulnerável da aplicação (IVA) será criado.

O Application Vulnerability Response inclui os seguintes recursos principais:

- Integre com scanners de terceiros compatíveis para importar dados de vulnerabilidade.
- Compare os dados relacionados à vulnerabilidade da aplicação e determine se as vulnerabilidades da aplicação foram encontradas em uma aplicação.
- Priorize, corrija e gerencie itens vulneráveis da aplicação (IVA). Cada vulnerabilidade da aplicação representa uma entrada de vulnerabilidade no CWE ou nas bibliotecas de terceiros.
- A partir da versão 18.0 do Vulnerability Response, você pode monitorar e corrigir AVIs no Vulnerability Manager Workspace e no IT Remediation Workspace, respectivamente. Para obter mais informações, consulte Explorando o Vulnerability Manager Workspace e Explorando o Espaço de correção de problemas de TI.
- Correlacione Application Vulnerability Response dados usando calculadoras e bibliotecas para ajudá-lo a executar as tarefas a seguir.
  - Crie itens vulneráveis da aplicação automaticamente usando as **Regras de pesquisa de IC**. Durante a importação, as vulnerabilidades de terceiros são associadas a um CWE para criar um AVI.
  - Crie regras de atribuição para automatizar as atribuições de item vulnerável da aplicação.

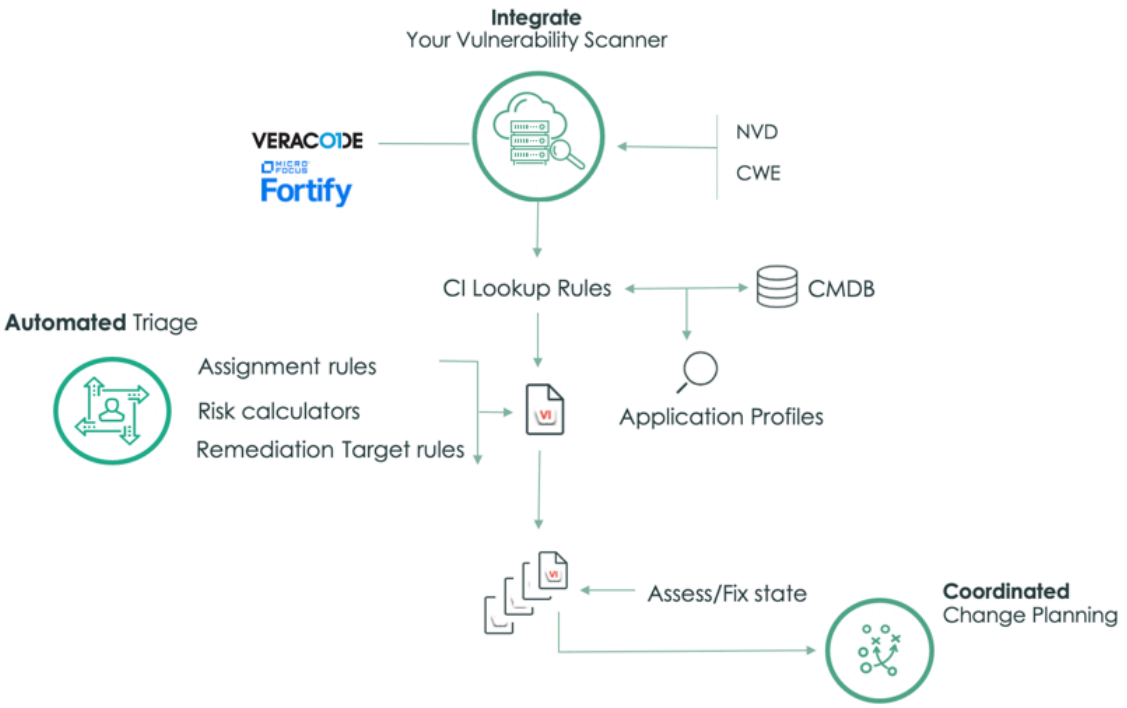
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Use grupos de calculadoras para determinar o impacto nos negócios, especificar condições variadas usando filtros, aplicar cálculos simples ou usar um script.
- Crie regras de destino de correção que definem o intervalo de tempo esperado para corrigir itens vulneráveis da aplicação para que você possa monitorar as próximas atividades de correção.

- Relacione uma única vulnerabilidade de terceiros a várias entradas do CWE e encontre o CWE primário de uma vulnerabilidade para ajudá-lo a determinar o risco. Para obter mais informações sobre o **CWE primário**, consulte Campos de vulnerabilidade da aplicação.
- Use registros do CWE que são baixados do banco de dados do CWE ou importados de integrações de terceiros para referência e ajudá-lo a decidir se você deve escalar uma vulnerabilidade. Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco.

Use Application Vulnerability Response para seguir o fluxo de informações, desde a integração até a investigação e, em seguida, até a resolução.



Tipos de dados de vulnerabilidade importados

Application Vulnerability Response O oferece suporte aos seguintes tipos de dados de vulnerabilidade da aplicação importados.

Nota:
Antes da v19.0, os dados de SAST, SCA, IAST e de teste de invasão não eram ingeridos e podem ser responsáveis pelas diferenças entre o que é mostrado em Veracode, Fortify e Invicti e o que aparece em Application Vulnerability Response.

Teste de segurança da aplicação dinâmico (DAST)

As verificações DAST localizam a aplicação de vulnerabilidades enviando entrada para suas aplicações e monitorando suas respostas enquanto elas estão sendo executadas. Esta abordagem pode imitar um ataque externo. Durante a verificação dinâmica, um serviço em execução (URL) é verificado quanto a vulnerabilidades. Os resultados de vulnerabilidade incluem um local de URL de uma vulnerabilidade descoberta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Teste de segurança da aplicação estático (SAST)

As verificações SAST revisam o código de origem das aplicações em repouso e ajudam a encontrar vulnerabilidades na maneira como você criou seu código. A verificação do SAST ocorre no código de origem não compilado e, portanto, existe independentemente de qualquer serviço de aplicativos. Os resultados retornados incluem um arquivo e um local de número de linha de uma vulnerabilidade descoberta.

Teste de segurança da aplicação interativo (IAST)

As verificações IAST detectam vulnerabilidades de software interagindo com o programa enquanto ele está em execução. Observação humana, testes automatizados e sensores são usados em combinação para interagir com a aplicação para localizar vulnerabilidades.

Análise de composição de software (SCA)

A partir da v19.0 de Vulnerability Response, você pode ingerir vulnerabilidades de Análise de composição de software (SCA). Os dados de vulnerabilidade do SCA para ajudam a identificar pontos fracos no software de código aberto que está sendo usado em seus aplicativos de software.

Teste de invasão

Você configura solicitações de avaliação de teste de invasão em Application Vulnerability Response para ajudá-lo a entender onde estão os pontos fracos da aplicação e o que você pode fazer para corrigi-los.

Lista de materiais de software

Carregue Lista de materiais de software (SBOM) dados para identificar vulnerabilidades em seus componentes de código aberto. Para obter mais informações, consulte Explorar o Lista de materiais de software.

Casos de uso

Alguns dos seguintes casos de uso de DAST são compatíveis:

- Relacione cada vulnerabilidade dos resultados da verificação a algum tipo de cmdb_ci (classe secundária).
- Relacione os resultados da verificação do DAST a uma aplicação existente quando houver um registro no CMDB de Descoberta ou uma integração de terceiros.
- Relacione o resultado da verificação do DAST a uma aplicação verificada recém-inserida quando uma nova aplicação não tiver sido identificada e/ou armazenada no CMDB.
- Armazene os resultados da verificação DAST para um CMDB ao gerenciar suas aplicações em um produto diferente de ServiceNow®.
- Armazene os resultados da verificação do DAST para um CMDB se você tiver personalizado anteriormente para outra finalidade.
- Crie uma aplicação para o repositório de código de origem manualmente.

Alguns dos casos de uso de SAST compatíveis são compatíveis:

- Relacione cada vulnerabilidade dos resultados da verificação a algum tipo de cmdb_ci (classe secundária).
- Crie um IC para o repositório de código de origem manualmente.
- Armazene resultados de verificação do SAST que não tenham um serviço de aplicações relacionado.

[store-future: BEGIN review]Alguns dos seguintes casos de uso de IAST são compatíveis: [End]

[store-future: BEGIN review]Alguns dos usos de SCA compatíveis são compatíveis:[End]

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações de terceiros

As integrações de terceiros compatíveis com Application Vulnerability Response estão disponíveis como aplicações separadas no ServiceNow Store. Para obter mais informações, consulte Integração do Application Vulnerability Response a outras aplicações.

Principais recursos

- Uma API compartilhada importa dados DAST, SAST, IASTe SCA e resultados de testes de invasão manuais. Consulte Teste de invasão.
- Uma API separada é usada para importar dados de SBOM. Para obter mais informações, consulte Explorar o Lista de materiais de software e Veracode Vulnerability Integration.

Regras de pesquisa de IC

Pesquise automaticamente correspondências nos dados da aplicação no Configuration Management Database (CMDB).

Regras de atribuição

Atribua automaticamente vulnerabilidades da aplicação com base em grupos de usuários, campos de grupo de usuários e scripts.

Calculadoras de Risco

Priorize e classifique automaticamente o impacto dos AVIs usando calculadoras, com base em qualquer critério, usando filtros de condição.

Mapeamento de severidade

Calcule automaticamente os valores iniciais dos campos em itens vulneráveis da aplicação. As entradas de vulnerabilidade têm severidade de origem e severidade normalizada (com base no mapeamento de severidade). A severidade está vinculada à Enumeração de Ponto Fraco Comum (CWE).

Regras de destino de correção

Defina o intervalo de tempo esperado para corrigir um item vulnerável da aplicação.

Relatórios

Obtenha rapidamente informações sobre sua postura de segurança, tendências de correção e as 10 principais aplicações ou unidades de negócios com os AVIs mais críticos.

O ponto comum para ambos os tipos de verificações é a versão da aplicação. Uma versão da aplicação, que define uma cadeia de caracteres de **Nome**, é o ponto de vinculação para agrupar os resultados de vulnerabilidade verificados no lado do scanner. Dessa forma, o AVR sabe a qual versão da aplicação os resultados pertencem ao importar os resultados da verificação por meio da integração.

Uma tabela secundária de item de configuração [cmdb_ci], Scanned Applications [sn_vul_app_scanned_application], foi criada na aplicação Vulnerability Response e no escopo. Esta tabela armazena a abstração da versão da aplicação e fornece gráficos de serviço por meio de seus relacionamentos do CMDB. Eles podem ser exibidos em **Todos** > **Application Vulnerability Response** > **Administração** > **Aplicações** módulo. A exibição de lista das aplicações escaneadas contém o **departamento** e **o grupo de suporte** adicionados durante a configuração.

Itens vulneráveis da aplicação (IVAs)

Para vulnerabilidades da aplicação, o AVR relaciona uma vulnerabilidade a uma aplicação para criar o registro de item vulnerável da aplicação (IVA). Por causa das várias definições

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

do que constitui uma aplicação no CMDB, Application Vulnerability Response limita as aplicações a aplicações verificadas. As aplicações verificadas são as aplicações verificadas em seu ambiente identificadas por AVR como **Nome** e **ID**. Os AVIs são baseados no resumo da verificação mais recente até a confirmação **Corrigida** pelo scanner. Se um AVI não for mais encontrado, ele permanecerá vinculado ao resumo da verificação de onde foi visto pela última vez.

Itens vulneráveis da aplicação podem ser exibidos em **Todos** > **Application Vulnerability Response** > **Vulnerabilidades** > **Itens vulneráveis** módulo.

Se uma aplicação for removida do CMDB, todos os AVIs associados serão encerrados.

Para obter informações sobre campos de formulário AVI, consulte Campos de item vulnerável da aplicação.

Grupos de usuários e funções no Application Vulnerability Response

Frequentemente, uma equipe trabalha em conjunto para criar, gerenciar e supervisionar a gestão de vulnerabilidades da aplicação. Existem funções estratégicas, bem como funções operacionais, entre os membros da equipe. Na maioria das organizações, você pode participar de mais de uma função e geralmente compartilhar funções com outras pessoas. Application Vulnerability Response usa três grupos de usuários que contêm funções granulares: Gerente de App-Sec, Campeão de segurança da aplicação e Desenvolvedor. Consulte Application Vulnerability Response grupos de usuários e funções para obter mais informações sobre esses grupos e funções.

Application Vulnerability Response estados

Application Vulnerability Response oferece um modelo de estado para o status dos itens vulneráveis da aplicação (IVAs) e ajuda a determinar quando e como corrigir seus AVIs.

Um item vulnerável da aplicação tem vários estados possíveis. Consulte Estados do item vulnerável da aplicação (IVA) para obter mais informações.

Configuração do Application Vulnerability Response

Antes de executar Application Vulnerability Response em sua instância Now Platform, você deve configurá-lo.

Configurar Application Vulnerability Response.

Conclua a check-list de configuração a seguir antes da configuração.

Antes de Iniciar

Tarefas de configuração	Descrição
Verifique se a aplicação Vulnerability Response está instalada e ativada.	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
Verifique se o Performance Analytics para Vulnerability Response está instalado e ativado para ver os relatórios Application Vulnerability Response.	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar e configurar a aplicação Performance Analytics para Vulnerability Response [PA].
Verifique se o Veracode Vulnerability Integration está instalado, ativado e configurado. [Não execute as integrações neste ponto.]	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar o Vulnerability Response Integration [ServiceNow com Veracode.
Versão 14.0: verifique se o Integrações de vulnerabilidade do Fortify está instalado, ativado e configurado. [Não execute as integrações neste ponto.]	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar o Vulnerability Response Integration [ServiceNow com Fortify e Configurar o Integrações de vulnerabilidade do Fortify.
Verifique se a integração do CWE 2000 está sendo executada em Vulnerability Response.	Para verificar, consulte Verifique se o trabalho programado para atualizar registros do NVD está em execução.
[Opcional] Verifique se a integração do NVD está sendo executada em Vulnerability Response.	Para verificar, consulte Verifique se o trabalho programado para atualizar os registros CWE está em execução.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o administrador do sistema [admin] instalará a aplicação e atribuirá usuários aos seguintes grupos de usuários: Gerente de App-Sec, Campeão de segurança e Desenvolvedor. Para obter informações sobre as funções do grupo, consulte Application Vulnerability Response grupos de usuários e funções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	• O grupo do App-Sec Manager supervisiona a configuração e verifica os resultados esperados. **Nota:** A configuraçãoApplication Vulnerability Response não está disponível no recurso Assistente de configuração em Vulnerability Response.

Função necessária: grupo de usuários do App-Sec Manager

Procedimento

1. Navegar até **Security Operations** > **CMDB** > **Regras de pesquisa**.
   Consulte Criar uma regra de pesquisa de IC para criar ou modificar Regras de Pesquisa de IC para o seu ambiente.
2. Navegar até **Application Vulnerability Response** > **Administração**.
3. Selecione **Regras de atribuição**.
   Consulte Criar ou editar Application Vulnerability Response regras de atribuição para criar ou modificar regras de atribuição de aplicação para o seu ambiente.
4. Selecione **Calculadoras de vulnerabilidade**.
   Consulte Calcular risco em Application Vulnerability Response automaticamente para criar ou modificar calculadoras de vulnerabilidade da aplicação para o seu ambiente.
5. Selecione **Regras de destino**de correção.
   Consulte Criar ou editar regras de destino de correção da aplicação para criar ou modificar destinos de correção de aplicação para o seu ambiente.
6. Selecione **Mapas de severidade normalizados**.
   Consulte Mapear a severidade de um item vulnerável da aplicação automaticamente para criar ou modificar mapas de severidade para seu ambiente.
7. Navegue até qualquer um dos **Integração de vulnerabilidade da Veracode** > **Integrações** ou **Integrações de vulnerabilidade do Fortify** > **Integrações**.
8. Abra a integração da lista de aplicações Veracode ou a integração da lista de aplicações Fortify On Demand.
9. Se ainda não tiver sido executado, clique em **Executar agora**.

   Nota:
   As outras integrações Veracode ou Fortify estão inativas por padrão.

   Para obter os status de execução da integração, consulte Exibir o status de execução de importação da integração de vulnerabilidade da aplicação Veracode ou Exibir o status de execução de importação Integrações de vulnerabilidade do Fortify.
10. Quando a integração da lista de aplicações Veracode ou Fortify on Demand tiver concluído a execução, navegue até **Application Vulnerability Response** > **Administração** > **Aplicações**.
11. Para cada aplicação, insira um valor para **Grupo de suporte** (usado por regras de atribuição) e para **Departamento** (usado em relatórios).
    Para atualizar várias entradas, consulte Editar vários registros em uma lista usando o editor de lista para concluir a tarefa em massa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Para ver a **unidade de negócios**atualizada automaticamente, atualize a página. Para obter informações sobre os campos de formulário da aplicação escaneados, consulte Campos da aplicação verificados.

12. Retorne à lista de integrações e ative as outras integrações Veracode ou Fortify.
Consulte Ativar Application Vulnerability Response integrações para definir suas importações de integração de dados delta.

As integrações Veracode e Fortify são encadeadas e serão executadas consecutivamente quando ativadas.

13. **Opcional:** Navegar até **Application Vulnerability Response** > **Administração** > **Regras de atribuição**.

    a. **Opcional:** Se você escolheu **Item de configuração: grupo de suporte** para **o campo Grupo de usuários** ao criar ou editar suas regras de atribuição anteriormente, os valores adicionados à exibição de lista Aplicações verificadas estão disponíveis para uso agora.
    Edite suas regras de atribuição de acordo.

    b. Clique em **Atualizar**.

    c. Na exibição de lista Regras de atribuição de vulnerabilidade, clique em **Aplicar mudanças** para reaplicar as regras de atribuição aos seus AVIs.

14. Sua configuração Application Vulnerability Response está concluída.

O que Fazer Depois

Navegar até **Application Vulnerability Response** > **Visão geral** e consulte Painel do Application Vulnerability Management [PA] para obter informações sobre sua postura geral de segurança.

Verifique se o trabalho programado para atualizar os registros CWE está em execução

Use registros de enumeração de pontos fracos comuns (CWE) baixados do banco de dados do CWE para referência ao decidir se uma vulnerabilidade deve ser escalonada. Atualize os registros de fraqueza comuns do banco de dados de Enumeração de Pontos Fracos Comuns em uma programação regular. Você também pode atualizar o script padrão ou escrever seus próprios scripts, conforme necessário.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec
Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Integrações**.
2. Selecione o trabalho programado **Integração abrangente do CWE 2000**.
3. Verifique se a caixa de seleção **Ativo** está marcada.

Nota:
As configurações neste formulário são compartilhadas por Vulnerability Response e Application Vulnerability Response. Modificar as configurações de integração requer coordenação com e experiência em Vulnerability Response e ServiceNow.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Se a caixa estiver selecionada, você terá concluído.

> **Nota:**
> Se a caixa não estiver marcada, esta integração pode precisar ser configurada em Vulnerability Response. Consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros para obter mais informações antes de selecioná-lo.

Conforme necessário, consulte Exibir bibliotecas de vulnerabilidades para ver as entradas importadas.

O campo **CWE primário** contém a entrada do CWE. Se houver mais de um CWE associado a uma vulnerabilidade, consulte Campos de vulnerabilidade da aplicação para obter informações sobre como o CWE primário é determinado.

Verifique se o trabalho programado para atualizar registros do NVD está em execução

Identifique os repositórios que você deseja atualizar regularmente. Você pode executar um trabalho programado para atualizar os registros do National Vulnerability Database (NVD) todas as noites ou semanas. Se ainda não estiver em execução, você poderá habilitar o trabalho

Antes de Iniciar
Funções necessárias: grupo de gerentes de App-Sec

A integração do NVD é executada como um trabalho programado diariamente às segundas-feiras às 00:00:00, por padrão.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Integrações**.
2. Selecione o trabalho programado do Banco de **Dados de Vulnerabilidades do NIST**.
3. Verifique se a caixa de seleção **Ativo** está marcada.

> **Nota:**
> As configurações neste formulário são compartilhadas por Vulnerability Response e Application Vulnerability Response. Modificar as configurações de integração requer coordenação com e experiência em Vulnerability Response e ServiceNow.

4. Se a caixa estiver selecionada, você terá concluído.

> **Nota:**
> Se a caixa não estiver marcada, esta integração pode precisar ser configurada em Vulnerability Response. Consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros para obter mais informações antes de selecioná-lo.

Conforme necessário, consulte Exibir bibliotecas de vulnerabilidades para ver as entradas importadas.

Ativar Application Vulnerability Response integrações

Habilite integrações Application Vulnerability Response para executar atualizações regulares.

Antes de Iniciar
Função necessária: gerente de App-Sec

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Integrações**.
2. Selecione uma integração.
3. Marque a caixa de seleção **Ativo**.
4. Selecione **Atualizar**.
5. Repita conforme necessário para cada integração.
   Após a execução inicial, as integrações são encadeadas para fazer importações delta para execuções subsequentes.

Gestão de exceções no Application Vulnerability Response

Quando sua organização não pode estar em conformidade com uma gestão de vulnerabilidades ou política de segurança, padrão ou diretriz publicada, você pode solicitar uma exceção. A gestão de exceções envolve solicitar, revisar, aprovar ou rejeitar exceções a um item vulnerável da aplicação (IVA) que não pode ser corrigido de acordo com a política.

Algumas vulnerabilidades podem não ter um patch, correção ou solução existente. Quando uma exceção é aprovada, isso também significa que você está aceitando um risco porque está reconhecendo e concordando com as consequências de não corrigir a vulnerabilidade.

Nota:

A partir da v21.0 de Application Vulnerability Response, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável da aplicação muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável da aplicação ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Ciclo de vida de uma exceção

Definição de uma exceção

Uma exceção é uma solicitação para adiar a correção de um AVI por um período especificado. Por exemplo, como desenvolvedor, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Solicitar uma exceção

Como desenvolvedor, você pode solicitar uma isenção para um AVI usando o processo de gestão de exceções. Depois que o analista de segurança da aplicação aprova essa solicitação, o AVI passa para o estado **Adiado**.

Regras de exceção

A partir da v20, você pode criar regras de exceção para adiar automaticamente os itens vulneráveis da aplicação (IVA) existentes e novos por um período específico se eles corresponderem às condições da regra. O uso de regras de exceção para adiar automaticamente AVIs minimiza o risco de perder acordos de nível de serviço. As regras podem ajudá-lo a gerenciar vários itens, pois você está eliminando a intervenção manual. Consulte Criar uma regra de exceção.

Solicitar uma extensão para uma regra de exceção

A partir da v20, você pode enviar uma solicitação de extensão para a data **Adiada até** de uma regra de exceção. Você pode solicitar uma extensão para uma regra se descobrir que um grande

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

número de registros criados pela regra não está sendo resolvido pela data **Adiado até**, a data em que a tarefa de correção para de aceitar novos AVIs. A extensão atualiza a regra de exceção para estender automaticamente a data de adiamento na regra existente. Você pode inserir datas de até um ano a partir da data atual e deve incluir um motivo para a extensão. Uma solicitação de extensão requer aprovação em dois níveis de grupos de aprovação separados.

Aprovação de uma solicitação de exceção

Os AVIs que não podem ser corrigidos imediatamente são revisados por analistas de segurança da aplicação, avaliados quanto ao risco e aprovados para adiamento até que possam ser corrigidos. A aprovação de uma solicitação de exceção pode ser um fluxo de dois níveis. Se somente o aprovador de primeiro nível estiver presente, a exceção poderá ser solicitada e aprovada. No entanto, se não houver nenhum aprovador de primeiro nível, uma exceção não poderá ser solicitada. Para obter mais informações, consulte Adicionar um aprovador de exceção para Application Vulnerability Response.

Nota:

Depois que uma solicitação de exceção para um AVI é aprovada, você pode executar as seguintes ações:

- Reabrir
- Obter mais detalhes

Como rastrear uma solicitação de exceção

Depois de gerar a exceção, você pode rastrear seu status usando a guia **Aprovações de mudança de estado** do AVI.

Vencimento de uma solicitação de exceção e solicitação de uma extensão para uma regra de exceção

Quando uma solicitação de exceção para um AVI específico expira, o AVI afetado é revertido para o estado **Aberto**.

No entanto, a partir do v20, você pode enviar uma solicitação para estender a data **Adiado até** na regra de exceção.

Configurar Gestão de exceções para Application Vulnerability Response

Limite a duração de uma exceção solicitada e adicione um questionário à exceção ou à solicitação de falso-positivo usando o módulo. Por padrão, uma exceção é solicitada usando o módulo ServiceNow® Application Vulnerability Response. Você também pode solicitar uma exceção usando a integração GRC: Policy and Compliance Management.

Antes de Iniciar

Função necessária: sn_vul.app_manage_exception_configuration

Por Que e Quando Desempenhar Esta Tarefa

Se Vulnerability Response estiver habilitado, você poderá limitar a duração pela qual uma exceção pode ser solicitada. Da mesma forma, se o módulo GRC: Policy and Compliance Management estiver instalado, você poderá selecionar GRC: Policy and Compliance Management na tela de configuração. Habilitar esta opção permite solicitar uma exceção que especifica a política e o objetivo de controle de GRC.

Se você adicionar um questionário, ele será enviado para a pessoa que gerou a exceção ou a solicitação de falso-positivo. Você pode usar o questionário padrão ou criar um com base em seus requisitos.

É útil que o aprovador de exceção entenda o motivo da solicitação da exceção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Gestão de exceção**.
2. No formulário Configuração de gestão de exceções, selecione como você deseja gerenciar uma exceção selecionando uma opção na lista Gerenciar exceções usando.

Nota:
A partir da Vulnerability Response versão 17.1, você pode selecionar Vulnerability Response ou GRC: Policy and Compliance Management. Você deve ativar o plug-in GRC para usar GRC: Policy and Compliance Management para solicitar uma exceção. Alterar a configuração não afeta os dados existentes.

3. Preencha os campos no formulário com base na opção selecionada.
   - Se você selecionou a opção Vulnerability Response, preencha os campos no formulário.

Configurações do formulário de gestão de exceções de VR

Campo	Descrição
Duração	Período para o qual uma exceção pode ser solicitada.
Unidade	Unidade de tempo para o período especificado.
Habilitar questionário para solicitar exceção	Opção para adicionar um questionário à solicitação de exceção que está sendo gerada.
Questionário para solicitar exceção	Opção para exibir o questionário selecionado por você para solicitar uma exceção. O Questionário de exceção é exibido por padrão.
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso-positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Opção para exibir o questionário selecionado por você para marcar como falso positivo. O questionário para solicitação de falso-positivo é exibido por padrão.

   - Se você selecionou a opção GRC: Policy and Compliance Management, preencha os campos no formulário.

Configurações do formulário de gestão de exceções de VR

Campo	Descrição
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso-positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Opção para exibir o questionário selecionado por você para marcar como falso positivo. O questionário para solicitação de falso-positivo é exibido por padrão.

4. Selecione **Salvar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar regras de aprovação para Gestão de exceções

A partir da Application Vulnerability Response v15.0, use o Flow Designer para aprovar solicitações de exceção para gestão de exceções, regras de exceção e gestão de falsos positivos. Se você estiver implantando Application Vulnerability Response (AVR) pela primeira vez, o Flow Designer será habilitado por padrão.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Se você for um usuário de VR existente, a opção padrão será fluxo de trabalho.
Se você implantou Application Vulnerability Response v15.0 ou posterior, o valor da propriedade do sistema *sn_vul.flow_designer_activation* será definido como verdadeiro. Isso significa que o Flow Designer está habilitado por padrão.

Se você já estiver usando Application Vulnerability Response antes da v15.0, o valor desta propriedade do sistema será definido como falso. Você pode ativar o Flow Designer alterando o valor para verdadeiro.

Nota:
Você não pode reverter para usando o fluxo de trabalho depois de ativar o Flow Designer. Para obter uma comparação detalhada entre o fluxo de trabalho e o Flow Designer, consulte Fluxo de trabalho de gestão de exceções versus Flow Designer.

Para usar o Flow Designer, crie regras usando o módulo Regras de aprovação. Usando este módulo, você pode configurar regras de aprovação para cada um dos seguintes fluxos de trabalho de gestão de exceções.

- Solicitação de exceção para tarefas de correção
- Solicitação de exceção para itens vulneráveis da aplicação
- Regra de exceção
- Falso-positivo para tarefas de correção
- Falso-positivo para itens vulneráveis da aplicação

Nota:
Você também pode definir condições que contenham vários níveis de aprovação em uma regra. O Flow Designer herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Regras de aprovação**.
2. Na página Regras de aprovação, selecione o grupo para o qual você deseja definir a regra de aprovação.
3. No formulário, preencha os campos.

Formulário Regra de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Tabela	Tabela na qual a regra é aplicada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aplicação	O valor padrão é Vulnerability Response.
Tipo de regra	Especifica o tipo de regra. Por exemplo, gestão de exceções, falso-positivo ou regra de exceção.
Ativo	Habilitado por padrão, o que significa que a regra de aprovação está em uso.
Descrição	Descrição resumida das regras de aprovação.
Expiração da aprovação (dias) A partir da v21.0 de Application Vulnerability Response	Data até quando o aprovador pode aprovar a solicitação.
Aprovador do Notify (dias) A partir da v21.0 de Application Vulnerability Response	Data após a qual o aprovador é notificado para agir.

4. Selecione **Atualizar**.
   Na guia Configurações de aprovação, há dois níveis de aprovadores configurados por padrão. Você pode selecionar uma regra para definir as condições com base em diferentes casos de uso em uma regra.

   Nota:
   Em cada página de configuração, você pode criar vários níveis de aprovação.

Example:
Com base em diferentes casos de uso, você pode definir diferentes processos de aprovação para as mesmas vulnerabilidades encontradas em diferentes itens de configuração.

Adiando correção em Application Vulnerability Response

A partir da v20.0, você pode adiar a correção com o estado **Aguardando implementação** que está disponível para itens vulneráveis da aplicação (IVA) e tarefas de correção conforme eles passam por seus ciclos de vida. Você só pode fazer a transição manual de registros para esse estado selecionando **Aguardando implementação** no AVI e registros de tarefa de correção no estado **Sob investigação**.

Caso de uso

Como especialista em correção, você pode mover um registro para **Aguardando implementação** para que sua equipe saiba que sua pesquisa e trabalho em uma tarefa foram concluídos. Você pode escolher esta atualização se achar que uma correção está pronta para implementação, mas não está disponível. Um exemplo de correção indisponível é um patch de software. Se a janela de manutenção de um patch não estiver disponível ao terminar sua pesquisa, você poderá mover a tarefa para **Aguardando implementação** até que o patch possa ser implantado.

Campos necessários

Há dois campos editáveis obrigatórios no AVI e nos registros de tarefa de correção que estão no estado Aguardando implementação:

Data do compromisso de correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A data de correção planejada.

Plano de correção

A descrição do plano de correção para correção. Este texto é exibido nas Anotações no registro.

Campos e propriedades do sistema

Há duas propriedades do sistema que são definidas como verdadeiras por padrão para o modal que aparece quando você faz a transição de um registro para **Aguardando implementação**. Se deixado em suas configurações padrão:

sn_vul.remediation_fields

Define a **data do compromisso** de **correção e o plano** de correção como campos obrigatórios. Se definido como falso, esses campos serão opcionais.

sn_vul.aguardando_implementation

Exibe o modal com a **data do compromisso**de correção, campos de **plano** de correção depois de selecionar **Aguardando implementação** em um registro. Se definido como falso, você pode alterar o estado de um AVI para Aguardando implementação sem um prompt para inserir uma data de compromisso ou um plano.

Módulo de data de compromisso de correção ausente

Exiba todos os AVIs que tenham perdido suas datas de compromisso de correção no módulo **Data** de compromisso de correção perdida. Navegar **Application Vulnerability Response** > **Itens vulneráveis** > **Data do compromisso de correção perdido** para exibir a lista.

Rolldown de estado de tarefas de correção para AVIs

O botão de ação de IU para fazer a transição de um registro para **Aguardando implementação** só fica visível em registros de item vulnerável da aplicação e de tarefa de correção no estado **Sob investigação**. Para a distribuição de estado, no modal que aparece quando você seleciona **Aguardando implementação** em uma tarefa de correção, há uma opção para **Substituir AVIs existentes**.

Opção	Descrição
Selecione **Substituir AVIs existentes**.	Selecione esta opção para substituir as datas do compromisso de correção e os planos de correção de todos os AVIs existentes na tarefa que já está no estado **Aguardando implementação**. Se selecionado, este recurso acumula a data e os dados do plano na tarefa de correção para os AVIs.
Deixe **Substituir AVIs existentes** desativado.	Deixe a opção desativada para manter a data e os valores do plano intactos para todos os AVIs existentes na tarefa que já está no estado **Aguardando implementação**. Se desativados, os AVIs que já estão em **Aguardando implementação** preservarão a

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	data e os dados do plano existentes e não serão afetados pela distribuição de estado.

Exemplos de rolldown

Digamos que você queira fazer a transição de uma tarefa de correção de **Aberto** para **Aguardando Implementação** para que possa atualizar a data de compromisso da tarefa e as informações do plano para uma janela de manutenção de patch de software. Suponha que haja um AVI nesta tarefa no estado **Aguardando implementação** e você deseja atualizar a data de compromisso e as informações do plano para corresponder à tarefa de correção.

Para substituir a data dos AVIs e os dados do plano para que correspondam à tarefa de correção, marque a caixa de seleção para **Substituir AVIs existentes** quando solicitado. Os valores de data e plano do AVI se tornam os valores de plano e data que você insere para a tarefa no prompt ao selecionar **Aguardando implementação**.

Se você não selecionar a opção de substituição neste caso e houver um AVI em **Aguardando implementação**, a data original e os dados do plano no AVI permanecerão intactos. Os valores de plano e data que você insere para a tarefa no prompt ao selecionar **Aguardando implementação** não são usados em nenhum AVIs que já esteja no estado **Aguardando implementação** na tarefa.

Se um AVI em uma tarefa estiver em **Resolvido** ou **Encerrado-fixo** e você fizer a transição da tarefa para **Aguardando implementação**, selecionar **Substituir AVIs existentes** não mudará os AVIs de **Encerrado-fixo** e **Resolvido** para **Aguardando implementação** devido a uma precedência de estado mais alta.

Se a substituição não for selecionada ao mover a tarefa para **Aguardando implementação** e já houver um AVI em **Aguardando implementação** e você mover a tarefa de volta para **Aberto** ou **Em investigação**, o AVI permanecerá em **Aguardando implementação**.

Adicionar um aprovador de exceção para Application Vulnerability Response

Adicione usuários aos grupos de aprovadores para que você possa solicitar uma exceção.

Antes de Iniciar

Função necessária: sn_vul.app_exception_approver

Por Que e Quando Desempenhar Esta Tarefa

Uma solicitação de exceção para um item vulnerável da aplicação é aprovada usando o fluxo de aprovação de dois níveis padrão. A solicitação pode ser aprovada por dois níveis de aprovadores. Adicionar usuários ao grupo de primeiro nível é obrigatório. Se não houver usuários no segundo nível, a solicitação será aprovada após a aprovação de primeiro nível.

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Grupos**.
2. Na coluna Nome, pesquise por **Exceção**e clique em **Aprovador de exceção da aplicação - Nível 1**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A partir de Application Vulnerability Response v12.8.1, você pode usar as propriedades do sistema fornecidas no sistema de base para aprovações de exceção por meio do fluxo de trabalho na tabela Propriedades do sistema [sys_properties]. Portanto, quando uma solicitação de falso-positivo ou exceção é gerada por meio do fluxo de trabalho, ela é enviada para aprovação dos IDs de grupo definidos na propriedade do sistema. Navegar até **Todos** > **Propriedades do sistema** e selecione *sn_vul.app_exception_approver_L1*, *sn_vul.app_exception_approver_L2*ou *sn_vul.app_false_positive_approver_group* para mudar o valor da propriedade.

3. No formulário Aprovador de exceção da aplicação de grupo - Nível 1, clique na lista relacionada Membros do grupo.
4. Clique em **Novo** para criar uma lista.
5. No formulário, preencha os campos.

Formulário do usuário

Campo	Descrição
ID do usuário	Identificador exclusivo do usuário.
Nome	Nome do usuário.
Sobrenome	Sobrenome do usuário.
Título	Cargo do usuário. Insira um título ou descrição do trabalho ou selecione um na lista.
Departamento	Departamento do usuário.
Senha	Senha atribuída ao usuário. Esta senha pode ser permanente ou temporária.
A senha precisa ser redefinida	Opção para permitir que o usuário redefina a senha para garantir a segurança.
Bloqueado	Opção para bloquear a saída do usuário da instância e encerrar todas as sessões ativas do usuário. O sistema evita que usuários com a função de administrador se bloqueiem.
Ativo	Opção para tornar este usuário ativo. Somente você pode ver um usuário inativo nestas áreas: ○ Listas de usuários ○ Lista de seleção nos campos de referência (ícone de lupa) ○ Lista de preenchimento automático que aparece quando você digita em um campo de referência
Acesso somente ao serviço Web	Opção para designar este usuário como um usuário não interativo.
Usuário de integração interna	Opção para designar este usuário como um usuário de integração interna.
E-mail	Endereço de e-mail do usuário.
Idioma	Idioma preferencial do usuário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Integração de calendário	Calendário usado para gerenciar a programação de trabalho. Por exemplo, Outlook.
Fuso horário	Fuso horário para a localização deste usuário.
Formato de data	Formato preferencial do usuário para datas.
Telefone comercial	Telefone comercial do usuário.
Telefone celular	Telefone celular do usuário.
Foto	Foto que você pode carregar clicando em **Clique para adicionar...**.

6. Clique em **Enviar**.
7. **Opcional:** Repita as etapas 1 a 5 para criar um Aprovador de exceção da aplicação - Nível 2.
   O aprovador deve navegar até **Application Vulnerability Response** > **Minhas aprovações** e aprovar as solicitações.

Como solicitar e aprovar uma exceção no Application Vulnerability Response

Você pode solicitar o adiamento da correção de um item vulnerável da aplicação e de uma tarefa de correção por um período especificado.

Por exemplo, como desenvolvedor, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina. Os aprovadores que têm acesso podem aprovar solicitações de outros usuários.

Você também pode criar regras de exceção e solicitar uma extensão de exceção para uma regra de exceção. Por padrão, são necessários dois níveis de aprovação para adiamentos, regras de exceção e solicitações de extensão de exceção.

Para solicitar ou aprovar uma exceção, consulte:

- Solicitar uma exceção para um item vulnerável da aplicação
- Solicitar uma exceção para vulnerabilidades da aplicação usando GRC: Policy and Compliance Management
- Aprovar regras de exceção e solicitações de extensão de regra de exceção no Application Vulnerability Response
- Solicitar uma extensão para uma regra de exceção no Application Vulnerability Response

Nota:

Notificações por e-mail são enviadas em todas as fases do gerenciamento de exceções, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma exceção é solicitada, o solicitante recebe um e-mail confirmando que a solicitação foi gerada. O aprovador também recebe um e-mail informando que uma exceção foi solicitada.

A partir da v21.0 de Application Vulnerability Response, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável da aplicação muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável da aplicação ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solicitar uma exceção para um item vulnerável da aplicação

Solicite uma exceção para um item vulnerável da aplicação que não pode ser corrigido imediatamente. Por exemplo, como desenvolvedor, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Antes de Iniciar

Função necessária: grupo de desenvolvedores

Procedimento

1. Navegar até **Application Vulnerability Response** > **Itens vulneráveis da aplicação** > **Todos** e selecione o item para o qual você deseja solicitar uma exceção.
   O item selecionado deve estar no estado Aberto ou Em investigação.

   Nota:

   A partir da v21.0 de Application Vulnerability Response, o estado anterior de um item vulnerável da aplicação é armazenado no campo **backup_state**.

2. No formulário Item vulnerável da aplicação, clique em **Solicitar exceção**.

   Nota:
   Dependendo se Vulnerability Response está selecionado ou GRC: Policy and Compliance Management no **Application Vulnerability Response** > **Gestão de exceção** tela, o formulário de Exceção de solicitação muda. Se GRC: Policy and Compliance Management, consulte Solicitar uma exceção para vulnerabilidades da aplicação usando GRC: Policy and Compliance Management

3. Se Vulnerability Response for selecionado na tela Gestão de exceções, preencha os campos no formulário Solicitar exceção.

Formulário de Exceção de solicitação

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração selecionada no **Todos** > **Application Vulnerability Response** > **Administração** > **Gestão de exceção** tela. Quando a solicitação de exceção expira, o grupo é revertido para o estado **Aberto**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: A partir da versão 18.0 do Application Vulnerability Response (AVR), um item vulnerável da aplicação adiado pode ser fechado e reaberto por um scanner. Se o item for reaberto antes que a janela de exceção expire, o estado do AVIT será revertido para o estado adiado, respeitando a janela de exceção ativa. Para habilitar essa funcionalidade, defina o valor da propriedade do sistema sn_vul.auto_defer_avit_in_active_exception_window como verdadeiro. Além disso, a data adiada até persiste mesmo depois que o AVIT é encerrado ou a exceção expira. A função necessária é sn_vul.app_manage_exception_configuration para leitura e gravação.
Motivo	Selecione o **Motivo**. As opções são: ○ Risco aceito ○ Aguardando janela de manutenção ○ Correção indisponível ○ Redução do controle no local ○ Outro Para ver como adicionar novas opções de motivo, consulte Definir mapeamento do motivo da política.
Informações adicionais	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo obrigatório deve ser atualizado pelo responsável pela correção.

4. Clique em **Solicitar aprovação** para enviar a solicitação de exceção.
   O estado do item de vulnerabilidade da aplicação muda para Em revisão. Use a guia **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

Solicitar uma exceção para vulnerabilidades da aplicação usando GRC: Policy and Compliance Management

Solicite exceções de política usando o recurso de gestão de exceções de política GRCPolicy and Compliance Management na aplicação [] de dentro de Application Vulnerability Response.

Antes de Iniciar

Antes de usar a integração de exceção de política para solicitar exceções de política, você deve baixar a aplicação GRC: Policy and Compliance Management do ServiceNow Store.

Função necessária: sn_vul.remediation_owner

Você também pode solicitar exceções na IU clássica:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Itens vulneráveis da aplicação** (ou **Tarefas**de correção)>**Todos**e abra o item ou grupo para o qual você deseja solicitar uma exceção.
   O item ou grupo selecionado deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. No formulário selecionado, clique em **Solicitar exceção**.
3. Se GRC: Policy and Compliance Management for selecionado na tela Gestão de exceções, preencha os campos no formulário Solicitar exceção.

Formulário de Exceção de solicitação

Campo	Descrição
Política	Política de gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válido de	Data em que a exceção será iniciada. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até	Data em que a exceção de política expira e o estado do item ou grupo vulnerável muda de Adiado para Aberto. **Nota:** O número de dias em que a exceção de política é válida não pode exceder a **Duração máxima da exceção (dias)** que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Criar uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo obrigatório deve ser preenchido pelo responsável pela correção.

a. Clique em **Solicitar aprovação** para enviar a solicitação de exceção.
   O estado dos itens vulneráveis muda para Em revisão e uma exceção de política é criada. Use a guia **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

b. Clique na lista relacionada Exceções de política para exibir a exceção de política.

c. Clique no número da exceção de política.

d. No campo **Aprovador**, selecione o nome do aprovador.

e. Clique na guia Origem e selecione um objetivo de **controle no campo Objetivo** de controle.

f. Clique na guia Avaliação de risco e selecione a classificação de **risco** no campo Classificação de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

g. Salve o formulário.

h. Clique na guia Controles afetados e clique em Adicionar para adicionar os controles.

i. Salve o formulário.

> **Nota:**
> Você pode gerar uma revisão de conformidade clicando em **Solicitar revisão de conformidade**.

j. O formulário de aprovação é enviado ao aprovador.

k. Como aprovador, você pode aprovar a solicitação clicando em **Aprovar** ou solicitar aprovação adicional clicando em **Solicitar aprovação adicional**.
O estado do registro muda para Adiado. O motivo declarado é aquele que você selecionou ao gerar a solicitação de exceção. A guia Adiamento fornece anotações adicionais sobre o registro.

> **Nota:**
> Se a solicitação for rejeitada, o registro será movido para o estado anterior.

4. Clique em **Enviar**.
Para obter mais informações sobre a integração de exceção de política e a transferência entre o proprietário de correção e o gerente de conformidade, consulte Configuração opcional do Policy and Compliance Management .

Solicitar uma exceção para uma tarefa de correção de aplicação

Solicite uma exceção para adiar uma tarefa de correção de aplicação por um período especificado se ela não puder ser resolvida imediatamente.

Antes de Iniciar

Você pode solicitar exceções nos espaços Vulnerability Response. Consulte Solicitar uma exceção no Espaço de correção de problemas de TI.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Funções necessárias: sn_vul.remediation_owner, sn_vul.app_security_Champion ou sn_vul_container.remediation_owner.

Você também pode solicitar exceções para tarefas de correção de aplicação no ambiente clássico.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Tarefas de correção** > **Todos**.
2. Selecione o grupo para o qual você deseja solicitar uma exceção.
A tarefa selecionada deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
3. No registro da tarefa de correção da aplicação, selecione **Solicitar exceção**.
4. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de Exceção de solicitação

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração da exceção definida na configuração.
Motivo	Justificativa para solicitar uma exceção.
Informações adicionais	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

5. Clique em **Solicitar Aprovação**.

Aprovar regras de exceção e solicitações de extensão de regra de exceção no Application Vulnerability Response

Aprovar solicitações de exceção para itens vulneráveis da aplicação que não podem ser corrigidos imediatamente. Você deve avaliar essas solicitações quanto ao risco e aprová-las para adiamento até que possam ser corrigidas.

Antes de Iniciar

Função necessária: sn_vul.app_exception_approver

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprove ou rejeite a solicitação com os comentários apropriados.

Definir mapeamento do motivo da política

Você pode definir as opções de motivo para que estejam disponíveis para qualquer usuário que solicite uma exceção.

Antes de Iniciar

Você deve ter a aplicação GRC: Policy and Compliance Management instalada. Esta aplicação está disponível na ServiceNow® Store com uma assinatura separada.

Para obter detalhes sobre os requisitos do sistema e a compatibilidade da família, consulte a lista de aplicativos no site ServiceNow Store .

Função necessária: sn_vul.compliance.manager e sn_vul.vulnerability_admin

Procedimento

1. Navegar até **Todos** > **Policy and Compliance** > **Exceções da Política** > **Registro de Integração**.

> **Nota:**
> Você pode selecionar um motivo nas opções de motivo disponíveis na tabela Opções de motivo ou adicionar um novo motivo.

2. Clique no registro de integração da sua aplicação, por exemplo, **Application Vulnerability Response**, **Vulnerability Response**e assim por diante.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Para adicionar uma opção de motivo existente, execute as seguintes etapas:
   a. Na lista de Opções de motivo, clique em **Novo**.
   b. Clique no ícone de lupa para selecionar um motivo.
4. Para adicionar novas opções de motivo à tabela Opções de motivo, execute as seguintes etapas:
   a. Na lista de Opções de motivo, clique em **Novo**.
   b. Clique no ícone de lupa.
   c. Clique em **Nova**.
   d. No formulário, preencha os campos.

Formulário Lista de seleção de motivos

Campo	Descrição
Rótulo	Rótulo exclusivo para esta opção.
Valor	Valor exclusivo para esta opção. Este valor é mapeado na tabela Mapeamentos de motivo de exceção de política para as respectivas aplicações. Para navegar até esta tabela, insira sn_vul_policy_reason_mapping.LIST no navegador de filtros.
Ordem	Ordem para esta opção. Os motivos são solicitados com base neste número.
Padrão	Opção para indicar que esta opção de motivo estará disponível sempre que uma exceção de política sob demanda for solicitada. Se o registro de integração não contiver opções específicas da aplicação, todas as opções de motivo que tenham o campo **Padrão** selecionado estarão disponíveis.
Ativo	Opção para exibir a opção na lista de opções de motivo.

5. Clique em **Enviar**.

Solicitar uma extensão para uma regra de exceção no Application Vulnerability Response

Solicite uma extensão para uma regra de exceção adiada antes que ela atinja o adiado até a data de vencimento. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar

Funções necessárias: Gerente de App-Sec sn_vul.app_sec_manager, Campeão de segurança sn_vul.app_security_Champion.

Por Que e Quando Desempenhar Esta Tarefa

Em um registro de regra de extensão, você pode solicitar uma extensão para a data **Adiado até** somente se a regra estiver no estado **Aprovado**. Você pode solicitar esta extensão para uma regra se descobrir que um grande número de registros criados pela regra não está sendo resolvido pela data **Adiado até**, a data em que a tarefa de correção para de aceitar novos AVIs. A extensão atualiza a regra de exceção para estender automaticamente a data de adiamento na regra existente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você também pode solicitar uma extensão nos espaços Vulnerability Response. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no Espaço do gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Regras de exceção**.
2. Selecione uma regra de exceção aprovada.
3. Selecione **Solicitar extensão**.
4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até quando a regra de exceção deve ser estendida.
Motivo	Insira o motivo para adiar a regra de exceção. As opções incluem: ○ Risco aceito ○ Aguardando janela de manutenção ○ Correção indisponível ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Na aprovação da solicitação, os campos Adiado até, Motivo e Informações adicionais são atualizados na regra de exceção e nas tarefas de correção associadas e nos itens vulneráveis da aplicação. Um e-mail também é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Solicitar uma extensão para uma tarefa de correção adiada no Application Vulnerability Response

Solicite uma extensão para uma tarefa de correção adiada (VUL) antes que ela atinja a data de vencimento. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão nos espaços Vulnerability Response. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no Espaço do gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Tarefas de correção**.
2. Abra uma tarefa de correção adiada.
3. Selecione **Solicitar extensão**.
4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Prorrogar até	Selecione a data em que o estado Adiar expira e a tarefa de correção é reativada.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Na aprovação da solicitação, as mudanças na tarefa de correção também são revertidas para os itens vulneráveis da aplicação, que fazem parte da tarefa de correção. No entanto, os itens vulneráveis da aplicação devem estar no estado adiado e seus dados atuais até precedem a data até a atualização. Um e-mail também é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma tarefa de correção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Solicitar uma extensão para um item vulnerável da aplicação adiado no Application Vulnerability Response

Solicite uma extensão para um item vulnerável da aplicação adiado antes que ele atinja o adiado até a data de vencimento. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você também pode solicitar uma extensão nos espaços Vulnerability Response. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no Espaço do gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Itens vulneráveis**.
2. Abre um item vulnerável da aplicação adiado.
3. Selecione **Solicitar extensão**.

Nota:
O botão Solicitar extensão fica visível somente quando o estado do item vulnerável da aplicação é Adiado.

4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até quando o item vulnerável da aplicação adiado deve ser estendido para correção.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
Um e-mail é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:
- A solicitação passa por dois níveis de aprovação.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

6. Depois que a solicitação é aprovada, as anotações Até, Motivo e Adiamento são atualizadas.

Criar, excluir e cancelar uma regra de exceção para Application Vulnerability Response

Crie uma regra para solicitar uma exceção automaticamente para itens vulneráveis da aplicação (IVA) que atendam a condições específicas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Por exemplo, você pode criar uma regra com uma condição baseada em uma vulnerabilidade conhecida ou crítica específica que você sabe que não pode corrigir imediatamente. Com esta regra, você pode adiar AVIs novos e existentes automaticamente se eles corresponderem à condição de regra aprovada.

- A regra de exceção é aplicada da data **Válido de** até **Válido até** que você inserir no registro da regra.
- A tarefa de correção (AVUL) é criada depois que a regra é aprovada para correspondência de AVIs no estado **Adiado**.
- O método de agrupamento para este AVUL é conhecido como Regras de exceção.
- Você não pode fechar, reabrir ou excluir este AVUL. AVIs novos e reabertos são adiados e adicionados a este AVUL da data **Válido** até até o grupo expirar na data **Válido até**.

Nota:

As notificações por e-mail são enviadas em todas as fases do fluxo de trabalho da regra de exceção. Esses e-mails fornecem o status e outros detalhes de uma solicitação. Por exemplo, quando uma regra de exceção é solicitada, o solicitante recebe um e-mail que confirma que a solicitação foi enviada.

Se a regra for rejeitada, você poderá reabri-la no estado Rascunho, atualizá-la e reenviá-la para aprovação.

Funções necessárias: App SEC Manager sn_vul.app_sec_manager e Campeão de segurança sn_vul.app_security_Champion.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Regras de exceção**.
2. Na página de novo registro da Regra de exceção, selecione **Novo**.
3. Preencha os campos.

Campo	Descrição
Nome	Nome da regra de exceção.
Estado	Somente leitura: rascunho
Válido de	Data a partir da qual esta regra está ativa para adiar AVIs.
Ordem de execução	Ordem exclusiva para cada regra de exceção. Um valor menor precede um maior.
Válido até	Data em que a tarefa de correção para de aceitar novos AVIs.
Adiado até	Data até que as tarefas de correção e os AVIs sejam adiados. Nesta data, os AVULs são encerrados e todos os AVIs são movidos para fora das tarefas e reabertos. As regras de grupo são reaplicadas a esses AVIs.
Motivo	Motivo para criar esta regra de exceção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Grupo de atribuição	Grupo ao qual a tarefa de correção está atribuída para rastrear os AVIs adiados.
Informações adicionais	Informações adicionais que o solicitante deseja fornecer ao aprovador. Essas informações são preenchidas no campo de descrição da tarefa de correção.
Condição	Filtrar condições para especificar quais AVIs correspondem a esta regra.
Executar em dados existentes	Opção que permite executar esta regra em dados existentes na primeira vez em que esta regra é executada. Se você deixar esta opção desativada, sua regra será executada diariamente pelo trabalho programado *Associate existing AVIs with Auto Exception Rule* começando com novos dados. Se você habilitar a opção Executar em dados existentes, um trabalho programado será executado uma vez nos dados existentes na data **Válido a partir de**.

4. Adicione o grupo de atribuição ao criar a regra.
5. Escolha um.

   Depois que a regra é aprovada, ela passa para o estado **Aprovado**. Sua regra avalia AVIs com o trabalho *Associate existing AVIs with Auto Exception Rule scheduled*. Se você selecionou **Executar em dados existentes**, ele avaliará os AVIs existentes. Uma tarefa de correção é criada automaticamente para a regra e todos os AVIs correspondentes que atendam às condições são associados à tarefa.

   O trabalho programado executa a regra de exceção uma vez nos dados existentes. A regra não será executada novamente nos dados existentes, mesmo se nenhum AVI for encontrado. Ele só avalia novos dados porque os AVIs existentes que correspondem à regra já foram adiados.

6. Para excluir uma regra, selecione **Excluir** no registro da regra de exceção.
   A seguinte mensagem é exibida: Se você excluir a regra, a tarefa de correção associada será excluída e os itens vulneráveis relacionados serão reabertos. As regras de tarefa de correção serão aplicadas aos AVIs individuais e a regra de exceção será excluída.
7. Selecione**Manter regra** para parar ou **Excluir regra** para continuar.
8. Para desativar uma regra, mas mantê-la na lista Regras de exceção, selecione **Cancelar**.
   A seguinte mensagem é exibida: Se você cancelar esta regra, a tarefa de correção associada será excluída e os itens vulneráveis relacionados serão reabertos. As regras de tarefa de correção serão aplicadas aos itens vulneráveis individuais e a regra de exceção será movida para o estado de rascunho.
9. Selecione**Manter regra** para parar ou **Cancelar** para mover a regra para **Rascunho** e desativá-la.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Application Vulnerability Response tarefas de correção e regras de tarefa visão geral

Configure tarefas de correção (AVULs) para ajudar analistas e especialistas em correção a organizar itens vulneráveis da aplicação (IVA) e analisá-los em massa. Os critérios pelos quais as tarefas de correção são formadas são configurados para que os AVIs sejam atribuídos automaticamente às tarefas de correção. Usando tarefas de correção, você pode monitorar o andamento e conduzir o processo de correção com mais eficiência.

Contagens de adiamento de rastreamento para itens vulneráveis da aplicação e tarefas de correção

Rastreie o número de vezes que um item vulnerável, item vulnerável de aplicação, item vulnerável de contêiner ou tarefa de correção é adiado. O trabalho programado *`set deferral counts`* é executado diariamente para publicar contagens dos registros que são adiados mais de uma vez na coluna Contagem de adiamento. Os registros são exibidos nos módulos Vários adiamentos para VR, AVR e CVR.

Noções básicas sobre regras de tarefa de correção

As regras de tarefa de correção permitem que você defina como os itens vulneráveis da aplicação são automaticamente agrupados e atribuídos. Uma **vulnerabilidade** de regra padrão está incluída no sistema de base que reúne AVIs com base em suas vulnerabilidades. No entanto, você pode agrupar por qualquer outro conjunto de valores em colunas acessíveis pelo AVI. Esses valores podem incluir item de configuração (IC), entrada de vulnerabilidade e assim por diante.

Existem regras de tarefa para o Application Vulnerability Response que estão incluídas com a aplicação Vulnerability Response que está disponível quando você a ativa.

Você pode criar várias condições com o construtor de condição. Na seção Agrupar por, depois de definir um par de campos, outra linha é exibida. Você pode ter até seis seleções **de Agrupar por**. Você também pode automatizar a atribuição de grupo. Para obter mais informações, consulte Atribuir itens vulneráveis da aplicação em Application Vulnerability Response automaticamente e Filtragem em Vulnerability Response.

Por exemplo, você pode agrupar os itens vulneráveis da aplicação pelo item de configuração ou pelo modelo de produto. Você pode ter uma regra de tarefa para vulnerabilidades de baixa severidade ou ICs de baixo risco. Você pode ter outra regra de tarefa para servidores críticos e vulnerabilidades que expõem a empresa a mais riscos. Consulte Criar, editar e excluir Application Vulnerability Response regras de tarefa de correção para obter mais informações sobre as opções disponíveis.

Um conjunto diferente de regras pode ser usado para itens vulneráveis da aplicação que expõem a empresa a mais riscos. O nome da tarefa de correção é anexado à regra de tarefa de correção **Agrupar por** valores para fazer a descrição resumida do novo registro.

Quando um novo item vulnerável da aplicação é criado, importado ou reaberto após ser encerrado, as regras são avaliadas em relação a ele. Um AVI é avaliado apenas uma vez, automaticamente, a menos que seja reaberto após ser fechado ou as regras sejam reaplicadas manualmente.

O processo a seguir é usado para cada AVI novo ou reaberto:

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Para cada regra de tarefa de correção, o AVI é comparado ao filtro de regra de tarefa de correção.

- Para cada regra em que a condição da regra da tarefa de correção corresponde, a regra extrai os dados do **Agrupar por** seleções no AVI. Ele cria um nome de grupo e um campo. Nesse caso, **Alto risco: QID-32342:***resumo de QID-3242* (Nome: ID da vulnerabilidade: resumo da vulnerabilidade).

  Nota:
  O campo de descrição resumida é limitado a 160 caracteres. Resumos de vulnerabilidade mais longos são truncados.

  A regra verifica se há uma tarefa de correção em **aberto** correspondente que esteja atribuída ao mesmo grupo de atribuição que o AVI.

  - Se a tarefa for encontrada, o AVI será adicionado à tarefa existente no estado **Aberto**.
  - Se nenhuma tarefa no estado **Aberto** for encontrada, a regra criará uma tarefa **de alto risco: QID-32342**, a atribuirá ao mesmo grupo de atribuição que o AVI e colocará o AVI na tarefa de correção.

Mais de uma regra de tarefa de correção pode ser definida para agrupar diferentes tipos de vulnerabilidades. Como cada vulnerabilidade é comparada com as condições de regra da tarefa de correção antes de ser colocada em uma tarefa de correção, o excesso de regras pode afetar o desempenho. Configure suas regras de tarefa para que as condições ajudem a evitar a criação de tarefas de correção duplicadas.

Por padrão, as regras de tarefa de correção usam o grupo de atribuição definido pelas **Regras de atribuição** no AVI ao agrupar os itens e atribuir a tarefa de correção para corresponder aos AVIs.

Como parte da regra de tarefa padrão, a atribuição dessas tarefas de correção é controlada pelas regras no módulo **Regras de atribuição**. Para obter mais informações sobre regras de atribuição, consulte Vulnerability Response visão geral de regras de atribuição.

Quando uma regra de tarefa é excluída do formulário ou da exibição de lista, você tem a opção de excluir todas as tarefas **abertas** criadas por essa regra. As tarefas que não estão no estado **Aberto** são excluídas.

Reaplicar regras de tarefa de correção

Quando você quiser mudar uma regra de tarefa de correção, use o botão **Reaplicar** na página de regra de tarefa de correção para executar novamente a regra alterada em todas as tarefas de correção em **aberto** ativas criadas por essa regra. Ele exclui e recria tarefas de correção com base na regra alterada automaticamente.

Reaplicar verifica somente as tarefas de correção existentes.

Depois de selecionar **Reaplicar**, a seguinte mensagem será exibida: A reaplicação desta regra de tarefa de correção excluirá e recriará as tarefas de correção para esta regra. As tarefas de correção que não estão no estado Aberto não são excluídas.

Criando tarefas de correção e adicionando AVIs manualmente

Você cria uma tarefa de correção de aplicação (AVUL) de outro registro de tarefa de correção de aplicação e adiciona itens vulneráveis de aplicação (AVITs) manualmente. Para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

obter mais informações, consulte Como criar uma tarefa de correção de aplicação manualmente no Application Vulnerability Response.

Regras de tarefa de correção e criação e atualização de AVI

Se um IC ou modelo de produto de uma verificação estiver associado a uma vulnerabilidade conhecida, um AVI será criado. Depois de criado, o AVI é avaliado em relação às condições das regras de tarefa de correção para uma correspondência. Se houver uma correspondência para uma tarefa de correção existente, o AVI será adicionado. Se uma tarefa de correção correspondente não for encontrada, uma será criada para o AVI.

Se alguma propriedade capturada nas condições de filtragem da tarefa de correção for atualizada ou alterada em um AVI, o AVI atualizado também será avaliado em relação às regras da tarefa de correção para uma correspondência. Se houver uma correspondência para uma tarefa de correção existente, o AVI será adicionado. Se uma tarefa de correção correspondente não for encontrada, uma será criada para o AVI.

Rollup e rolldown de estado

Se você atualizar uma tarefa de correção para Aberto ou de Aberto para Sob investigação, o novo estado será transferido para todos os AVIs associados. A rolagem de estado ocorre imediatamente após a mudança do estado.

O acúmulo de estado de AVIs para a tarefa de correção ocorre somente se todos os AVIs na tarefa estiverem nos estados **Adiado** ou **Encerrado-fixo**. O acúmulo é feito com o trabalho programado *`Rollup application vulnerable item values to vulnerability and group`*, que é executado a cada 15 minutos. O estado não é acumulado até que o trabalho seja executado. Para que um estado seja acumulado para ocorrer dos AVIs para a tarefa de correção, todos os AVIs devem estar no mesmo estado.

Criar, editar e excluir Application Vulnerability Response regras de tarefa de correção

Você pode criar regras para agrupar automaticamente itens vulneráveis da aplicação (AVI) em tarefas de correção (AVUL) com base nas condições do filtro. Essas regras agrupam automaticamente os AVIs conforme eles são importados ou criados manualmente.

Antes de Iniciar

Se você criar uma nova regra, ela não se aplicará aos dados existentes. Depois de enviá-lo, ele será executado em novas importações.

Função necessária: gerente de App-Sec

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Regras de tarefa de correção**.
2. Abra a regra ou selecione **Novo**.
3. Preencha os campos no formulário ou edite-os.

Regra de tarefa de correção

Campo	Descrição
Nome	Nome da regra de tarefa.
Ativo	Indica se a tarefa está ativa.
Descrição	Descrição da regra.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Diferenciação entre maiúsculas e minúsculas	Determina se uma condição faz distinção entre maiúsculas e minúsculas ou não. **Nota:** O valor padrão não faz distinção entre maiúsculas e minúsculas.
Condição	Condições de filtro opcionais para a regra. Por padrão (caixa de seleção que**diferencia maiúsculas de minúsculas** não marcada), o texto de pesquisa inserido no construtor de condição em registros e formulários de regras de tarefa não diferencia maiúsculas de minúsculas. Você tem a opção de habilitar pesquisas que diferenciam maiúsculas de minúsculas em registros e formulários de tarefa. Um exemplo de condição é **Vulnerabilidade** > **é** > **VULNENT123451** (uma vulnerabilidade importada conhecida). Todos os AVIs que têm esta vulnerabilidade correspondem a esta condição.
Agrupar por (até seis conjuntos de condições estão disponíveis)	
Agrupar itens vulneráveis da aplicação de	A tabela que a regra usa para agrupar AVIs. Selecione os elementos da árvore: ○ Item vulnerável da aplicação [sn_vuln_vulnerable_item] ○ Item de configuração do item vulnerável da aplicação [cmdb_ci] ○ Vulnerabilidade da aplicação do item vulnerável da aplicação [sn_vul_third_party_entry] ○ Modelo de produto de item vulnerável da aplicação **Nota:** Se você escolher uma tabela estendida, o **campo Usando** será aplicado somente para itens vulneráveis de aplicação que usam essa tabela estendida.
Usando o campo	Campo na tabela que a regra usa para agrupar AVIs. Selecione condições na árvore. **Nota:** Você pode criar agrupar por condições para que nem todos os AVIs que compartilham dados sejam atribuídos à mesma tarefa de correção. Por exemplo, se você selecionar Grupo de atribuição e Endereço IP como Usando campos e vários AVIs corresponderem à condição de filtragem inicial **Vulnerabilidade**, esses AVIs poderão ser atribuídos a grupos de atribuição distintos para correção usando as várias opções disponíveis na seção Agrupar por. As condições Agrupar por oferecem a flexibilidade para criar tarefas de correção distintas que podem ser atribuídas a grupos diferentes, mesmo que eles compartilhem alguns dados.
Atribuição	
Atribuir tarefas de correção por	Ao atribuir automaticamente tarefas de correção, a opção Atribuição é usada além das opções **Agrupar por** para agrupar os itens vulneráveis. Novas tarefas são criadas, conforme necessário, para que cada AVI

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	seja colocado em uma tarefa com um conjunto de grupo de atribuição correspondente. Para automatizar a atribuição de tarefas criadas com base nesta regra, escolha uma das opções disponíveis. ○ Agrupar por campo: se você selecionou qualquer campo de grupo de usuários na seção **Usar valores de campo** na seção **Agrupar por**, eles serão exibidos no menu suspenso. ○ Grupo de usuários: use a lista de pesquisa para selecionar um grupo de usuários estático.

se você excluir uma regra do formulário ou da exibição de lista, terá a opção de excluir todas as tarefas de correção em **aberto** criadas por essa regra. Os grupos que não estão no estado **Aberto** são excluídos.

4. Selecione **Enviar** para novas regras.
   Depois de selecionar **Enviar**, sua regra será exibida na lista Regras de tarefa de correção [sn_vul_grouping_rule]. As situações a seguir iniciam sua regra.
   - Quando novos AVIs são criados.
   - Ao selecionar **Reaplicar**. Selecione **Reaplicar** para avaliar as regras de tarefa somente em tarefas de correção existentes.
   - Quando os AVIs são atualizados, por você ou pelo sistema.

     Se um AVI for atualizado, as regras de tarefa serão avaliadas quanto a correspondências com as tarefas de correção existentes. Algumas atualizações comuns que iniciam uma verificação de regras são:
     - Quando o Estado muda de Encerrado para Aberto ou de Encerrado para Sob investigação.
     - O item de configuração (IC) foi alterado.
     - A vulnerabilidade foi alterada.

   O sistema verifica todas as regras de tarefa em busca de correspondências com o AVI atualizado. Se as condições de uma regra corresponderem às condições de uma tarefa de correção, os AVIs correspondentes serão atribuídos a ela.

   Se nenhuma correspondência for encontrada, uma nova tarefa de correção será criada.

   Para obter mais informações sobre a distribuição de estado de AVIs para tarefas de correção e a distribuição de estado de tarefas de correção para AVIs, consulte Application Vulnerability Response tarefas de correção e regras de tarefa visão geral.

   Para obter um exemplo de uma regra de tarefa de correção, consulte Application Vulnerability Response exemplos de regra de tarefa de correção.

5. Para excluir uma regra de tarefa, selecione a regra na lista Regras de tarefa de correção e selecione **Excluir**.
   A seguinte mensagem é exibida: A regra de tarefa de correção selecionada criou n tarefas de correção. Das tarefas de correção, n estão no estado Aberto..

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Caixa de seleção desativada (padrão).	Exclua somente a regra. As tarefas que não estão no estado **Aberto** são excluídas.
Caixa de seleção selecionada.	Inclua as tarefas de correção no estado **Aberto** ao excluir a regra de tarefa de correção. Exclua a regra e todas as tarefas de correção no estado **Aberto**.

6. Escolha uma opção e selecione **Excluir**.

Como criar uma tarefa de correção de aplicação manualmente no Application Vulnerability Response

Crie uma tarefa de correção de aplicação (AVUL) a partir de outro registro de tarefa de correção de aplicação e adicione itens vulneráveis de aplicação (AVITs) manualmente.

Antes de Iniciar
Função necessária: sn_vul.app_sec_manager

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Tarefas de correção** > **Todos**.
2. No canto superior direito da página, selecione **Novo**.
3. Na guia Configuração de grupo, para Método de agrupamento, selecione **Manual**.
4. Selecione **Enviar**.
5. Localize seu novo registro de tarefa (AVUL) na tabela Tarefas de correção da aplicação [sn_vul_app_vulnerability].
   O registro é criado no estado **Aberto**.
6. Abra o registro e adicione itens vulneráveis da aplicação novos ou existentes a este grupo usando a lista relacionada de itens vulneráveis da aplicação (**Editar** ou **Adicionar**).
7. Selecione **Atualizar** para salvar o registro ou outras ações de IU para fazer a transição do registro para outro estado.

Configurar teste de invasão

Você pode configurar a duração do sprint e o esforço estimado para os tipos de avaliação de teste de invasão. Isso fornece a funcionalidade de programação para proprietários de aplicações, ajudando-os a determinar um intervalo de tempo provisório para suas solicitações de avaliação de teste de invasão.

Antes de Iniciar
Função necessária: Ethical Hacker

Por Que e Quando Desempenhar Esta Tarefa
Definir as configurações de avaliação de teste de invasão para a equipe de hacking ético também ajuda a determinar o grupo e o ponto de contato que recebe a solicitação de avaliação de teste de invasão.

A partir da v19.0 de Vulnerability Response, se você estiver usando o Veracode Vulnerability Integration, os testes de avaliação de invasão no Veracode Vulnerability Integration serão descobertas manuais de Veracode. Eles não estão vinculados a nenhuma solicitação de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

avaliação de teste de invasão configurada em Application Vulnerability Response. Para obter mais informações sobre avaliações de teste de invasão de Veracode, consulte o Veracode Vulnerability Integration.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Configuração de testes de invasão**.
2. Use a primeira seção para configurar o grupo de atribuição.
3. No formulário, preencha os campos.

Formulário de configuração de teste de invasão

Campo	Descrição
Grupo de usuários da equipe de testes de invasão	Grupo ao qual a solicitação de avaliação de teste de invasão é atribuída.
Designado padrão das solicitações de avaliação de testes de invasão	Ponto de contato para a solicitação de avaliação de teste de invasão.

4. Selecione **Atualizar**.
5. Use a segunda seção para configurar sprints.
   Para obter detalhes, consulte Configurar sprints para teste de invasão.
6. Use a terceira seção para configurar os tipos de avaliação.
   Para obter detalhes, consulte Configurar tipos de avaliação para teste de invasão.

Configurar sprints para teste de invasão

Configure a duração e a capacidade do sprint para que a equipe de hackers éticos possa gerenciar a capacidade do sprint para avaliações de teste de invasão.

Antes de Iniciar

Função necessária: Ethical Hacking

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Configuração de testes de invasão**.
2. Selecione a opção **Configurar** para Configurar sprints.
3. No formulário, preencha os campos.

Formulário Configuração do sprint

Campo	Descrição
Duração do sprint (dias)	Número de dias em um sprint.
Data de início	Data de início da duração do sprint.
Número de sprints	Número de sprints que podem ser gerados, com base nas datas de início e término do intervalo de sprints.
Data de término	Data de término da duração do sprint.
Capacidade de sprint	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Capacidade de sprint (h)	Capacidade de um sprint em horas.

4. Selecione **Gerar Sprints**.
   Para exibir os sprints criados, selecione **Exibir sprints**.

> **Nota:**
> Depois que os sprints forem gerados e estiverem em andamento, se você selecionar **Gerar sprints** para a mesma duração, o sprint atual será concluído normalmente. Os sprints restantes são recalculados com base na configuração de sprint atualizada.

Configurar tipos de avaliação para teste de invasão

Configure o esforço estimado para cada tipo de avaliação de teste de invasão. Isso permite que você gerencie a capacidade de cada sprint, estimando o esforço necessário para cada tipo de avaliação.

Antes de Iniciar
Função necessária: Ethical Hacking

Por Que e Quando Desempenhar Esta Tarefa
Cada sprint é atribuído a uma solicitação de teste de invasão. Com base no esforço estimado para o tipo de avaliação, as horas são ajustadas para refletir as horas de saldo do sprint.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Configuração de testes de invasão**.
2. A partir da v19.0 de Vulnerability Response, selecione **Configurar** para exibir os tipos de avaliação, o tamanho da aplicação e o esforço estimado.
3. **Opcional:** Selecione um registro de tipo de avaliação para atualizar os campos conforme necessário ou criar novos registros.

   (Optional) Os valores de tamanho da aplicação fornecem mais opções para ajudar a estimar o tempo e o esforço do teste com mais precisão. Você pode editar as horas desses registros ou selecionar **Novo** para criar suas próprias combinações.

   Você pode modificar o tipo de avaliação e o tamanho da aplicação em valores nos registros de solicitação de teste de invasão existentes para que possa programar testes para corresponder à capacidade do sprint. Por exemplo, se você preencher uma solicitação de teste, talvez não veja o número de sprints que configurou, porque alguns sprints já foram usados para teste. Se as horas de esforço estimadas de um sprint corresponderem à combinação necessária para o tipo e o tamanho de um teste, elas não estarão disponíveis para novas solicitações.

   Você pode ver os sprints atribuídos às solicitações de teste em registros na lista de Sprints de teste de invasão em **Todos** > **Application Vulnerability Response** > **Administração** > **Configuração de testes de invasão** > **Configurar sprints**. Consulte Configurar sprints para teste de invasão para obter mais informações sobre como configurar sprints.

   Os valores base para Tipo de avaliação, Tamanho da aplicação e Esforço estimado são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de configuração do tipo de avaliação de teste de invasão

Tipo de avaliação	Tamanho da aplicação	Esforço estimado (h)
Teste focado	Pequeno	20
Teste focado	Média	30
Teste focado	Grande	40
Teste focado	Padrão	40
Testar novamente	Pequeno	10
Testar novamente	Média	15
Testar novamente	Grande	20
Testar novamente	Padrão	20
Teste de invasão completo	Pequeno	60
Teste de invasão completo	Média	70
Teste de invasão completo	Grande	80
Teste de invasão completo	Padrão	80

4. Selecione Atualizar para salvar suas mudanças ou Enviar para um novo registro.
5. Antes da v19.0, selecione a opção **Configurar** para Configurar tipos de avaliação.
6. Atualize os valores dos tipos de avaliação conforme necessário.
   Os valores base são:

Formulário de configuração do tipo de avaliação de teste de invasão

Tipo de avaliação	Esforço estimado (h)
Teste focado	40
Testar novamente	20
Teste de invasão completo	80

7. Salve as mudanças.

Integração do Application Vulnerability Response a outras aplicações

Vulnerability Response inclui suporte para integrações de terceiros.

Integrações de terceiros

As integrações de vulnerabilidade da aplicação ajudam a aprimorar os dados de vulnerabilidade da aplicação em sua instância, recuperando dados de sistemas e fornecedores externos. Consulte os seguintes tópicos de visão geral para obter mais informações sobre integrações compatíveis:

- Integrações de vulnerabilidade do Fortify
- Integrações de vulnerabilidade de aplicação do GitHub

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Integrações de vulnerabilidade do Invicti
- Veracode Vulnerability Integration

Nota:

Integrações de várias origens não são compatíveis com Application Vulnerability Response. Integrações de terceiros são tratadas separadamente. Se mais de uma aplicação de integração de terceiros estiver em uso em seu ambiente, não haverá desduplicação de item vulnerável da aplicação (IVA) entre as integrações.

Anotações adicionais para integrações

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Application Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota:

O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- `sn_sec_cmn.record_threshold_heartbeat`: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- `sn_sec_cmn.maximum_heartbeat_delay`: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Integrações de vulnerabilidade do Fortify

O Integrações de vulnerabilidade do Fortify usa dados importados do produto Fortify para ajudar a determinar o impacto e a prioridade das falhas no seu código.

Integrações de vulnerabilidade do Fortify

O produto Fortify coleta dados do scanner e disponibiliza esses dados para o Now Platform®. Ele se integra facilmente ao recurso [ServiceNow® Application Vulnerability Response de Vulnerability Response para mapear vulnerabilidades de terceiros que enriquecem os dados em sua instância.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Todos os dias, os trabalhos programados invocam as integrações automaticamente. Depois que todas as integrações forem ativadas, elas serão encadeadas para serem executadas em sequência. Você também pode executar trabalhos programados individuais

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

manualmente. Os trabalhos programados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Versões disponíveis

Versão de lançamento	Notas de versão
Vulnerability Response integration with Fortify v2.2 Fortify v2.1 Fortify v2.0	Application Vulnerability Response release notes Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Integrações de vulnerabilidade do Fortify

Para exibir o Integrações de vulnerabilidade do Fortify, navegue até **Integrações de vulnerabilidade do Fortify** > **Integrações**.

As integrações a seguir estão incluídas no sistema de base. Essas integrações não estão ativas por padrão.

Após a execução inicial, todos os dias, os trabalhos programados são encadeados para executar as integrações automaticamente na ordem. Você também pode executar trabalhos programados individuais manualmente. Os trabalhos programados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Fortify Integrações de vulnerabilidade

Integração	Descrição
Fortify on Demand Application List Integration	Recupera Fortify dados do scanner da aplicação (vulnerabilidades, metadados) e enriquece os dados da aplicação de terceiros. Esta integração está definida para ser executada diariamente às 00:00:00. Está ativo por padrão.
Fortify On Demand Scan Summary Integration	Recupera registros de verificação de Fortify. Esta integração é encadeada para ser executada após a integração da lista de aplicações Fortify on Demand quando ativada. Está inativo, por padrão.
Fortify integração de item vulnerável da aplicação sob demanda	Recupera resultados de verificação de Fortify, insere AVIs e aprimora seus dados de vulnerabilidade de terceiros. Se o registro do scanner estiver no estado **Encerrado**, os AVIs não serão criados. Os AVIs existentes ainda serão atualizados. Esta integração é encadeada para ser executada após a Fortify Integração de resumo de verificação sob demanda quando ativada. Está inativo, por padrão.

Para obter os status de execução da integração, consulte Exibir o status de execução de importação Integrações de vulnerabilidade do Fortify.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para exibir dados em vulnerabilidades de terceiros, consulte Exibir bibliotecas de vulnerabilidades.

Preparando para o Integrações de vulnerabilidade do Fortify

Um Integrações de vulnerabilidade do Fortify bem-sucedido requer planejamento e execução de tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. O Integrações de vulnerabilidade do Fortify pressupõe que você esteja familiarizado com o produto Fortify e a API.

Antes de Iniciar

A integração de CWE (Common Weakness Enumeration) também é usada por Application Vulnerability Response e deve estar em execução antes de instalar e configurar o Integrações de vulnerabilidade do Fortify.

Nota:
Os dados do banco de dados de vulnerabilidades do NIST (NVD) não são necessários para instalar o Integrações de vulnerabilidade do Fortify, no entanto, eles fornecem aprimoramento e seria útil ter.

Para obter informações sobre NVD, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Função necessária: gerente de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Nota:
Antes de executar a integração, faça as mudanças de configuração necessárias com base em seus requisitos.

Valide o dimensionamento da instância com base no número de itens vulneráveis da aplicação que você espera importar. Uma instância subdimensionada pode levar a longos tempos de carregamento. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente.

O Integrações de vulnerabilidade do Fortify requer uma chave de API, um segredo de API e um URL raiz de API, disponíveis na sua conta Fortify on Demand.

Procedimento

Para criar uma chave secreta de API:

a. Faça login no portal Fortify on Demand.

b. Navegar até **Todos** > **Administração** > **Configuração** > **API**.

c. Adicione a ServiceNow como uma aplicação.

d. Clique em **Novo segredo** para gerar um segredo de API.

e. Registre seu segredo de API para uso posterior.

Instalar o Vulnerability Response Integration [ServiceNow® com Fortify

Antes de executar a integração na sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto Fortify se integre corretamente com Application Vulnerability Response. Esta aplicação está disponível como uma assinatura separada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Tarefas de configuração	Descrição
Verifique se a aplicação Vulnerability Response está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Vulnerability Response.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o administrador do sistema [admin] instalará a aplicação e atribuirá usuários ao grupo de gerentes de App-Sec. Para obter informações sobre as funções do grupo, consulte Application Vulnerability Response grupos de usuários e funções. • O grupo do App-Sec Manager supervisiona a configuração e verifica os resultados esperados.

Função necessária: gerente de App-Sec

Procedimento

1. Faça login na instância na qual você deseja instalar o Integrações de vulnerabilidade do Fortify.
2. Navegue até o ServiceNow Store.
3. Na aplicação ServiceNow Store, pesquise a aplicação Vulnerability Response Integration with Fortify.
4. Clique no bloco da aplicação.
   Informações detalhadas sobre a aplicação que você está instalando são exibidas.

   Nota:
   Considere a leitura das seções **Outros requisitos** e **Dependências**, conforme aplicável.

5. Clique em **Solicitar app** e insira suas Now Support credenciais de login.
6. Clique **em Obter**.
7. Insira o **Nome da instância** e **o Motivo da instância**e clique em **Validar instância**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Candidaturas**.
10. Localize a aplicação, selecione-a e clique em **Instalar**.
    Sua aplicação é instalada automaticamente na sua instância.

O que Fazer Depois

Configure o Integrações de vulnerabilidade do Fortify para o seu ambiente. Consulte Configurar o Integrações de vulnerabilidade do Fortify.

Configurar o Integrações de vulnerabilidade do Fortify

Antes de executar a integração na sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto Fortify se integre corretamente ao recurso [Application Vulnerability Response de Vulnerability Response. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Funções necessárias: gerente de App-Sec

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Tarefas de configuração	Descrição
Verifique se a aplicação Vulnerability Response está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Vulnerability Response.
Verifique se a aplicação Vulnerability Response Integration with Fortify está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar o Vulnerability Response Integration [ServiceNow com Fortify.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	• Se ainda não estiver atribuído, o administrador do sistema [admin] instalará o app e atribuirá usuários ao grupo de gerentes de App-Sec. • O gerente de App-Sec supervisiona a configuração e verifica os resultados esperados.
Para o Integrações de vulnerabilidade do Fortify, tenha seu **ID** de **API e chave** de API prontos.	Entre em contato com Fortify para obter o **ID da API** e **a chave**da API.

Procedimento

1. Faça login na instância em que você deseja instalar as integrações de vulnerabilidade da aplicação Fortify.
2. Navegue até o ServiceNow Store.
3. No ServiceNow Store, pesquise a integração [Vulnerability Response com a aplicação Fortify.
4. Clique no bloco da aplicação.
   Informações detalhadas sobre a aplicação que você está instalando são exibidas.

   Nota:
   Considere ler as seções **Outros requisitos** e **Dependências**, conforme aplicável.

5. Clique em **Solicitar app** e insira suas Now Support credenciais de login.
6. Clique **em Obter**.
7. Insira o **Nome da instância** e **o Motivo da instância**e clique em **Validar instância**.
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Candidaturas**.
10. Localize a aplicação, selecione-a e clique em **Instalar**.
    Sua aplicação é instalada automaticamente na sua instância.
11. Quando a instalação for concluída, navegue até **Integrações de vulnerabilidade do Fortify** > **Configuração do FoD**.
12. No formulário, preencha os campos.

Formulário de configuração do Fortify on Demand

Campo	Descrição
URL raiz da API	URL da instância do Fortify do usuário.
Chave de API	Identificador exclusivo enviado para a API Fortify.
Segredo da API	Segredo do cliente fornecido por Fortify.
Incluir DAST	Opção para incluir vulnerabilidades de verificações DAST. As verificações DAST identificam vulnerabilidades no comportamento da aplicação geral.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Incluir SAST	Opção para incluir vulnerabilidades de verificações SAST. As verificações do SAST identificam vulnerabilidades no código.
Exceções de triagem e falsos positivos na ServiceNow (começando com v20.0 do Vulnerability Response)	Selecione opções para gerenciar fluxos de trabalho de gestão de exceções e falso-positivos para AVIs com ServiceNow automaticamente na importação. Essas opções são ativadas por padrão. Para obter um exemplo de caso de uso, consulte Como gerenciar o mapeamento de estado para adiamentos e falsos positivos no Application Vulnerability Response. **Gerenciar exceções no ServiceNow** Deixe esta opção ativada se quiser fazer a triagem de AVIs importados marcados para o estado **Adiado**. AVIs com estados de **Origem** que normalmente são mapeados para um estado **Adiado** em sua instância são mapeados para **Aberto**. Você **solicita uma exceção** do registro AVI. **Gerenciar falsos positivos no ServiceNow** Deixe esta opção ativada se quiser fazer a triagem de AVIs importados com estados de **origem** marcados como **Falso-positivo** ou **Possível falso-positivo**. AVIs com esses estados de **origem** que normalmente são mapeados para um estado **Closed** em sua instância são mapeados para **Open**. Você solicita um **falso-positivo** do registro AVI. ○ Desative uma ou ambas as caixas de seleção se quiser preservar os estados de **origem** importados do scanner. ○ Esses AVIs são mapeados para os estados de Destino e Motivo de destino conforme são importados, mas não são triados pelos fluxos de trabalho de exceção e falso-positivos. As ações **Solicitar exceção** e **Falso-positivo** não são visíveis em AVIs.
Triagem na ServiceNow (anterior à v20.0 do Vulnerability Response)	Gerencie a triagem de vulnerabilidade da aplicação na instância ServiceNow :

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Marque a caixa de seleção para fazer a triagem dos AVIs em ServiceNow. Se esta opção for selecionada, os AVIs serão importados no estado Aberto. Você pode solicitar uma exceção ou marcar o AVI como um falso positivo. ○ Para reter o estado de origem, ou seja, o estado importado do scanner, certifique-se de que a caixa de seleção não esteja marcada. **Nota:** As opções **Marcar como falso-positivo** e **Solicitar exceção** estão disponíveis somente para AVIs que estão sendo triados em ServiceNow.

13. Selecione **Salvar e testar credenciais**.

O que Fazer Depois

Se o seu ambiente requer importações separadas por domínio, consulte Criar importações separadas por domínio para uma integração.

Na instalação inicial, consulte Configurar Application Vulnerability Response. para obter mais instruções.

Após a instalação inicial, consulte as modificações em Integrações de vulnerabilidade do Fortify modificação e atividades.

Exibir o status de execução de importação Integrações de vulnerabilidade do Fortify

Use a lista relacionada Execuções de integração de **vulnerabilidade** para verificar o sucesso de suas execuções de integração, localizar problemas e informar suas decisões de correção.

Antes de Iniciar

Para exibir o status de execução de importação Fortify :

- As aplicações Vulnerability Response e Integrações de vulnerabilidade do Fortify devem ser instaladas e configuradas.
- As importações Integrações de vulnerabilidade do Fortify devem ser programadas e em execução.

Função necessária: gerente de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Application

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Integrações de vulnerabilidade do Fortify** > **Integrações**.
2. Selecione uma integração.
3. Clique na lista relacionada **Execuções de integração de vulnerabilidade**.
4. Verifique se todas as importações foram bem-sucedidas.

Integrações de vulnerabilidade do Fortify modificação e atividades

Configure modificações opcionais especificamente para o Integrações de vulnerabilidade do Fortify.

Nota:
Alterar outras configurações de Integrações de vulnerabilidade do Fortify, além das listadas aqui, requer conhecimento avançado de ServiceNow e Application Vulnerability Response e está além do escopo da documentação do produto.

Executar uma importação manual de vulnerabilidade da aplicação Fortify

Se a importação inicial falhar ou você não quiser aguardar a importação inicial programada, poderá executar uma importação de dados completa independentemente do trabalho programado diariamente.

Antes de Iniciar

Função necessária: gerente de App-Sec

Procedimento

1. Navegar até **Todos** > **Integrações de vulnerabilidade do Fortify** > **Integrações**.
2. Escolha uma integração, por exemplo, a Fortify Integração da lista de aplicações.
3. Selecione **Executar agora**.

Nota:
Para obter a recuperação de dados completa, execute as integrações de vulnerabilidade da aplicação Fortify em sequência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importar dados usando o Integrações de vulnerabilidade do Fortify

Importe dados do scanner Fortify para mapear itens vulneráveis de aplicação (IVAs), enriquecendo assim os dados em sua instância.

Antes de Iniciar

Função necessária: gerente de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Após a importação inicial, Fortify integrações de vulnerabilidade fazem uma importação delta sempre que são executadas, recuperando os dados mais recentes. Consulte Executar uma importação manual de vulnerabilidade da aplicação Fortify para obter mais informações sobre importações completas.

Procedimento

1. Navegar até **Todos** > **Integrações de vulnerabilidade do Fortify** > **Integrações**.
2. Escolha uma integração.
3. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome da execução da integração.
Ativo	Opção para ativar uma integração.
Executar	Frequência da execução da integração.
Hora	
Aplicação	Aplicação que contém este registro.
Integração de origem	Integração de origem para esta integração.
Instância de origem	Instância de origem para esta integração.
Próxima integração	Próxima integração de sequência, a ser executada após a execução da integração atual.
Hora de início	Data e hora de início da última execução de integração bem-sucedida. O tempo é calculado como Horas no horário local. A hora padrão da execução inicial é 00:00:00.
Detalhes de Integração	
Script de integração	Inclusão de script que estende o `VulnerabilityIntegrationBase` a ser executado quando a integração é executada. Este script define como recuperar dados de um sistema de terceiros.
Script de fábrica de integração	Script que define como construir o script include selecionado para o script de integração.
Estratégia do processador de relatórios	Estratégia que você deseja usar para lidar com os dados retornados pelo script de integração quando a integração é executada.

4. Selecione **Executar agora** para executar a integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Incluir itens vulneráveis da aplicação Fortify on Demand encerrados

Por padrão, os itens vulneráveis da aplicação (IVAs) **encerrados** não são criados durante as importações de integração de item vulnerável Fortify. Se você quiser criá-los, deverá alterar uma propriedade do sistema.

Antes de Iniciar

O Integrações de vulnerabilidade do Fortify deve estar instalado e em execução.

Função necessária: gerente de App-Sec

Procedimento

1. Na caixa de texto **Navegador de filtro** esquerdo, digite `sys_properties.list`.
2. Na caixa de pesquisa **Nome** da lista, insira `sn_vul.create_closed`.
3. Clique duas vezes no campo **Valor** e defina como **Verdadeiro**
4. Clique no ícone de marca ícone de marca de seleção verde para salvar.
   Registros no estado **Encerrado** na próxima importação Fortify são criados como AVIs em Application Vulnerability Response.

Integrações de vulnerabilidade de aplicação do GitHub

O Integrações de vulnerabilidade de aplicação do GitHub importa dados de teste de segurança da aplicação estático (SAST) e análise de composição de software (SCA) para ajudá-lo a exibir alertas de vulnerabilidade nos repositórios em seu ambiente GitHub.

GitHub Vulnerability Integration

O Integrações de vulnerabilidade de aplicação do GitHub coleta dados do scanner e disponibiliza esses dados para o Now Platform®. Ele se integra facilmente ao recurso [ServiceNow® Application Vulnerability Response de Vulnerability Response para mapear vulnerabilidades de terceiros e alertas do GitHub em sua instância.

O ambiente GitHub oferece suporte a várias organizações. Essas organizações, tanto no local quanto no Enterprise, podem conter vários departamentos, como Engenharia, Qualidade, Documentação e assim por diante. Cada organização, por sua vez, pode oferecer suporte a vários repositórios. Esta integração importa dados de alerta de vulnerabilidade desses repositórios. Os dados importados são processados como uma aplicação na aplicação Application Vulnerability Response. Quando os scanners detectam vulnerabilidades e geram alertas para os repositórios, as vulnerabilidades são criadas no Application Vulnerability Response.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

O escopo necessário para extrair dados é **repo**.

Versões disponíveis

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do GitHub

Integração	Descrição
GitHub CodeScan Integration	Recupera alertas de vulnerabilidade de verificação de código dos repositórios do GitHub para vulnerabilidades de segurança e erros de codificação. Os dados importados são mapeados para resultados SAST em sua instância.
GitHub Dependentebot Integration	Recupera alertas de Dependentebot para dependências com vulnerabilidades conhecidas de repositórios. Os dados importados são mapeados para resultados de SCA em sua instância.

Exibição de dados importados

Os dados importados (descobertas) do GitHub Dependendabot Integration são exibidos nas tabelas a seguir.

- Aplicações descobertas [sn_vul_app_release].
- Resumos de verificação de vulnerabilidade da aplicação [sn_vul_app_vul_scan_summary].
- Itens vulneráveis da aplicação [sn_vul_app_vulnerable_item].
- Pacotes [sn_vul_app_package].

Os dados importados da integração do GitHub CodeScan são exibidos nas tabelas a seguir.

- Aplicações descobertas [sn_vul_app_release].
- Resumos de verificação de vulnerabilidade da aplicação [sn_vul_app_vul_scan_summary].
- Entradas de vulnerabilidade da aplicação [sn_vul_app_vul_entry].
- Itens vulneráveis da aplicação [sn_vul_app_vulnerable_item].

Preparando para o Integrações de vulnerabilidade de aplicação do GitHub

Prepare-se para a integração executando estas tarefas. O Integrações de vulnerabilidade de aplicação do GitHub pressupõe que você esteja familiarizado com o produto e a API do GitHub.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Funções necessárias:

- administrador para baixar, instalar e ativar aplicações e atribuir funções.
- Administrador do GitHub para obter credenciais e gerar tokens no console do GitHub.
- admin para configurar conexões e registros de alias em sua instância.

Tarefas de configuração

Tarefas de configuração	Descrição
Verifique se a aplicação Vulnerability Response está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração

Tarefas de configuração	Descrição
	exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Vulnerability Response.
Verifique se o Integrações de vulnerabilidade de aplicação do GitHub está instalado e ativado.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instale o ServiceNow Integrações de vulnerabilidade de aplicação do GitHub.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para a configuração e a verificação dos resultados esperados: • Se ainda não estiver atribuído, o administrador do sistema [admin] instalará o app e atribuirá usuários ao grupo de usuários do App-Sec Manager. • O gerente de App-Sec supervisiona a configuração e verifica os resultados esperados. • sn_vul_github_config_integration é herdado pelo grupo de usuários do App-Sec Manager. Esta função contém as funções connection_admin e oauth_admin.
Obtenha sua credencial do GitHub e informações da conta.	As informações da conta são necessárias nos registros criados para autenticação. Consulte Crie os registros necessários para autenticação OAuth para o Integrações de vulnerabilidade de aplicação do GitHub para obter mais informações sobre como configurar os registros necessários para autenticação OAuth.
Verifique se você está importando dados de CWE (Common Weakness Enumeration).	A integração de CWE (Common Weakness Enumeration) também é usada por Application Vulnerability Response e deve estar em execução antes de instalar e configurar a integração de vulnerabilidade do GitHub. Ele é instalado com Vulnerability Response, por padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração

Tarefas de configuração	Descrição
	Nota: Os dados do banco de dados de vulnerabilidades do NIST (NVD) não são necessários para instalar a integração de vulnerabilidades do GitHub. No entanto, eles fornecem aprimoramento e são úteis. Para obter informações sobre NVD, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

Crie os registros necessários para autenticação OAuth para o Integrações de vulnerabilidade de aplicação do GitHub

Se você não tiver credenciais de OAuth, configure suas Credenciais e Informações de conexão para autenticação OAuth se quiser usar este método para conexão e autenticação.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **OAuth de Sistema** > **Registro de aplicações**.
2. Na lista Registros da aplicação, selecione **Novo**.
3. Na página da aplicação OAuth, selecione **Conectar ao provedor OAuth de terceiros**.
4. No registro Registros da aplicação, preencha o formulário.
5. Selecione **Enviar**.
   Seu novo registro de Registros de aplicações (Provedor OAuth) é exibido na lista de Registros de aplicações.
6. Selecione seu novo registro para abri-lo.

   Na guia da lista relacionada **Perfis de entidade OAuth** no seu novo registro, um registro de perfil de entidade OAuth foi criado quando você enviou o registro.
7. Selecione este registro de perfil para abri-lo e criar um escopo para extrair repositórios.
8. Na seção Escopos de perfil de entidade OAuth, clique duas vezes em **Inserir uma nova linha**.
9. No campo, selecione o ícone de pesquisa.
10. No modal exibido, selecione **Novo** e preencha os campos.
11. Selecione **Enviar**, selecione a marca de seleção verde e selecione **Atualizar**.
    Seu registro de Registros de aplicações é exibido. Este registro está concluído.
12. Navegar até **Credenciais e conexões** > **Credenciais**.
13. Selecione **Novo**.
14. Selecione **Credenciais do OAuth 2.0** e preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

15. Selecione **Enviar**.
    A lista Credenciais é exibida.
16. Abra o registro que você criou e selecione o link relacionado **Obter token OAuth**.
    A página de login do GitHub é exibida. Você obtém as permissões e gera o token no console do GitHub.
17. Navegar até **Credenciais e conexões** > **Aliases de conexão e credencial**.
18. Selecione **Novo** e preencha os campos.
19. Selecione **Enviar**.
    A lista de Aliases de conexões e credenciais é exibida.
20. Abra seu registro e, na guia da lista relacionada Conexões, selecione **Novo** e preencha os campos no registro da conexão HTTP.
21. Selecione **Enviar**.
    A lista de Aliases de conexões e credenciais é exibida. Agora você está pronto para concluir as etapas para Configurar o Integrações de vulnerabilidade de aplicação do GitHub. No campo Conexão, você insere as credenciais criadas nas etapas anteriores.

Instale o ServiceNow® Integrações de vulnerabilidade de aplicação do GitHub

Antes de executar a integração na sua instância, as etapas de instalação e configuração devem ser concluídas para que o Integrações de vulnerabilidade de aplicação do GitHub se integre corretamente com Application Vulnerability Response. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Faça login na instância na qual você deseja instalar o Integrações de vulnerabilidade de aplicação do GitHub.
2. Navegue até o ServiceNow Store.
3. Na aplicação ServiceNow Store, pesquise a aplicação Integrações de vulnerabilidade de aplicação do GitHub.
4. Selecione o bloco da aplicação.
   Informações detalhadas sobre a aplicação que você está instalando são exibidas.

   Nota:
   Considere a leitura das seções **Outros requisitos** e **Dependências**, conforme aplicável.

5. Selecione **Solicitar app** e insira suas Now Support credenciais de login.
6. Selecione **Obter**.
7. Insira o **Nome da instância** e **o Motivo da instância**e selecione **Validar instância**.
8. Selecione **Solicitação**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Candidaturas**.
10. Localize a aplicação, selecione-a e selecione **Instalar**.
    Sua aplicação é instalada automaticamente na sua instância.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar o Integrações de vulnerabilidade de aplicação do GitHub

Antes de executar a integração na sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto GitHub se integre corretamente a Application Vulnerability Response. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

O escopo necessário para extrair dados é **repo**. Você define este parâmetro em Crie os registros necessários para autenticação OAuth para o Integrações de vulnerabilidade de aplicação do GitHub.

Funções necessárias:

- Grupo de usuários do App-Sec Manager
- administrador necessário para a configuração do OAuth

Procedimento

1. Navegar até **Todos** > **Integração de vulnerabilidade do GitHub** > **Configuração**.
2. Preencha os campos.
3. Selecione **Salvar e testar credenciais**.

Exibir o status de execução de importação Integrações de vulnerabilidade de aplicação do GitHub

Use a lista relacionada Execuções de integração de **vulnerabilidade** para verificar o sucesso de suas execuções de integração, localizar problemas e informar suas decisões de correção.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **GitHub Vulnerability Integration** > **Integrações**.
2. Selecione uma integração.
3. Selecione a lista relacionada **Execuções de integração de vulnerabilidade**.
4. Verifique se todas as importações foram bem-sucedidas.

   Trouble?

   As causas mais comuns para uma execução com falha incluem:

   - Interrupção de rede.
   - Um problema na transferência de dados que resulta em dados corrompidos durante a transformação.

   Se você encontrar qualquer uma dessas condições, selecione **Executar agora**e execute novamente a integração.

Exibir Integrações de vulnerabilidade de aplicação do GitHub conjuntos de importação

Exiba detalhes das informações de importação para Integrações de vulnerabilidade de aplicação do GitHub.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até o **GitHub Vulnerability Integration** > **Tabelas do conjunto de importação**.
2. Selecione um registro para uma integração.
3. Selecione um link Relacionado para exibir as seguintes informações:
   - Conjuntos de importação
   - Mapas de transformação
   - Histórico de Transformações

Integrações de vulnerabilidade do Invicti

O Integrações de vulnerabilidade do Invicti usa dados de aplicação importados do produto Invincti para ajudá-lo a determinar o impacto e a prioridade das falhas em seu código.

Integrações de vulnerabilidade do Invicti

O Integrações de vulnerabilidade do Invicti coleta dados do scanner e disponibiliza esses dados para o Now Platform®. Ele se integra facilmente ao recurso [ServiceNow® Application Vulnerability Response de Vulnerability Response para mapear informações de vulnerabilidade de aplicação de terceiros importadas para sua instância.

A integração importa os seguintes tipos de dados digitalizados.

- Teste de segurança da aplicação dinâmico (DAST)
- Teste de segurança da aplicação interativo (IAST)

Para obter mais informações sobre DAST e IAST, consulte Explorar o Application Vulnerability Response.

Versões disponíveis

Versão de lançamento	Notas de versão
Vulnerability Response integration with Invincti Versão inicial	Application Vulnerability Response release notes Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Integrações

As integrações a seguir estão incluídas no sistema de base. As integrações são encadeadas para que, após a conclusão bem-sucedida de uma integração, a próxima integração seja iniciada. As integrações são executadas na ordem listada na tabela a seguir.

Após a execução inicial, todos os dias, os trabalhos programados são encadeados para executar essas integrações automaticamente na ordem. Você também pode executar trabalhos programados individuais manualmente. Os trabalhos programados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações de vulnerabilidade da aplicação Invincti

Integração	Descrição
Aplicação de lista da aplicação Invincti	Importa aplicações verificadas pelo Invicti para a tabela Aplicações descobertas [sn_vul_app_release] ou a tabela Aplicação verificada [sn_vul_app_scanned_application] com base em como a propriedade do sistema `sn_vul.use_product_model` está definida para os registros de regra de pesquisa de IC. • Se a propriedade do modelo do produto estiver definida como verdadeira, uma aplicação será inserida na tabela de versão da aplicação descoberta. • Se a propriedade do modelo do produto estiver definida como falsa, uma aplicação será inserida na tabela Aplicação verificada. Você pode optar por ativar as regras de pesquisa com itens de configuração (ICs) como os destinos de pesquisa, modificando a propriedade do sistema. Se você modificá-lo, também deverá ativar as regras de Pesquisa de IC para corresponder ao destino da pesquisa. Para obter mais informações, consulte: • Configurar o Integrações de vulnerabilidade do Invicti • Criar uma regra de pesquisa de IC • Reaplicar regras de Pesquisa de IC no Application Vulnerability Response
Integração da lista de verificação do Invincti	Esta integração é iniciada depois que a integração da lista de aplicações é concluída com sucesso. Esta integração importa dados sobre a data e a hora em que uma verificação foi executada.
Integração de item vulnerável da aplicação Invincti	Esta integração é iniciada após a conclusão bem-sucedida da integração da lista de verificação. Cada vulnerabilidade no Invincti tem um tipo, por exemplo,**DirectoryListing**. Este tipo é mapeado como um ID exclusivo em sua instância e exibido como parte do valor no campo Vulnerabilidade no registro do item vulnerável (IVA) da aplicação: **Invincti-DirectoryListing**. Para obter mais informações sobre mapeamento, consulte Integrações de vulnerabilidade do Invicti mapeamento de estado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O limite superior para itens por página para todas as três integrações é 200.

Preparar para o Integrações de vulnerabilidade do Invicti

Uma integração bem-sucedida requer planejamento e execução de tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. O Integrações de vulnerabilidade do Invicti pressupõe que você esteja familiarizado com o produto Invincti e a API.

A integração de CWE (Common Weakness Enumeration) também é usada por Application Vulnerability Response e deve ser executada antes de instalar e configurar a integração de vulnerabilidade Invincti.

Nota:
Os dados do NIST Vulnerability Database (NVD) não são necessários para instalar a integração, no entanto, eles fornecem aprimoramento de vulnerabilidade e são úteis.

Para obter informações sobre NVD, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Nota:
Antes de executar a integração, faça as mudanças de configuração necessárias com base em seus requisitos.

Valide o dimensionamento da instância com base no número de itens vulneráveis da aplicação que você espera importar. Uma instância subdimensionada pode levar a longos tempos de carregamento. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente. A função de administrador é necessária para instalar e configurar aplicações em sua instância da Now Platform.

Obtenha suas credenciais de API e token de API no console Invincti. Revise as informações disponíveis no site do produto Invicti em Visão geral da API .

Instalar o ServiceNow® Vulnerability Response Integration with Invincti

Antes de executar a integração na sua instância, as etapas de instalação e configuração devem ser concluídas para que a aplicação Integrações de vulnerabilidade do Invicti se integre corretamente com Application Vulnerability Response. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Faça login na instância na qual você deseja instalar o Integrações de vulnerabilidade do Invicti.
2. Navegue até o ServiceNow Store.
3. No ServiceNow Store, pesquise a aplicação Integrações de vulnerabilidade do Invicti.
4. Selecione o bloco da aplicação.
   Informações detalhadas sobre a aplicação que você está instalando são exibidas.

Nota:
Considere ler as seções **Outros requisitos** e **Dependências**, conforme aplicável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione **Solicitar app** e insira suas Now Support credenciais de login.
6. Selecione **Obter**.
7. Insira o **Nome da instância** e **o Motivo da instância**e selecione **Validar instância**.
8. Selecione **Solicitação**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
10. Localize a aplicação, selecione-a e selecione **Instalar** para ativá-la.
    Sua aplicação é instalada automaticamente na sua instância.

Configurar o Integrações de vulnerabilidade do Invicti

Antes de executar a integração na sua instância, as etapas de instalação e configuração devem ser concluídas para que o Integrações de vulnerabilidade do Invicti funcione corretamente com o recurso [Application Vulnerability Response de Vulnerability Response.

Antes de Iniciar

Funções necessárias:

- administrador para instalar e ativar aplicações
- Grupo de usuários do App-Sec Manager para configurar a integração

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Verifique se a aplicação Vulnerability Response está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Vulnerability Response.
Verifique se o Integrações de vulnerabilidade do Invicti está instalado e ativado.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Instalar o ServiceNow Vulnerability Response Integration with Invincti.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	• Se ainda não estiver atribuído, o administrador do sistema [admin] instalará o app e atribuirá usuários ao grupo de gerentes de App-Sec. • O gerente de App-Sec supervisiona a configuração e verifica os resultados esperados.
Para a integração de vulnerabilidade Inviciti, tenha seu **ID de usuário** e **token de API** prontos.	Entre em contato com o administrador do Invincti para obter o **ID do usuário** e o **token da API** se você não os souber. Para obter mais informações, consulte o site do produto Invincti em Visão geral da API .

Procedimento

1. Navegar até **Todos** > **Invicti** > **Configuração do Invicti**.
2. Preencha os campos.

Campo	Descrição
URL da API	URL da instância do Invincti do usuário. Estas são as informações que você obteve de Preparar para o Integrações de vulnerabilidade do Invicti.
ID do usuário	ID de usuário exclusivo.
Token de API	Token de API gerado a partir do console Invincti. Estas são as informações que você obteve de Preparar para o Integrações de vulnerabilidade do Invicti.
Escolha o tipo de verificação. Você deve selecionar pelo menos um.	
Importar DAST	Opção para incluir vulnerabilidades de verificações DAST. As verificações DAST encontram vulnerabilidades para uma aplicação dinamicamente enquanto ela está em execução. Esta abordagem pode imitar um ataque externo.
Importar IAST	Opção para incluir vulnerabilidades das verificações do IAST. As verificações IAST detectam vulnerabilidades de software interagindo com o programa enquanto ele está em execução. Observação humana, testes automatizados e sensores são usados em combinação para interagir com a aplicação para localizar vulnerabilidades.
Formato de data	Parâmetro que converte a hora de início para o formato compatível com a API Invicti usada pela Integração de item vulnerável da aplicação Invicti. Este parâmetro deve corresponder ao formato que você definiu ou selecionou em sua conta Invicti, por exemplo, **dd/MM/**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	aaaa. Verifique se os formatos de data e hora no console Invicti correspondem aos inseridos para o formato de data na sua instância Now Platform. Para mudar este formato no seu console Invicti: **a.** Faça login em Invincti Sign In . **b.** Selecione **Nome de usuário** no canto superior direito. **c.** Navegar até **Configurações do usuário** > **Formato de data e hora**. **Nota:** Falha nas importações pode ocorrer se você inserir um formato de data inválido na sua instância Now Platform. Se você inserir um formato válido em sua instância que seja diferente do formato de data no console Invicti, o Invicti retornará uma carga vazia.
Gerenciar exceções no ServiceNow	Selecione um: **Ativado (selecionado)** Os itens vulneráveis da aplicação (AVIT) do Invicti com estados como **Presente** e **Risco Aceito** que podem ser adiados em sua instância são mapeados para **Aberto** automaticamente. **Desativado (não selecionado)** Os estados de origem dos itens vulneráveis da aplicação (AVITs) importados do Invincti são preservados. Você deve gerenciar exceções para esses AVITs (adiá-los) de registros de AVIT. Para obter mais informações sobre estados de origem e campos de destino do Invincti, consulte Integrações de vulnerabilidade do Invicti mapeamento de estado.
Gerenciar falsos positivos no ServiceNow	Selecione um: **Ativado (selecionado)** AVITs com estados do Invincti, como **Presente** e **Falso-positivo**, que podem fazer a transição para **Encerrado** em sua instância

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	são mapeados para **Aberto** automaticamente. **Desativado (não selecionado)** Os estados de AVIT importados do Invincti são preservados. Você deve gerenciar falsos positivos ou possíveis falsos positivos para esses AVITs de registros de AVIT.

3. Selecione **Salvar e testar credenciais**.
4. **Opcional:** Modifique suas regras de pesquisa para que elas sejam baseadas em itens de configuração.

   (Optional) Por padrão, a propriedade do sistema **sn_vul.use_product_model** é ativada (definida como verdadeiro) para suas regras de pesquisa listadas na tabela [sn_sec_cmn_ci_lookup_rule] com base no modelo do produto. Quando esta regra é ativada:

   - Esta regra identifica correspondências entre os dados importados e os dados em Configuration Management Database (CMDB) com base no modelo do produto.
   - Os registros são criados ou atualizados na tabela Aplicações descobertas [sn_vul_app_release].
   - Quando você cria ou edita suas regras de pesquisa para o Invicti, o **modelo do produto** é exibido no campo de **destino da pesquisa** no formulário da regra.

   Para modificar suas regras para que sejam baseadas em itens de configuração, você deve desativar manualmente (definir como falso) a propriedade do sistema **sn_vul.use_product_model**.

   a. Navegar até **Todos** > **Propriedades do sistema** e localize o registro **sn_vul.use_product_model** e defina o valor como falso.

   b. Selecione **Atualizar**.

   c. Navegar até **Todos** > **Security Operations** > **CMDB** > **Regras de pesquisa**.

   d. Localize as regras de nome da aplicação e ID da aplicação de origem que têm o destino de pesquisa como **item de configuração**.

   e. Marque a caixa de seleção Ativa para essas regras.

   f. Selecione **Atualizar**.
   Ao criar ou editar suas regras de pesquisa para o Invicti, observe que o **Item de configuração** é exibido no campo de **destino da pesquisa** no formulário da regra. Os registros são criados ou atualizados na tabela Aplicações verificadas [sn_vul_app_scanned_application].

Exibição do status e dos registros da execução de importação Integrações de vulnerabilidade do Invicti

Use a lista relacionada Execuções de integração de **vulnerabilidade** para verificar o sucesso de suas execuções de integração, localizar problemas e informar suas decisões de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de status de importação, conjuntos de importação e registros

Para exibir o status de suas importações, como um usuário no grupo de usuários do App-Sec Manager, navegue até **Todos** > **Integração da vulnerabilidade do Invicti** > **Integrações** e selecione um registro de integração. Selecione a lista relacionada **Execuções de integração de vulnerabilidade**.

Para exibir os conjuntos de importação, navegue até **Todos** > **Integração da vulnerabilidade do Invicti** > **Integrações** > **Tabelas do conjunto de importação** e selecione uma integração.

A integração da lista de aplicações cria ou atualiza registros com base no destino de pesquisa:

- Modelo do produto: tabela Aplicações descobertas [sn_vul_app_release]
- Item de configuração: tabela Aplicações verificadas [sn_vul_app_scanned_application]

A integração da lista de verificação cria ou atualiza registros na tabela Aplicações verificadas [sn_vul_app_scan_summary].

A integração de item vulnerável da aplicação cria ou atualiza registros na tabela Itens vulneráveis da aplicação [sn_vul_app_vulnerable_item] e CWEs [sn_vul_cwe].

Nota:
Cada vulnerabilidade no Invincti tem um "tipo", por exemplo, ProductDirectoryListing. Este tipo é importado mapeado como um ID exclusivo para sua instância e exibido como parte do valor no campo Vulnerabilidade no registro do item vulnerável da aplicação (AVIT). Neste exemplo, o valor é Invincti-ProductDirectoryListinge esse valor também é exibido como o ID exclusivo no registro de entrada de vulnerabilidade da aplicação. Os AVITs do Invicti oferecem suporte a várias entradas de Enumeração de Ponto Fraco Comum (CWE), portanto, os CWEs não são usados como IDs exclusivos. Os CWEs também são exibidos no registro AVIT.

Para AVITs Invicti, se houver tipos duplicados no Invicti para uma vulnerabilidade, a palavra "custom" será inserida no valor, por exemplo, Invincti-custom-ProductDirectoryListing. Se você criar um tipo personalizado para vulnerabilidades, o ID da vulnerabilidade poderá ser Invincti-Custom-<title of vulnerability>.

Novos campos: para scan type=Invicti, os campos Afetado e Personalizado podem incluir dados que podem ajudar você a entender a vulnerabilidade e ajudá-lo a corrigi-la. Se não houver dados, esses campos não serão exibidos no AVIT.

Integrações de vulnerabilidade do Invicti mapeamento de estado

Os seguintes estados de origem de Integrações de vulnerabilidade do Invicti e seus estados de destino em sua instância estão listados na tabela a seguir.

Estados de origem do Invincti e seus estados correspondentes da Now Platform

Estados de origem do Invincti	Descrição dos estados de origem	Estado de destino na Now Platform
Present	O problema é identificado.	Em aberto
Presente, Risco Aceito, Revivido	O problema foi considerado e está marcado como uma vulnerabilidade de baixo risco.	Adiado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados de origem do Invincti e seus estados correspondentes da Now Platform

Estados de origem do Invincti	Descrição dos estados de origem	Estado de destino na Now Platform
Presente, falso-positivo	O problema foi considerado e está marcado como uma vulnerabilidade não original.	Encerrado
Corrigido não confirmado, corrigido não confirmado	O problema foi corrigido, mas não confirmado pela Invincti Enterprise.	Resolvido
Corrigido (Confirmado), CorrigidoConfirmado, CorrigidoConfirmado, AcceptedRisk, CorrigidoConfirmado, Falso-positivo	O problema foi corrigido e confirmado pela Invicti Enterprise e nenhuma ação adicional é necessária.	Encerrado
Corrigido (não é possível testar novamente)	O problema foi identificado, mas o Invicti não pode testar novamente para confirmar se o problema foi corrigido ou não.	Resolvido
Revivido	O problema foi corrigido em verificações anteriores, mas foi encontrado novamente.	Em aberto
Adiado, Ignorado	O problema foi ignorado pelo usuário. No Invincti Enterprise, para ignorar um problema, um usuário atualiza seu status para "risco aceito".	Risco aceito

Mapeamento de versão da aplicação

Campo de origem	Campo de destino na Now Platform
ID	source_app_id
Criado em	app_creation_date
Atualizado em	app_updation_date
Nome	app_name
URL da Raiz	Source_additional_info
Descrição	descrição
Marcadores	Marcadores

Mapeamento de vulnerabilidade

Campo de origem	Campo de destino na Now Platform
Tipo	Nome da categoria
Detalhe da vulnerabilidade	Resumo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Impact	Ameaça
Referências de origem	Referências da Web
Recomendação de origem	Solução
Tipo	source_entry_id/ID
Gravidade	source_severity
Classificação [“Cwe”]	Lista do CWE
Cadeia de caracteres CVSS	Campos do CVVS v3

Mapeamento de resumo de verificação

Campo de origem	Campo de destino
Origem	Origem
TotalVulnerabilityCount	Contagem_de_falha_detectada
Data de início	Data de verificação dinâmica
id	source_scan_id

Mapeamento de item vulnerável da aplicação (AVIT)

Campo de origem	Campo de destino na Now Platform
Tipo	Tipo de verificação
ID do site	ID de aplicação de origem
ID	ID de AVIT de origem
Data da última exibição	Último encontrado
Data da primeira exibição	Primeiro encontrado
Data da última atualização	Data da última verificação
parâmetros	Parâmetro afetado
URL	URL afetado
Gravidade	Gravidade de origem
Url	Link de origem
Detalhe da vulnerabilidade	Resumo da vulnerabilidade de origem
Referências externas	Referências de origem
Referências de correção + correção	Recomendação de origem
Estado	Status da correção da origem
Impact	Explicação da vulnerabilidade de origem

Veracode Vulnerability Integration

A aplicação Vulnerability Response Integration with Veracode usa dados importados do produto Veracode para ajudar a determinar o impacto e a prioridade das falhas no seu código.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Veracode Vulnerability Integration

O produto Veracode coleta dados de teste de segurança de aplicações dinâmico (DAST), teste de segurança de aplicações estático (SAST) e scanner manual e disponibiliza esses dados para o Now Platform®. Ele se integra facilmente ao recurso [Application Vulnerability Response de Vulnerability Response para mapear vulnerabilidades de terceiros que enriquecem os dados em sua instância.

A partir da v19.0 de Vulnerability Response, você pode importar vulnerabilidades da Análise de composição de software (SCA) e dados de vulnerabilidade Lista de materiais de software (SBOM) para ajudá-lo a identificar pontos fracos em seus aplicativos de software. Para obter mais informações, consulte Explorar o Lista de materiais de software.

Uma API compartilhada ingere dados de DAST, SAST, SCA e resultados de testes de invasão manuais.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Todos os dias, os trabalhos programados invocam as integrações automaticamente na ordem em que estão listadas. Você também pode executar trabalhos programados individuais manualmente. Os trabalhos programados simplificam o ciclo de vida de correção de vulnerabilidades, mantendo a instância sincronizada com outros sistemas de gestão de vulnerabilidades.

Versões disponíveis

Versão de lançamento	Notas de versão
Veracode 4,1 Veracode 4,0	Application Vulnerability Response release notes Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Grupo de usuários e funções

O Veracode Vulnerability Integration é instalado por um administrador do sistema [admin] e configurado por um membro do grupo App-Sec Manager. Para obter mais informações, consulte Application Vulnerability Response grupos de usuários e funções.

Veracode Vulnerability Integration

Para exibir as Veracode integrações de vulnerabilidade, navegue até **Todos** > **Integração de vulnerabilidade da Veracode** > **Integrações**.

As integrações a seguir estão incluídas no sistema de base.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Veracode Vulnerability Integration

Integração	Descrição
A partir da v4.1: Veracode Vincular projetos de integração	Esta integração é ativada por padrão. Recupera todos os projetos associados a cada aplicação de Veracode. As aplicações podem ter vários projetos na aplicação Veracode. Os dados importados desta integração são exibidos nos seguintes registros: • A Data da**última verificação de SCA, a Data**de **criaçãodo app e a Data de atualização do app** são listadas nos registros em **Aplicações descobertas**. • Nos registros de resumo de verificação de vulnerabilidade da aplicação e nos itens vulneráveis da aplicação (AVIs), o **status do SDLC de origem** (ciclo de vida de desenvolvimento de software) é exibido. • **A exploração de origem** é exibida nos registros de item vulnerável da aplicação (IVA).
A partir da v4.0: Veracode Integração da lista de aplicações (JSON)	Esta integração está inativa por padrão. Recupera Veracode dados do scanner da aplicação (vulnerabilidades, metadados) e enriquece os dados da aplicação. Recupera registros de verificação de Veracode por meio de uma API baseada em JSON.
A partir da v4.0: Veracode Application List Integration (XML)	Esta integração está inativa por padrão. A versão baseada em XML desta integração foi desativada (descontinuada). Recupera Veracode dados do scanner da aplicação (vulnerabilidades, metadados) e enriquece os dados da aplicação. Esta integração está definida para ser executada diariamente às 00:00:00. **Nota:** Uma API baseada em JSON de Veracode é usada para recuperar a lista de aplicações. Esta API importa a "última data de verificação de conformidade da política" dessas aplicações, o que significa quando essas aplicações foram verificadas pela última vez por Veracode.
A partir da v4.0: Veracode Lista de materiais de software (SBOM) Integração	Esta integração é ativada por padrão. Importa arquivos Lista de materiais de software no formato CycloneDX gerados por Veracode e os enfileira para análise em sua instância. Você deve ter as aplicações Lista de materiais de software instaladas para importar esses dados e exibi-los.
A partir da v4.0: Veracode Integração de resumo de verificação (JSON)	Esta integração está inativa por padrão. Recupera registros de verificação de Veracode por meio de uma API baseada em JSON. Esta integração substitui a integração de API baseada em XML. Ele é encadeado e segue a integração da lista de aplicações Veracode quando ativado.
A partir da v4.0: Veracode	Esta integração está inativa por padrão. A versão baseada em XML desta integração foi desativada (descontinuada). Recupera registros de verificação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Veracode Vulnerability Integration

Integração	Descrição
Resumo da verificação (XML)	de Veracode. Esta integração é encadeada e segue a integração da lista de aplicações Veracode quando ativada. **Nota:** Segue automaticamente a integração da lista de aplicações Veracode quando ela é ativada. Com a "Última data de verificação de conformidade da política" das aplicações de Veracode, esta integração recupera dados somente das aplicações que foram verificadas após o "delta_start_time" desta integração.
A partir da v4.0: Veracode Integração de JSON de item vulnerável da aplicação	Esta integração está inativa por padrão. Recupera resultados de verificação com mais dados de vulnerabilidade do que a integração baseada em XML de Veracode. Ele insere AVIs e aprimora seus dados de vulnerabilidade de terceiros.
A partir da v4.0: Veracode Integração de item vulnerável da aplicação (XML)	Esta integração está inativa por padrão. Recupera resultados de verificação de Veracode, insere AVIs e aprimora seus dados de vulnerabilidade de terceiros. Por padrão, se o registro do scanner estiver no estado **Encerrado**, os AVIs não serão criados. Os AVIs existentes ainda serão atualizados. Esta integração é encadeada e segue a integração do Resumo de verificação Veracode quando ativada. A API baseada em XML está obsoleta para a integração JSON de resumo de verificação Veracode. **Nota:** Segue automaticamente a Veracode Integração do resumo de verificação. Com a "Última data de verificação de conformidade da política" das aplicações de Veracode, esta integração recupera dados somente das aplicações que foram verificadas após o "delta_start_time" desta integração.
A partir da v4.0: Veracode Integração de categorias	Esta integração está inativa por padrão. Recupera dados de categorias aprimoradas de Veracode.
A partir da v4.0: Veracode Integração do CWE	Esta integração é ativada por padrão. Recupera Veracode - dados específicos de Enumeração de Ponto Fraco (CWE) para informações de ameaça e recomendações de correção. Esses dados são preenchidos e atualizados nos registros de entrada de vulnerabilidade da aplicação. Esta integração do CWE opera independentemente do trabalho programado para a Integração abrangente do CWE 2000 que você ativa para a aplicação Vulnerability Response. Seus dados não serão duplicados se você tiver a Integração do CWE Veracode e a Integração do CWE Abrangente 2000 ativada.
A partir da v4.0:	Esta integração está inativa por padrão. A integração pode ser visualizada na lista Integrações de vulnerabilidade da aplicação em Application Vulnerability Response. Se você tiver uma

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Veracode Vulnerability Integration

Integração	Descrição
Veracode Integração de DevOps	licença do DevOps Change Velocity, este recurso será estruturado para que os usuários do DevOps não precisem de uma licença do SecOps para exibir detalhes de resumo das verificações de vulnerabilidade de terceiros. Não há impacto ou mudança em Application Vulnerability Response.

Para obter os status de execução da integração, consulte Exibir o status de execução de importação da integração de vulnerabilidade da aplicação Veracode.

Para exibir dados em vulnerabilidades de terceiros, consulte Exibir bibliotecas de vulnerabilidades.

Preparando para o Veracode Vulnerability Integration

Um Veracode Vulnerability Integration bem-sucedido requer planejamento e execução de tarefas de pré-integração. Prepare-se para a integração executando estas tarefas. O Veracode Vulnerability Integration pressupõe que você esteja familiarizado com o produto Veracode e a API.

Antes de Iniciar

A integração de CWE (Common Weakness Enumeration) também é usada por Application Vulnerability Response e deve estar em execução antes de instalar e configurar o Veracode Vulnerability Integration. Ele é instalado com Vulnerability Response, por padrão.

Nota:
Os dados do banco de dados de vulnerabilidades do NIST (NVD) não são necessários para instalar a integração de vulnerabilidades da aplicação Veracode. No entanto, eles fornecem aprimoramento e seria útil ter. Para obter informações sobre NVD, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

Há um usuário executado configurado para cada registro de integração. O valor padrão para este usuário é **VR.System**. Não altere este valor.

Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Nota:
Antes de executar a integração, faça as mudanças de configuração necessárias com base em seus requisitos.

Valide o dimensionamento da instância com base no número de itens vulneráveis da aplicação que você espera importar. Uma instância subdimensionada pode levar a longos tempos de carregamento. Se você não souber o tamanho da sua instância, entre em contato com Suporte e atendimento ao cliente.

O Veracode Vulnerability Integration requer um ID de API e uma chave de API.

Procedimento

Para criar o ID da API e as credenciais de chave:

a. Faça login na plataforma Veracode.

b. Vá para o menu da conta do usuário e selecione **Credenciais de API**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Clique **em Gerar credenciais de API**.

d. Registre suas credenciais para uso posterior.

Instalar o Vulnerability Response Integration [ServiceNow® com Veracode

Antes de executar a integração na sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto Veracode se integre corretamente com Application Vulnerability Response. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Tarefas de configuração	Descrição
Verifique se a aplicação Vulnerability Response está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Vulnerability Response.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o administrador do sistema [admin] instalará a aplicação e atribuirá usuários ao grupo de gerentes de App-Sec. Para obter informações sobre as funções do grupo, consulte Application Vulnerability Response grupos de usuários e funções. • O grupo do App-Sec Manager supervisiona a configuração e verifica os resultados esperados.

Função necessária: administrador

Procedimento

1. Faça login na instância na qual você deseja instalar o Veracode Vulnerability Integration.

2. Navegue até o ServiceNow Store.

3. Na aplicação ServiceNow Store, pesquise a aplicação Vulnerability Response Integration with Veracode.

4. Clique no bloco da aplicação.
Informações detalhadas sobre a aplicação que você está instalando são exibidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Considere ler as seções **Outros requisitos** e **Dependências**, conforme aplicável.

5. Clique em **Solicitar app** e insira suas Now Support credenciais de login.
6. Clique **em Obter**.
7. Insira o **Nome da instância** e **o Motivo da instância**e clique em **Validar instância**.
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Candidaturas**.
10. Localize a aplicação, selecione-a e clique em **Instalar**.
    Sua aplicação é instalada automaticamente na sua instância.

O que Fazer Depois

Configure o Veracode Vulnerability Integration para o seu ambiente. Consulte Configurar o Veracode Vulnerability Integration.

Configurar o Veracode Vulnerability Integration

Antes de executar a integração na sua instância, as etapas de instalação e configuração devem ser concluídas para que o produto Veracode se integre corretamente com Application Vulnerability Response. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Tarefas de configuração	Descrição
Verifique se a aplicação Vulnerability Response está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Vulnerability Response.
Verifique se a aplicação Vulnerability Response Integration with Veracode está instalada e ativada.	Para verificar se esta aplicação está ativada, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	Se a aplicação não estiver instalada e ativada, consulte Instalar o Vulnerability Response Integration [ServiceNow com Veracode.
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para a configuração e a verificação dos resultados esperados: • Se ainda não estiver atribuído, o administrador do sistema [admin] instalará o app e atribuirá usuários ao grupo de usuários do App-Sec Manager. • O gerente de App-Sec supervisiona a configuração e verifica os resultados esperados.
Para a integração de vulnerabilidade da aplicação Veracode, tenha seu **ID** de **API e chave** de API prontos.	Entre em contato com Veracode para obter o**ID da API** e **a chave**da API. Consulte Preparando para o Veracode Vulnerability Integration. A partir da versão 4.0, se você estiver usando o Veracode Vulnerability Integration, os testes de avaliação de invasão no Veracode Vulnerability Integration serão descobertas manuais de Veracode. Essas descobertas não estão vinculadas a nenhuma solicitação de avaliação de teste de invasão configurada em Application Vulnerability Response. Para obter mais informações sobre solicitações de teste de invasão em Application Vulnerability Response, consulte Configurar teste de invasão.

Função necessária: grupo de usuários do App-Sec Manager

Procedimento

1. Navegar até **Todos** > **Integração de vulnerabilidade da Veracode** > **Configuração**.
2. Preencha os campos **ID da API** e **Chave** de API.
3. Escolha seus resultados de teste.

Opção	Descrição
Versão 4.0:	**a.** Selecione os tipos de dados **DAST** ou **SAST** a serem incluídos na importação. **Nota:** Você pode escolher um ou outro, ou ambos, mas deve selecionar pelo menos um.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	b. Selecione **SCA** para importar vulnerabilidades de Análise de composição de software (SCA). **c.** Selecione **Incluir manual** para importar resultados de testes de invasão manuais de Veracode. AVIs são criados para esses resultados.
Versão 3.0	Selecione os tipos de dados **DAST** ou **SAST** a serem incluídos na importação. **Nota:** Você pode escolher um ou outro, ou ambos, mas deve selecionar pelo menos um.
Versão 1.0:	Os resultados de testes de segurança da aplicação dinâmicos são selecionados, por padrão.

4. Adicione o nível de **severidade** Veracode para filtrar os dados importados.
Este valor é importado do Veracode. Você pode adicionar vários valores ao campo. Se preenchida, a importação coletará somente dados que correspondam aos níveis de Severidade que você adicionou.

5. Salve e valide suas escolhas.

Opção	Descrição
Versão 3.0:	Clique **em Salvar e testar credenciais**. **Nota:** A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida. Se uma mensagem de erro for exibida durante a configuração, insira novamente seus dados.
Versão 1.0:	Clique em **Salvar**. Verifique a configuração bem-sucedida clicando em **Testar credenciais**. **Nota:** A configuração é concluída com sucesso, a menos que uma mensagem de erro seja exibida. Se uma mensagem de erro for exibida durante a configuração, insira novamente seus dados.

6. Selecione como você deseja gerenciar exceções e falsos positivos para AVIs na importação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opções para gerenciar AVIs na importação com ServiceNow Gestão de exceções e fluxos de trabalho de Falso-positivo são ativadas por padrão. Os fluxos de trabalho são acionados com base em como os estados de **origem** nos AVIs são mapeados em sua instância. Para obter um exemplo de caso de uso, consulte Como gerenciar o mapeamento de estado para adiamentos e falsos positivos no Application Vulnerability Response.

7. Selecione **Salvar e testar credenciais**.

O que Fazer Depois

Se o seu ambiente requer importações separadas por domínio, consulte Criar importações separadas por domínio para uma integração.

Na instalação inicial, consulte Configurar Application Vulnerability Response. para obter mais instruções.

Após a instalação inicial, consulte as modificações em Veracode Vulnerability Integration modificações e atividades.

Exibir o status de execução de importação da integração de vulnerabilidade da aplicação Veracode

Use a lista relacionada Execuções de integração de **vulnerabilidade** para verificar o sucesso de suas execuções de integração, localizar problemas e informar suas decisões de correção.

Antes de Iniciar

Para exibir o status de execução de importação Veracode Vulnerability Integration :

- Application Vulnerability Response e Veracode Vulnerability Integration devem ser instalados e configurados.
- As importações Veracode Vulnerability Integration devem ser programadas e em execução.

Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Application Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. [store-future: BEGIN review]Se você não estiver usando o Veracode gráfico de status de execução de integração, [End] Navegar até **Todos** > **Integração de vulnerabilidade da Veracode** > **Integrações**.
2. Selecione uma integração.
3. Clique na lista relacionada **Execuções de integração de vulnerabilidade**.
4. Verifique se todas as importações foram bem-sucedidas.

Trouble?

As causas mais comuns para uma execução com falha incluem:

- Interrupção de rede.
- Um problema na transferência de dados que resulta em dados corrompidos durante a transformação.

Se você encontrar alguma dessas condições, clique em **Executar agora**e execute novamente a integração.

Exibir Veracode resumos de verificação

Exiba detalhes das informações de resumo da verificação da Veracode Integração de vulnerabilidade.

Antes de Iniciar
Função necessária: grupo de gerentes de App-Sec

Procedimento

1. Navegue até a tabela Resumos de verificação de vulnerabilidade da aplicação [sn_vul_app_vul_scan_summary_list].
2. Selecione um registro para uma verificação Veracode.
3. A partir da v19.0 de Vulnerability Response e v4.0 do Veracode Vulnerability Integration, use o ícone de lista de personalização (ícone de engrenagem) para exibir as seguintes colunas.
   - Tamanho da verificação estática
   - Contagem de biblioteca de terceiros
   - Contagem de biblioteca de vulnerabilidades de terceiros
   - Contagem de falhas de terceiros por gravidade
   - Contagem do problema de biblioteca de terceiros
   - Contagem do problema de licença de terceiros
   - Contagem de falhas mistas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Contagem de falhas mitigadas
- Contagem de falhas não mitigadas
- Contagem de falhas estáticas por gravidade
- Nova contagem de falhas por gravidade
- contagem de falhas não mitigadas por severidade
- Total de contagem de falhas por gravidade
- Classificação da última verificação de SCA
- Data da última verificação de SCA
- Data publicada da verificação
- Marcadores

Transformação de dados para a integração de vulnerabilidade Veracode

Depois de identificar os dados que deseja importar, os dados são recuperados da aplicação Veracode, processados por meio de um conjunto de fontes de dados e transformados em sua instância.

Veracode Integração de item vulnerável da aplicação

Os dados da API são carregados primeiro na tabela Veracode AppVul Item Import [sn_vul_veracode_appvul_item_import] e a Veracode AppVul Item Transform é usada para transformar as informações importadas.

Para acessar este mapa de transformação, navegue até *System Import Sets* > *Transform Maps* e pesquise por Veracode Transformação de item do AppVul. A tabela a seguir lista os campos do mapa de transformação por integração.

Veracode Campos do mapa de transformação de item do AppVul

Campo de origem	Campo de destino	Descrição
app_id	source_app_id	ID da aplicação.
ID do problema	source_avit_id	ID do AVIT.
app_name	app_name	Nome da aplicação.
versão	app_version	Versão da aplicação.
build_id	source_scan_id	ID de compilação da aplicação.
account_id	account_id	ID da conta.
sandbox_id	sandbox_id	ID da área restrita.
last_update_time	data_última_verificação	Hora da última atualização.
app_name + last_scan_date	scan_summary_name	Resumo da verificação.
life_cycle_stage	source_sdlc_status	Status do SDLC de origem.
nível	source_severity	Severidade de origem.
category_name	categoria	Categoria.
source_severity	source_severity	Severidade de origem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Veracode Campos do mapa de transformação de item do AppVul

Campo de origem	Campo de destino	Descrição
category_id + "CWE-" + cweId	source_entry_id	ID de entrada de origem.
source_vulnerability_summary	source_vulnerability_summary	Resumo da vulnerabilidade de origem.
source_recommendation	source_recommendation	Recomendação de origem.
descrição	descrição	Descrição da origem.
descrição	source_vulnerability_explanation	Explicação da vulnerabilidade de origem.
mitigação_status_desc	source_mitigação_status	Status de mitigação de origem.
remediation_status	source_remediation_status	Status de correção de origem.
linha	line_number	Linha em que a falha foi encontrada.
módulo	application_module	Módulo da aplicação.
arquivo de origem	source_notes	Anotações de origem.
afeta_policy_compliance	conformidade_com_política	Os valores podem ser Sim ou Não, com base nas informações de origem verdadeiras ou falsas.
Sourcefilepath + sourcefile	local	Mapeamento de local em caso de falha `static`.
url	local	Mapeamento de local em caso de falha `dynamic`.
escopo, tipo,exploitLevel	source_additional_info	Campo de valor de nome preenchido com os valores da origem em caso de falhas estáticas.

Os scripts de transformação a seguir são executados durante o processo de transformação.

Veracode tempo e finalidade do script de mapa de transformação

Quando o script é executado	Finalidade
onComplete (quando um conjunto de importação tiver concluído a transformação)	Script usado para processar a fonte de dados e atualizar a contagem de AVITs criados, atualizados ou inalterados e os importados como parte desta integração de Veracode. Este script é para uso interno e não deve ser modificado ou excluído.

Veracode Vulnerability Integration modificações e atividades

Configure modificações opcionais especificamente para o Veracode Vulnerability Integration.

Nota:
Alterar outras configurações de Veracode Vulnerability Integration, além das listadas aqui, requer conhecimento avançado de ServiceNow e Application Vulnerability Response e está além do escopo da documentação do produto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modificar Veracode parâmetros de instância de integração

Após a instalação inicial, você pode modificar os parâmetros das integrações [Veracode na instância de integração Veracode.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Você pode modificar os parâmetros de uma integração de sua instância para determinar que tipo de dados você ingere. Para algumas dessas configurações, você também pode modificar esses parâmetros na página de configuração da integração.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Integrações**.
2. Selecione **Vulnerabilidade da aplicação Veracode** na coluna Instância de origem para a integração Veracode que você deseja modificar.
3. Selecione a guia **Parâmetros de instância de integração** e clique duas vezes em um campo na coluna Valor para modificar os valores.

   Começando com v19.0 de Vulnerability Response e v4.0 de Veracode Vulnerability Integration, você pode configurar os seguintes parâmetros para as integrações de Veracode.

   importar manual

   Insira `verdadeiro` para importar resultados de testes de invasão manuais de Veracode. Você também pode modificar este valor na página de configuração da integração.

   Os testes de avaliação de invasão no Veracode Vulnerability Integration são descobertas manuais de Veracode. Essas descobertas não estão vinculadas a nenhuma solicitação de avaliação de teste de invasão configurada em Application Vulnerability Response. Para obter mais informações sobre solicitações de teste de invasão em Application Vulnerability Response, consulte Configurar teste de invasão.

   import_sca

   Insira `verdadeiro` para importar vulnerabilidades de Análise de composição de software (SCA). Você também pode modificar este valor na página de configuração da integração.

   status

   Insira `Aberto` ou `Encerrado` para importar descobertas para os estados desejados. Se você deixar este campo em branco, a integração importará descobertas para os estados Aberto e Fechado.

   policy_sandbox

   Insira uma `política` ou uma `área restrita` para importar registros que correspondam a uma política ou a uma área restrita. Esses registros podem estar relacionados à forma como as aplicações são testadas em seu ambiente.

   regra_política_passada

   Insira `verdadeiro` ou `falso` para importar registros que foram aprovados em uma regra de política. Esses registros podem estar relacionados à forma como as aplicações são testadas em seu ambiente.

4. Selecione **Atualizar** para salvar suas mudanças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Executar uma importação manual de vulnerabilidade da aplicação Veracode

Se a importação inicial falhar ou você não quiser aguardar a importação inicial programada, poderá executar uma importação de dados completa independentemente do trabalho programado diariamente.

Antes de Iniciar
Função necessária: grupo de gerentes de App-Sec

Procedimento

1. Navegar até **Todos** > **Integração de vulnerabilidade da Veracode** > **Integrações**.
2. Escolha uma integração, por exemplo, a Veracode Integração da lista de aplicações.
3. Clique em **Executar agora**.

   Nota:
   Cada uma das Veracode integrações de vulnerabilidade da aplicação tem como objetivo fornecer a recuperação de dados mais completa. Executá-los fora de ordem requer a experiência de ServiceNow e Application Vulnerability Response e pode resultar em dados incompletos.

   Quando a importação estiver concluída, as importações programadas serão retomadas.
4. Para obter os status de execução da integração, consulte Exibir o status de execução de importação da integração de vulnerabilidade da aplicação Veracode.
5. Se você quiser modificar outros parâmetros de integração, navegue até a instância de integração.

Definir horários de importação Veracode Vulnerability Integration

Para sua conveniência, você pode redefinir a hora de início dos Veracode Vulnerability Integration s.

Antes de Iniciar
Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa
Após a importação inicial, as integrações de vulnerabilidade Veracode fazem uma importação completa sempre que são executadas. Consulte Executar uma importação manual de vulnerabilidade da aplicação Veracode para obter mais informações sobre como realizar importações.

Procedimento

1. Navegar até **Todos** > **Integração de vulnerabilidade da Veracode** > **Integrações**.
2. Escolha uma integração.
3. Defina a nova **hora de início**.
   O tempo é calculado como Horas no horário local. O tempo padrão para as importações de Integração da lista de aplicações Veracode é 00:00:00. As outras integrações são **Sob demanda** e encadeadas para serem executadas após a Veracode Integração da lista de aplicações. Alterar a **hora de início** de qualquer um desses requer conhecimento avançado de ServiceNow e Gerenciamento de vulnerabilidade de aplicação.
4. Clique em **Atualizar**.
   A nova hora é usada para a próxima importação programada.

Incluir itens vulneráveis da aplicação Veracode encerrados

Por padrão, os itens vulneráveis da aplicação (IVAs) **encerrados** não são criados durante as importações de integração de item vulnerável Veracode. Se você quiser criá-los, deverá alterar uma propriedade do sistema.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

O Veracode Vulnerability Integration deve estar instalado e em execução.

Função necessária: administrador

Procedimento

1. Na caixa de texto **Navegador de filtro** esquerdo, digite `sys_properties.list`.
2. Na caixa de pesquisa **Nome** da lista, insira `sn_vul.create_closed`.
3. Clique duas vezes no campo **Valor** e defina como **Verdadeiro**
4. Clique no ícone de marca ícone de marca de seleção verde para salvar.
   Registros no estado **Encerrado** na próxima importação Veracode são criados como AVIs em Application Vulnerability Response.

Corrigindo Application Vulnerability Response vulnerabilidades

O monitoramento de correção é um processo que começa com a revisão do status e termina com o fechamento dos itens vulneráveis da aplicação (IVAs). Application Vulnerability Response oferece ferramentas e procedimentos para tornar esse processo mais produtivo e eficiente.

Application Vulnerability Response processo de correção

A correção de item vulnerável da aplicação é feita manualmente.

Uma visão geral do processo:

- Faça login na sua instância Application Vulnerability Response.
- Valide se as regras (Pesquisa de IC, Atribuição) para itens vulneráveis da aplicação estão funcionando conforme o esperado. Para obter informações sobre como revisar as Regras de pesquisa de IC, consulte Identificar aplicações em Application Vulnerability Response automaticamente. Para obter informações sobre regras de atribuição, consulte Atribuir itens vulneráveis da aplicação em Application Vulnerability Response automaticamente.
- Valide se as metas de correção estão corretas. Consulte Automatizar o acompanhamento de destino de correção no Application Vulnerability Response para obter informações sobre como as regras de destino de correção funcionam e como revisá-las. Exibir o status do destino de correção de um item vulnerável da aplicação.

  Nota:
  As regras de destino de correção pertencem aos AVIs. Essas regras são executadas quando o AVI é importado.

- Revise os painéis ou relatórios. Por exemplo, exiba painéis que mostram o envelhecimento dos AVIs por estados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Quando a aplicação Performance Analytics para Vulnerability Response (com.snc.vulnerability.analytics) é ativada, os usuários com determinadas funções podem exibir dados de interesse para os membros dos grupos do App-Sec Manager e do Campeão de segurança.

Para gerentes de App-Sec, Performance Analytics para Vulnerability Response contém a Application Vulnerability Response visão geral, que pode ajudá-lo a monitorar áreas de interesse. Consulte Soluções de análise e relatório para o painel Application Vulnerability Response e Application Vulnerability Management [PA].

A partir da versão 13.0 da aplicação Vulnerability Response : para os Campeões de segurança, Performance Analytics para Vulnerability Response contém o painel Minhas vulnerabilidades da aplicação, que pode ajudá-lo a monitorar suas áreas de interesse. Consulte Meu painel de vulnerabilidades da aplicação.

A partir da versão 13.0 da aplicação Vulnerability Response : para limitar a quantidade de dados coletados para relatórios ou listas relacionadas, consulte Definir classificações de serviço para relatórios Vulnerability Response e listas relacionadas.

- Revise o estado dos AVIs, em ordem de prioridade, procurando o que mudou.
- Revise o risco dos AVIs, conforme necessário. Para obter mais informações, consulte Criar uma calculadora de vulnerabilidade da aplicação.
- Reatribua o AVI a um grupo de atribuição para correção, se necessário.
- As novas verificações são acionadas automaticamente pela programação de importação de terceiros.
- Após a nova verificação, se o estado for **Fixo**, os AVIs serão fechados automaticamente durante a importação.
- Após a verificação, se o estado não for **Corrigido**, o AVI será reaberto.

Exibir bibliotecas de vulnerabilidades

Você pode exibir dados de vulnerabilidade importados do National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) ou de terceiros para decidir se deve escalar um grupo de vulnerabilidades.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > para **Bibliotecas**.

As seguintes bibliotecas estão disponíveis:

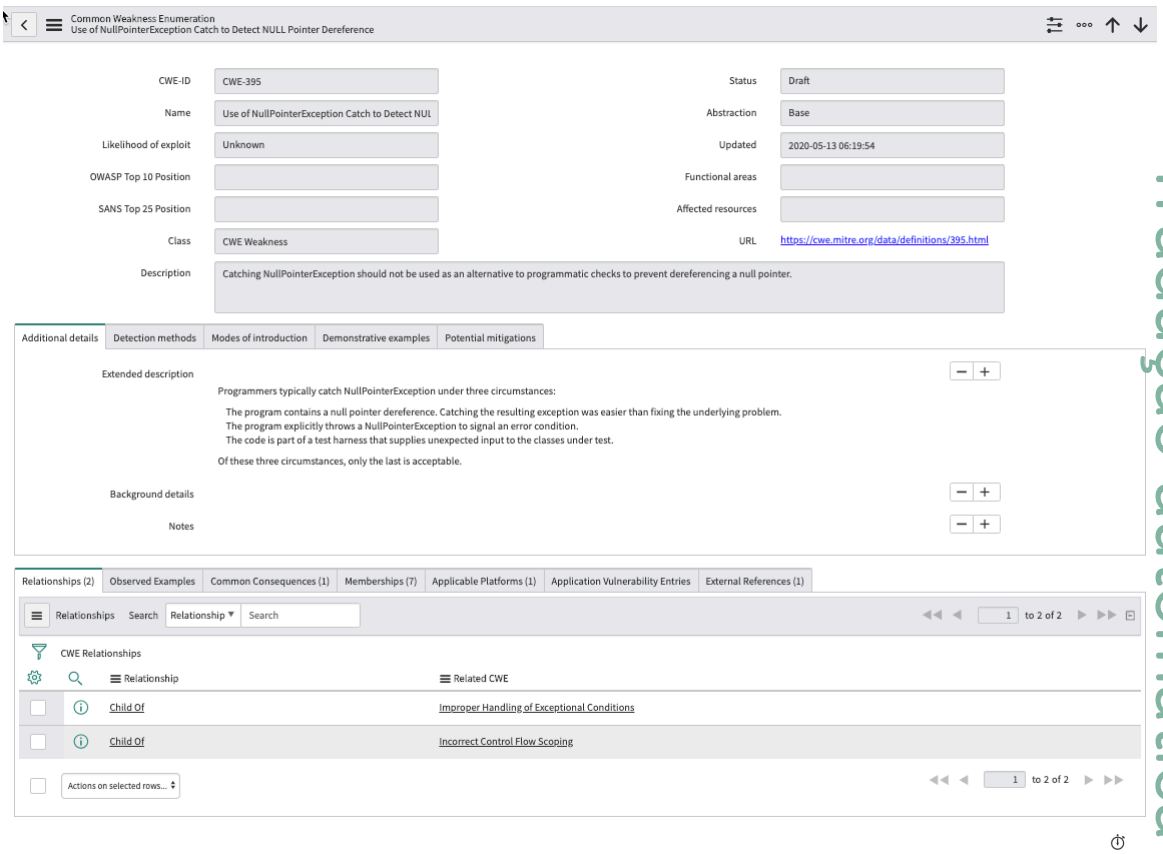
Bibliotecas	Descrição
NVD	Lista de vulnerabilidades encontradas pelo NVD e inclui check-lists de segurança, falhas de software relacionadas à segurança, configurações incorretas, nomes de produtos e métricas de impacto, incluindo explorações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Bibliotecas	Descrição
CWE	Lista de tipos de pontos fracos de software desenvolvidos pela comunidade. Cada registro CWE também inclui um artigo de conhecimento associado que descreve o ponto fraco. Você não pode escalar uma vulnerabilidade na tela Enumerações de Pontos Fracos Comuns, é apenas para referência.
Terceiros	Lista de vulnerabilidades de terceiros importadas em sua instância. Contém uma lista de referências relacionadas, itens vulneráveis, explorações, CWEs e CVEs.

2. Escolha uma biblioteca para exibir as vulnerabilidades.



Para obter informações sobre campos específicos, consulte Campos de vulnerabilidade da aplicação.

Campos de vulnerabilidade da aplicação

As vulnerabilidades são criadas automaticamente quando os registros são baixados do National Vulnerability Database (NVD), Common Weakness Enumeration (CWE) ou integrações de terceiros. O NVD e o CWE são armazenados em **Bibliotecas** em Vulnerability Response ou em **Vulnerabilidades** em Application Vulnerability Response.

Campos de entrada de vulnerabilidade do CWE

Os campos nesta tabela são somente leitura.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
CWE-Identificador	Identificador desta entrada de vulnerabilidade. Este identificador é usado para categorias e pontos fracos e é exclusivo entre os dois conjuntos de dados.
Nome	Nome descritivo atribuído a este CWE-ID.
Probabilidade de exploração	Qual a probabilidade de o ponto fraco ser explorado, em uma escala qualitativa. Um dos seguintes: • Baixa • Média • Alto(a)
10 principais posições da OWASP	A posição numérica desta vulnerabilidade na lista das 10 principais da OWASP.
SANS para a posição 25	A posição numérica desta vulnerabilidade na lista das 25 principais da SAN.
Classe	Tipo de fraqueza
Status	Um dos seguintes: • Incompleto • Rascunho • Estável • Preterido • descontinuado • Instável
Subtração	Um dos seguintes: • Variante • Classe • Base • Composto
Atualizado em	Última vez em que o registro foi atualizado na instância.
Áreas funcionais	Lista de áreas funcionais afetadas. Por exemplo, **Processamento de arquivos**. Preenchido somente para pontos fracos do 24/862.
Recursos afetados	Lista de recursos afetados. Por exemplo, **Arquivo** ou **Diretório**. Preenchido somente para pontos fracos 51/863.
URL	Artigo da base de conhecimento associado a esta vulnerabilidade.
Descrição	Descrição da vulnerabilidade.
Execução de integração	A execução de integração em que este CWE foi importado.
Seções	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Detalhes adicionais	Descrições do conceito de software que explicam melhor o ponto fraco. Inclui: • Descrição estendida • Detalhes do plano de fundo • Anotações
Métodos de detecção	Detalhes sobre como você pode detectar esse ponto fraco em uma aplicação.
Modos de introdução	As fases em que o ponto fraco é introduzido, por exemplo, **Implementação**, **Arquitetura e Design**e assim por diante.
Exemplos demonstrativos	Exemplos de código do ponto fraco com descrições de acompanhamento.
Mitigações potenciais	Detalhes sobre como evitar o ponto fraco, incluindo em que fase do ciclo de vida da aplicação ele ocorre e a eficácia da mitigação.
Listas relacionadas	
Relacionamentos	CWEs associados a esta vulnerabilidade. Lista os relacionamentos entre este CWE e outros. Pode incluir primário/secundário, segue/precede, obrigatório por/requer (para pontos fracos compostos), CanAlsoBe, PeerOf, MemberOf .
Exemplos observados	Alguns CVEs que são representativos desse ponto fraco.
Consequências Comuns	Consequências de uma exploração bem-sucedida, em termos de escopo e impacto. Por exemplo: Escopo: confidencialidade Impacto: ler dados da aplicação
Associações	Associações do CWE com esta vulnerabilidade.
Plataformas aplicáveis	Plataformas associadas a esta vulnerabilidade.
Entradas de vulnerabilidade da aplicação	Outras entradas de vulnerabilidade da aplicação associadas a uma.
Referências externas	Informações sobre a vulnerabilidade de fontes externas.

Tradução automática

Campos de entrada de vulnerabilidade da aplicação

Os campos nesta tabela são somente leitura.

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Fonte	Origem da vulnerabilidade, seja um scanner ou um teste físico.
Gravidade	Grau normalizado de severidade desta vulnerabilidade. Mapas de severidade são fornecidos para NVD e com ServiceNow integrações de terceiros. Para obter mais informações sobre como criar ou ajustar mapas de severidade, consulte Mapear a severidade de um item vulnerável da aplicação automaticamente.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Versão 13.0: CWE primário Versão 12.1: entrada do CWE	Referência ao elemento de Enumeração de Pontos Fracos Comuns no qual esta vulnerabilidade melhor se encaixa. Se houver mais de um CWE associado à vulnerabilidade, o CWE primário será determinado da seguinte forma: • O CWE está mapeado para os 10 principais da OWASP. Em caso afirmativo, use este CWE. Caso contrário, continue. • O CWE está mapeado para os 25 principais SANs? Em caso afirmativo, use este CWE. Caso contrário, continue. • O CWE tem a severidade mais alta? Em caso afirmativo, use este CWE. Caso contrário, continue. • Selecione o mais recente de todos os CWEs. O CWE mais recente é aquele com o valor do campo **Atualizado** mais recente no registro do CWE.
Nome da categoria	Classificação fornecida pela integração de terceiros. Auxilia na atribuição.
Detalhes da Vulnerabilidade	
Ameaça	Descrição da ameaça desta vulnerabilidade.
Descrição da mitigação	Descrição das etapas que podem ser realizadas para atenuar a vulnerabilidade.
Lista relacionada	
Versão 13.0: CWEs	Lista dos CWEs associados a esta vulnerabilidade. Não aplicável para Veracode Vulnerability Integration.

Campos de entrada do NVD

Os campos importados nesta tabela são somente leitura.

Nota:

Os dados do NVD não são usados em Application Vulnerability Response e as entradas representam somente os dados Vulnerability Response.

Os CWEs, que são usados em Application Vulnerability Response, podem apontar para entradas de NVD, como exemplos de um ponto fraco, e são fornecidos aqui apenas para fins informativos.

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Pontuação de risco	(Oculto quando não há Vulnerability Response itens vulneráveis (IVs) associados à vulnerabilidade) **Pontuação de risco** quantificada que separa os IVs em Crítico, Alto, Médio, Baixo e Nenhum.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Pontuação de risco	(Oculto quando não há IVs associados à vulnerabilidade) Valor calculado de risco que o item vulnerável representa para o seu ambiente.
Gravidade	Grau normalizado de severidade desta vulnerabilidade em Vulnerability Response. Mapas de severidade são fornecidos para NVD e com ServiceNow integrações de terceiros. Application Vulnerability Response **A severidade** é derivada da **severidade de origem** importada e não do NVD. Para obter informações sobre Application Vulnerability Response mapeamento de severidade, consulte Mapear a severidade de um item vulnerável da aplicação automaticamente.
Explorar itens existentes	Sim, se pelo menos uma exploração estiver associada a esta vulnerabilidade.
Nível de habilidade Exploit	Nível de habilidade mais baixo necessário para explorar esta vulnerabilidade.
Vetor de ataque Exploit	Vetor de ataque mais vulnerável das explorações para esta vulnerabilidade.
IVs ativos	(Oculto quando não há IVs associados à vulnerabilidade) Número de itens vulneráveis associados a esta vulnerabilidade, não no estado Encerrado. Se não houver AVIs ativos para esta vulnerabilidade, a **Classificação** de **risco e a Pontuação** de risco não serão exibidas.
Entrada de CWE	Referência ao elemento de Enumeração de Pontos Fracos Comuns no qual esta vulnerabilidade melhor se encaixa de acordo com o NVD.
Data de publicação	Data em que a vulnerabilidade foi publicada.
Última modificação	Data em que a vulnerabilidade foi modificada pela última vez.
Resumo	Descrição da vulnerabilidade.
Detalhes da Vulnerabilidade	
CVSS v2	Dados do CVSS v2 importados
CVSS v3	Dados do CVSS v3 importados, não disponíveis antes de 2015.
Solução preferencial	(Oculto quando não há IVs associados à vulnerabilidade) Solução da substituição mais alta na cadeia, derivada das soluções referenciadas na vulnerabilidade. Se houver mais de uma substituição mais alta na cadeia, nenhum valor será definido. Qualquer valor definido manualmente pode ser substituído nas importações subsequentes. A definição manual deste valor deve ser feita no item vulnerável.
Status da Correção (Oculto quando não há IVs associados à vulnerabilidade)	
Exclui os adiados	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Itens vulneráveis	Número de itens vulneráveis da aplicação ativos com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
% IVs corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade. Esta contagem exclui itens vulneráveis adiados.
Inclui os adiados	
Itens vulneráveis	Número de itens vulneráveis ativos com esta vulnerabilidade.
Total de IVs	Número total de itens vulneráveis com esta vulnerabilidade.
% IVs corrigidos	Percentual concluído da correção de itens vulneráveis com esta vulnerabilidade.
Links relacionados	
Antes da v13.0: forçar importação de vulnerabilidade de software **Nota:** Removido em v13.0	(Obsoleto) Recalcula o mapeamento do produto com Gestão de ativos de software ITSM com base nas informações do NVD. Atualiza a biblioteca de software vulnerável.
Atualizar status	Exibe a data e a hora da última atualização. Atualiza o seguinte: • Estado do grupo de vulnerabilidades • Pontuação e classificação de risco • Métricas como IVs ativos, total de IVs da seção Status de correção
Listas relacionadas	
Itens vulneráveis	(Oculto quando não há IVs associados à vulnerabilidade) Itens vulneráveis associados a esta vulnerabilidade.
Referências de vulnerabilidade	Informações sobre a vulnerabilidade de fontes externas, citadas pelo NVD.
Explorações	Explorações associadas a esta vulnerabilidade.
Soluções	(Oculto quando não há IVs associados à vulnerabilidade) Todas as Solução de gerenciamento de vulnerabilidade soluções de integração associadas a esta vulnerabilidade.
Versão 13.0: Pontos fracos	Dados importados de pontos fracos do CWE associados a um CVE (Common Vulnerabilities and Exposures, vulnerabilidades e exposições comuns).
Versão 13.0:	(Oculto quando não há IVs associados à vulnerabilidade)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Software Vulnerável	Dados de enumeração de plataforma comum (CPE) associados à vulnerabilidade.

Identificar aplicações em Application Vulnerability Response automaticamente

Quando os dados são importados de uma integração de terceiros, Application Vulnerability Response usa automaticamente os dados da aplicação para pesquisar correspondências no Configuration Management Database (CMDB). Ele faz isso usando **Regras de Pesquisa de IC**. Essas regras identificam aplicações para o registro de item vulnerável da aplicação (IVA) para ajudar na correção.

Conforme as aplicações são importadas, uma pesquisa é realizada na aplicação escaneada [sn_vul_app_scanned _application] tusando source_app_id e app_name para encontrar correspondências com aplicações de importações anteriores. Quando uma correspondência de ID de aplicação é encontrada, seus valores são usados nos campos **Aplicação** e **Versão** da aplicação no registro do item vulnerável da aplicação.

Se uma correspondência não for encontrada ou o campo ID da aplicação estiver vazio, as regras usarão as outras informações da aplicação para tentar identificar corretamente a aplicação. Se uma correspondência ainda não for encontrada, um registro de aplicação escaneado de espaço reservado será criado somente com os campos **Nome** da **aplicação e ID** da aplicação.

As regras de pesquisa **de ID da aplicação de origem** e **Nome** da aplicação são enviadas com o Veracode Vulnerability Integration, por padrão.

Nota:
As regras de pesquisa de IC padrão para Application Vulnerability Response estão disponíveis somente para a integração de vulnerabilidade Veracode.

Ao tentar uma correspondência, as regras de pesquisa são avaliadas primeiro pelo valor de **Ordem** mais baixo. Eles param quando uma regra retorna um único IC como correspondência.

Nota:
Se uma regra for criada de forma a retornar mais de um IC, somente a primeira correspondência será usada.

Para facilitar a localização de problemas de correspondência, quando uma correspondência é encontrada, a regra de pesquisa de IC usada para localizá-la é adicionada ao campo de **regra de correspondência de IC** para aplicações verificadas. Clique no de engrenagem na parte superior da exibição de lista da aplicação escaneada para adicioná-la à exibição.

Nota:
As regras, depois de removidas, não podem ser recuperadas. Em vez de remover as regras existentes, desative-as ao criar novas.

As regras de pesquisa de IC podem ser separadas por domínio e são específicas da origem. Se compatível, cada origem pode ter várias implantações. Por exemplo, a Veracode Integração de vulnerabilidade, pode ter várias implantações da Veracode Integração de vulnerabilidade. Cada implantação tem seu próprio conjunto de regras de pesquisa de IC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
As regras de pesquisa de IC são compartilhadas por todas as implantações da integração de vulnerabilidade. Se uma regra for excluída ou modificada, a exclusão ou as mudanças afetarão todas as implantações da integração de vulnerabilidade.

A importação de dados de vulnerabilidade pode sobrecarregar uma instância e podem ocorrer problemas de desempenho com recursos se as regras não forem construídas com cuidado. A lógica usada para iterar e executar a correspondência dentro do CMDB pode resultar em longos tempos de processamento. Para evitar qualquer degradação potencial de recursos ou complicações de desempenho, teste todas as regras de pesquisa de IC personalizadas ou modificações nas **regras de pesquisa de IC** predefinidas. Consulte Impedir registros duplicados ou órfãos após executar as regras de pesquisa de IC do Application Vulnerability Response para obter mais informações sobre como evitar registros órfãos duplicados, excluir dados e limpar dados.

Tópicos relacionados

Gestão de configuração e o CMDB

Criar uma regra de pesquisa de IC

O módulo **Regras de pesquisa de IC** contém regras que definem quais campos têm dados correspondentes no Configuration Management Database (CMDB). Essas regras são usadas para identificar aplicações e versões de aplicações e adicioná-las ao registro de item vulnerável da aplicação (IVA) para ajudar na correção.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Criar regras de pesquisa de IC requer conhecimento avançado de ServiceNow e Gerenciamento de vulnerabilidade de aplicação. Em vez de modificar uma das regras de pesquisa existentes, considere copiá-la e modificar a cópia. Quando você estiver satisfeito com o fato de a nova regra fazer o que você deseja, desative a original.

Nota:
As regras, depois de removidas, não podem ser recuperadas. Em vez de remover as regras existentes, desative-as ao criar novas.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **CMDB** > **Regras de Pesquisa de IC**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de regra de pesquisa de IC

Campo	Descrição
Nome	Nome da regra.
Método de pesquisa	Método usado para correspondência. As opções são: ○ **Script**: script pré-criado ou personalizado. ○ **Correspondência de campo**: pesquise na tabela ou no campo no CMDB.
Tipo	Tipo usado com o **método Pesquisa**de script.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

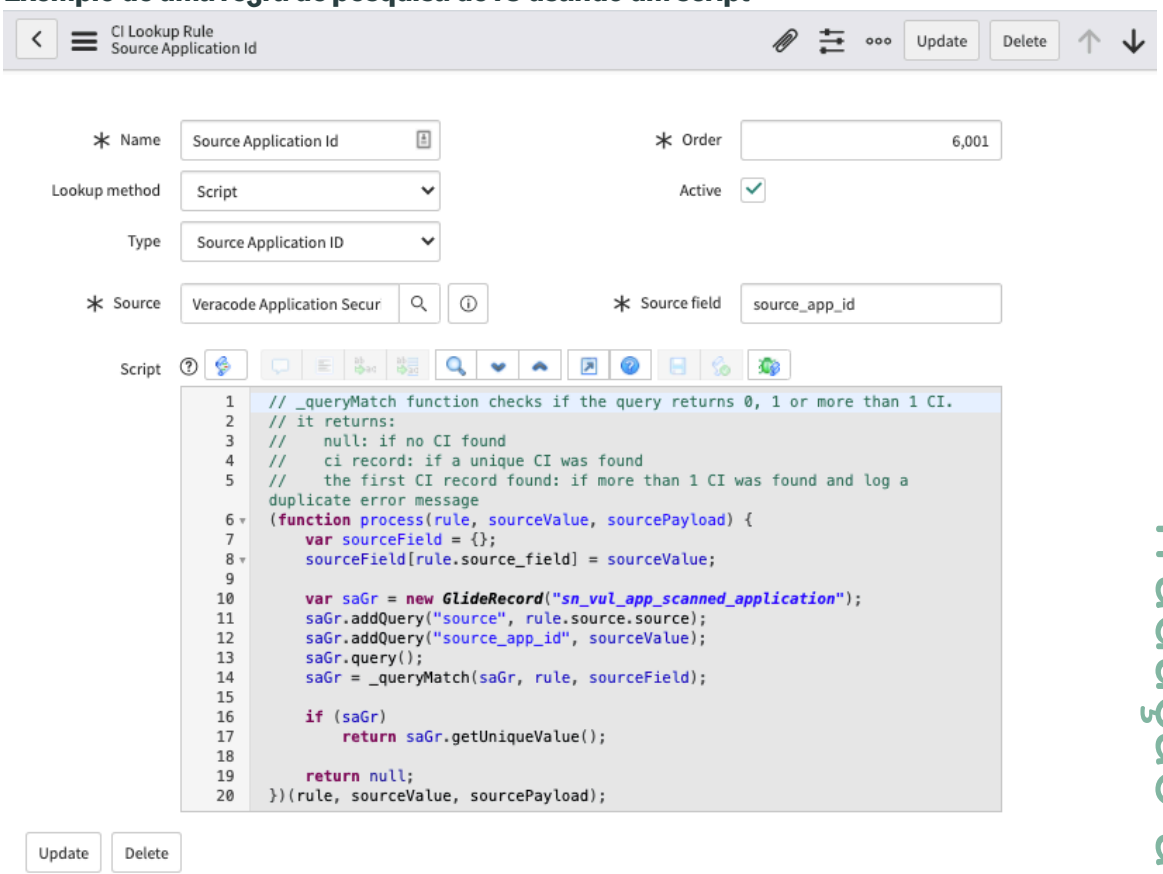
Campo	Descrição
Ordem	Ordem de precedência da regra. Correspondências com a ordem mais baixa são avaliadas primeiro.
Ativo	Caixa de seleção para saber se a regra está ativa ou desabilitada.
Fonte	Origem usada como entrada para esta regra. Depois de escolhido, os filtros de condição são exibidos.
Campo de origem	Campo de origem usado como entrada para esta regra. Os campos devem ser uma cadeia de caracteres ou um número.
Descrição	Texto que descreve a regra.
V19.0: destino de pesquisa	Abordagem de pesquisa que você deseja seguir. Selecione entre: ◦ Item de configuração ◦ Modelo de produto
Script	Um exemplo de script editável, com base no **Tipo**, é mostrado. Implemente o script personalizado seguindo os comentários incluídos no modelo da função padrão. **Nota:** A função de processo tem três parâmetros: `rule`, `sourceValue`e `sourcePayload`
Pesquisar na tabela IC	Tabela a ser pesquisada no CMDB. Usado com o campo correspondente ao **Método de pesquisa**.
V19.0: pesquisar na tabela de produtos	Se você escolher o **destino Pesquisa**do modelo de produto , o valor padrão será Modelo de aplicação.
Pesquisar no campo IC	Campo que contém informações que podem ser usadas para localizar um IC. Usado com o campo correspondente ao **método de pesquisa**. Este campo pode estar no registro de IC ou em um registro relacionado, como um adaptador de rede.
V19.0: pesquisar no campo do modelo do produto	Se você escolher o **destino de pesquisa**do modelo de produto , o valor padrão será Nome.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Enviar**.

Exemplo de uma regra de pesquisa de IC usando um script



Tópicos relacionados

Campos de item vulnerável da aplicação

Reaplicar regras de Pesquisa de IC no Application Vulnerability Response

Você pode reaplicar suas regras de pesquisa de item de configuração (IC) para atualizar os ICs existentes (aplicações verificadas e modelos de produto) em registros de aplicações descobertos.

Reaplicar uma regra de pesquisa

A reaplicação das regras de pesquisa de IC aplicará todas as regras ativadas às aplicações descobertas existentes. Atualizar os registros da aplicação descobertos pode levar algum tempo.

Para reaplicar as regras às aplicações descobertas existentes, navegue até **Todos** > **Security Operations** > **CMDB** > **Regras de pesquisa** e selecione **Aplicar mudanças**.

Definir o destino da pesquisa

Por padrão, a propriedade do sistema *sn_vul.use_product_model* está ativada (definida como **verdadeiro**). Dependendo de como a propriedade do sistema está definida nos registros de regra de pesquisa de IC, os registros da aplicação descobertos são atualizados da seguinte maneira:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se o campo Valor estiver definido como **verdadeiro**, o modelo de produto será o destino de pesquisa das regras de Pesquisa de IC e as aplicações descobertas serão atualizadas com os modelos de produto.
- Se o campo Valor estiver definido como **falso**, o item de configuração (aplicações verificadas) será o destino da pesquisa e as aplicações descobertas serão atualizadas com os itens de configuração (aplicações verificadas).

Para modificar a propriedade do sistema *sn_vul.use_product_model* para que os itens de configuração sejam usados como destino:

1. Como um usuário com a função sn_vul.app_sec_manager, navegue até **Todos** > **Propriedades do sistema** > **Todos**
2. Localize *sn_vul.use_product_model*.
3. Abra o registro.
4. Defina o campo Tipo como **falso**.
5. Selecione **Atualizar**.

Se você redefinir esta propriedade do sistema, deverá modificar suas regras para que os destinos de pesquisa correspondam à configuração da propriedade do sistema. Por exemplo, se você redefinir a propriedade do sistema para usar o item de configuração como destino, localize as regras que têm o destino de pesquisa como item de configuração.

1. Marque a caixa de seleção Ativa para essas regras e selecione **Atualizar**.
2. Localize as regras que usam o modelo de produto como destino e desative-as desmarcando a caixa de seleção Ativo e selecionando **Atualizar**.

Se você estiver criando uma nova regra de pesquisa, defina o destino de pesquisa para a regra no formulário de regra. Para obter mais informações, consulte Criar uma regra de pesquisa de IC.

Impedir registros duplicados ou órfãos após executar as regras de pesquisa de IC do Application Vulnerability Response

Tome medidas para evitar registros duplicados ou órfãos resultantes da correspondência (itens de configuração (ICs) dentro de CMDB.

A importação de dados de vulnerabilidade pode sobrecarregar uma instância e podem ocorrer problemas de desempenho com recursos se as regras não forem construídas com cuidado. A lógica usada para iterar e executar a correspondência no CMDB pode resultar em longos tempos de processamento. O teste completo e a depuração de scripts de processamento nas regras ajudam a reduzir o potencial de problemas posteriormente no processo.

Como evitar registros duplicados ou órfãos

- Use pequenos subconjuntos de dados que são específicos à regra de pesquisa de IC que está sendo testada.
  - Defina todas as **Regras de pesquisa de IC**, exceto a que está sendo testada, como **Inativas**.
  - Analise as aplicações importadas e os itens de configuração (ICs) para garantir que você esteja observando o comportamento esperado e que a correspondência esteja ocorrendo corretamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Revise os estados de IC, como **Descontinuado**.
- Remover dados de teste. Depois de começar a observar o comportamento correto ou esperado na correspondência de IC, reinicie. Isso pode ser feito por:
  - Excluindo os dados usados para teste: (consulte a seção **Excluindo dados de tabelas**)
    - Aplicações verificadas
    - Itens vulneráveis da aplicação (IVAs)
  - Execute novamente as integrações manualmente.

.

Excluindo dados de tabelas

Às vezes, você importou dados e percebeu que algo está errado. Se isso acontecer em um ambiente de desenvolvimento ou desempenho, você poderá reclonar de um ambiente melhor, mas isso nem sempre é uma opção.

Nota:
A execução dessas ações requer conhecimento avançado ServiceNow.

Existem quatro opções para excluir dados de tabelas:

- Usando **Excluir todos os registros** na **configuração da tabela**.
- Configure o **limpador de tabela** navegando até **Limpezas automáticas** (sys_auto_flush.list) e criando um novo registro **de limpeza automática**.
- Truncar gs.truncateTable usando um script em segundo plano.

Nota:
Nunca use *`truncateTable`* em um ambiente de produção. Consulte o representante do Suporte antes de executar grandes exclusões em ambientes de produção ou compartilhados.

- Crie uma solicitação no HI para excluir os dados.

Atribuir itens vulneráveis da aplicação em Application Vulnerability Response automaticamente

Atribua automaticamente vulnerabilidades de aplicação com base em marcadores de aplicação ou em qualquer um dos grupos de atribuição no item de configuração [cmdb_ci] ou grupos de atribuição de plataforma, para reduzir o tempo médio de atribuição.

Atribuição automática de itens vulneráveis da aplicação

Existem três maneiras diferentes de atribuir AVIs usando **Atribuir usando**:

Nota:
O recurso de recomendação de atribuição em Vulnerability Response não está disponível para Application Vulnerability Response.

- Grupo de usuários: esta opção permite selecionar qualquer um dos grupos de usuários Now Platform® existentes.
- Campo de grupo de usuários: esta opção permite escolher qualquer campo de grupo de atribuição disponível usando a tabela cmdb_ci. Por padrão, você vê os três campos de grupo a seguir no menu de lista no **campo Grupo de usuários**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

  - Nenhum: indica que não há valor padrão para este campo obrigatório
  - Item de configuração: grupo de aprovação
  - Item de configuração: grupo de atribuição
  - Item de configuração: grupo de suporte
- Script: esta opção permite definir as condições usando um script. Esta opção requer codificação ou conhecimento avançado ServiceNow.

Execute regras de alta prioridade (itens que precisam de tratamento especial, onde o risco é crítico ou um AVI deve ser tratado pela conformidade regulatória) primeiro. Em seguida, execute suas regras gerais, onde nenhum tratamento especial é necessário, e você saberá quem deve ser responsável por elas. Por fim, crie uma regra padrão para atribuir AVIs ao grupo que descobrirá a qual grupo de atribuição ele deve pertencer. Este grupo pode adicionar outra regra para cobrir suas decisões. Esta regra padrão seria executada por último.

Processo de avaliação da regra de atribuição

Quando um novo AVI é criado, importado ou reaberto após ser encerrado, as regras de atribuição são avaliadas em relação a ele. Um AVI só é avaliado uma vez, a menos que seja reaberto após ser fechado. Você pode reaplicar as regras manualmente após as mudanças.

O processo a seguir é usado para cada AVI novo, atualizado ou reaberto:

- Para cada regra de atribuição de vulnerabilidade, o AVI é comparado ao filtro de atribuição, a regra de ordem mais baixa primeiro.
- Onde a condição corresponde, o AVI é atribuído a um grupo de atribuição. A pesquisa é interrompida.
- Quando as condições não encontrarem uma correspondência entre todas as outras regras, o AVI será atribuído ao grupo de atribuição padrão, se houver uma regra padrão.

Nota:
Se não houver regra padrão, o AVI permanecerá não atribuído.

O**tipo de atribuição**, seja **Manual** ou **Regra** e Regra de **atribuição,** está disponível na interface de caixa de listagem dupla de Layout de formulário no formulário de item vulnerável (IVA) da aplicação. Qualquer AVI que foi originalmente atribuído por uma regra, mas posteriormente reatribuído manualmente, contém uma referência à regra original. Use as informações de **Regra** de **atribuição e Tipo** de atribuição para identificar casos em que as regras de atribuição não encontraram uma correspondência correta para o destinatário pretendido. Ou quais regras tiveram mais reatribuições.

Nota:
As regras de atribuição não reavaliam as atribuições criadas manualmente.

Reaplicar regras de atribuição

Ao mudar uma regra de atribuição, use o botão **Aplicar mudanças** na exibição da lista Regras de atribuição para executar novamente todas as regras alteradas em todos os AVIs abertos ativos (exceto aqueles que foram atribuídos manualmente).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Se o trabalho programado *Reapply all vulnerability assignment rules* não tiver sido executado antes da primeira vez em que você usa **Aplicar mudanças**, ele executará todas as regras de atribuição em todos os AVIs abertos, exceto os AVIs que foram atribuídos manualmente. Depois disso, todos os usos subsequentes de **Aplicar mudanças** executam novamente somente as regras alteradas e todas as regras dependentes. Mudanças em uma regra podem resultar em um AVI correspondente a uma regra não modificada diferente. [store-future: BEGIN review]A reaplicação das regras de atribuição não reagrupa os itens vulneráveis.[End]

O trabalho programado [*Reapply all assignment rules*] está inativo, por padrão. Quando ativado, ele aplica todas as regras a todos os AVIs abertos, exceto aqueles atribuídos manualmente. Ele pode ser executado **diariamente**, **semanalmente**, **mensalmente**, **periodicamente**, **uma vez**ou **sob demanda**. Dependendo de quantos AVIs ativos você tem em seu ambiente, lembre-se de definir o campo **Executar** corretamente após a execução inicial para evitar impactos no desempenho.

Criar ou editar Application Vulnerability Response regras de atribuição

Você pode criar regras para atribuir automaticamente itens vulneráveis da aplicação (IVAs) com base nas condições do filtro. Essas regras atribuem AVIs conforme eles são importados ou criados manualmente.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Com as regras de atribuição, você define a condição de atribuição e a ordem de execução. Quando um AVI corresponde a uma condição de regra, a pesquisa de atribuição é interrompida. Para obter mais informações, consulte Filtragem em Gerenciamento de vulnerabilidade de aplicação.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Regras de atribuição**.
2. Clique em **Nova**.
3. Se **Novo**, preencha os campos no formulário, conforme apropriado.

Regra de atribuição de vulnerabilidade da aplicação

Campo	Descrição
Nome	Nome da regra de grupo.
Ativo	Indica se a regra de atribuição está ativa.
Ordem de execução	Ordem na qual as regras são avaliadas. Regras de alta prioridade, itens que precisam de tratamento especial, onde o risco é crítico, ou um AVI deve ser tratado pela conformidade regulatória, para ser executado primeiro. Em seguida, execute suas regras gerais, onde nenhum tratamento especial seja rnecessário, e você saberá quem deve ser responsável por elas. Por fim, crie uma regra padrão para atribuir AVIs ao grupo que descobrirá a qual grupo de atribuição ele deve pertencer. Este

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	grupo pode adicionar outra regra para cobrir suas decisões. Esta regra padrão seria executada por último.
Descrição	Descrição da regra de atribuição.
Condição	
Campos de condição	Condições que devem ser atendidas.
Novos critérios	Adiciona mais campos de filtro de condição para você escolher.
Atribuir usando	Para automatizar a atribuição de grupos criados com base nesta regra, escolha uma das opções disponíveis. ○ Grupo de usuários: selecione um grupo de usuários na tabela de pesquisa. ○ Campo de grupo de usuários: selecione um campo de grupo de usuários no menu da lista. ○ Script: crie ou edite um script. **Nota:** Criar ou editar um script requer experiência em ServiceNow.

4. Clique em **Enviar**.
   Regras novas ou atualizadas são avaliadas na próxima importação.

Calcular risco em Application Vulnerability Response automaticamente

As calculadoras de vulnerabilidade da aplicação automatizam o cálculo dos valores de risco iniciais para os campos nos itens vulneráveis da aplicação (IVAs). Os cálculos de risco oferecem informações sobre como priorizar a correção. A condição de cada calculadora é avaliada na ordem e a primeira calculadora correspondente é usada.

Calculadoras de vulnerabilidade da aplicação

O sistema base Application Vulnerability Response inclui duas calculadoras de vulnerabilidade que definem a **pontuação de risco** base no item vulnerável da aplicação.

- **Calculadora de risco básico**
- **Calculadora do Advanced Risk**

As calculadoras de vulnerabilidade da aplicação podem ser criadas para priorizar e classificar o impacto dos AVIs com base em qualquer critério usando filtros de condição. Seja o impacto nos negócios da vulnerabilidade, a classe do item de configuração (IC) ou a idade do AVI, você pode criar calculadoras de vulnerabilidade adicionais para definir outros campos nos AVIs. Ou você pode personalizar as calculadoras de vulnerabilidade existentes. Uma calculadora pode ser escrita para refletir qualquer conjunto de prioridades. Para obter mais informações, consulte Filtragem em Gerenciamento de vulnerabilidade de aplicação.

Os AVIs contêm o valor de **pontuação de risco** derivado das calculadoras de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Um AVI exibe a **severidade de origem**, mas não a severidade normalizada. A severidade normalizada é usada pelas calculadoras para obter o valor da **pontuação de risco**, mas não é mostrada nos AVIs.

Cada calculadora contém uma lista de regras da calculadora, com uma condição que determina quando aplicá-la. Quando a calculadora é executada, a condição de cada regra da calculadora é avaliada na ordem e a primeira regra da calculadora correspondente é usada.

Todas as calculadoras de vulnerabilidade habilitadas definem os campos selecionados sempre que um AVI é criado, quando um IC ou vulnerabilidade associada muda.

A calculadora de **risco básico** calcula a **pontuação** de risco para AVIs usando a severidade da vulnerabilidade normalizada.

Nota:
Somente uma calculadora por campo de destino (**pontuação de risco**) pode estar ativa de cada vez.

O **risco básico** está habilitado por padrão. A **calculadora de risco avançada** está desabilitada por padrão.

Regras da calculadora de vulnerabilidade da aplicação

A **Calculadora de Risco Básica do** sistema básico contém regras de calculadora que atribuem a cada nível de severidade (Nenhum a Crítico) um valor (0-100) para a **Pontuação de Risco** com base na severidade. A**Severidade Desconhecida** recebe automaticamente uma pontuação de risco de 100. Esses valores podem ser ajustados e, como a **Calculadora de risco avançada**, novas regras de calculadora ou novas regras de risco podem ser criadas.

A **Calculadora de risco avançada** do sistema básico contém uma regra de calculadora de vulnerabilidade especializada chamada **Regra de risco padrão**. Ele calcula a **pontuação de risco** com base em vários valores:

- Gravidade da vulnerabilidade
- 10 principais da OWASP
- 25 principais da SANS

Você pode personalizar os critérios para a regra de risco padrão. Para obter mais informações, consulte Definir campos e pesos para a regra de risco.

Você pode ajustar os valores a serem usados na **Regra de risco padrão** e quanto peso atribuir a cada um desses valores. Os pesos são usados para ajustar o quanto cada elemento conta ao definir a **pontuação de risco**.

Cada regra tem uma configuração de **Ordem**. No entanto, a primeira a corresponder às condições atualiza o campo **Pontuação de risco** no AVI. Regras de calculadora sem script normalmente criam menos impacto no desempenho do que regras de calculadora com script.

Ponderações de Pontuação de Risco de Vulnerabilidade

Todas as vulnerabilidades são atribuídas a uma pontuação de risco e classificação com base em fatores como severidade, criticidade, informações de exploração e assim por diante. A regra de negócios `Update Risk Rating from Risk Score` na tabela de item vulnerável é responsável pelo cálculo da classificação de risco. Sempre que a pontuação de risco muda, a classificação de risco é calculada e preenchida nos itens vulneráveis. Antes da

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

versão 17.1 da aplicação Vulnerability Response (VR), as classificações de risco a seguir eram fornecidas como parte da inclusão de script VulnerabilityUtils, que eram codificadas.

Valor (classificação de risco)	Peso (pontuação de risco)
1	90–100
2	70–89
3	40–69
4	1 a 39
5	0

Começando com a versão 18.0 de Vulnerability Response,

- Os tipos de classificação de risco são enviados na tabela base como avr_risk_rating. Esses tipos são passados como parte da regra de negócios em cada tabela em que a classificação de risco é calculada.
- O script foi modificado para que você possa consultar as entradas nos valores da tabela Ponderações de pontuação de risco para o cálculo da classificação de risco.
- Adicione entradas adicionais para um tipo existente ou crie um novo tipo. Ao criar um novo tipo, certifique-se de adicionar os rótulos para a nova classificação de risco e também de modificar os scripts e as regras de negócios relacionados. Você também deve adicionar um novo estilo para a nova pontuação de risco.
- Modifique o script para consultar os registros na tabela base.

Você pode acessar a tabela Ponderações de pontuação de risco inserindo sn_sec_cmn_risk_score_weight no navegador de filtros.

Além disso, a pontuação de risco é recalculada automaticamente nos seguintes cenários:

- Quando um item de configuração (IC) muda de não voltado para a internet para voltado para a internet.
- Quando as Vulnerabilidades e exposições comuns (CVEs) associadas ou as entradas de terceiros (TPEs) nos itens de vulnerabilidade (IVs) estão vinculadas a uma Vulnerabilidade de exploração conhecida (KEV) de CVE.

Definir campos e pesos para a regra de risco

Personalize os parâmetros e pesos da regra de risco para que você possa gerar pontuações de risco que usam os dados de vulnerabilidade e ativo exclusivos da sua organização. Ao selecionar os campos incluídos na regra de risco, você pode definir uma estrutura de pontuação de risco eficaz.

Antes de Iniciar

Função necessária: sn_vul.app_manage_risk_score_configuration

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Calculadoras de vulnerabilidade**.
2. Na página Calculadoras de vulnerabilidade, clique **em Calculadora de risco avançada**.
3. Navegar até **Página da calculadora de vulnerabilidade** > **Guia Regras da Calculadora de Vulnerabilidade** > **Regra de Risco Padrão**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. **Opcional:** Na seção Critérios da calculadora de risco da página Regra de risco de vulnerabilidade, defina o peso de cada critério de acordo com sua importância no cálculo de pontuação de risco geral.
5. Para desativar a regra, você deve desmarcar a caixa de seleção **Ativo**.
6. Para adicionar campos de regra de risco aos Critérios da calculadora de risco, clique em **Adicionar critérios**.
7. No formulário, preencha os campos.

Formulário de campo de regra de risco

Campo	Descrição
Escolher tabela de referência	Tabela que você usa para definir a ponderação da pontuação de risco. Você pode selecionar uma destas opções: ○ **Item vulnerável da aplicação**: adicione campos que podem ser percorridos com pontos diretamente do item vulnerável (IV). ○ **Item vulnerável da aplicação - Item de configuração**: adicione campos de referência com pontos que fazem parte das extensões da tabela base, como a tabela Hardware. Esses campos não fazem parte da tabela base (cmdb_ci). ○ **Item vulnerável da aplicação - Vulnerabilidade**: adicione campos de referência com pontos que fazem parte das tabelas que estendem a tabela base, por exemplo, Entrada de terceiros. Esses campos não fazem parte da tabela base de entrada de vulnerabilidade. ○ **Tabela de referência de item vulnerável da aplicação**: adicione campos que fazem parte das tabelas relacionadas (m2m) ou tabelas que têm uma referência ao item vulnerável. Esses campos não podem ser usados como referência com pontos diretamente do IV. ○ **Tabela de referência do item de configuração**: adicione campos que fazem parte das tabelas relacionadas (m2m) de cmdb_ci ou tabelas que têm uma referência a cmdb_ci. Esses campos não podem ser usados como referência com pontos diretamente do IV. ○ **Tabela de referência de vulnerabilidade**: adicione campos que fazem parte das tabelas relacionadas (m2m) de sn_vul_entry ou tabelas que têm uma referência a sn_vul_entry. Esses campos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	não podem ser usados como referência com pontos diretamente do IV. ○ **Condições personalizadas**: use esta opção para atribuir pesos à regra avaliando a condição. Por exemplo, o filtro voltado para a Internet determina se um item de configuração (IC) é externo ou interno.
Tabela	Campo que aparece somente quando uma das seguintes opções é selecionada na tabela Escolher referência: ○ **Item vulnerável da aplicação -> Item de configuração** ○ **Item vulnerável da aplicação -> Vulnerabilidade** ○ **Tabela de referência do item vulnerável da aplicação** ○ **Tabela de referência do item de configuração** ○ **Tabela de referência de vulnerabilidade**
Campo	Campo a ser usado para cálculo de pontuação de risco para esta regra.
Agregação	Campo que aparece somente quando uma tabela de referência é selecionada na tabela Escolher referência. Selecione o valor mínimo ou máximo a ser considerado para cálculos quando Campo for selecionado nas Tabelas relacionadas (m2m).
Ponderação	Ponderação deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
Definir ponderação do valor	Componente para atribuir pesos a cada valor de campo. Para campos numéricos, os valores de campo podem ser definidos como um intervalo (por exemplo, 1 a 5). Os pesos devem ser um número inteiro entre 0 e 100. **Nota:** Este campo não será exibido se a opção Condições personalizadas for selecionada na tabela Escolher referência.
Tabela de condição	Campo que aparece somente quando Condições personalizadas são selecionadas na tabela Escolher referência. Selecione uma condição na lista.
Nome do campo	Campo que aparece somente quando Condições personalizadas são selecionadas na tabela Escolher referência. Insira um nome para os critérios de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Condição	Campo que aparece somente quando Condições personalizadas são selecionadas na tabela Escolher referência. Visualize os itens nesta tabela que correspondem às condições definidas.

8. Clique em **Enviar**.
9. Na página Regra, ative e reaplique a regra para reavaliar a pontuação de risco nos itens vulneráveis ativos.

Example:
Adicione a severidade de origem como critério para uma regra de risco.

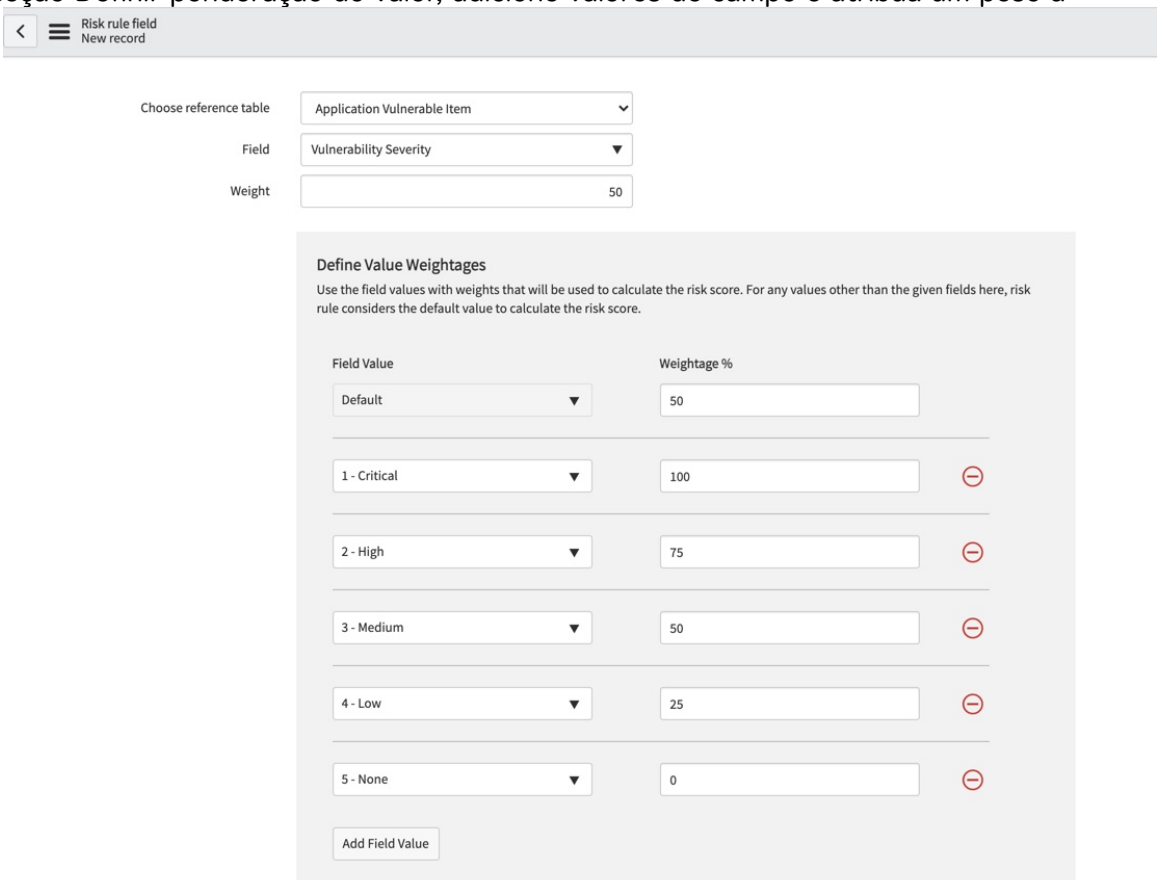
Caso de uso: fornecedores terceirizados, como Qualys e Tenable, fornecem suas próprias pontuações. Essas pontuações são preenchidas no campo **Severidade de origem** na tabela sn_vul_entry. Use este campo para cálculos de pontuação de risco. Para usar essa pontuação para calcular a pontuação de risco, faça o seguinte:

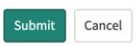
1. Navegue até a página Regra de risco.
2. Para desativar a regra, desmarque a caixa de seleção **Ativo**.
3. Para adicionar campos de regra de risco aos Critérios da calculadora de risco, clique em **Adicionar critérios**.
4. Na lista Escolher tabela de referência, selecione o **item Vulnerável da aplicação**.
5. Na lista Campo, selecione **Vulnerability.Severity**.
6. No campo **Peso**, insira a importância relativa deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Na seção Definir ponderação do valor, adicione valores de campo e atribua um peso a



eles. 

8. Clique em **Enviar**.

Tópicos relacionados

Calculadoras do Vulnerability Response e regras da calculadora de vulnerabilidade

Criar uma calculadora de vulnerabilidade da aplicação

Uma calculadora de vulnerabilidade da aplicação é uma fórmula predefinida para calcular um campo de destino quando determinados critérios são atendidos. As calculadoras, que calculam a **pontuação de risco**do item vulnerável da aplicação (IVA), podem conter **regras de risco**. Os cálculos de risco oferecem informações para priorizar a correção.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Nota:

Você pode observar uma degradação no desempenho ao executar calculadoras de vulnerabilidade da aplicação que contêm scripts.

Solicite que suas regras executem as regras mais simples primeiro. Execute scripts somente nos itens que não podem ser tratados com uma condição e valor de modelo ou uma regra de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Calculadoras de vulnerabilidade**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Formulário Calculadora de vulnerabilidade

Campo	Descrição
Nome	O nome da calculadora de vulnerabilidade da aplicação.
Tabela	Preenchido automaticamente com o nome da tabela AVI.
Aplicação	Preenchido automaticamente com Vulnerability Response.
Campo de destino	Campo a ser calculado.
Descrição	Descrição de texto da calculadora.
Ativo	Liga ou desliga a calculadora.

4. Clique com o botão direito do mouse no cabeçalho para **Salvar**.
   A seção **Regras da calculadora de vulnerabilidade** é exibida.
5. Crie uma regra para a calculadora clicando em **Novo**.

Nota:
Para obter o formulário **Novas regras de risco** (disponível somente quando o **campo Destino** for **Pontuação de risco**), consulte a etapa 10.

6. Preencha os campos, se for o caso.

Formulário Regra da Calculadora de Vulnerabilidade

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual a calculadora de vulnerabilidade será executada. Uma calculadora com uma entrada de ordem de 100 é executada antes de uma calculadora com uma entrada de ordem de 200.
Calculadora	Preenchido automaticamente com a calculadora primária.
Ativo	Por padrão, a caixa de seleção **Ativa** está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará aos novos itens vulneráveis criados no sistema.
Exibição avançada	Quando selecionadas, as condições de script e os valores de script podem ser selecionados em Tipo de **condição** e **Tipo de valor**.

7. Preencha os campos na guia **Quando esta condição for atendida**, conforme apropriado.

Guia Quando esta condição for atendida

Campo	Descrição
Tipo de condição	Disponível quando você seleciona a **exibição Avançado**. As opções incluem:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	◦ Filtro: usa condições de filtro. ◦ Grupo de filtros: consulte Criar e definir grupos de filtros para definir os critérios da calculadora. ◦ Script: condição de script usada para determinar quando aplicar esta calculadora. **Nota:** Antes de escrever scripts para determinar quando aplicar as calculadoras, retorne à lista **Calculadoras de vulnerabilidade da aplicação**. Explore os registros da calculadora de vulnerabilidade enviados com o sistema de base.
Condição	Define condições básicas de filtro para determinar se a calculadora deve ser usada ou não. Selecionar o **grupo de filtros** ou os tipos de condição de **script** oculta este campo.

8. Clique na guia **Definir estes valores** e preencha os campos no formulário, conforme apropriado.

Guia Definir estes campos

Campo	Descrição
Tipo de valor	Disponível quando você seleciona a **exibição Avançado**. As opções incluem: ◦ Modelo: defina os valores a serem definidos em cada campo. ◦ Script: usado para definir os valores em cada campo.
Valores de Script	Disponível se você selecionou o tipo de valor de **Script**. Define a quais valores os cálculos serão aplicados.
Modelo	Selecione os campos e valores que você deseja usar para a calculadora. Selecionar o tipo de valor de **Script** oculta este campo.

9. Quando tiver concluído todas as entradas, clique em **Enviar**.

Nota:
Ao editar uma calculadora existente e quiser atualizar todas as pontuações existentes, você pode usar o botão **Reaplicar Calculadora**. Ele é executado em todos os AVIs ativos e, se essa calculadora for usada para definir seu valor, recalcula o valor desses AVIs. Como a reaplicação de uma calculadora pode levar muito tempo, um trabalho programado lida com isso.

10. Para o formulário **Novas regras de risco**, preencha os campos conforme apropriado.

Defina cada peso de acordo com a porcentagem do resultado que deve vir desse valor. Para quaisquer dados que o seu scanner não forneça, ou para dados que não devam fazer parte da pontuação de risco, defina o peso como zero.

Conforme você atualiza os pesos, os cenários exibem os pesos restantes, bem como os resultados da **Pontuação de risco** antecipada.

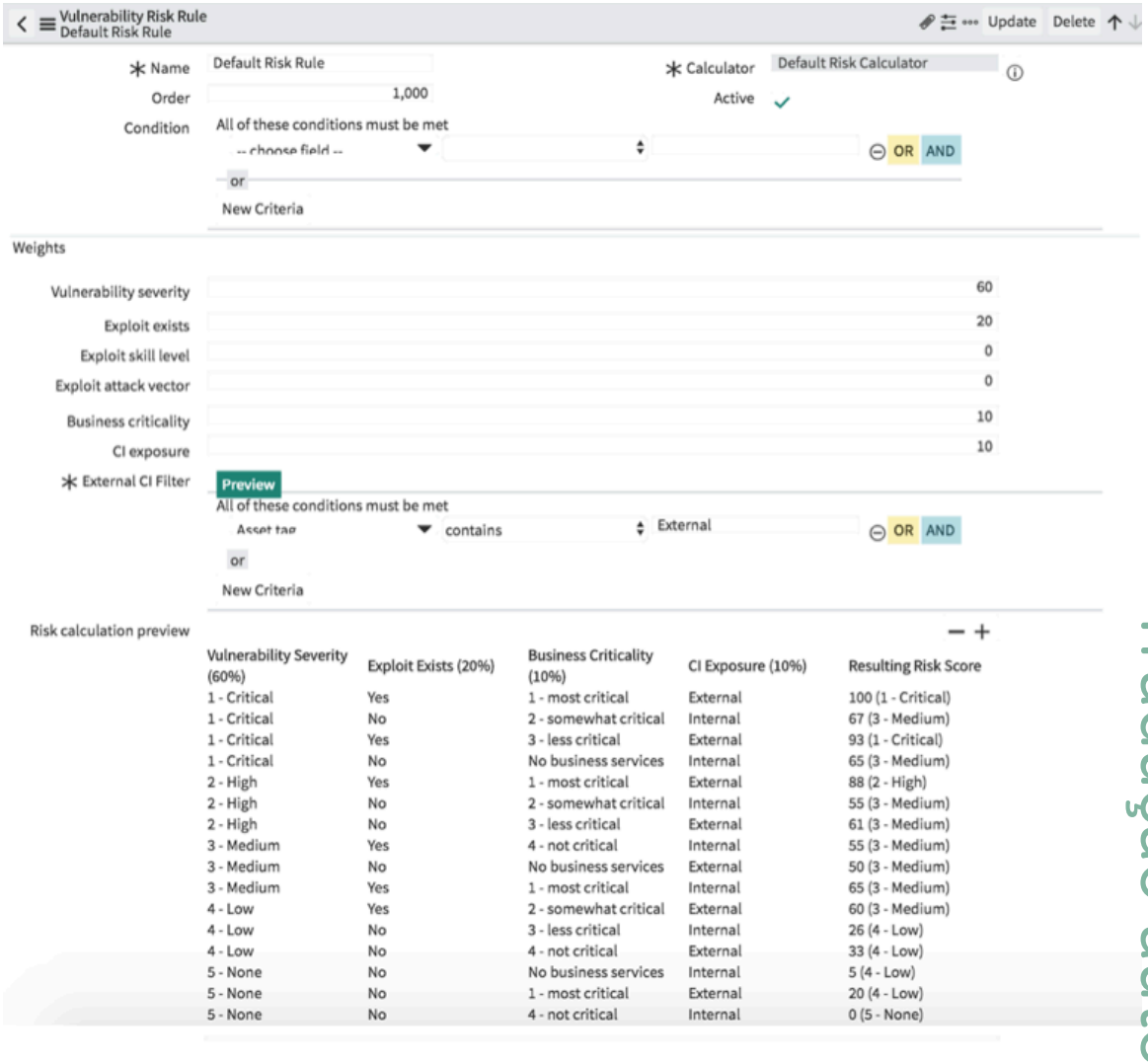
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Nome da regra da calculadora.
Ordem	A ordem na qual a calculadora será executada. Uma calculadora com uma entrada de ordem de 100 é executada antes de uma calculadora com uma entrada de ordem de 200.
Calculadora	Preenchido automaticamente com a calculadora primária.
Ativo	Por padrão, a caixa de seleção **Ativa** está marcada, o que significa que a regra da calculadora está ativa. Se você desmarcar esta caixa de seleção, esta regra não se aplicará aos novos itens vulneráveis criados no sistema.
Condição	Define condições básicas de filtro para determinar se a calculadora deve ser usada. Selecionar o **grupo de filtros** ou os tipos de condição de **script** oculta este campo.
Ponderações	
Severidade da Vulnerabilidade	Percentual do resultado proveniente da severidade.
10 principais da OWASP	Percentual do resultado proveniente da presença da vulnerabilidade na lista das 10 principais da OWASP. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.
25 principais da SANS	Percentual do resultado proveniente da presença da vulnerabilidade na lista das 25 principais da SANS. Se essas informações não estiverem presentes em suas vulnerabilidades, defina o peso como zero.
Total da execução	Percentuais totais calculados automaticamente. Quando esse valor atinge 100, a visualização do cenário mostra amostras de pontuações de risco em diferentes cenários.
Cenários de exemplo	Quando todos os pesos totalizam 100%, os cenários de pontuação de risco são exibidos, fornecendo uma visualização da pontuação de risco em alguns dos cenários possíveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



11. Clique em **Enviar**.

Mapear a severidade de um item vulnerável da aplicação automaticamente

Application Vulnerability Response mapeamento de severidade transforma campos de severidade de origem de terceiros em campos reconhecíveis em Vulnerability Response.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa

Application Vulnerability Response integrações de terceiros, como Veracode Vulnerability Integration fornecem mapeamentos de severidade na instalação. Esses mapas podem ser ajustados alterando os campos nos mapas existentes.

Criar ou editar um mapa de severidade destina-se somente a mapeamentos de terceiros personalizados ou não padrão em seu ambiente e requer experiência em Application Vulnerability Response e ServiceNow.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Mapeamento de severidade normalizado**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Mapeamento de campo

Campo	Descrição
Fonte	O nome da origem do mapeamento de severidade.
Valor de origem	O valor de severidade de origem.
Valor de meta	O valor de severidade da meta. As opções são: ○ 1- Crítico ○ 2 - Alta ○ 3 – Médio ○ 4 - Baixo(a) ○ 5 - Nenhum

4. Repita a etapa 3 para cada nível de severidade de origem.
5. Clique em **Enviar**.

Filtragem em Gerenciamento de vulnerabilidade de aplicação

Calculadoras e regras de atribuição usam condições durante a importação, criadas usando o **construtor de condição**. Mudanças em seus critérios podem afetar o desempenho, já que cada registro é avaliado usando esses filtros.

As regras e calculadoras enviadas com o sistema básico são otimizadas para desempenho. Editar ou criar regras ou calculadoras é cuidadoso e pode exigir experiência em ServiceNow e Application Vulnerability Response. Dito isso, algumas orientações estão disponíveis.

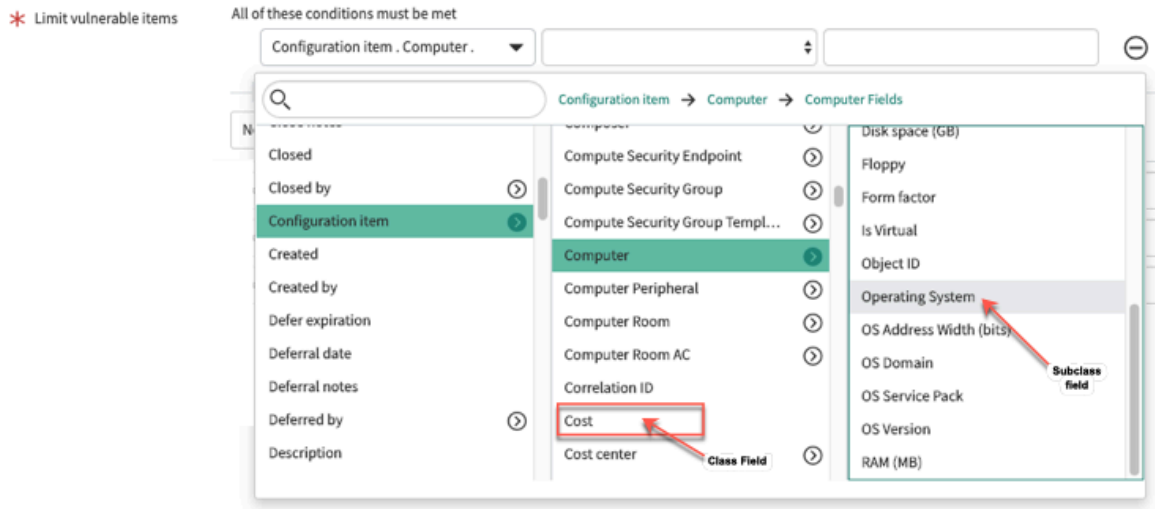
Evite filtrar com base em campos de subclasse

Algumas tabelas oferecem suporte à extensão. Um exemplo disso é a tabela IC do CMDB [cmdb_ci]. Tabelas como cmdb_ci_hardware e cmdb_ci_computer estendem esta tabela. Se você filtrar com base em um campo que não está na tabela primária, esse filtro poderá ser caro de construir e avaliar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Menu suspenso de filtro de condição



Por exemplo, filtrar em **Item de Configuração** > **Custo** não afetaria negativamente o desempenho porque **Custo** é um campo de classe, e não um campo de subclasse, de **Item de configuração**.

Item de Configuração > **Computador**, no entanto, é uma subclasse que requer uma referência com pontos para outro campo, neste caso, **Sistema operacional**. Este processo pode levar muitos milissegundos que se somam rapidamente, quando milhões de itens vulneráveis estão sendo importados e afetam o desempenho.

Nota:
Usar a condição [contains] é como uma pesquisa de caractere curinga e pode causar impacto no desempenho. Usar [is] sempre que possível é mais eficiente.

Automatizar o acompanhamento de destino de correção no Application Vulnerability Response

As Regras de destino de correção da aplicação definem o intervalo de tempo esperado para corrigir itens vulneráveis (IVAs) da aplicação, fornecendo um intervalo de tempo para corrigir a própria vulnerabilidade. Por exemplo, se um item vulnerável da aplicação contiver uma classificação de risco crítica, a vulnerabilidade desse item precisará ser corrigida em 15 dias.

Os gerentes de App-Sec podem criar regras de destino de correção de aplicação, definindo:

- O destino de correção.
- O destino do lembrete.
- [store-future: BEGIN review]Os destinatários do lembrete e da notificação - que devem ser notificados quando os AVIs passarem da data de destino do lembrete ou da correção e não tiverem sido corrigidos.[End]

Os gerentes de App-Sec podem ver a data de destino da correção no formulário AVI e nas exibições de lista. No entanto, as datas não são atualizadas para AVIs no estado **Adiado**, **Resolvido**ou **Encerrado**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A **data de destino** da correção é codificada por cores na exibição de lista do AVI como pontos, da seguinte forma:

- Os AVIs que não atingiram a data de notificação são mostrados em verde.
- Os AVIs que se aproximam da data de destino da correção são mostrados em laranja.
- Os AVIs após a data de destino da correção são mostrados em vermelho.

[store-future: BEGIN review]Um e-mail de resumo, por regra de destino de correção da aplicação, é enviado quando um ou mais AVIs estão se aproximando da data de meta de correção ou a data de meta de correção já passou.[End]

Regras padrão

Application Vulnerability Response é fornecido com três regras padrão que estão inativas por padrão:

- Regra de classificação de risco crítico: uma meta de correção com uma classificação de risco **1-Crítico**, uma meta de correção de 15 dias e um lembrete de **7** dias antes da data de meta.
- Regra de classificação de risco médio-alto: uma meta de correção com uma classificação de risco **2-alto** ou **3-médio**, uma meta de correção de 30 dias e um lembrete de **7** dias antes da data de destino.
- Regra de classificação de risco menos crítica: uma meta de correção com uma classificação de risco **4-baixo**, uma meta de correção de 45 dias e um lembrete de **7** dias antes da data de destino.

As regras de destino de correção podem ser desativadas ou excluídas

Quando uma regra é desativada, as datas de destino de correção atuais dos AVIs aos quais ela foi aplicada são apagadas. Se um AVI atender a qualquer regra ativa, essa regra será aplicada, caso contrário, o AVI não terá regra ou data de destino e seu status será **Sem meta**.

Quando as regras são excluídas, a data de **destino** da correção e os campos relacionados nos AVIs encerrados são preservados. A data de **destino** da correção e os campos relacionados em AVIs não encerrados são limpos e todas as regras dependentes são reaplicadas.

Cenário de regra de correção

Quando várias regras de destino de correção são aplicadas ao mesmo AVI, a regra mais restritiva é aplicada.

Por exemplo, se um AVI atender à condição de duas regras de destino de correção da aplicação:

Cenário: o AVI foi aberto pela última vez em 01/03/2018 às 10:00:00.

- Regra de destino de correção da aplicação 1: aberta pela última vez em 03/07/2018; a meta de correção é de 15 dias desde que foi aberta pela última vez; A data de destino da correção calculada é 16/03/2018 10:00:00.
- Regra de destino de correção da aplicação 2: aberta pela última vez em 10/03/2018; a meta de correção é de 10 dias desde que foi aberta pela última vez; A data de destino da correção calculada é 11/03/2018 10:00:00.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Neste cenário, a regra de destino de correção da aplicação 2 se aplica ao AVI, já que ele tem a data mais restritiva. 10 dias desde que o IVA foi identificado pela primeira vez versus 15 dias.

Nota:
As metas de correção da aplicação são calculadas a partir da data da **última abertura** mais o número de dias (medidos como incrementos de 24 horas). Você pode adicionar este campo ao formulário AVI da interface de caixa de listagem dupla do Layout de formulário. É a data em que o AVI foi aberto mais recentemente em sua instância.

A partir da V17.1, as metas de correção são calculadas a partir da **meta de (data)**. O valor padrão permanece **Data da última abertura**.

Nota:
Depois que a regra de destino de correção da aplicação é definida, as datas de destino de correção são calculadas pelo trabalho programado *`Evaluate remediation targets`* ou pelo botão **Aplicar mudanças** na exibição de lista Regras de destino de correção.

Sobre o trabalho programado Avaliar destinos de correção

`Evaluate remediation targets` é executado uma vez às 4:00:00 diariamente.

`Evaluate remediation targets` itera por meio de todas as regras de vulnerabilidade ativas, começando pelas regras com a data de meta de correção mais antiga. Ele analisa todos os AVIs que:

- Não estejam em um estado **Encerrado**, **Adiado**ou **Resolvido**.
- Não tem data de meta de correção.
- Ter uma data de destino de correção posterior à data na regra de destino de correção da aplicação.

`Evaluate remediation targets` adiciona uma data de destino de correção, se não houver uma, ou se esta regra contiver uma data anterior à do registro, ele atualizará a data de destino existente. Por fim, ele atualiza os campos **Data de destino** da correção e **Status** da correção no formulário AVI. Para regras inativas, **Avaliar destinos de correção** limpa os campos de correção no AVI.

Reaplicar regras de destino de correção

Ao alterar uma regra de destino de correção, use o botão **Aplicar mudanças** na página da lista Regras de destino de correção para executar novamente todas as regras alteradas em todos os AVIs em aberto ativos, exceto aqueles no estado **Encerrado**, **Adiado** ou **Resolvido**.

Nota:

Se o trabalho programado, *`Evaluate remediation targets`* estiver em execução, você não poderá iniciar um processo de reaplicação. No entanto, se um processo de reaplicação já estiver em execução e o trabalho programado for acionado, eles serão executados em paralelo.

Os processos de reaplicação em Vulnerability Response e Application Vulnerability Response são independentes e podem ser executados em paralelo.

Criar ou editar regras de destino de correção da aplicação

Impulsione a correção de vulnerabilidades de alto risco em tempo hábil configurando uma regra de destino de correção no nível de item vulnerável (IVA) da aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: grupo de gerentes de App-Sec

Nota:
O sistema de base é fornecido com três regras de destino de correção.

- Regra de classificação de risco crítico
- Regra de classificação de risco menos crítico
- Regra de classificação de risco médio-alto

Essas regras estão inativas por padrão. Se você optar por editar um, em vez de criar um novo, lembre-se de marcar a caixa**Ativa** antes de salvar.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Administração** > **Regras de destino de correção**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Nome	Nome da regra.
Meta (dias)	Especifique o número de dias em que os AVIs devem ser corrigidos, desde a última abertura.
V17.1: meta de (data)	Data a partir da qual os SLAs de destino são calculados. Você pode especificar somente a data ou os campos de tipo de data e hora. O valor padrão é Data da última abertura. Para personalizar os valores deste campo, consulte KB1185029 .
Ativo	Por padrão, a caixa de seleção **Ativo** está marcada, o que significa que a regra de destino de correção está ativa. Se esta caixa de seleção estiver desmarcada, esta regra não se aplicará a novos AVIs criados no sistema.
Notificar (dias antes do vencimento)	Número de dias antes da hora de correção desejada para que um lembrete seja definido. A data de notificação calculada usando este valor é usada para mostrar o status da correção e a codificação de cores. Se a data for anterior à data de notificação, o status da correção será "Em andamento". Se passar da data de notificação e antes da data de meta de correção, o status será mostrado como se aproximando da meta. **Nota:** Se este campo for definido como 0, somente uma notificação de **Meta** não atingida será definida.
A regra se aplica a	Usando o filtro de condição, selecione os critérios para aplicar a regra aos AVIs. Para evitar impacto no desempenho, teste suas condições em escala de produção total. O teste permite determinar quanto tempo o trabalho **Avaliar destinos de correção** leva para ser executado, de acordo com as condições e o tamanho do seu Configuration Management Database (CMDB).
Atualizar histórico	
Atividades	Não usado para a criação inicial de uma regra. Posteriormente, as anotações de trabalho do sistema são registradas aqui.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Clique em **Enviar**.
   Esta regra entra em vigor durante a próxima execução do trabalho programado, *`Evaluate remediation targets`*. O mesmo é verdadeiro quando uma regra existente é atualizada ou ao usar o botão **Aplicar mudanças** na exibição da lista Regras de destino de correção. O mesmo é verdadeiro quando uma regra existente é atualizada. Para obter mais informações sobre o trabalho programado e **Aplicar mudanças**, consulte Automatizar o acompanhamento de destino de correção no Application Vulnerability Response.

Exibir o status do destino de correção de um item vulnerável da aplicação

Quando um item vulnerável da aplicação (IVA) quase atinge (ou ultrapassa) sua data de destino de correção, conforme definido por uma regra de destino de correção, o registro AVI é atualizado com um status. Essas informações podem ajudá-lo a monitorar proativamente as próximas atividades de correção.

Antes de Iniciar
Função necessária: grupo de gerentes de App-Sec

Por Que e Quando Desempenhar Esta Tarefa
O trabalho programado **Avaliar destinos de correção** é executado uma vez por dia para comparar a data atual com a data de correção do item vulnerável especificada na regra de destino de correção associada. Quando a data atual está dentro do número de dias antes do vencimento da correção, um status de correção é adicionado ao registro do item vulnerável.

Procedimento

Navegar até **Todos** > **Application Vulnerability Response** > **Itens vulneráveis**.
Se a data de correção do AVI estiver dentro do intervalo das condições definidas na regra de destino de correção, verifique as colunas Status do destino de correção, visíveis na exibição da lista de itens vulneráveis. Se a data de destino da correção tiver passado para um AVI, uma anotação será exibida no formulário AVI.

Nota:
Para exibir o número de AVIs que estão se **aproximando da meta**, **em andamento** e **meta passada**, consulte Painel do Application Vulnerability Management [PA].

Tópicos relacionados

Criar ou editar regras de destino de correção da aplicação

Teste de invasão

O teste de invasão em Application Vulnerability Response permite que os responsáveis pela aplicação avaliem a postura de segurança de sua aplicação. É o teste manual de uma aplicação pela equipe de hackers éticos.

Funções necessárias

O teste de invasão requer as seguintes funções:

App-Sec Manager: contém gerentes de segurança e responsáveis pela aplicação que gerenciam as solicitações de avaliação de teste de invasão. Ele contém as seguintes funções granulares:

- sn_vul.app_manage_pen_test_request
- sn_vul.app_read_all
- cmdb_read

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Hacker ético: contém membros da equipe de hackers éticos que realizam testes de invasão de aplicações. Ele inclui as seguintes funções granulares:

- sn_vul.app_update_assignment_group
- sn_vul.app_update_assigned_to
- sn_vul.app_manage_manual_avits
- sn_vul.app_manage_pen_test_request_config
- itil
- sn_vul.app_read_all
- sn_vul.app_manage_pen_test_request
- sn_vul.app_update_state

Para obter mais informações sobre essas funções, consulte Application Vulnerability Response grupos de usuários e funções.

A partir da v19.0 de Vulnerability Response, se você estiver usando o Veracode Vulnerability Integration, os testes de avaliação de invasão no Veracode Vulnerability Integration serão descobertas manuais de Veracode. Eles não estão vinculados a nenhuma solicitação de avaliação de teste de invasão configurada em Application Vulnerability Response. Para obter mais informações sobre avaliações de teste de invasão de Veracode, consulte o Veracode Vulnerability Integration.

Ciclo de vida dos testes de invasão

Como proprietário da aplicação, você pode solicitar à equipe de invasão ética uma avaliação de teste de invasão da sua aplicação. A equipe de invasão ética atua nesta solicitação e cria descobertas de teste de invasão. Essas descobertas são itens vulneráveis de aplicação (IVAs) criados manualmente.

O fluxo de trabalho de teste de invasão cobre o ciclo de vida do teste de invasão, desde o aumento da solicitação de teste até a resolução das descobertas da equipe de invasão ética.

Como solicitar uma avaliação de teste de invasão

A partir da v19.0, você pode criar novas solicitações ou copiar solicitações existentes em **Todos** > **Solicitações de avaliação de teste de invasão** > **Todos**.

Antes da v19.0, como proprietário da aplicação, você pode solicitar uma avaliação de teste de invasão para sua aplicação usando o Catálogo de serviços do ITSM.

Revisando a solicitação de avaliação de teste de invasão

A equipe de invasão ética revisa e avalia a aplicação e o escopo da solicitação de avaliação de teste de invasão e os adiciona ao backlog existente.

Preparando um ambiente

A equipe de invasão ética envia uma solicitação ao proprietário da aplicação para fornecer um ambiente para que ele inicie o teste. Quando o ambiente estiver pronto, o proprietário da aplicação informará a equipe de hackers éticos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre como configurar solicitações de teste, consulte Configurar teste de invasão.

Testar e relatar as descobertas do teste de invasão

A equipe de invasão ética testa a aplicação e relata as descobertas ao responsável pela aplicação. A equipe de hackers éticos também define os Acordos de nível de serviço (ANSs) para as descobertas do teste de invasão usando a data de meta de correção. Essas descobertas são os AVIs criados manualmente. O proprietário da aplicação, por sua vez, revisa os AVIs criados pela equipe de hackers éticos. Eles planejam as correções e as atribuem à equipe de aplicações.

Nota:
As regras de destino de correção não se aplicam às descobertas do teste de invasão.

A equipe de hackers éticos pode criar uma biblioteca de entradas de vulnerabilidade da aplicação (AVEs) e reutilizá-las ao relatar os AVIs. Eles também podem rastrear o status das descobertas do teste de invasão.

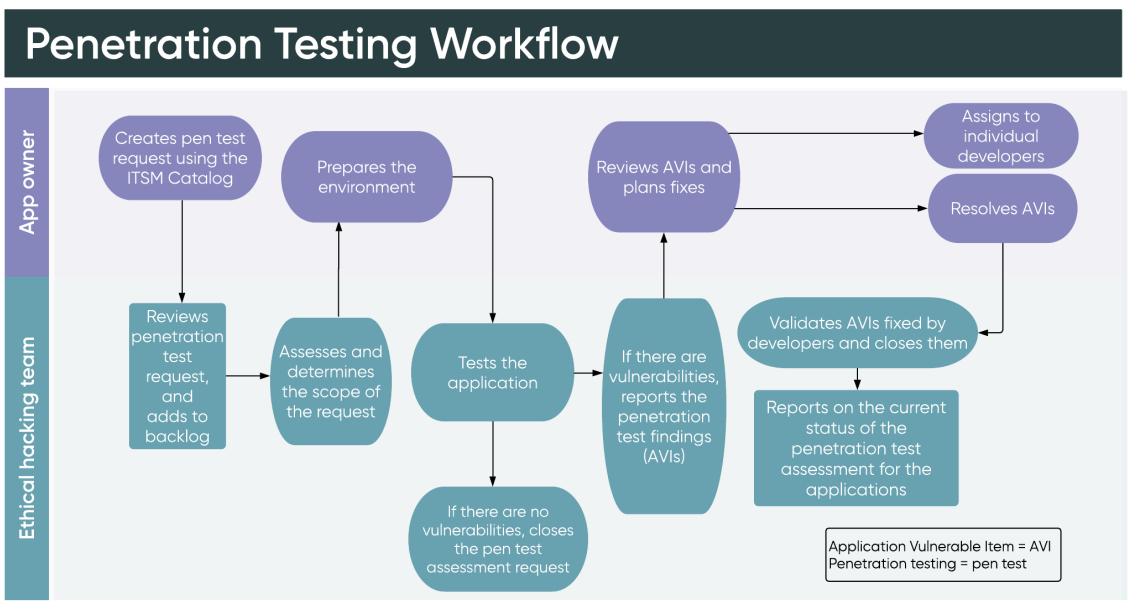
Corrigindo e validando as descobertas do teste de invasão

Depois que as descobertas do teste de invasão são corrigidas e resolvidas pela equipe de aplicações, as correções são validadas manualmente e encerradas pela equipe de hackers éticos.

Gerenciamento de vulnerabilidade de aplicação relatórios

Use os relatórios disponíveis no painel Gerenciamento de vulnerabilidade de aplicação do PA para rastrear as descobertas do teste de invasão.

Ciclo de vida do teste de invasão



Criar uma solicitação de avaliação de teste de invasão a partir de solicitações existentes (v19.0)

A partir da v19.0, você cria solicitações de avaliação de teste de invasão diretamente da lista de solicitações existentes. Você também pode copiar solicitações existentes no estado Encerrado nesta lista para criar solicitações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: gerente de App-Sec

Por Que e Quando Desempenhar Esta Tarefa
A partir da v19.0 de Vulnerability Response, se você estiver usando o Veracode Vulnerability Integration, os testes de avaliação de invasão no Veracode Vulnerability Integration serão descobertas manuais de Veracode. Eles não estão vinculados a nenhuma solicitação de avaliação de teste de invasão configurada em Application Vulnerability Response. Para obter mais informações sobre avaliações de teste de invasão de Veracode, consulte o Veracode Vulnerability Integration.

Procedimento
1. Navegar até **Todos** > **Solicitações de avaliação de teste de invasão** > **Todos**.
2. **Opcional:** Como alternativa, você pode criar uma solicitação replicando solicitações encerradas. Todos os valores da solicitação original são preservados no novo formulário. Os itens vulneráveis da aplicação (IVAs) são copiados automaticamente para a nova solicitação. Selecione **Copiar e criar solicitação** de registros no estado Encerrado.
3. Selecione Novo e preencha os campos.

Formulário de solicitação de avaliação de teste de invasão

Campo	Descrição
Número	Identificador exclusivo gerado para a solicitação de avaliação de teste de invasão.
Estado	Selecione um valor com base no status da solicitação.
Solicitados por	Pessoa que está solicitando a avaliação da aplicação.
Grupo de atribuição	Grupo selecionado para trabalhar nas descobertas do teste de invasão. Pode ser adicionado ou editado manualmente por um gerente de App-Sec. Para configurar grupos, consulte Configurar teste de invasão.
Aplicação	Selecione uma aplicação usando a opção de pesquisa.
Atribuído a	Indivíduo do grupo de atribuição selecionado que trabalha nas descobertas do teste de invasão. Pode ser adicionado ou editado manualmente por um gerente de App-Sec.
Tipo de aplicação	Selecione uma opção de: ○ Serviço Web (conhecido como API antes da v16.1) ○ Aplicação Web ○ Cliente espesso ○ Móvel (se você selecionar **Móvel**, a guia Móvel será exibida na parte inferior do formulário com campos adicionais)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Sprint	Exibe os sprints com largura de banda disponível para acomodar a solicitação de avaliação com base no campo de tipo de avaliação selecionado. Consulte Configurar sprints para teste de invasão e Configurar tipos de avaliação para teste de invasão para obter mais informações sobre como modificar a capacidade do sprint e o escopo de teste.
v19.0: tamanho da aplicação	Selecione o tamanho da aplicação que você deseja testar. ○ Pequeno ○ Médio(a) ○ Grande ○ Padrão (selecione esta opção se você não tiver certeza do tamanho) Consulte mais Configurar teste de invasão mais informações sobre como modificar a capacidade de sprint e testar o escopo com o tamanho da aplicação e a capacidade de sprint.
Criado em	Data e hora em que a solicitação foi criada.
Tipo de avaliação	Selecione o tipo de avaliação em: ○ Teste de invasão completo ○ Teste focado ○ Testar novamente Para obter mais detalhes sobre como testar combinações e escopo de teste, consulte Configurar tipos de avaliação para teste de invasão.
Atualizado em	Data e hora em que a solicitação foi atualizada pela última vez.
Data da demonstração	Data em que esta aplicação pode ser demonstrada.
Implantação de produto planejada em	Data planejada para implantar esta aplicação na produção.
Versão/liberação da aplicação planejada para implantação	Versão da aplicação planejada para implantação de produção.
v19.0: aplicação de propriedade de fornecedor terceirizado ou de uma guia de empreendimento conjunto Se você selecionar Sim para este campo, a guia Informações do fornecedor/empreendimento conjunto será exibida. Preencha os campos adicionais.	
Existe uma cláusula que nos permite executar o teste de invasão?	O termo "Cláusula" pode se referir a padrões de teste que incluem quaisquer acordos existentes entre duas ou mais partes que você deseja adicionar. Se você selecionar **Sim**, adicione a cláusula.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
A cláusula que menciona a permissão para executar o teste de invasão	
Nome jurídico completo e endereço do fornecedor	
Sistema de detecção de intrusão	
Contato técnico do fornecedor	
As informações registradas em log foram revisadas para formar atividade mal-intencionada?	
A aplicação é hospedada por outro fornecedor terceirizado?	
Contato do fornecedor que encerrará o teste de invasão	
Guia Detalhes da aplicação	
Finalidade da aplicação	Descrição da funcionalidade da aplicação.
Detalhes das stacks de tecnologia	Pilha de tecnologia completa do front-end ao back-end, bancos de dados e outras tecnologias importantes.
É uma aplicação de terceiros?	Confirma se esta aplicação pertence a um fornecedor terceirizado.
Tipos de lista de dados confidenciais acessíveis pela aplicação	Tipos de dados confidenciais acessíveis pela aplicação. Por exemplo, dados PII, dados PHI e dados financeiros, como números de cartão de crédito.
Tipo de autenticação	Especifica se esta aplicação usa autenticação LDAP, sua própria autenticação nativa ou outras formas de autenticação.
A aplicação está no escopo de algum programa de conformidade?	Especifica se esta aplicação afeta algum programa de conformidade, como o PCI.
Contatos da equipe de aplicações	Membros da equipe de aplicações a serem contatados pela equipe de hacking ético em caso de dúvidas.
Lista de programas de conformidade	
Interfaces ou aplicações de terceiros relacionados	
Endereço IP	
Número aproximado de usuários em produção?	
Existe um script automatizado?	
A versão de produção desta aplicação é externa?	
v 19.0: Impacto nos negócios	
Dano financeiro	Selecione um na lista.
Não conformidade	Selecione um na lista.
Dano à reputação	Selecione um na lista.
Violação de privacidade	Selecione um na lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Guia Detalhes do teste	
URLs para teste	URLs que devem ser incluídos no teste de invasão.
URLs a serem excluídos	URLs que devem ser excluídos do teste de invasão.
Essa aplicação já foi testada?	Especifica se esta aplicação já foi testada quanto à invasão.
Motivo para testar novamente	Motivo para solicitar uma reavaliação do teste de invasão se a aplicação foi testada anteriormente.
Quando a aplicação foi testada?	Intervalo de tempo em que a aplicação foi testada quanto à invasão.
Detalhes da conta de teste	Detalhes da conta de teste que podem ser usados pela equipe de hackers éticos para testes de invasão.
Funções da aplicação	Funções compatíveis com a aplicação para seus usuários.
Funções mais usadas	Funções usadas com mais frequência na aplicação.
Guia Comentários adicionais	
Anotações de trabalho	

4. Selecione **Salvar** para salvar suas edições ou **Enviar** para iniciar a solicitação.

Criar uma solicitação de avaliação de teste de invasão (antes da v19.0)

Inicie uma solicitação de avaliação de teste de invasão para suas aplicações Web ou APIs. Essas solicitações são enviadas para a equipe de hackers éticos, que então testa esses aplicativos e relata manualmente as descobertas do teste de invasão.

Antes de Iniciar
Função necessária: gerente de App-Sec

Por Que e Quando Desempenhar Esta Tarefa
O proprietário da aplicação gera uma solicitação de avaliação de teste de invasão para verificar manualmente a aplicação ou as APIs. A equipe de invasão ética testa a aplicação e cria manualmente as descobertas do teste de invasão. Essas descobertas são itens vulneráveis da aplicação (IVAs) criados manualmente.

O grupo de atribuição padrão para a descoberta do teste de invasão é o grupo configurado no campo "Equipe de aplicação" da solicitação de avaliação de teste de invasão associada. O tipo de atribuição da descoberta do teste de invasão é Manual. As regras de atribuição não podem substituir a atribuição dessas descobertas de teste de invasão.

A partir da v19.0, você pode criar solicitações de avaliação de teste de invasão diretamente da tabela Solicitações de avaliação de teste de invasão [sn_vul_pen_test_assessment_request_list]. Para obter mais informações, consulte Criar uma solicitação de avaliação de teste de invasão a partir de solicitações existentes (v19.0).

Procedimento

1. Antes da v19.0, navegue até até **Todos** > **Autoatendimento** > **Catálogo de serviços** > **Serviços** > **Solicitação de avaliação de teste de invasão**.
2. **Opcional:** Como alternativa, você pode criar uma solicitação replicando solicitações encerradas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Todos os valores da solicitação original são preservados. Os itens vulneráveis da aplicação (IVAs) são copiados automaticamente para a nova solicitação.

3. No formulário, preencha os campos.

Formulário de solicitação de avaliação de teste de invasão

Campo	Descrição
Número	Identificador exclusivo gerado para a solicitação de avaliação de teste de invasão.
Solicitados por	Pessoa que está solicitando a avaliação da aplicação.
Solicitação de avaliação primária	Solicitação de avaliação de teste de invasão original usada para criar a solicitação secundária. Ele é criado usando uma solicitação de avaliação encerrada. Visível somente no formulário de solicitação de avaliação secundária.
Aplicação	Selecione uma aplicação usando a opção de pesquisa.
Tipo de aplicação	Selecione uma opção de: ○ Serviço Web (conhecido como API antes da v16.1) ○ Aplicação Web ○ Cliente espesso ○ Móvel (se você selecionar Móvel, a guia Móvel será exibida na parte inferior do formulário com campos adicionais)
v19.0: tamanho da aplicação	Selecione o tamanho da aplicação que você deseja testar. ○ Pequeno ○ Médio(a) ○ Grande ○ Padrão (selecione esta opção se você não tiver certeza do tamanho)
Tipo de avaliação	Selecione o tipo de avaliação em: ○ Teste de invasão completo ○ Teste focado ○ Testar novamente Para obter detalhes, consulte Configurar tipos de avaliação para teste de invasão.
Finalidade da aplicação	Descrição da funcionalidade da aplicação.
Detalhes das stacks de tecnologia	Pilha de tecnologia completa do front-end ao back-end, bancos de dados e outras tecnologias importantes.
É uma aplicação de terceiros?	Confirma se esta aplicação pertence a um fornecedor terceirizado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tipos de lista de dados confidenciais acessíveis pela aplicação	Tipos de dados confidenciais acessíveis pela aplicação. Por exemplo, dados PII, dados PHI e dados financeiros, como números de cartão de crédito.
Tipo de autenticação	Especifica se esta aplicação usa autenticação LDAP, sua própria autenticação nativa ou outras formas de autenticação.
A aplicação está no escopo de algum programa de conformidade?	Especifica se esta aplicação afeta algum programa de conformidade, como o PCI.
Contatos da equipe de aplicações	Membros da equipe de aplicações a serem contatados pela equipe de hacking ético em caso de dúvidas.
Data da demonstração	Data em que esta aplicação pode ser demonstrada.
Implantação de produto planejada em	Data planejada para implantar esta aplicação na produção.
Versão/liberação da aplicação planejada para implantação	Versão da aplicação planejada para implantação de produção.
v19.0: aplicação de propriedade de fornecedor terceirizado ou empreendimento conjunto	Se você selecionar Sim para este campo, a guia Informações do fornecedor/empreendimento conjunto será exibida com campos adicionais. O termo "Cláusula" pode se referir a padrões de teste que incluem quaisquer acordos existentes entre duas ou mais partes.
Estado	Selecione um valor com base no status da solicitação.
Grupo de atribuição	Grupo selecionado para trabalhar nas descobertas do teste de invasão. Pode ser adicionado ou editado manualmente por um gerente de App-Sec.
Atribuído a	Indivíduo do grupo de atribuição selecionado que trabalha nas descobertas do teste de invasão. Pode ser adicionado ou editado manualmente por um gerente de App-Sec.
Sprint	Exibe os sprints com largura de banda disponível para acomodar a solicitação de avaliação com base no campo de tipo de avaliação selecionado.
Criado em	Data e hora em que a solicitação foi criada.
Data de início dos testes	Data e hora em que o teste começa.
Atualizado em	Data e hora em que a solicitação foi atualizada pela última vez.
Detalhes do teste	
URLs para teste	URLs que devem ser incluídos no teste de invasão.
URLs a serem excluídos	URLs que devem ser excluídos do teste de invasão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Essa aplicação já foi testada?	Especifica se esta aplicação já foi testada quanto à invasão.
Motivo para testar novamente	Motivo para solicitar uma reavaliação do teste de invasão se a aplicação foi testada anteriormente.
Quando a aplicação foi testada?	Intervalo de tempo em que a aplicação foi submetida a teste de invasão.
Detalhes da conta de teste	Detalhes da conta de teste que podem ser usados pela equipe de hackers éticos para testes de invasão.
Funções da aplicação	Funções compatíveis com a aplicação para seus usuários.
Funções mais usadas	Funções usadas com mais frequência na aplicação.

4. Selecione **Enviar**.
   Uma notificação por e-mail é enviada para a equipe de invasão ética de que a solicitação foi criada para a aplicação relevante.

Replicar uma solicitação de teste de invasão no estado encerrado

Crie uma solicitação de avaliação de teste de invasão replicando uma solicitação no estado Encerrado. Os itens vulneráveis da aplicação (IVAs) são copiados para a nova solicitação.

Antes de Iniciar

Função necessária: equipe de aplicações

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Solicitações de avaliação de teste de invasão** > **Todos**.
2. Selecione uma solicitação no estado Encerrado.
3. Selecione **Copiar e criar solicitação**.
   Uma nova solicitação é criada e os AVIs ativos são copiados para esta solicitação com dados atualizados. Para exibir o estado original dos AVIs da solicitação primária, navegue até a guia **Snapshot dos resultados do teste de invasão**.

Criar descobertas de testes de invasão com base em solicitações de avaliação (antes da v19.0)

Crie descobertas de teste de invasão com base na solicitação de avaliação de teste de invasão. Essas descobertas são itens de vulnerabilidade da aplicação (IVAs) criados manualmente.

Antes de Iniciar

Função necessária: Ethical Hacker

Procedimento

1. Navegar até **Todos** > **Autoatendimento** > **Catálogo de serviços** > **Serviços** > **Solicitações de avaliação de teste de invasão**.
2. Para criar um AVI para uma solicitação de avaliação de teste de invasão, selecione a solicitação relevante.
3. Na seção Itens vulneráveis da aplicação, selecione **Novo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. No formulário, preencha os campos.

Formulário de item vulnerável da aplicação (exibição do teste de invasão)

Campo	Descrição
Número	Identificador AVI gerado automaticamente para este registro.
Solicitação de avaliação	Solicitação de avaliação de teste de invasão à qual este AVI está associado.
Vulnerabilidade	Vulnerabilidade selecionada na tabela Entradas de vulnerabilidade usando a opção de pesquisa.
Pontuação de risco	**Pontuação de risco** quantificada que separa itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Calcular risco em Application Vulnerability Response automaticamente. A partir da V16.1, por padrão, o valor é igual à severidade da vulnerabilidade.
Impacta algum programa de conformidade?	Confirma se há um impacto em algum programa de conformidade. As opções são Sim e Não.
Lista de programas de conformidade afetados	Este campo é exibido quando o valor do campo "Afeta qualquer programa de conformidade" é definido como *Yes*. Lista os programas de conformidade afetados.
Versão planejada de liberação/correção	Liberar até quando as descobertas do teste de invasão devem ser resolvidas.
Estado	O valor padrão é **Aberto** quando o AVI é criado. Consulte Estados do item vulnerável da aplicação (IVA) para obter mais informações sobre como os estados são mapeados.
Grupo de atribuição	Grupo selecionado para trabalhar neste AVI. Pode ser adicionado ou editado manualmente por um gerente de App-Sec.
Atribuído a	Indivíduo do grupo de atribuição selecionado que trabalha neste AVI. Pode ser adicionado ou editado manualmente por um gerente de App-Sec.
Destino de correção	Data em que os AVIs devem ser corrigidos, desde a primeira identificação. Este campo é exibido somente quando aplicável. Para obter mais informações sobre destinos de correção, consulte Automatizar o acompanhamento de destino de correção no Application Vulnerability Response.
Criado em	Carimbo de data/hora de quando o item vulnerável da aplicação (IVA) foi criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Atualizado em	Carimbo de data/hora de quando o item vulnerável da aplicação (IVA) foi atualizado.
Aberto por	Usuário que criou esta descoberta de teste de invasão.
Contato da equipe de segurança	Ponto de contato na equipe de hacking ético.
Descrição resumida	Breve explicação da descoberta do teste de invasão.
Detalhes	
Detalhes técnicos	Detalhes técnicos da descoberta do teste de invasão.
Impact	Avaliação do impacto da descoberta do teste de invasão.
Etapas para reproduzir	Documente as etapas para reproduzir e revisar a descoberta do teste de invasão.
Recomendação	Registre as ações recomendadas neste campo.
Anotações	
Anotações de trabalho	Adicione anotações para comunicar informações sobre transições de estado e outras atualizações de campo.
V16.1: URLs afetados	Mais informações relacionadas aos URLs afetados.
V16.1: parâmetros afetados	Mais informações relacionadas aos parâmetros afetados.
V16.1: funcionalidades afetadas	Mais informações relacionadas às funcionalidades afetadas.

5. Para salvar o formulário, selecione **Enviar**.

Criar uma entrada de vulnerabilidade da aplicação

Crie uma entrada de vulnerabilidade da aplicação para a vulnerabilidade especificada para a descoberta do teste de invasão. As vulnerabilidades da aplicação são vulnerabilidades nas aplicações de software personalizadas.

Antes de Iniciar

Função necessária: Ethical Hacker

Por Que e Quando Desempenhar Esta Tarefa

Application Vulnerability Response relaciona uma vulnerabilidade a uma aplicação para criar a descoberta do teste de invasão. Essas descobertas são itens vulneráveis da aplicação (IVAs) criados manualmente. Você pode reutilizar uma entrada existente ou criar uma manualmente para cada vulnerabilidade durante o teste de invasão.

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Bibliotecas** > **Terceiros**.
2. Na página Entradas de vulnerabilidade da aplicação, selecione **Novo**.
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de entrada de vulnerabilidade da aplicação (exibição do teste de invasão)

Campo	Descrição
ID	Identificador desta entrada de vulnerabilidade.
Gravidade	Grau normalizado de severidade desta vulnerabilidade. Mapas de severidade são fornecidos para NVD e com integrações de terceiros da ServiceNow. Para obter mais informações sobre como criar ou ajustar mapas de severidade, consulte Mapear a severidade de um item vulnerável da aplicação automaticamente.
CVE primário	Referência ao elemento de Enumeração de Pontos Fracos Comuns no qual esta vulnerabilidade melhor se encaixa.
Nome da categoria	Classificação fornecida pela integração de terceiros. Auxilia na atribuição.
Detalhes da Vulnerabilidade	
Vetor de ataque	Vetor de ataque mais vulnerável para esta vulnerabilidade.
Complexidade de ataque	Métrica que descreve as condições fora do controle do invasor que devem existir para explorar a vulnerabilidade.
Escopo	Métrica para medir a capacidade de uma vulnerabilidade de software de afetar os recursos além de seus recursos.
Integridade	Métrica para medir o impacto na integridade de uma vulnerabilidade explorada com sucesso.
Vetor CVSS	Estrutura aberta para capturar as características e a severidade das vulnerabilidades do software.
Privilégios necessários (PN):	Nível de privilégios que um invasor deve possuir antes de explorar a vulnerabilidade com êxito.
Interação do usuário	Requisito de interação humana para explorar uma vulnerabilidade com sucesso.
Confidencialidade	Impacto na confidencialidade dos recursos de informação devido a uma vulnerabilidade explorada com sucesso. Esses recursos são gerenciados por um componente de software.
Disponibilidade	Impacto na disponibilidade do componente afetado resultante de uma vulnerabilidade explorada com sucesso.
Pontuação base de CVSS	Representação numérica (0-10) da severidade de uma entrada de vulnerabilidade da aplicação.
Ameaça	Descrição da ameaça desta vulnerabilidade.
Descrição da mitigação	Descrição das etapas para atenuar a vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Para salvar o formulário, selecione **Enviar**.

Nota:
Os AVEs são criados na tabela Entrada de vulnerabilidade da aplicação (sn_vul_app_vul_entry). A tabela de entrada de vulnerabilidade da aplicação é secundária da tabela de entrada de vulnerabilidade (*sn_vul_entry*). Portanto, os AVEs criados também são adicionados à tabela de entrada de vulnerabilidade.

Soluções Análise da plataforma para Application Vulnerability Response

Soluções Análise da plataforma contêm conteúdo Platform Analytics] pré-empacotado para uso com outros produtos Now Platform. Este Solução Análise da plataforma apresenta métricas importantes para analisar seu processo de Gestão de vulnerabilidades de aplicações.

Visão geral

O pacote de conteúdo do Performance Analytics para Vulnerability Response está disponível em ServiceNow® Store como uma assinatura separada. A aplicação não é instalada automaticamente com a aplicação Vulnerability Response. O pacote de conteúdo do Application Vulnerability Response faz parte do pacote de conteúdo do Performance Analytics para Vulnerability Response.

Para obter mais informações sobre como instalar e configurar a aplicação Performance Analytics for Vulnerability Response, consulte Instalar e configurar a aplicação Performance Analytics for Vulnerability Response [PA].

Termos-chave

Performance Analytics (PA)

Solução que cria painéis de gestão, relatórios sobre KPIs e métricas e responde às principais perguntas de negócios para ajudar a aumentar a qualidade e reduzir custos.

Item vulnerável da aplicação (IVA)

Uma vulnerabilidade da aplicação relatada por um scanner de vulnerabilidade de terceiros que está presente em um item de configuração (IC).

Indicador de PA

Define uma medição de desempenho feita em intervalos regulares de uma atividade ou comportamento organizacional, por exemplo, as 10 principais aplicações com os itens vulneráveis de aplicação mais críticos.

Origem do indicador de PA

Conjuntos de dados que filtram registros de uma tabela ou exibição de banco de dados, por exemplo, AVI ativo.

- O painel Minhas vulnerabilidades da aplicação rastreia o volume, o desempenho e o andamento das vulnerabilidades da aplicação, desde a análise/detecção inicial até a contenção ou correção.
- Exiba as taxas de cumprimento da meta de correção e determine com eficiência quais itens vulneráveis da aplicação (IVAs) apresentam mais risco para sua organização.

Funções necessárias

As seguintes funções e tarefas estão associadas a esta Solução:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Now Platform administrador (admin): instale e ative esta Solução de análise e relatório e faça as mudanças necessárias nas propriedades do sistema.
- Performance Analytics Administrador (pa_admin): revise os indicadores, detalhamentos, widgets e painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.

Os painéis a seguir fornecem uma exibição gráfica da atividade do AVI para ajudar a determinar os planos de correção e o andamento do status. Você pode se concentrar nos KPIs associados a aplicações críticas afetadas e vulnerabilidades de alta visibilidade.

- O painel do Application Vulnerability Management (PA) comunica os KPIs de risco e predominância de vulnerabilidade, aplicações afetadas, tendências de correção e andamento da correção. O padrão para tendências é três meses, mas pode ser alterado para 7 dias, um mês, 3 meses, 6 meses, acumulado no ano, 1 ano ou Todos.
- O painel Minhas vulnerabilidades da aplicação rastreia o volume, o desempenho e o andamento das vulnerabilidades da aplicação, desde a análise/detecção inicial até a contenção ou correção.

Nota:
O painel Minhas vulnerabilidades da aplicação é um subconjunto do painel Visão geral e só está disponível quando um membro do grupo de usuários do Campeão de segurança faz login em uma instância. Para obter mais informações sobre o painel Minhas vulnerabilidades da aplicação, consulte Meu painel Vulnerabilidades da aplicação.

Gerenciamento de vulnerabilidade de aplicação Painel (PA)

Rastreie o volume, o desempenho e o andamento das vulnerabilidades da aplicação, desde a análise e detecção iniciais até a contenção ou correção.

Casos de uso

Usuário	Uso do painel
Gerenciadores de vulnerabilidade	Com o painel Gerenciamento de vulnerabilidade de aplicação, a gestão de vulnerabilidades pode determinar quais itens vulneráveis da aplicação (IVAs) apresentam mais risco para suas organizações. Esses painéis fornecem uma exibição gráfica da atividade do AVI para ajudá-los a determinar os planos de correção e o andamento do status. Concentre-se nos KPIs associados a aplicações críticas afetadas e vulnerabilidades de alta visibilidade.

Obrigatório Now Platform funções, configuração e guias do painel

O painel do Application Vulnerability Management (PA) está incluído como parte do pacote de conteúdo do Performance Analytics para Vulnerability Response. O pacote de conteúdo do Performance Analytics para Vulnerability Response não é instalado automaticamente

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

com a aplicação Vulnerability Response. Ele está disponível no ServiceNow® Store como uma assinatura separada.

Para obter mais informações sobre como instalar e configurar a aplicação Performance Analytics for Vulnerability Response, consulte Instalar e configurar a aplicação Performance Analytics for Vulnerability Response [PA].

Para exibir o painel, como um usuário atribuído aos grupos de usuários do Campeão de Segurança, Gerente de App-Sec ou Desenvolvedor, navegue até **Application Vulnerability Response** > **Visão geral**.

Nota:
O painel Minhas vulnerabilidades da aplicação é um subconjunto do painel Visão geral e só está disponível quando um membro do grupo de usuários do Campeão de segurança faz login em uma instância. Para obter informações sobre o painel Minhas vulnerabilidades da aplicação, consulte Meu painel de vulnerabilidades da aplicação.

A partir da versão 19.0 do Application Vulnerability Response, este painel também pode ser exibido na IU da nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique no ícone**Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Visão geral dos painéis e Visão geral dos painéis.

O painel Visão geral comunica os KPIs de risco de vulnerabilidade e predominância, aplicações afetadas, tendências de correção e andamento da correção. O padrão para tendências é três meses, mas pode ser alterado para 7 dias, um mês, 3 meses, 6 meses, acumulado no ano, 1 ano ou Todos.

Detalha os dados no painel Gerenciamento de vulnerabilidade de aplicação por **tipo de verificação**, **aplicação** ou **unidade de negócios**. Cada uma dessas opções tem um filtro adicional, **Selecionar elementos**, para refinar suas seleções. A partir de Application Vulnerability Response v15.0, as aplicações de negócios e de IC foram adicionadas às opções do filtro **Aplicação**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

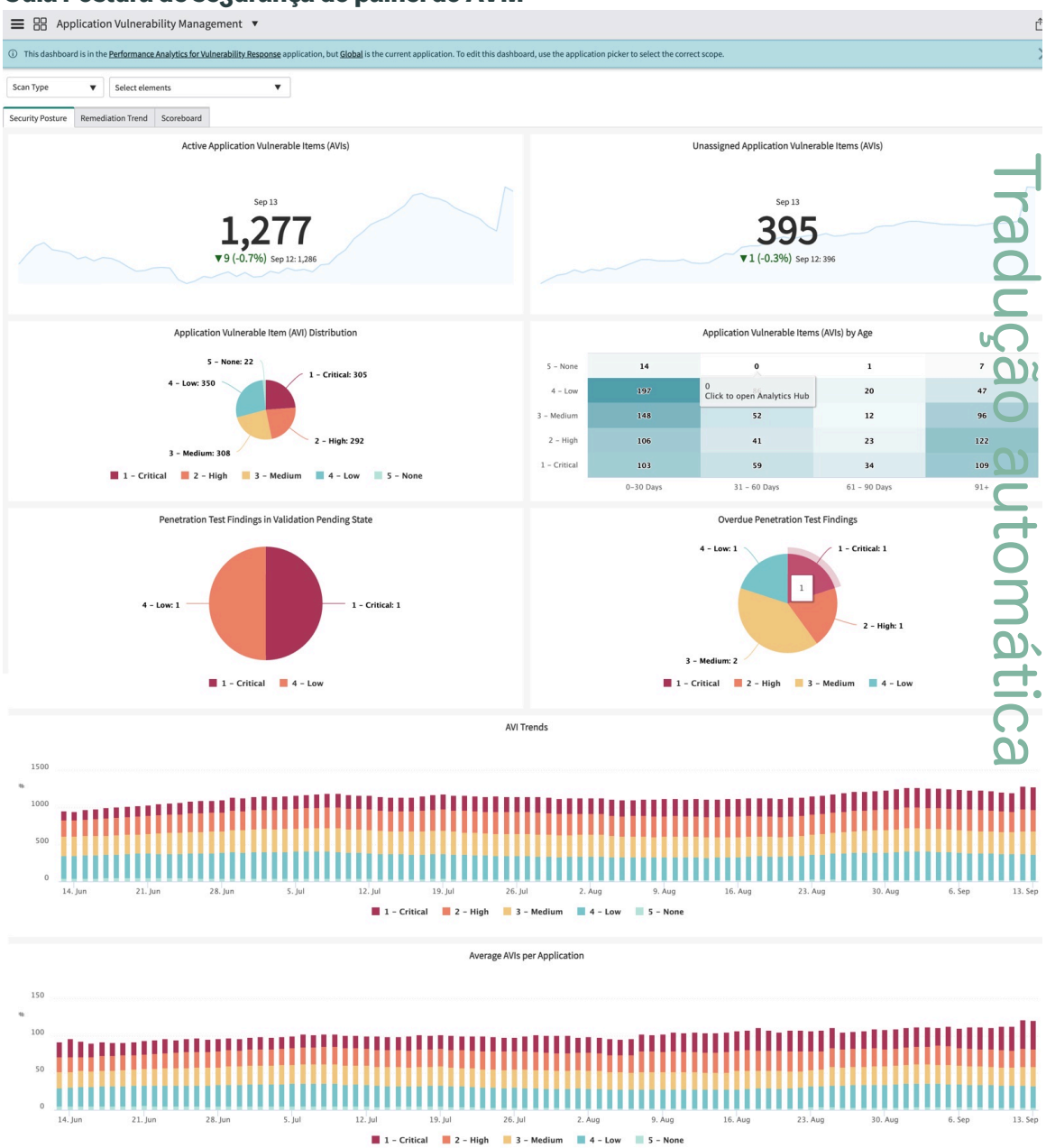
Guia Postura de segurança

A guia Postura de segurança ajuda a entender sua postura de segurança e o andamento de suas ações de correção.

A partir de Application Vulnerability Response v15.0, você pode exibir os relatórios de descobertas do teste de invasão. As descobertas do teste de invasão são itens vulneráveis de aplicação (IVAs) que são criados manualmente com base nas solicitações de avaliação do teste de invasão.

Nota:
O tipo de verificação desses widgets é Manual.

Guia Postura de segurança do painel do AVM

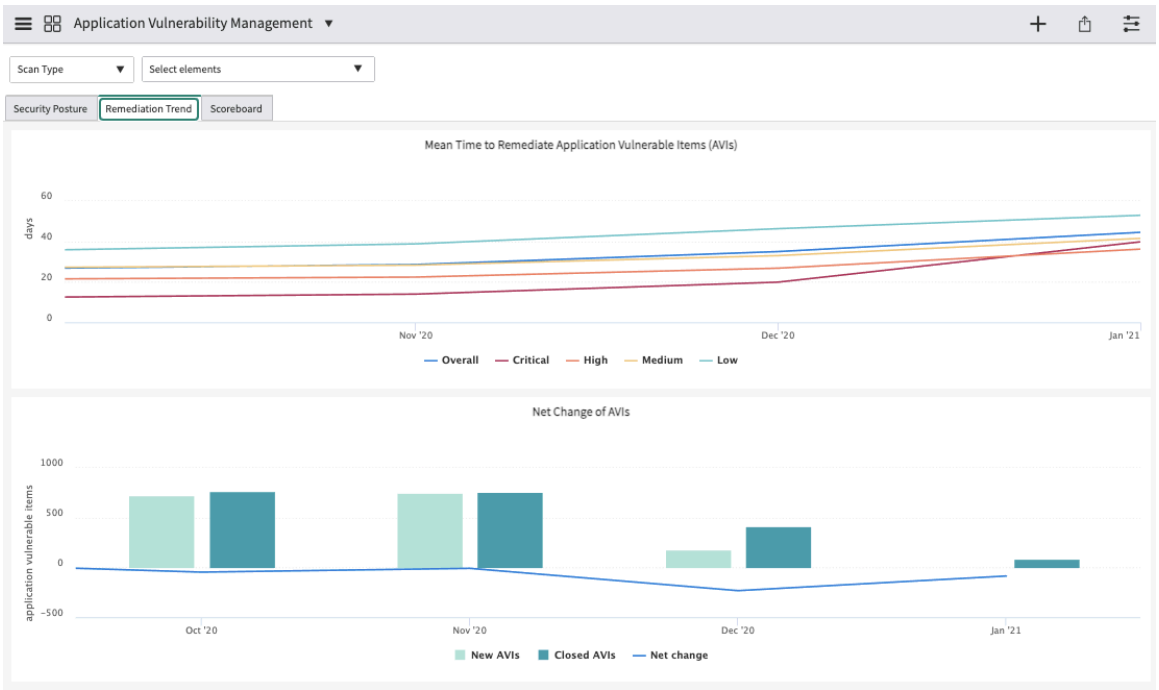


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Tendência de correção

A guia Tendência de correção ajuda a entender o andamento das ações de correção.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

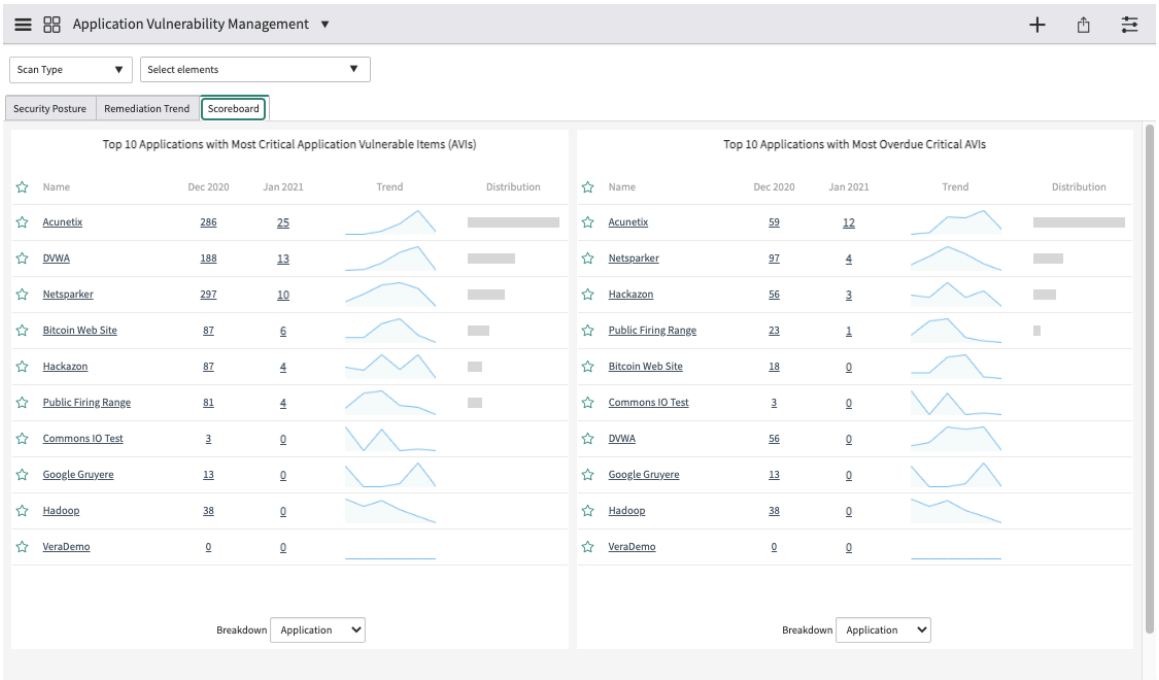
Guia Quadro de pontuação

A guia Painel de pontuação ajuda a entender o andamento das suas ações de correção e quais AVIs precisam de mais assistência para concluí-las.

Elementos do tipo de verificação:

- Dinâmico: use somente métricas da importação de dados dinâmicos
- Estático: use somente métricas da importação de dados estáticos

Você pode escolher um ou ambos.



Indicadores

Tempo médio para corrigir IVAs baixos

[[Soma da duração dos itens vulneráveis da aplicação encerrados > Classificação de risco = 4 - Baixo]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco = 4 - Baixo]]. O objetivo é minimizar.

Versões da aplicação

É a contagem em aplicações distinta de AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação

É a contagem de itens de vulnerabilidade do app AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

IVAs médios por aplicação

[Itens vulneráveis da aplicação ativos]] / [[Versões da aplicação]]. O objetivo é minimizar.

IVs não atribuídos

É a contagem na origem do indicador AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Tempo médio para corrigir IVAs

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

[[Soma da duração dos itens vulneráveis da aplicação encerrados]] / [[Itens vulneráveis da aplicação encerrados]]. O objetivo é minimizar.

Tempo médio para corrigir IVAs altos

[[Soma da duração dos itens vulneráveis da aplicação encerrados > Pontuação de risco = 2 - Alto]] / [[Itens vulneráveis da aplicação encerrados > Pontuação de risco = 2 - Alto]]. O objetivo é minimizar.

Itens vulneráveis da aplicação encerrados

É a contagem na origem do indicador AVI.Closed, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é maximizar.

Tempo médio para corrigir IVAs críticos

[[Soma da duração dos itens vulneráveis da aplicação encerrados > Classificação de risco = 1 - Crítico]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco = 1 - Crítico]]. O objetivo é minimizar.

Novos itens vulneráveis da aplicação

É a contagem na origem do indicador AVI.New, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Tempo médio para corrigir IVAs médios

[[Soma da duração dos itens vulneráveis da aplicação encerrados > Pontuação de risco = 3 - Médio]] / [[Itens vulneráveis da aplicação encerrados > Pontuação de risco = 3 - Médio]]. O objetivo é minimizar.

Mudança líquida em IVs

[[Novos itens vulneráveis da aplicação]] - [[Itens vulneráveis da aplicação encerrados]]. O objetivo é minimizar.

Soma da duração de itens vulneráveis da aplicação encerrados

É a contagem na origem do indicador AVI.Closed, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação atrasados críticos

É a contagem na fonte de dados AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação críticos

É a contagem nas aplicações de origem do indicador com AVIs ativos, que está usando a tabela: sn_vul_analytics_app_ci_dept_bu. O objetivo é minimizar.

Detalhamentos

- Idade
- Momento do fechamento
- Aplicação
- Unidade de Negócios
- Pontuação de risco
- Tipo de Verificação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações de dados

Postura de segurança

Nome	Tipo	Descrição
V15.0: descobertas do teste de invasão no estado de validação pendente	Gráfico	Descobertas do teste de invasão no estado Resolvido, mas com validação pendente, agrupadas por classificação de risco.
V15.0: resultados de testes de invasão atrasados	Gráfico	Descobertas críticas do teste de invasão que não atingiram a data de meta de correção, agrupadas por classificação de risco.
Itens vulneráveis de aplicação (IVAs) ativos	Pontuação	Número de itens vulneráveis da aplicação ativos (não encerrados).
Itens vulneráveis de aplicação (IVAs) não atribuídos	Pontuação	Número de itens vulneráveis de aplicação (IVAs) sem um designado ou grupo de atribuição.
Distribuição de item vulnerável da aplicação (IVA)	Gráfico	Distribuição de todos os itens vulneráveis de aplicação (IVAs) agrupados por avaliação de risco.
Itens vulneráveis de aplicação (IVAs) por idade	Mapa térmico	Número de itens vulneráveis da aplicação (IVAs) agrupados por classificação de risco e idade (em dias).
Tendências de IVA	de tendências	Tendência de todos os itens vulneráveis da aplicação (IVAs) ativos agrupados por avaliação de risco.
IVAs médios por aplicação	de tendências	Tendência dos itens vulneráveis de aplicação (IVAs) por aplicação, agrupado pela avaliação de risco.

Tendência de correção

Nome	Tipo	Descrição
Tempo médio para corrigir itens vulneráveis da aplicação (IVAs)	Linha de linha	Tendência do tempo médio de correção dos itens vulneráveis da aplicação (IVAs) por classificação de risco.
Mudança líquida de AVIs	Ícone de	Tendência de novos itens vulneráveis da aplicação (AVIs) detectados versus encerrados por mês.

Placar

Nome	Tipo	Descrição
10 principais aplicações com itens vulneráveis da aplicação (IVAs) mais críticos	Cartão de pontuação e barra de distribuição de cartão de pontuação Ícone de distribuição	Aplicações com o número maior de itens vulneráveis da aplicação (IVAs).
10 principais aplicações com itens vulneráveis de aplicação (IVAs) mais atrasados	Cartão de pontuação e barra de distribuição de cartão de pontuação Ícone de distribuição	Aplicações com o maior número de itens vulneráveis de aplicação (IVAs) que já passaram das datas de destino de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Meu painel de vulnerabilidades da aplicação

Este painel apresenta métricas importantes para analisar o processo do Application Vulnerability Management, como a exibição das taxas de cumprimento da meta de correção.

Now Platform funções necessárias e exibição do painel

Nota:

- Este painel faz parte do pacote de conteúdo do Application Vulnerability Response. O pacote de conteúdo do Application Vulnerability Response faz parte do pacote de conteúdo do Performance Analytics para Vulnerability Response.
- O pacote de conteúdo do Performance Analytics para Vulnerability Response está disponível em ServiceNow® Store como uma assinatura separada.
- O pacote de conteúdo do Performance Analytics para Vulnerability Response não é instalado automaticamente com a aplicação Vulnerability Response.

O painel Minhas vulnerabilidades da aplicação está disponível somente quando um membro do grupo de usuários do Campeão de segurança faz login em uma instância. Para obter informações sobre o painel Visão geral, consulte Painel Application Vulnerability Management [PA].

Para exibir o painel, navegue até **Application Vulnerability Response** > **Minhas vulnerabilidades de aplicações**.

A partir da versão 19.0 do Application Vulnerability Response, este painel também pode ser exibido na IU da nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique no ícone**Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Visão geral dos painéis e Visão geral dos painéis.

Exiba relatórios que mostram dados de tendências ao longo do tempo. Exiba tendências de métricas importantes em uma programação regular para analisar seus processos de negócios gerais e identificar áreas de melhoria.

O painel de vulnerabilidades das minhas aplicações está incluído no pacote de conteúdo do Performance Analytics para Vulnerability Response. O pacote de conteúdo do Performance Analytics para Vulnerability Response não é instalado automaticamente com a aplicação Vulnerability Response. Ele está disponível no ServiceNow® Store como uma assinatura separada.

Casos de uso

Usuário	Uso do painel
Especialistas em TI, responsáveis pela correção ou analistas que corrigem vulnerabilidades atribuídas a eles ou a um grupo ao qual pertencem.	Um campeão de segurança usa o painel Minhas vulnerabilidades da aplicação para rastrear o volume, o desempenho e o andamento da correção das vulnerabilidades da aplicação. Determine com eficiência quais itens vulneráveis de aplicação (IVAs) apresentam mais risco para sua organização.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usuário	Uso do painel
	Esses painéis fornecem uma exibição gráfica da atividade do AVI para ajudar a determinar os planos de correção e o andamento do status. Você pode se concentrar nos KPIs associados a aplicações críticas afetadas e vulnerabilidades de alta visibilidade. Obtenha rapidamente informações sobre sua exposição a vulnerabilidades e postura de segurança. Rastreie desde a análise inicial e detecção até a contenção ou correção.

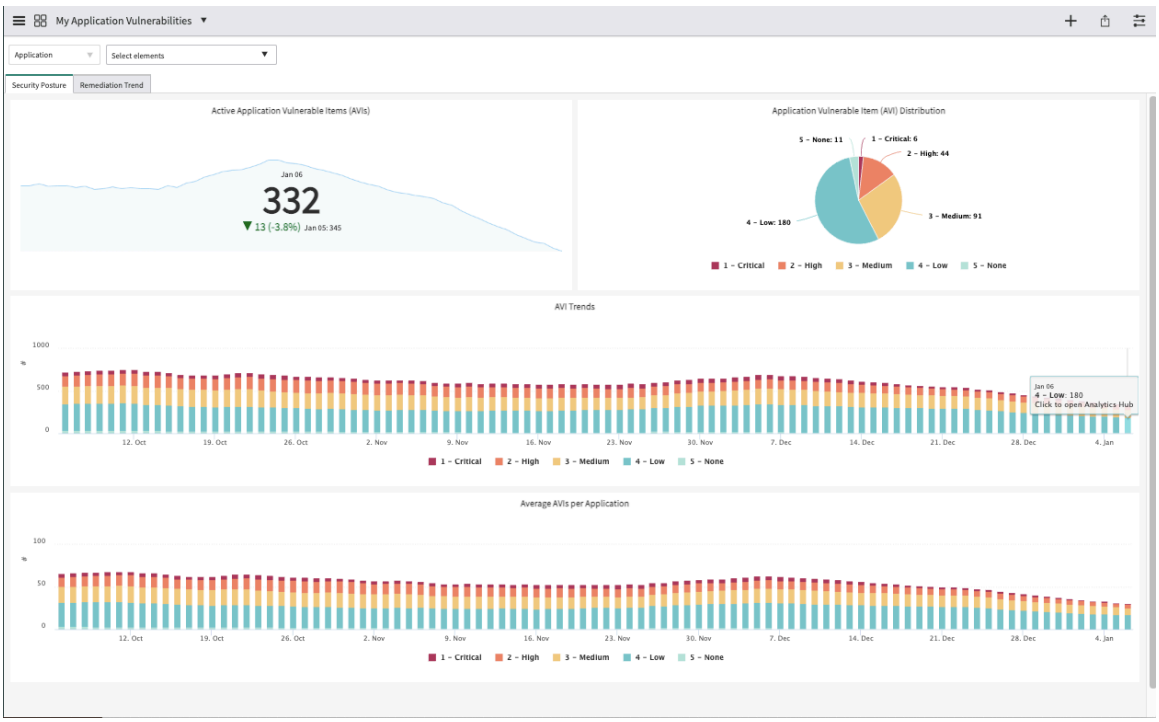
Guias do meu painel Vulnerabilidades da aplicação [PA]

O painel Minhas vulnerabilidades da aplicação comunica os KPIs de risco e predominância de vulnerabilidade, aplicações afetadas, tendências de correção e andamento da correção. O padrão para tendências é três meses, mas pode ser alterado para 7 dias, um mês, 3 meses, 6 meses, acumulado no ano, 1 ano ou Todos.

Os dados são divididos no painel por **Aplicação**. Use a lista **Selecionar elementos** para refinar suas seleções.

Guia Postura de segurança

A guia Postura de segurança ajuda a entender sua postura de segurança e o andamento de suas ações de correção. Detalha os dados no painel do Application Vulnerability Management por **tipo de verificação, aplicação** ou **unidade de negócios**. Cada uma dessas opções tem um filtro adicional, **Selecionar elementos**, para refinar suas seleções.

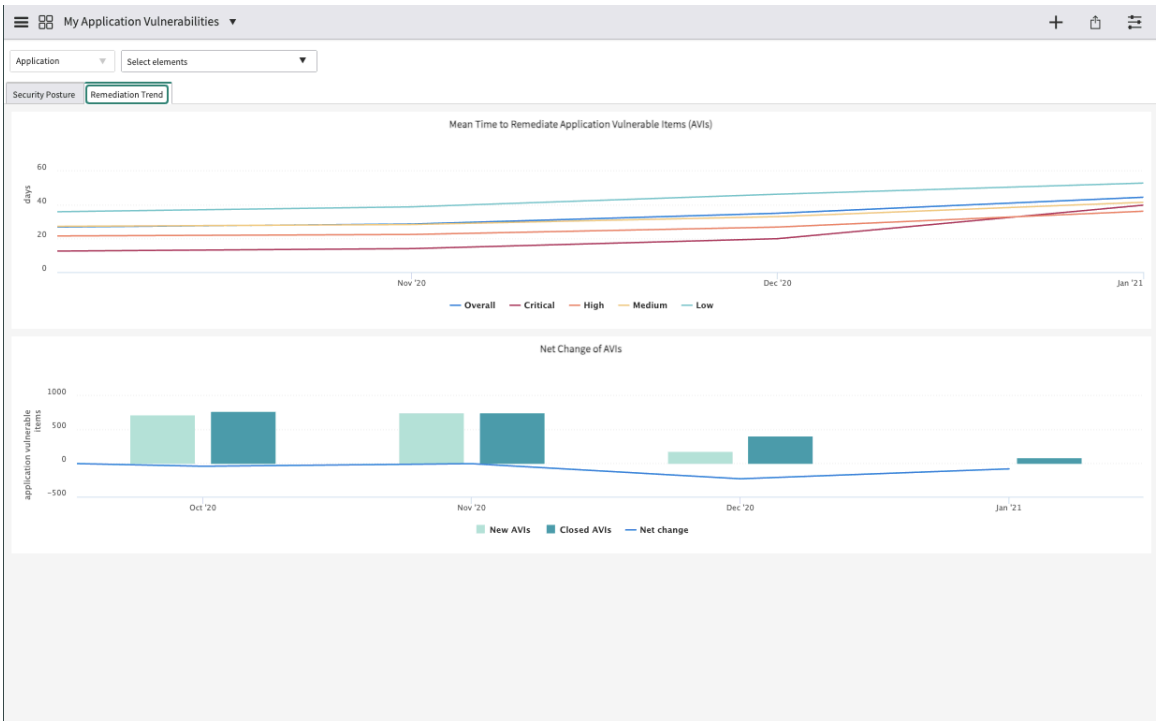


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Tendência de correção

A guia Tendência de correção ajuda a entender o andamento das ações de correção.



Indicadores

Tempo médio para corrigir IVAs baixos

[[Soma da duração dos itens vulneráveis da aplicação encerrados > Classificação de risco = 4 - Baixo]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco = 4 - Baixo]]. O objetivo é minimizar.

Versões da aplicação

É a contagem em aplicações distinta de AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação

É a contagem de itens de vulnerabilidade do app AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

IVAs médios por aplicação

[Itens vulneráveis da aplicação ativos]] / [[Versões da aplicação]]. O objetivo é minimizar.

IVs não atribuídos

É a contagem na origem do indicador AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Tempo médio para corrigir IVAs

[[Soma da duração dos itens vulneráveis da aplicação encerrados]] / [[Itens vulneráveis da aplicação encerrados]]. O objetivo é minimizar.

Tempo médio para corrigir IVAs altos

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

[[Soma da duração dos itens vulneráveis da aplicação encerrados > Pontuação de risco = 2 - Alto]] / [[Itens vulneráveis da aplicação encerrados > Pontuação de risco = 2 - Alto]]. O objetivo é minimizar.

Itens vulneráveis da aplicação encerrados

É a contagem na origem do indicador AVI.Closed, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é maximizar.

Tempo médio para corrigir IVAs críticos

[[Soma da duração dos itens vulneráveis da aplicação encerrados > Classificação de risco = 1 - Crítico]] / [[Itens vulneráveis da aplicação encerrados > Classificação de risco = 1 - Crítico]]. O objetivo é minimizar.

Novos itens vulneráveis da aplicação

É a contagem na origem do indicador AVI.New, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Tempo médio para corrigir IVAs médios

[[Soma da duração dos itens vulneráveis da aplicação encerrados > Pontuação de risco = 3 - Médio]] / [[Itens vulneráveis da aplicação encerrados > Pontuação de risco = 3 - Médio]]. O objetivo é minimizar.

Mudança líquida em IVs

[[Novos itens vulneráveis da aplicação]] - [[Itens vulneráveis da aplicação encerrados]]. O objetivo é minimizar.

Soma da duração de itens vulneráveis da aplicação encerrados

É a contagem na origem do indicador AVI.Closed, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação atrasados críticos

É a contagem na fonte de dados AVI.Active, que está usando a tabela: sn_vul_app_vulnerable_item. O objetivo é minimizar.

Itens vulneráveis da aplicação críticos

É a contagem nas aplicações de origem do indicador com AVIs ativos, que está usando a tabela: sn_vul_analytics_app_ci_dept_bu. O objetivo é minimizar.

Detalhamentos

- Idade
- Momento do fechamento
- Aplicação
- Unidade de Negócios
- Pontuação de risco
- Tipo de Verificação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações de dados

Postura de segurança

Nome	Tipo	Descrição
Itens vulneráveis de aplicação (IVAs) ativos	Pontuação	Número de itens vulneráveis da aplicação ativos (não encerrados).
Distribuição de item vulnerável da aplicação (IVA)	Gráfico	Distribuição de todos os itens vulneráveis de aplicação (IVAs) agrupados por avaliação de risco.
Tendências de IVA	de tendências	Tendência de todos os itens vulneráveis da aplicação (IVAs) ativos agrupados por avaliação de risco.
IVAs médios por aplicação	de tendências	Tendência dos itens vulneráveis de aplicação (IVAs) por aplicação, agrupado pela avaliação de risco.

Tendência de correção

Nome	Tipo	Descrição
Tempo médio para corrigir itens vulneráveis da aplicação (IVAs)	Linha de linha	Tendência do tempo médio de correção dos itens vulneráveis da aplicação (IVAs) por classificação de risco.
Mudança líquida de AVIs	Ícone de	Tendência de novos itens vulneráveis da aplicação (AVIs) detectados versus encerrados por mês.

referências de Application Vulnerability Response

Tópicos de referência que contêm informações sobre tabelas, funções e propriedades instaladas com a aplicação Application Vulnerability Response.

Para obter detalhes, consulte:

- Application Vulnerability Response grupos de usuários e funções
- Componentes instalados com Application Vulnerability Response
- Estados do item vulnerável da aplicação (IVA)
- Campos da aplicação verificados
- Campos de item vulnerável da aplicação
- Campos de vulnerabilidade da aplicação
- Estados do teste de invasão

Application Vulnerability Response grupos de usuários e funções

Antes de corrigir vulnerabilidades com Application Vulnerability Response (AVR), você deve atribuir usuários a grupos de usuários.

As funções definem o que você e seus grupos podem ver e fazer em Application Vulnerability Response, Performance Analytics para Vulnerability Responsee integrações de terceiros com Application Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Grupos de usuários

A seguir estão os grupos de usuários padrão que oferecem suporte a Application Vulnerability Response:

- App-Sec Manager: contém gerenciadores de segurança. A partir de Application Vulnerability Response v15.0, ele também conterá responsáveis pela aplicação que gerenciam as solicitações de avaliação de teste de invasão.
- Campeão de segurança: contém ligações entre o grupo de desenvolvimento e os gerentes de segurança.
- Desenvolvedor: contém colaboradores individuais.
- V15.0: Ethical Hacker: contém membros da equipe de hackers éticos que realizam testes de invasão de aplicações.

A função de administrador do sistema [admin] é necessária para atribuir usuários aos grupos de usuários padrão Application Vulnerability Response usando o módulo Administração de usuários.

Nota:

A atribuição de usuários de AVR aos grupos de usuários Application Vulnerability Response para Application Vulnerability Response não está disponível no recurso Assistente de configuração Vulnerability Response. Somente Vulnerability Response funções são atribuídas lá.

A tabela a seguir lista os grupos de usuários Application Vulnerability Response disponíveis e as funções associadas a eles. Use esta tabela para determinar quais usuários devem ser atribuídos a quais grupos.

Grupo de Usuários	Funções neste grupo
Campeão de segurança Os membros deste grupo podem: • Ler e gravar itens vulneráveis da aplicação (AVIs) atribuídos a você. • Atribua um AVI atribuído a você a outro indivíduo ou grupo. • V20.0: criar, atualizar, excluir e cancelar (desativar) regras de exceção.	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_manage_auto_exception_rule
Gerente App-Sec Os membros deste grupo podem: • V20.0: criar, atualizar, excluir e cancelar (desativar) regras de exceção. • Ler, gravar, excluir e todas as operações nas regras de tarefa de correção da aplicação. • Ler e gravar todos os AVIs.	• sn_vul.app_manage_auto_exception_rule • sn_vul.app_manage_group_rules • sn_vul.app_read_all • sn_vul.app_write_all • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_configure_integrations

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Grupo de Usuários	Funções neste grupo
• Configure o AVR criando e gerenciando regras, calculadoras e mapas de severidade. • Configurar integrações. • Exclua AVIs. • Atribua AVI a indivíduos ou grupos. • Gerenciar aplicações. • Permite acesso ao módulo Aplicação. • Programe, configure e execute a integração. • Ler e executar integrações. • Exiba painéis e relatórios de AVR Performance Analytics. • V15.0: gerencie solicitações de avaliação de teste de invasão.	**Nota:** Por padrão, esta função contém funções granulares para configuração de integração de terceiros. Para definir ou editar um grupo de usuários do App-Sec Manager por integrações únicas ou específicas, consulte Vulnerability Response personas e funções granulares. • sn_vul.app_manage_assignment_rules • sn_vul.app_manage_remediation_target_rules • sn_vul.app_manage_risk_score_configurations • sn_vul.app_manage_applications • sn_vul.app_manage_app_vul_permissions • sn_vul.app_manage_normalized_severity • Versão 13.0: sn_vul.app_manage_app_sc • Somente versão 12.0: sn_vul.app_read_application_release [Removido em v12.1. Não use] • sn_sec_int.admin • Versão 13.0: pa_power_user • pa_viewer **Nota:** A partir da Vulnerability Response v13.0, o pa_viewer está incluído no pa_power_user e não é mais necessário sozinho. • V15.0: sn_vul.app_manage_pen_test_request • V15.0: sn_vul.app_update_state • V15.0: cmdb_read
Desenvolvedor Os membros deste grupo podem: • Ler e gravar registros AVR atribuídos a você. • Atribua um AVI atribuído a você a outro indivíduo ou grupo.	• sn_vul.app_read_assigned • sn_vul.app_write_assigned • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_pa_sc_view

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Grupo de Usuários	Funções neste grupo
V15.0: hacker ético Os membros deste grupo podem: • Configure o grupo de atribuição padrão e o designado para solicitações de avaliação de teste de invasão. • Gerenciar as descobertas do teste de invasão. • Gerenciar solicitações de avaliação de teste de invasão. • Exibir itens vulneráveis da aplicação. • Atualize a atribuição de itens vulneráveis da aplicação.	• V15.0: sn_vul.app_update_state • V15.0: sn_vul.app_manage_pen_test_request • V15.0: itil • V15.0: sn_vul.app_read_all • V15.0: sn_vul.app_manage_pen_test_request_config • V15.0: sn_vul.app_manage_manual_avits • V15.0: sn_vul.app_update_assigned_to • V15.0: sn_vul.app_update_assignment_group

Atribuir usuários a grupos de usuários no Application Vulnerability Response

Atribua usuários a grupos usando o módulo Administração de usuários em sua instância.

Antes de Iniciar
Função necessária: administrador

Procedimento

Para atribuir ou remover um usuário de um grupo:

a. Navegar até **Administração** > **Grupos**.

b. Localize e abra o grupo apropriado, por exemplo, **App-Sec Manager**.
O registro do grupo é exibido.

c. Selecione a guia **Membros do grupo**.
Os membros atuais do grupo são exibidos.

d. Clique em **Editar**.
O formulário Editar membros é exibido.

e. Na lista **Coleção**, selecione usuários para adicionar ou remover do grupo.

f. Depois que todos os usuários tiverem sido adicionados à **Lista de Membros do Grupo** ou removidos, clique em **Salvar**.
Você retornará à guia **Membros do grupo**.

g. Clique em **Atualizar** para salvar suas mudanças e retornar à lista Grupos.

Tópicos relacionados

Componentes instalados com Application Vulnerability Response

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Componentes instalados com Application Vulnerability Response

Vários tipos de componentes são instalados com a ativação do recurso Application Vulnerability Response, incluindo tabelas, funções de usuário e trabalhos programados.

Nota:
A tabela Arquivos da Aplicação lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

Funções instaladas

Funções granulares em Application Vulnerability Response são atribuídas a grupos de usuários específicos, por padrão.

Nota:
O uso de funções granulares fora desses grupos de usuários requer codificação e conhecimento avançado Application Vulnerability Response ou ServiceNow.

Título da função [nome]	Descrição	Contém as funções
V20.0: sn_vul.app_manage_auto_exception_rule	Crie, atualize, exclua e cancele (desative) regras de exceção.	sn_vul.app_read_auto_exception_rule
sn_vul.app_manage_group_rules	Ler, gravar, excluir e todas as operações nas regras de tarefa de correção da aplicação.	• sn_vul.app_read_all • sn_vul.app_read_group_rules
V20.0: sn_vul.app_exception_approver	Aprova regras de exceção e solicitações de extensão de regra de exceção. A partir da v20.0, a função granular, sn_vul.app_read_all, foi removida desta função para que você possa acessar os itens vulneráveis da aplicação e as tarefas de correção atribuídos a você e seu grupo, em vez de todos os itens vulneráveis da aplicação e tarefas de correção.	sn_vul.app_read_auto_exception_rule
sn_vul.app_read_assigned	Exibir itens vulneráveis da aplicação (IVAs) atribuídos a você.	
sn_vul.app_read_all	Exibir todos os AVIs e informações relacionadas.	
sn_vul.app_write_assigned	Atualize os AVIs atribuídos a você.	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
sn_vul.app_write_all	Atualize todos os AVIs e informações relacionadas.	
sn_vul.app_update_assignment_group	Atualize o grupo de atribuição de AVI.	**Nota:** Quando usado fora do grupo de usuá padrão, requer sn_vul.app_write_all sn_vul.app_write_assigned.
sn_vul.app_update_assigned_to	Atualizar designado de AVI.	**Nota:** Quando usado fora do grupo de usuá padrão, requer sn_vul.app_write_all sn_vul.app_write_assigned.
sn_vul.app_configure_integrations	Configure integrações de terceiros.	sn_vul.app_read_all sn_vul.app_read_integrations sn_sec_int.admin sn_vul_veracode.configure_integra sn_vul.configure_nvd_administratio [store-future: BEGIN review]sn_vul_fortify.configure_int **Nota:** Para definir ou editar um grupo de us App-Sec Manager por integrações úr específicas, consulte Vulnerability R personas e funções granulares.
sn_vul.app_read_integrations	Exibir todas as integrações de terceiros.	
sn_vul_veracode.configure_integration	Defina, atualize e exclua integrações do Veracode.	
sn_vul.app_manage_assignment_rules	Defina, atualize e exclua regras de atribuição de AVI.	sn_vul.app_read_all sn_vul.app_read_assignment_rules
sn_vul.app_read_assignment_rules	Exibir regras de atribuição.	
sn_vul.app_manage_remediation_target_rules	Defina, atualize e exclua regras de destino de correção de AVI.	sn_vul.app_read_all sn_vul.app_read_remediation_targ
sn_vul.app_manage_risk_score_configurations	Defina, atualize e exclua calculadoras AVR e regras de risco.	sn_vul.app_read_all sn_vul.app_read_risk_score_config

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
		sn_sec_cmn.calcul.write
sn_vul.app_read_risk_score_configuration	Exibir calculadoras AVR e regras de risco.	
sn_vul.app_manage_applications	Exiba, atualize e exclua registros da aplicação.	
sn_vul.app_manage_app_sc	Concede a um campeão de segurança a capacidade de adicionar ou remover a si mesmo da lista relacionada de aplicações verificadas.	
sn_vul.app_pa_sc_view	Fornece exibição relevante para o campeão de segurança específico.	
sn_vul.app_manage_app_vul_permissions	[interno] Usado por sn_vul.app_manage_applications.	
sn_vul.app_manage_normalized_severity	Atualize o mapeamento para a severidade normalizada.	sn_vul.app_read_normalized_severity
sn_vul.app_read_normalized_severity [Removido em v12.1. Não use.]	Exibir registros de severidade normalizados.	
sn_vul.app_read_application_release	Exibir registros de versão da aplicação.	
sn_sec_int.admin	Fornece acesso a integrações.	
pa_power_user	Fornece acesso a relatórios	pa_viewer
sn_vul.app_sec_manager	Prioriza e gerencia itens vulneráveis da aplicação.	
sn_vul.app_developer	Desenvolvedor responsável por corrigir as vulnerabilidades da aplicação.	
sn_vul.app_create_watch_topic	Crie tópicos de observação para vulnerabilidades da aplicação.	
sn_vul.app_read_watch_topic	Leia os tópicos de observação para vulnerabilidades da aplicação.	
sn_vul.app_edit_watch_topic	Edite os tópicos de observação para vulnerabilidades da aplicação.	

Trabalhos programados instalados

Para Vulnerability Response trabalhos programados compartilhados, consulte Componentes instalados com Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho programado	Descrição
Associar AVIs existentes à regra de exceção automática	Avalia itens vulneráveis da aplicação para correspondências com regras de exceção.
Preencher entrada e CVE M2M	Torna os registros existentes consistentes com vários registros CWE. Execute uma vez após a atualização para preencher e desabilitar.
Ressincronizar o CWE primário	Para cálculos CWE primários personalizados. Execute uma vez após a atualização para ressincronizar e desabilitar.
Acumular valores de item vulnerável da aplicação para vulnerabilidade e grupo	Calcula vulnerabilidades e acúmulos de grupo para itens vulneráveis da aplicação.

Tabelas instaladas

Tabela	Descrição
Versão da aplicação [sn_vul_app_release]	Contém informações de versão da aplicação.
Versão 13.0: Campeões de segurança da aplicação [sn_vul_app_m2m_app_sc]	Contém os registros de grupo do Campeão de Segurança Application Vulnerability Response.
Entrada de vulnerabilidade da aplicação [sn_vul_app_vul_entry]	Contém entradas de vulnerabilidade da aplicação.
Integração de vulnerabilidade da aplicação [sn_vul_app_integration]	Contém Application Vulnerability Response registros de integração.
Localização de verificação de vulnerabilidade da aplicação [sn_vul_app_vul_scan_location]	Contém informações do local de verificação de terceiros.
Resumo de verificação de vulnerabilidade da aplicação [sn_vul_app_vul_scan_summary]	Contém informações de resumo de verificação de terceiros.
Item vulnerável da aplicação [sn_vul_app_vulnerable_item]	Contém registros AVI. A partir da v19.0, as seguintes colunas foram adicionadas à Lista de materiais de software: • sn_sbm_config_rule • sn_sbom_component • vex_justification

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
	• vex_detail • vex_response • vex_state • sca_type (SBOM-SCA)
Aplicação escaneada [sn_vul_app_scanned_application]	Contém informações da aplicação.
Mapa de Estado [sn_vul_app_state_map]	Contém mapeamento de estado de integrações de terceiros para estados de item vulnerável da aplicação (IVA).
CWEs de vulnerabilidade [sn_vul_m2m_entry_cwe]	Vincula os dados de CVE às entradas vulneráveis da aplicação.
Manifesto de tarefa de correção da aplicação sn_vul_app_rt_manifest	Todas as atualizações na tarefa de correção são feitas usando esta tabela de manifesto por trabalhos programados.
Tarefa de correção da aplicação sn_vul_app_vulnerability	Contém tarefas de correção da aplicação.
Item da Tarefa de correção da aplicação sn_vul_app_m2m_vul_group_item	Tabela M2M entre o AVI e as tarefas de correção da aplicação.
Versão 21.0: Itens vulneráveis da aplicação sn_vul_app_vulnerable_item	Contém registros AVI.
Versão 21.0: Pacote [sn_vul_app_package]	Contém detalhes do pacote de aplicações.
Versão 21.0: Licenças sn_vul_app_license	Contém licenças de aplicação.
Versão 21.0: Tarefas de correção da aplicação sn_vul_app_vulnerability	Contém tarefas de correção da aplicação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados do item vulnerável da aplicação (IVA)

Application Vulnerability Response oferece um modelo de estado para o status dos itens vulneráveis da aplicação (IVAs), a qualquer momento. Saber como cada estado se relaciona e afeta um ao outro ajuda a determinar quando e como corrigir seus AVIs.

Estados de item vulnerável da aplicação

Entender como os estados funcionam ajuda na criação ou edição de regras de item vulnerável (IVA) da aplicação. Os AVIs têm vários estados possíveis que são mapeados do status de correção importado da integração de terceiros. Em um AVI, o campo **Estado** é somente leitura.

Application Vulnerability Response diagrama de fluxo de estado

Estado	Descrição
Em aberto	Estado após a criação. A partir deste estado, você pode: **V16: obter mais detalhes** Obtenha as seguintes informações sobre um AVI importado do Fortify: • Resumo da vulnerabilidade • Explicação da vulnerabilidade • Recomendação • Referências • Solicitação • Resposta **V16: marcar como falso-positivo** Marque um item como falso positivo se o scanner relatar que existe uma vulnerabilidade no sistema, mas na realidade não há nenhuma vulnerabilidade. **V16: Solicitar exceção** Solicite uma exceção, uma data de reabertura (até), um motivo e, opcionalmente, forneça informações adicionais. Adia a correção do item até a data em que uma exceção é solicitada. **V15: fechar** Selecione o estado Encerrado, um motivo na caixa de diálogo Fechar item vulnerável e forneça informações adicionais. Fecha o AVI. **V15: Resolver** Marque um AVI aberto como Resolvido para movê-lo para um

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Application Vulnerability Response diagrama de fluxo de estado

Estado	Descrição
	estado resolvido. Você deve adicionar anotações de resolução na caixa de diálogo Resolver item vulnerável da aplicação.
Adiado	**V15:** é acionado pela opção **Solicitar exceção**. Como parte do fluxo de trabalho de aprovação, o estado Adiado é Em revisão e não pode ser fechado até ser aprovado. A partir deste estado, você pode: **V16: obter mais detalhes** Obtenha as seguintes informações sobre um AVI importado do Fortify: • Resumo da vulnerabilidade • Explicação da vulnerabilidade • Recomendação • Referências • Solicitação • Resposta **Reabrir** Faz a transição de um AVI encerrado ou resolvido de volta para um estado Aberto. **Fechar** Selecione o estado Encerrado, um motivo e forneça informações adicionais. Fecha o AVI.
Sob Investigação	Selecione esta opção na lista **Estado**. A partir deste estado, você pode: **V20.0** Faça a transição manual de uma tarefa de correção ou registro AVI para **Aguardando implementação**. **V16: obter mais detalhes** Obtenha as seguintes informações sobre um AVI importado do Fortify: • Resumo da vulnerabilidade • Explicação da vulnerabilidade • Recomendação • Referências

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Application Vulnerability Response diagrama de fluxo de estado

Estado	Descrição
	• Solicitação • Resposta **V16: marcar como falso-positivo** Marque um item como falso positivo se o scanner relatar que existe uma vulnerabilidade no sistema, mas na realidade não há nenhuma vulnerabilidade. **V16: Solicitar exceção** Solicite uma exceção, uma data de reabertura (até), um motivo e, opcionalmente, forneça informações adicionais. Adia a correção do item até a data em que uma exceção é solicitada. **V15: fechar** Selecione o estado Encerrado, um motivo na caixa de diálogo Fechar item vulnerável e forneça informações adicionais. Fecha o AVI. **V15: Resolver** Marque um AVI aberto como Resolvido para movê-lo para um estado resolvido. Você deve adicionar anotações de resolução na caixa de diálogo Resolver item vulnerável da aplicação.
Aguardando Implementação	Você só pode fazer a transição manual de registros para esse estado selecionando Aguardando implementação no AVI e registros de tarefa de correção no estado Sob investigação. A partir deste estado, você pode: **Em aberto** Faz a transição do AVI de volta para um estado Aberto. **Sob Investigação** Obtenha mais informações para resolução. Transi para Sob investigação. **Resolver** Marque um AVI aberto como Resolvido para movê-lo para um estado resolvido. Você deve adicionar

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Application Vulnerability Response diagrama de fluxo de estado

Estado	Descrição
	anotações de resolução na caixa de diálogo Resolver item vulnerável da aplicação. **Fechar** Selecione o estado Encerrado, um motivo na caixa de diálogo Fechar item vulnerável e forneça informações adicionais. Fecha o AVI. Nesse estado, faça a transição de um registro para Aguardando implementação quando sua pesquisa e trabalho em uma tarefa estiver concluída e, embora uma correção esteja pronta para implementação, ela ainda não estará disponível. Defina a **data do compromisso** de correção e os campos do **plano** de correção. Após a implementação, você resolve ou fecha os registros.
Resolvido	Acionado a partir do botão Resolver. A partir deste estado, você pode: **V16: obter mais detalhes** Obtenha as seguintes informações sobre um AVI importado do Fortify: • Resumo da vulnerabilidade • Explicação da vulnerabilidade • Recomendação • Referências • Solicitação • Resposta **Reabrir** Faz a transição de volta para um estado **Aberto**. **Fechar** Selecione o estado **Encerrado**, um motivo e forneça informações adicionais. Fecha o grupo. As informações de Anotações e Resolução aparecem na guia **Anotações**.
Encerrado	Acionado a partir do botão Fechar. A partir deste estado, você pode:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Application Vulnerability Response diagrama de fluxo de estado

Estado	Descrição
	Reabrir: faz a transição de volta para um estado Aberto.

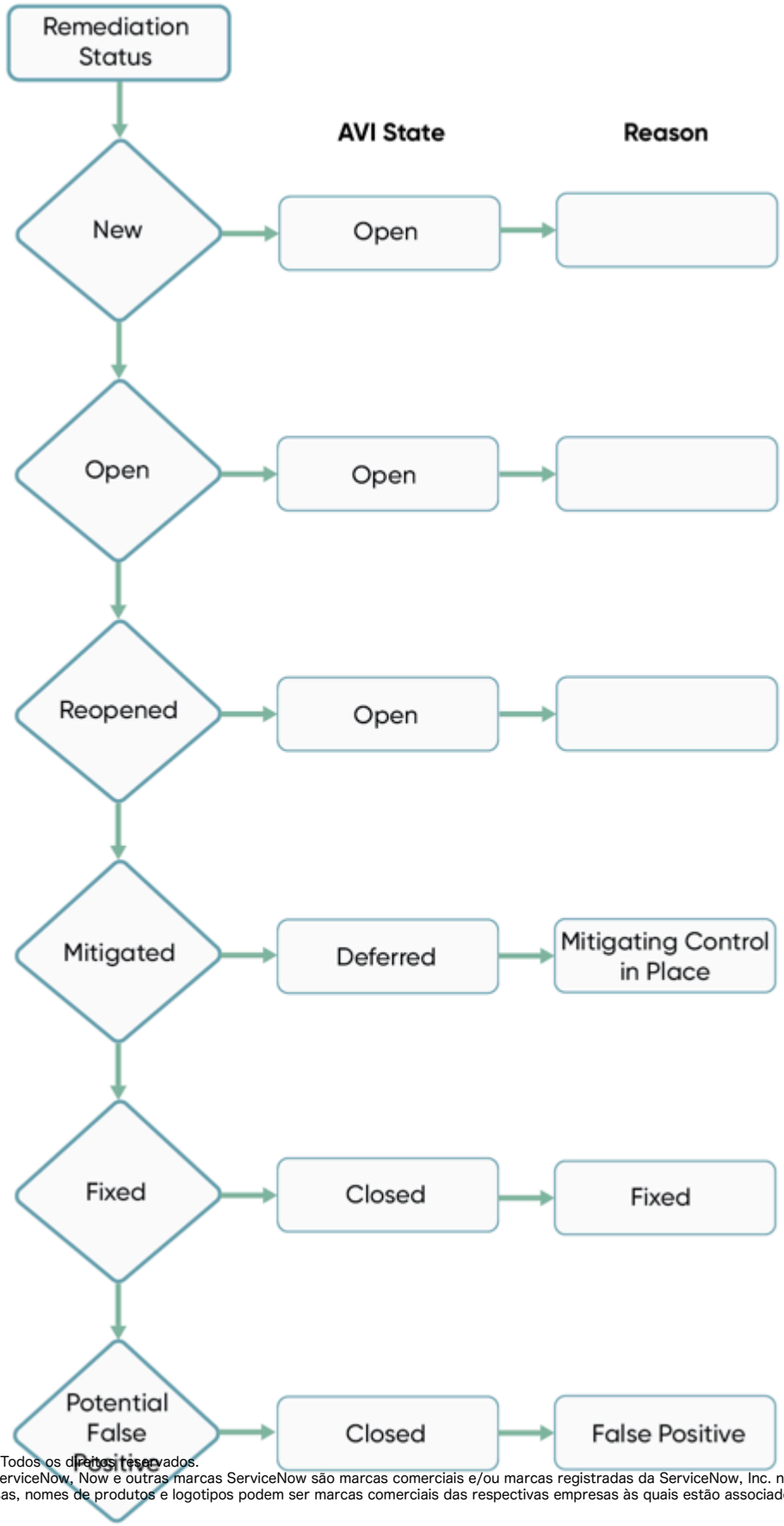
O mapeamento de estados por integração é mostrado a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de estado para Veracode

Nota:
Este mapeamento de estado é aplicável somente quando a opção de triagem em ServiceNow não está selecionada.

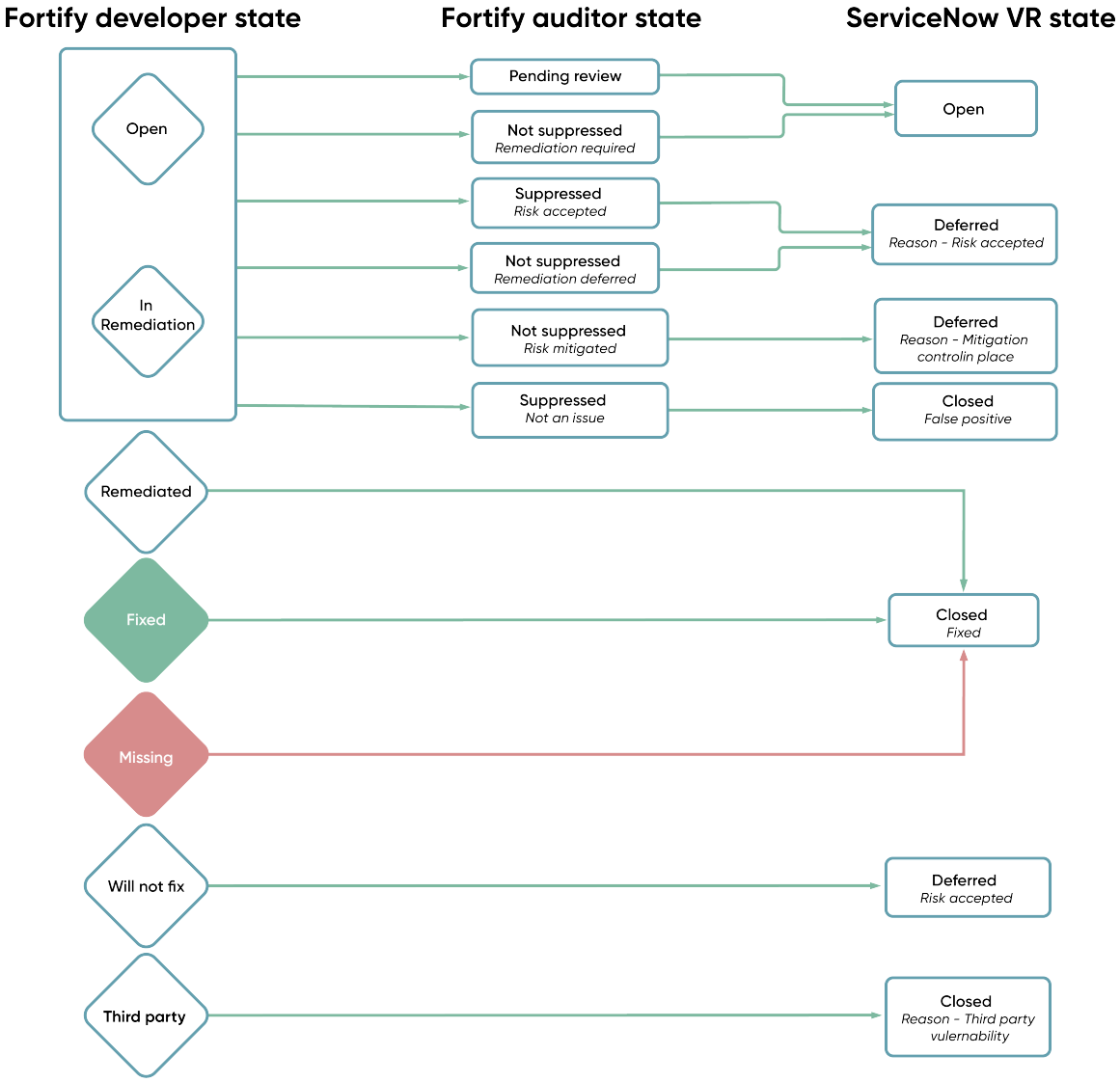


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de estado para Fortify

Nota:
Este mapeamento de estado é aplicável somente quando a opção de triagem em ServiceNow não está selecionada.



Application Vulnerability Response exemplos de regra de tarefa de correção

Um exemplo de regra de tarefa de correção usando o construtor de condição.

Uma regra de tarefa de correção usando vulnerabilidade, modelo de produto, endereço IP e grupo de atribuição

1. No construtor de condição em um novo registro, defina a condição como **Vulnerabilidade** > **é** e insira uma vulnerabilidade conhecida.

   As vulnerabilidades são importadas das integrações do Nation Vulnerability Database (NVD) e do Common Weakness Enumeration (CWE), conforme descrito em Configurar Application Vulnerability Response..

2. Na seção Agrupar por, selecione o **item Vulnerável** da aplicação para o campo **Agrupar itens vulneráveis da aplicação de**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No campo Usando, selecione **Grupo de atribuição**.

   Use Regras de atribuição para definir automaticamente o campo **Grupo de atribuição** para uso em sua regra de tarefa de correção. Você pode usar uma regra fornecida com a aplicação ou configurar suas próprias regras de atribuição. Para obter mais informações, consulte Atribuir itens vulneráveis da aplicação em Application Vulnerability Response automaticamente.

4. Selecione outra condição, por exemplo, item de configuração de item **vulnerável da aplicação no campo Agrupar item vulnerável da aplicação de** e endereço IP ou modelo de produto no campo **Usando**.
5. Na seção Atribuição, para Atribuir tarefa de correção de campo por campo, selecione **Agrupar por campo**.
6. No campo Agrupar por, selecione **Grupo de atribuição**.

   Conforme descrito nesta seção, esta seleção atribui itens vulneráveis a vários grupos com base nas condições definidas na seção agrupar por. Embora os AVIs compartilhem a vulnerabilidade, eles são atribuídos a diferentes grupos com base no modelo de produto de IC ou por endereço IP.

7. Selecione **Enviar** para salvar sua regra.

Campos da aplicação verificados

As aplicações são armazenadas durante a importação em **Administração** > **Aplicações** em Application Vulnerability Response.

Campos da aplicação verificados

Os campos importados nesta tabela são somente leitura, a menos que especificado de outra forma. As entradas de**departamento** e **grupo de suporte** podem ser adicionadas ou editadas manualmente por um gerente de App-Sec.

Campo	Descrição
Nome	Nome importado da aplicação.
Versão	Versão importada da aplicação, quando aplicável.
Status operacional	Status operacional importado da aplicação.
Departamento	Departamento importado ao qual a aplicação pertence. Se estiver vazio, ele poderá ser adicionado manualmente.
Unidade de negócios	Unidade de negócios importada à qual o departamento pertence. Quando o campo **Departamento** é preenchido, esse campo é preenchido automaticamente com a unidade de negócios à qual o departamento pertence. Caso contrário, ele será deixado em branco e somente leitura.
Grupo de suporte	Grupo de suporte importado ao qual a aplicação pertence. Se estiver vazio, ele poderá ser adicionado manualmente.
Descrição	Descrição importada da aplicação.
Data da última verificação de conformidade com a política	Data em que a aplicação foi verificada pela última vez pelo Veracode quanto à conformidade com a política. Ela é usada nas integrações encadeadas da integração da Lista de aplicações, em que o suporte está disponível para ingestão delta para aplicações, comparando esta data com a hora de início delta das respectivas integrações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Os dados são recuperados para aplicações extraídas do Veracode, cujo valor de "Data da última verificação de conformidade da política" é maior ou igual à "Hora de início" (delta_start_time) das integrações encadeadas.
Lista relacionada (visível somente para um gerente de App-Sec ou um campeão de segurança)	
Campeão de segurança	Lista as aplicações associadas a um campeão de segurança. Os gerentes de App-Sec podem adicionar ou remover membros da lista.

Campos de item vulnerável da aplicação

Os itens vulneráveis da aplicação (IVAs) são criados automaticamente durante as importações de integração de vulnerabilidade de terceiros.

Campos de item vulnerável da aplicação

Exceto para os campos **Grupo de atribuição**, **Atribuído a** e **Anotações**, todos os outros campos no AVI são somente leitura.

Campo	Descrição
Número	Identificador AVI gerado automaticamente para este registro.
Tipo de verificação	Tipo de scanner que encontrou este AVI. As opções são: • Dinâmico • Estático • SCA
Pontuação de risco	**Pontuação de risco** quantificada que separa itens vulneráveis em Crítico, Alto, Médio, Baixo e Nenhum. Para obter mais informações sobre classificações de risco, consulte Calcular risco em Application Vulnerability Response automaticamente.
Pontuação de risco	Valor calculado de risco que o AVI representa para o seu ambiente. Para obter mais informações, consulte Calcular risco em Application Vulnerability Response automaticamente.
Data do compromisso de correção	A data em que os AVIs devem ser corrigidos depois de serem movidos para **Sob investigação**. Este campo será exibido somente se o AVI estiver em **Sob investigação**.
Destino de correção	Data em que os AVIs devem ser corrigidos, desde a primeira identificação. Somente aparece quando aplicável. Para obter mais informações sobre destinos de correção, consulte Automatizar o acompanhamento de destino de correção no Application Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Status da Correção	Status da correção do AVI. É determinado pelo AVI com a data de vencimento mais próxima, quando aplicável. Os estados incluem: • Em andamento • Perto da meta • Destino anterior
Nome da categoria	Nome da categoria da vulnerabilidade.
Vulnerabilidade	ID da vulnerabilidade associada a este item vulnerável da aplicação.
Versão da aplicação	Versão da aplicação.
Módulo da aplicação	Aplicação afetada na verificação DAST. Oculto para verificações SAST.
Local Versão 14.0: SAST	DAST: local da URL da vulnerabilidade na aplicação. SAST: caminho do arquivo e número da linha da vulnerabilidade na aplicação.
Estado	Este campo é padronizado como **Aberto** quando criado. Consulte Estados do item vulnerável da aplicação (IVA) para obter mais informações sobre como os estados são mapeados.
Motivo	[Somente visível quando o AIV está no estado **Encerrado**.] Explicação do estado.
Grupo de atribuição	Grupo selecionado para trabalhar neste AVI. Pode ser adicionado ou editado manualmente por um gerente de App-Sec.
Atribuído a	Indivíduo do grupo de atribuição selecionado que trabalha neste AVI. Pode ser adicionado ou editado manualmente por um gerente de App-Sec
Primeiro encontrado	Data em que a origem de terceiros encontrou o item vulnerável da aplicação pela primeira vez.
Último encontrado	Data em que a origem de terceiros encontrou o item vulnerável da aplicação pela última vez.
Encerrado	[Somente visível quando o AVI está no estado **Encerrado**.] Data em que o AVI foi encerrado.
Encerrado por	[Somente visível quando o AVI está no estado **Encerrado**.] Entidade que fechou o AVI.
Resumo	Descrição importada da vulnerabilidade.
Descobertas Dados somente leitura importados da integração de terceiros.	
ID de AVIT de origem	Identificador importado para o AVI de origem.
Gravidade de origem	Severidade importada da aplicação de origem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Data de correção de destino da origem	Data de importação em que a origem espera que o AVI seja corrigido.
Status de mitigação da origem	Status de mitigação importado da aplicação de origem.
Status da correção da origem	Status de correção importado da aplicação de origem.
Status de descoberta da origem	[Somente visível quando preenchido] Status do problema importado da aplicação de origem.
Status SDLC	Status do ciclo de vida de desenvolvimento de software importado.
Cumpre a política	Status de conformidade importado. Se nenhum status for fornecido, este campo será definido como **Não aplicável**.
Link de origem	URL para o AVI de origem.
Anotações de origem	Anotações importadas da origem.
Resumo da vulnerabilidade	Resumo importado da origem.
Explicação da vulnerabilidade	Explicação importada da origem.
Recomendação	Recomendação importada da origem.
Referências	Referências importadas da origem.
Solicitação/resposta HTTP (visível somente para verificações DAST)	
Solicitação de origem	Solicitação HTTP
Resposta de origem	Resposta HTTP
Anotações	
Plano de correção	Detalhes de como os AVIs serão corrigidos. O plano deve ser implementado até a **data do compromisso**de correção. Este campo será exibido somente se o AVI estiver em **Sob investigação**.
Comentários adicionais/Anotações de trabalho	Qualquer informação relevante. Selecione a caixa de texto das Anotações de trabalho para adicionar informações. A partir da Vulnerability Response v20.0, você pode adicionar anotações de trabalho na seção Anotações para um item vulnerável da aplicação adiado.

Estados do teste de invasão

Os responsáveis pela aplicação podem solicitar avaliação de teste de invasão para suas aplicações e monitorar o progresso da equipe de invasão ética até que a solicitação seja resolvida.

A solicitação de avaliação de teste de invasão passa pelos seguintes estados de transição até que seja resolvida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fases da solicitação de avaliação de teste de invasão

Campo	Descrição
Estados do teste de invasão	
Em aberto	Estado quando a solicitação de avaliação é criada pelo responsável pela aplicação.
Escopo	A equipe de invasão ética avalia a solicitação e o escopo da aplicação.
Preparação do ambiente	O proprietário da aplicação cria um ambiente com funções e outras informações e o fornece para a equipe de invasão ética para teste.
Teste	A equipe de invasão ética testa manualmente a aplicação para identificar as descobertas do teste de invasão.
V16.1: teste em andamento	A equipe de hackers éticos indica que o teste está em andamento. Se este estado for selecionado, a opção **Teste em espera** ficará disponível no formulário.
V16.1: teste em espera	Este campo é exibido somente quando o estado Teste em andamento é selecionado. A equipe de invasão ética controla os acordos de nível de serviço (ANSs) das solicitações de avaliação de teste de invasão selecionando este estado, se necessário. Isso garante que SLAs precisos sejam relatados.
V16.1: Teste em revisão	A equipe de invasão ética indica que o teste foi concluído e está sendo revisado por um especialista no assunto.
Encerrado	A equipe de invasão ética fecha as solicitações de avaliação de teste de invasão depois que as descobertas do teste de invasão são relatadas. **Nota:** A partir da V16.1, é possível usar a opção **Copiar e criar solicitação** no formulário para replicar a solicitação no estado Encerrado e criar uma nova solicitação. Para obter detalhes, consulte Replicar uma solicitação de teste de invasão no estado encerrado.
V16.1: cancelado	O proprietário da aplicação cancela a solicitação de avaliação do teste de invasão.
V16.1: rascunho	O proprietário da aplicação cria uma solicitação e a salva como rascunho antes de enviar a solicitação.
Estados de item vulnerável da aplicação	
Em aberto	Quando a equipe de invasão ética identifica e cria as descobertas do teste de invasão, seu status é Aberto.
Resolvido	Quando a equipe de aplicações resolve as descobertas do teste de invasão, seu status é movido para Resolvido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fases da solicitação de avaliação de teste de invasão

Campo	Descrição
	Nota: Se a descoberta do teste de invasão tiver sido resolvida, mas ainda não tiver sido validada pela equipe de hackers éticos, o subestado será `Validation Pending`.
Encerrado	A equipe de invasão ética valida que as descobertas do teste de invasão foram resolvidas e move o status para Encerrado.

Como gerenciar o mapeamento de estado para adiamentos e falsos positivos no Application Vulnerability Response

Você pode gerenciar como os estados de **origem** nos itens vulneráveis da aplicação (IVAs) importados por Veracode Vulnerability Integration e Integrações de vulnerabilidade do Fortify são mapeados em sua instância após a importação.

A partir da v20.0 de Vulnerability Response, você tem mais opções para fazer a triagem de seus AVIs importados com ServiceNow fluxos de trabalho.

Quando você Configurar o Integrações de vulnerabilidade do Fortify ou o Configurar o Veracode Vulnerability Integration, as páginas de configuração de integração fornecem duas opções para ajudá-lo a gerenciar exceções e falsos positivos em sua instância.

- Gerenciar exceções no ServiceNow
- Gerenciar falsos positivos no ServiceNow

Função necessária: gerente de App-Sec.

Caso de uso para gestão de exceções

Os AVIs são importados dessas integrações com os estados de **origem**. Na importação, esses estados são mapeados para os estados **Destino** e **Motivo** de destino em sua instância, porque em alguns casos não há correspondências exatas entre os estados de origem do scanner e os estados usados pela instância.

Por exemplo, estados de origem como **Não corrigirá**, **Correção adiada**, **Risco aceito**e **Risco atenuado** de Integrações de vulnerabilidade do Fortify são mapeados para o estado **Adiado** com um subestado de **Risco aceito** ou **Controle de atenuação no local** em sua instância.

Você tem as seguintes opções nas páginas de configuração dessas integrações:

Opção	Caixa de seleção selecionada	Descrição
Gerenciar exceções no ServiceNow	Y (por padrão)	Se você deixar esta opção selecionada, deverá solicitar exceções de registros AVI. Os AVIs importados marcados para o estado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Caixa de seleção selecionada	Descrição
		Adiado são triados com o fluxo de trabalho ServiceNow Gestão de exceções. AVIs com estados de **origem** que normalmente são mapeados para um estado **adiado** são mapeados para o estado de **triagem de destino no estadoaberto**.
	N	Se você desativar a caixa de seleção, preservará os estados de **origem** importados do scanner. Esses AVIs são mapeados para o **estado de destino** como **Adiado**e para um estado de **motivo de destino** em sua instância. Eles não são triados pelo fluxo de trabalho de exceção, porque não são mapeados para o estado de **triagem** de **destino e os estados de motivo de triagem** de destino. A ação de IU **Solicitar exceção** não está disponível no registro AVI porque o registro já está no estado Destino **adiado**.

Caso de uso para Falso-positivo

Para falsos positivos de Veracode Vulnerability Integration como um exemplo, estados de origem como **Falso-positivo** ou **Possível falso-positivo** são mapeados para o **estado Destinofechado** com um subestado de **Falso-positivo**.

Opção	Caixa de seleção selecionada	Descrição
Gerenciar falsos positivos no ServiceNow	Y (por padrão)	Se você deixar esta opção selecionada, deverá solicitar um **falso-positivo** dos registros AVI. Os AVIs importados marcados para os estados **Falso-positivo** ou **Possível falso** -positivo são triados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Caixa de seleção selecionada	Descrição
		com o fluxo de trabalho ServiceNow Gestão de exceções. AVIs com estados de **origem** que normalmente são mapeados para um **estado de destinoencerrado** são mapeados para um estado de **triagem de destino** em **aberto**. A ação de IU **de falso-positivo** está disponível no registro AVI.
	N	Se você desativar a caixa de seleção, preservará os estados de **origem** importados do scanner. Esses AVIs são mapeados para o **estado de Destino** como **Encerrado** e um estado de **Motivo de destino** em **Falso-positivo** em sua instância. Eles não são triados pelo fluxo de trabalho de falso-positivo. A ação de IU **de falso positivo** não está disponível no registro AVI porque o registro já está no estado Destino **encerrado**.

Tradução automática

referências de Application Vulnerability Response

Os termos a seguir são usados em Application Vulnerability Response.

Itens vulneráveis da aplicação (IVAs)

Pares de entradas de vulnerabilidade e aplicações potencialmente vulneráveis no ambiente da sua empresa.

Regras de atribuição

Regras usadas para atribuir AVIs com base nos critérios definidos.

Enumeração de plataforma comum (CPE)

Um esquema de nomenclatura estruturado do NIST NVD para sistemas de tecnologia da informação, software e pacotes.

Vulnerabilidades e Exposições Comuns (CVE)

Dicionário de vulnerabilidades e exposições de segurança da informação conhecidas publicamente.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Enumeração de pontos fracos comuns (CWE)

Lista de tipos de pontos fracos de software desenvolvidos pela comunidade.

Integrações

Trabalhos programados que extraem dados de relatório do CWE ou de um sistema de terceiros, como Veracode, para recuperar dados de vulnerabilidade.

Nota:
Se a integração do banco de dados nacional de vulnerabilidades do NIST em Vulnerability Response estiver ativada e configurada, o aprimoramento de CVE estará disponível para CWEs, mas não será obrigatório. Para obter informações sobre a integração do NIST National Vulnerability Database, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.

Banco de dados nacional de vulnerabilidades (NVD)

Repositório do governo dos EUA de dados de gestão de vulnerabilidades baseados em padrões representados usando o Security Content Automation Protocol (SCAP).

Regras de destino de correção

Regras usadas para atribuir datas de destino de AVIs para correção com base nos critérios definidos.

Calculadoras de vulnerabilidade

Calculadoras usadas para priorizar e categorizar vulnerabilidades da aplicação com base nos critérios definidos.

Exemplo de regra de exceção para Application Vulnerability Response

Um exemplo de regra com base em uma vulnerabilidade conhecida para uma regra de exceção.

Campo	Descrição
Nome	Um nome exclusivo para ajudá-lo a identificar sua finalidade e localizar a regra facilmente, por exemplo, `Veracode-1 cwe-22 exception`.
Estado	Somente leitura: rascunho
Válido de	Data em que esta regra está ativa para adiar AVIs.
Ordem de execução	Ordem exclusiva para cada regra de exceção. Um valor menor precede um maior.
Válido até	Data em que a tarefa de correção para de aceitar novos IVs.
Adiado até	Data até quando as tarefas de correção e os AVIs são adiados. Nesta data, o AVUL é encerrado, todos os AVIs são movidos para fora da tarefa e são reabertos. As regras de grupo são reaplicadas a esses AVIs.
Motivo	Motivo para criar esta regra de exceção. Selecione um na lista, por exemplo, **Correção indisponível**.
Grupo de atribuição	Grupo atribuído para rastrear os IVs adiados, por exemplo, APP Sec Manager.
Informações adicionais	Informações adicionais que o solicitante deseja fornecer ao aprovador. Essas informações são

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	preenchidas no campo de descrição da tarefa de correção. Neste exemplo, adiar AVIs com a vulnerabilidade – Veracode-1-22.
Condição	Filtrar condições para especificar quais AVIs correspondem a esta regra. Para este exemplo, a vulnerabilidade é Veracode-1-22.
Executar em dados existentes	Opção que permite executar esta regra em dados existentes na primeira vez em que esta regra é executada. Se você deixar esta opção desativada, sua regra será executada diariamente pelo trabalho programado *`Associate existing AVIs with Auto Exception Rule`* começando com novos dados. Se você habilitar a opção Executar em dados existentes, um trabalho programado será executado uma vez nos dados existentes na data **Válido a partir de**.

Exibição de produto do Application Vulnerability Response

O produto Application Vulnerability Response (AVR) ingere os pontos fracos e as vulnerabilidades detectados por suas ferramentas de teste de segurança de aplicações e fornece um único painel para entender a postura de segurança de todas as aplicações em seu ambiente.

O AVR permite reduzir os riscos com os fluxos de trabalho de correção. O objetivo desta exibição de produto é ajudar você a entender como as principais entidades de AVR funcionam com a estrutura principal do CSDM.

Terminologia atualizada

A partir do AVR v19.0, os seguintes nomes de tabela e coluna de chave foram atualizados. Como resultado, você verá referências aos nomes mais antigos e mais recentes na documentação.

Lista atualizada de termos, tabela e nomes de campo para AVR

Antes do AVR v19.0	A partir do AVR v19.0
Regras de pesquisa de IC	Regras de pesquisa
Formulário de regra de pesquisa de IC	Formulário de regra de pesquisa
Regra de correspondência de IC	Regra de correspondência
Pesquisar na tabela	Pesquisar na tabela de IC
Pesquisar no campo	Pesquisar no campo de IC
Versão da aplicação	Aplicações descobertas
Tabela de versão da aplicação	Tabela de aplicações descobertas

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista atualizada de termos, tabela e nomes de campo para AVR

Antes do AVR v19.0	A partir do AVR v19.0
Criticalidade dos negócios	Criticalidade dos negócios de origem

Pré-requisitos

Instale as versões mais recentes dos seguintes aplicativos:

- Security Support Common
- Vulnerability Response
- Security Integration Framework
- Orquestração de suporte de segurança
- Integrações de scanner, como Veracode e Fortify

AVR e CSDM 4.0

Antes do AVR v19.0, quando as vulnerabilidades da aplicação eram ingeridas, a aplicação para a qual as vulnerabilidades foram ingeridas era pesquisada usando as regras de pesquisa de IC, em relação às aplicações verificadas (sn_vul_app_scanned_application). Se o registro do nome da aplicação não estiver lá, será feita uma entrada.

A partir do AVR v19.0, para alinhar com a estrutura do CSDM 4.0, as tabelas de modelo de produto são usadas em vez da tabela Aplicações verificadas. Se a aplicação tiver a versão, a pesquisa será na tabela de Modelo de Software. Se não houver versão, a pesquisa será na tabela Modelo de aplicação. O Modelo de aplicação e o Modelo de software são tabelas secundárias da tabela Modelo de produto, que é a tabela base no CMDB. A captura de tela a seguir explica o modelo do produto.

Propriedade do sistema

Para usar o processo de pesquisa baseado em modelo de produto do CSDM 4.0, defina a propriedade do sistema *sn_vul.use_product_model* como *true*.

Considerações de propriedade do sistema

Nome da propriedade do sistema	Valor da propriedade do sistema	Pesquisar valor de destino	Considerações
sn_vul.use_product_model	verdadeiro	Selecione o **modelo de produto**de valor	Os novos usuários devem selecionar o valor **Modelo de produto** para usar as regras de pesquisa de modelo de produto da estrutura do CSDM 4.0.
	falso	Selecione o valor **Item de configuração**	Os usuários existentes podem continuar usando o processo de pesquisa de IC e as **regras de pesquisa de IC**existentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Para definir o valor de destino da pesquisa, navegue até a página **Regra de pesquisa** > **[Regra de pesquisa de integração de AVR]** > Campo de **destino da pesquisa**.

Regras de pesquisa no AVR

Na estrutura do CSDM 4.0, as regras de pesquisa baseadas no modelo de produto são usadas em vez das regras de pesquisa de IC para criar entradas nas respectivas classes de modelo de produto. Da mesma forma para scripts, você pode definir as regras de pesquisa na estrutura do modelo CSDM 4.0.

A partir do AVR v19.0, ao criar uma regra de pesquisa, você deve definir se deseja usar o item de configuração ou a abordagem de modelo de produto usando o campo de **destino de pesquisa**. Para obter mais informações, consulte Criar uma regra de pesquisa de IC.

Aplicações descobertas

Navegar até **Todos** > **Aplicações descobertas**. A tabela Aplicações descobertas exibe as aplicações ingeridas dos scanners. Se a propriedade do sistema `sn_vul.use_product_model` estiver definida como `true`, você poderá ver os modelos de produto correspondentes para as aplicações.

Considerações de AVR

Presença de IC ou registros de modelo de produto duplicados

Verifique se a propriedade do sistema `sn_vul.use_product_model` foi configurada corretamente para o processo de pesquisa. Certifique-se de selecionar o **item de configuração** ou o **modelo de produto** como o destino da pesquisa ao configurar o formulário de regra de pesquisa.

Vulnerability Response contêiner

A aplicação ServiceNow® Vulnerability Response contêiner importa itens vulneráveis de contêiner (CVITs) e, de acordo com as regras, permite corrigir vulnerabilidades de contêiner. Os dados de vulnerabilidade são extraídos de fontes internas e externas, como o National Vulnerability Database (NVD) ou integrações de terceiros.

A partir da versão 18.0 do Vulnerability Response, é possível monitorar e corrigir CVITs no Vulnerability Manager Workspace e no IT Remediation Workspace, respectivamente. Para obter mais informações, consulte Espaço para gerentes de vulnerabilidades e Explorando o Espaço de correção de problemas de TI.

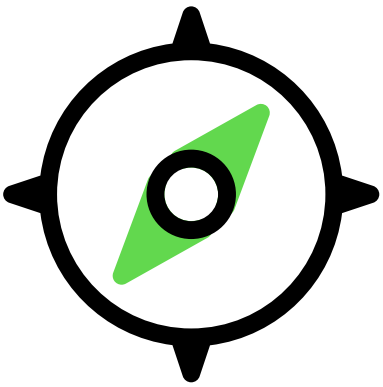
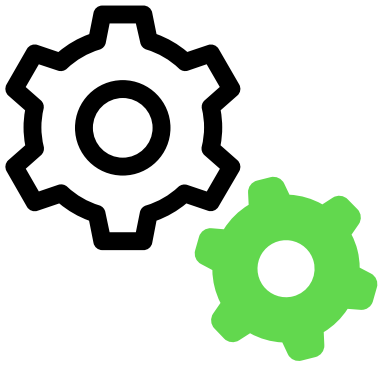
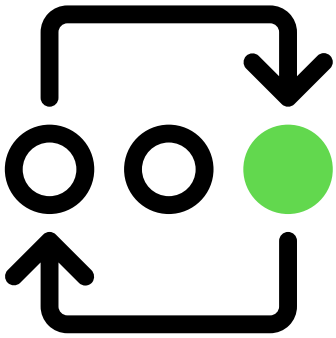
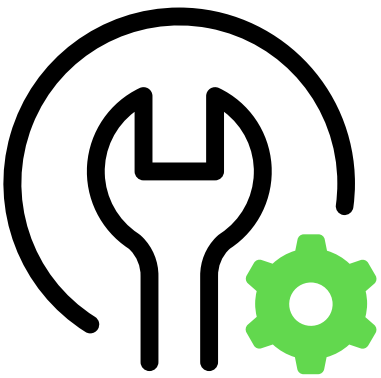
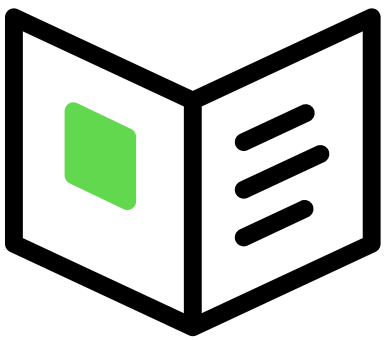
Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vulnerability Response contêiner

Explorar	Configurar	Integrar
		
Saiba mais sobre os conceitos e recursos do Container Vulnerability Response.	Configure o Vulnerability Response do contêiner.	Estenda o Vulnerability Response do contêiner integrando-o a outras aplicações.
Corrigir	**Análise e relatório**	**Referência**
		
Saiba como corrigir vulnerabilidades de contêiner.	Exibir análise do Vulnerability Response do contêiner	Veja os detalhes sobre os componentes do Vulnerability Response do contêiner, como campos, tabelas e propriedades.

Tradução automática

Benefícios

A aplicação Vulnerability Response contêiner fornece os seguintes benefícios:

- Integra-se a produtos de segurança de contêiner de terceiros, como o Prisma Cloud Compute da Palo Alto Networks.
- Importa dados de vulnerabilidade para as imagens implantadas no tempo de execução e aprimora os dados de vulnerabilidade com informações contextuais de tempo de execução (hosts, clusters do Kubernetes, serviços e namespaces).

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Fornece uma lista das referências criadas a partir de vulnerabilidades para as entidades relevantes do Kubernetes no Configuration Management Database (CMDB) usando ServiceNow Descoberta do Kubernetes.
- Oferece um painel de relatórios abrangente, fornecendo informações sobre as tendências de vulnerabilidade e correção.

Principais recursos

A aplicação Vulnerability Response contêiner gerencia vulnerabilidades detectadas nos contêineres. Ele fornece os seguintes recursos:

- Aponte para a imagem do Docker de origem de CVITs em vez de executar contêineres.
- Configure a granularidade de CVITs para rastrear na imagem, no cluster do Kubernetes, no namespace ou no nível de serviço.
- Rastreie novas versões de imagem para identificar vulnerabilidades corrigidas. Todas as vulnerabilidades relatadas em versões mais antigas são resolvidas automaticamente em ServiceNow quando novas versões de imagem são implantadas no tempo de execução.
- Rastreie CVITs em imagens de base separadamente das imagens da aplicação para habilitar a correção independente.
- Gere solicitações de exceção ou solicitações de falso-positivo, que podem ser revisadas por meio de um processo de aprovador de vários níveis.
- Defina regras de exceção para adiar CVITs automaticamente.

Casos de uso

Os contêineres são uma ótima maneira de implantar e escalonar aplicações em vários ambientes com menos sobrecarga e maior portabilidade. No entanto, as vulnerabilidades nas imagens de contêiner podem representar risco para o host subjacente e, em última análise, para a infraestrutura em que os contêineres foram iniciados a partir dessas imagens. Embora existam muitos produtos de segurança de contêiner que verificam as imagens de contêiner em busca de vulnerabilidades, há algumas considerações e problemas associados à correção das vulnerabilidades. Vulnerability Response contêiner pode ajudar a resolver vários problemas ou casos de uso envolvidos na correção de vulnerabilidades de imagem de contêiner. Explore maneiras de aproveitar o módulo Vulnerability Response contêiner :

Contexto de tempo de execução

Vulnerabilidades em imagens de contêiner podem ser descobertas verificando a imagem nas seguintes fases do ciclo de vida da aplicação.

- Fase 1: quando as imagens estão sendo criadas no pipeline de IC/CD.
- Fase 2: quando as imagens são publicadas no registro
- Fase 3: quando as imagens são implantadas no tempo de execução.

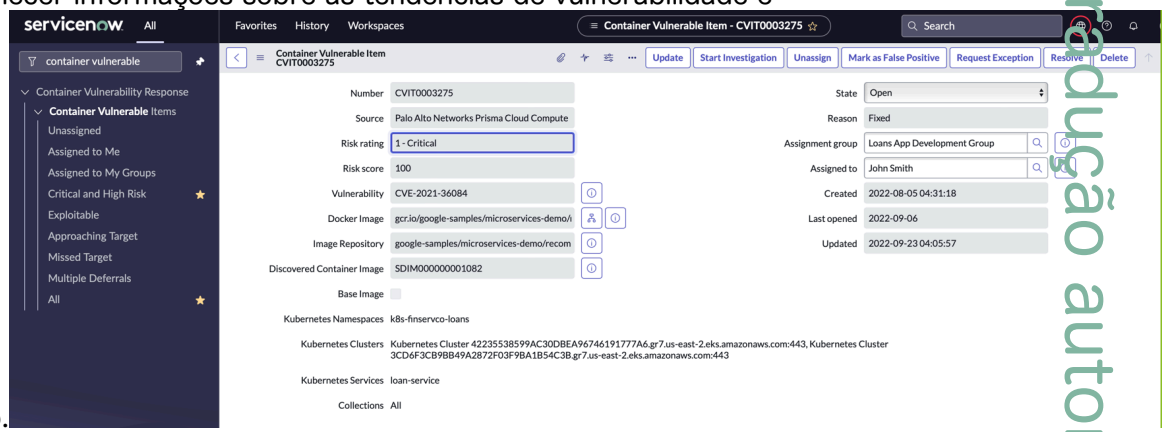
Embora seja importante identificar vulnerabilidades o mais cedo possível na fase 1 e na fase 2, é igualmente importante executar uma verificação nas imagens implantadas em um ambiente de tempo de execução. Ele oferece os seguintes benefícios:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Identificar novas vulnerabilidades e exposições comuns (CVEs) que foram publicadas.
- Fornece visibilidade precisa da postura de risco das aplicações implantadas.
- Priorização de vulnerabilidades que devem ser resolvidas. O contexto de tempo de execução em termos de serviços de aplicações ou serviços de negócios afetados devido a uma vulnerabilidade pode ajudar na priorização.

Vulnerability Response contêiner se integra a produtos de segurança de contêiner, como Prisma Cloud Compute de Palo Alto Networks para extrair os dados de vulnerabilidade das imagens implantadas no tempo de execução e enriquece os dados de vulnerabilidade com as informações contextuais do tempo de execução, como hosts, clusters do Kubernetes, serviços e namespaces onde essas imagens de contêiner são implantadas. Os clientes que usam a descoberta ServiceNow do Kubernetes podem ver as referências criadas a partir de vulnerabilidades para as entidades relevantes do Kubernetes em seus Configuration Management Database (CMDB). Além de aprimorar os metadados, o ServiceNow também oferece um painel de relatórios abrangente para fornecer informações sobre as tendências de vulnerabilidade e correção.



Identificar propriedade

Pré-requisitos

- **Metadados e referências do Kubernetes**: para que Vulnerability Response contêiner preencha metadados do Kubernetes (namespace, cluster e assim por diante) e referências a Configuration Management Database (CMDB) entradas, você deve implementar a descoberta do Kubernetes de Information Technology Operations Management (ITOM). A descoberta do Kubernetes preenche a imagem do Docker, os contêineres do Docker em execução, pods, clusters do Kubernetes e assim por diante, no CMDB. Vulnerability Response contêiner identifica a imagem do Docker em CMDB com base no ID da imagem e, em seguida, identifica as entidades do Kubernetes relacionadas e preenche as referências a essas entidades de itens vulneráveis.
- **Metadados em nuvem e rótulos de imagem do Docker**: Vulnerability Response contêiner também preenche rótulos de imagem do Docker, IDs de conta de nuvem, regiões onde uma imagem é implantada. Esses dados são mantidos no registro "Imagem de contêiner descoberta" associado ao item vulnerável. Não há pré-requisitos para que esses dados sejam preenchidos. Vulnerability

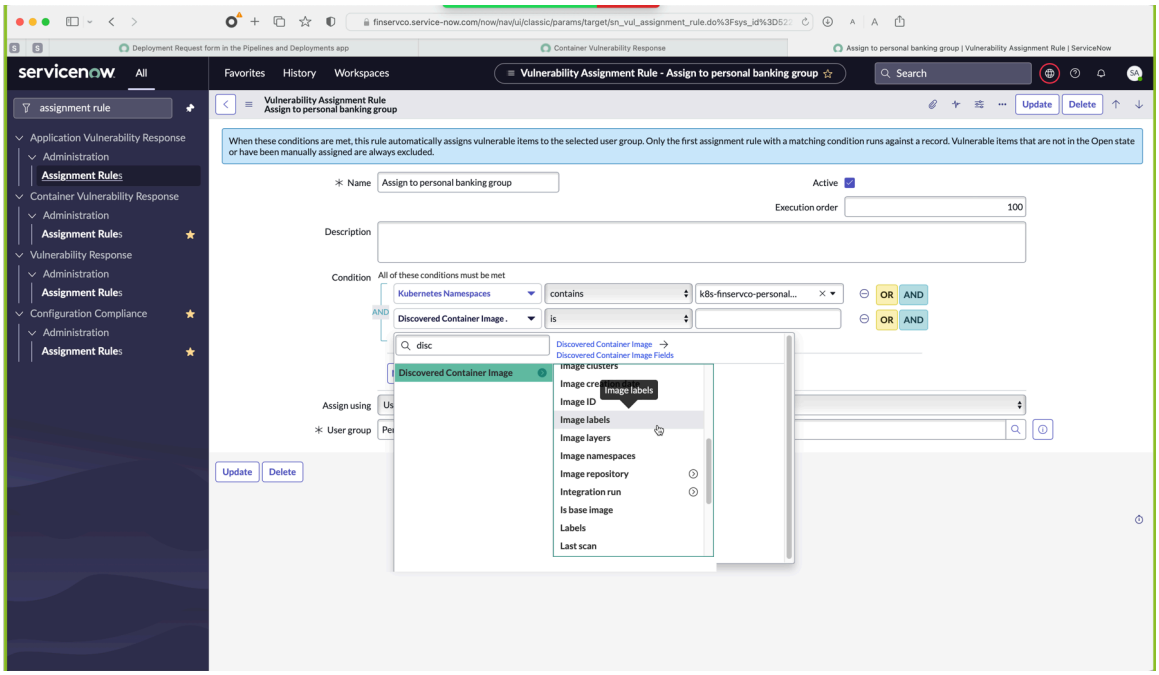
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Response contêiner usa os dados retornados por produtos de segurança de contêiner (por exemplo, Palo Alto Prisma Cloud Compute) para preencher essas entradas.

A propriedade de corrigir uma vulnerabilidade em uma imagem de contêiner pode variar de organização para organização. Essas informações podem ser capturadas em locais diferentes. Algumas organizações usam rótulos de imagem do Docker como uma forma de identificar as equipes de aplicações que possuem uma determinada imagem de contêiner, enquanto outras organizações podem usar o namespace do Kubernetes ou a conta de nuvem em que uma imagem de contêiner é implantada para identificar o proprietário certo.

Vulnerability Response contêiner fornece os elementos de modelo de dados necessários para capturar e usar os rótulos de imagem do Docker, os metadados de cluster/serviço/namespace do Kubernetes ou os metadados da conta de nuvem (ID da conta de nuvem, região, provedor e assim por diante) nas "Regras de atribuição" e atribua vulnerabilidades automaticamente à equipe de aplicações certa com base nos metadados da imagem ou no ambiente de tempo de execução.



Tradução automática

Rastrear vulnerabilidades nas imagens de base

Pré-requisitos

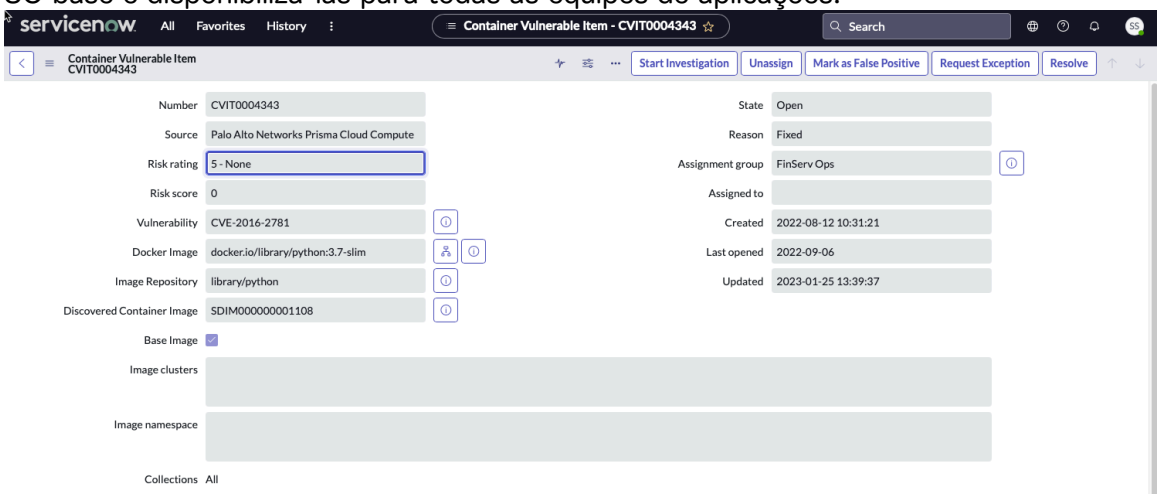
Para que a propriedade "Imagem de base" seja preenchida em Vulnerability Response contêiner, as imagens de base devem ser configuradas explicitamente no console Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Para obter mais informações sobre como configurar imagens de base no Prisma Cloud, consulte https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin-calculate/vulnerability_management/base_images.

Vulnerability Response contêiner permite a criação de registros de vulnerabilidade separados para uma camada base para que eles possam ser atribuídos a uma equipe diferente.

Rastreie as vulnerabilidades identificadas em uma imagem do SO base, como o Alpine, a partir das vulnerabilidades detectadas em

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

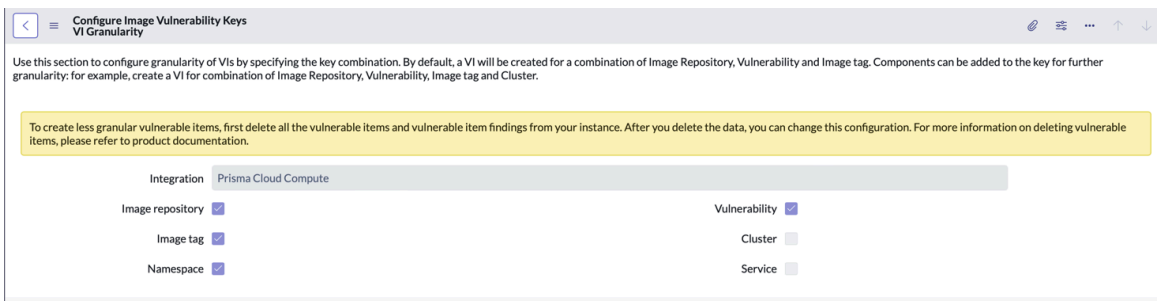
outras camadas da imagem do contêiner. Muitas organizações têm equipes dedicadas que são responsáveis por corrigir imagens do SO base e disponibilizá-las para todas as equipes de aplicações.



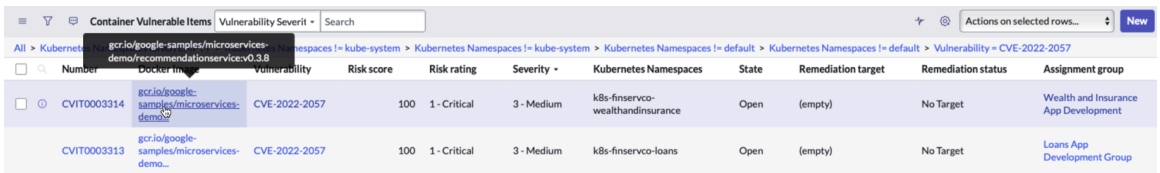
Definir granularidade para itens vulneráveis

Pré-requisitos

Configure a granularidade de CVITs navegando até **Todos** > **Vulnerability Response do contêiner** > **Administração** > **Configurar granularidade de IV**.



Por padrão, um item vulnerável é criado para cada combinação exclusiva de CVE e a versão da imagem do Docker (referência + marcador). No entanto, algumas imagens do Docker podem ser implantadas em mais de um namespace do Kubernetes e cada namespace pode pertencer a diferentes unidades de negócios ou equipes. Cada equipe pode seguir sua própria cadência para implantar novas versões de imagens de contêiner para corrigir vulnerabilidades. Para acomodar este cenário, Vulnerability Response contêiner permite que você defina a granularidade para itens vulneráveis: se um item vulnerável deve ser criado para cada namespace/cluster/serviço do Kubernetes, mesmo para cada combinação exclusiva de versão e vulnerabilidade da imagem do Docker.



No exemplo, você pode ver dois itens vulneráveis criados para a mesma combinação de imagem do Docker e CVE. Um para o namespace do Kubernetes "k8s-finservco-loans" e o outro para "k8s-finservco-wealthandinsurance".

Identifique serviços afetados usando a identificação de serviço baseada em marcador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pré-requisitos

- Identifique vários serviços em sua aplicação e defina os marcadores/pares de chave-valor que representam esses serviços.
- Implante imagens do Docker e pods do Kubernetes com essas tags ou rótulos.
- Implantar o ITOM Kubernetes Discovery Defina "Serviços baseados em marcador" com os marcadores ou rótulos corretos.
- Implantar ITOM Kubernetes Discovery
- Defina "Serviços baseados em marcador" com os marcadores corretos ou pares de chave-valor.
- Importar dados de vulnerabilidade para ServiceNow usando Vulnerability Response contêiner

O cálculo de risco para itens vulneráveis pode ser feito observando o IC (imagem do Docker) e a criticidade dos serviços associados em CMDB. No entanto, para facilitar a identificação dos serviços afetados, Vulnerability Response contêiner oferece identificação de serviço baseada em marcador.

Quando os pods ou entidades do Kubernetes são publicados com valores-chave ou rótulos correspondentes aos valores-chave definidos em qualquer "Serviço baseado em marcador" em ServiceNow, Vulnerability Response contêiner estabelece automaticamente o relacionamento entre uma imagem do Docker e o serviço de aplicações afetado e usa o criticidade desse serviço de aplicativos no cálculo de risco.

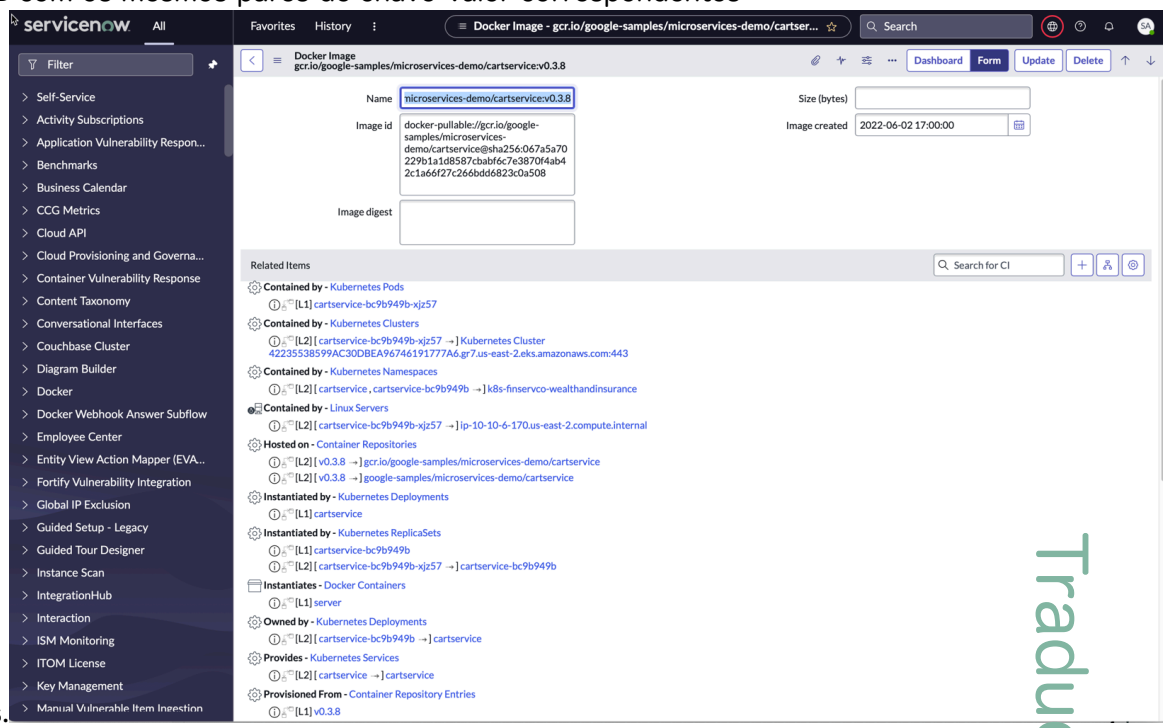
O fluxo é o seguinte:

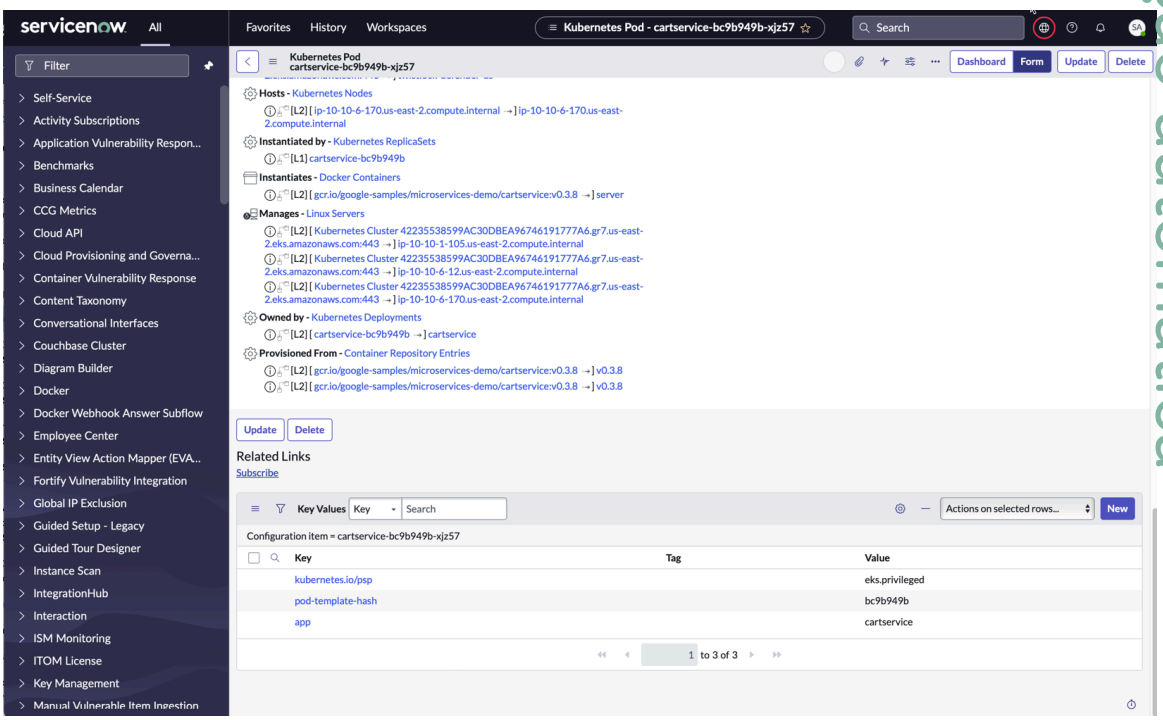
1. Vulnerability Response contêiner importa dados de vulnerabilidade do produto de segurança do contêiner.
2. Para cada item vulnerável de contêiner, Vulnerability Response contêiner preenche a imagem do Docker de CMDB que tem a vulnerabilidade.
3. Vulnerability Response contêiner O analisa os rótulos da imagem do Docker ou os rótulos/valores-chave publicados com os pods do Kubernetes em que esta imagem está implantada. Esta imagem estará disponível em CMDB se você tiver a descoberta do Kubernetes em execução.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Vulnerability Response contêiner pesquisa "Serviços baseados em marcador" em CMDB com os mesmos pares de chave-valor correspondentes definidos.

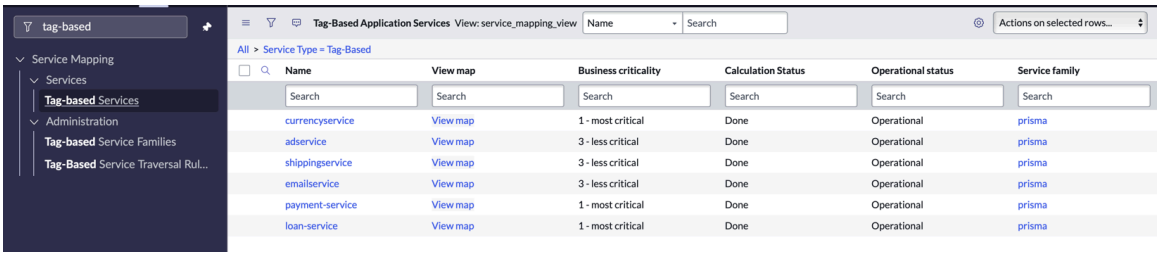


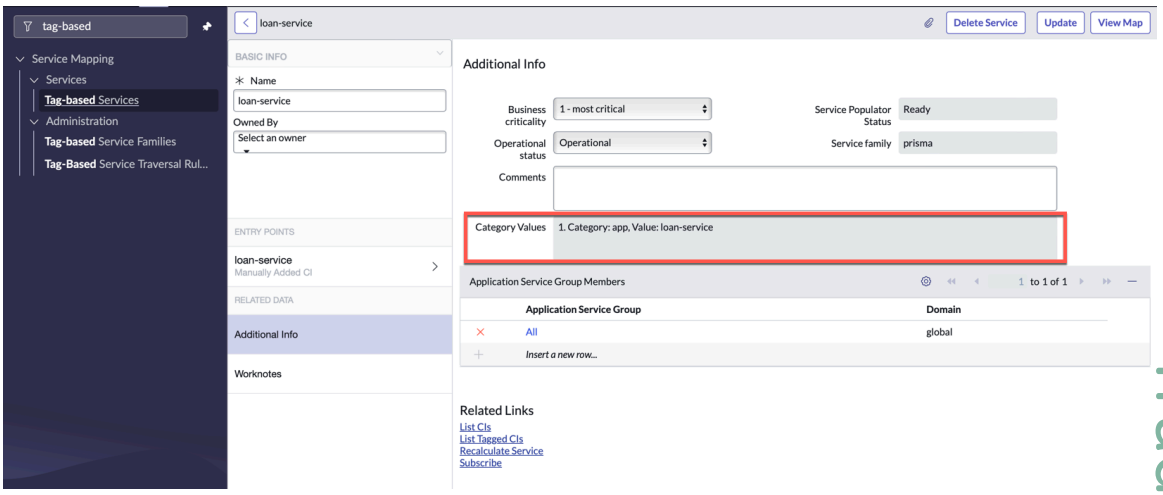


5. Vulnerability Response contêiner O usa a "Criticidade dos negócios" do "Serviço baseado em marcador" correspondente (se houver algum encontrado) para calcular o risco de um item vulnerável de contêiner.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

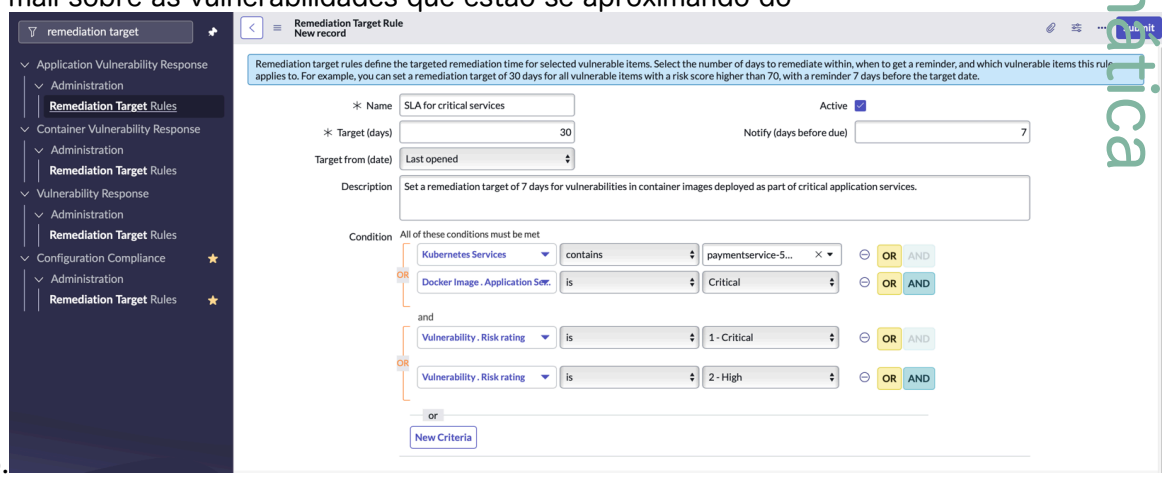




Vulnerabilidades de acompanhamento

Definir destinos de correção

ServiceNow permite que os gerentes de vulnerabilidade definam "Regras de destino de correção" para definir acordos de nível de serviço (ANSs) para corrigir vulnerabilidades encontradas em imagens de contêiner. A data de destino da correção pode ser definida com base em uma condição/critério nos metadados da imagem ou nas informações de vulnerabilidade. Os responsáveis pela correção recebem comunicação por e-mail sobre as vulnerabilidades que estão se aproximando do prazo.



Identificar vulnerabilidades corrigidas

Ao contrário das vulnerabilidades de host que podem ser corrigidas aplicando um patch em um host, as vulnerabilidades de contêiner não podem ser corrigidas. Novas versões de imagens de contêiner devem ser criadas e implantadas para substituir as versões mais antigas. As novas versões têm um identificador diferente (ID de imagem) em comparação com as versões

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

anteriores, o que dificulta o acompanhamento de quais vulnerabilidades já foram corrigidas.

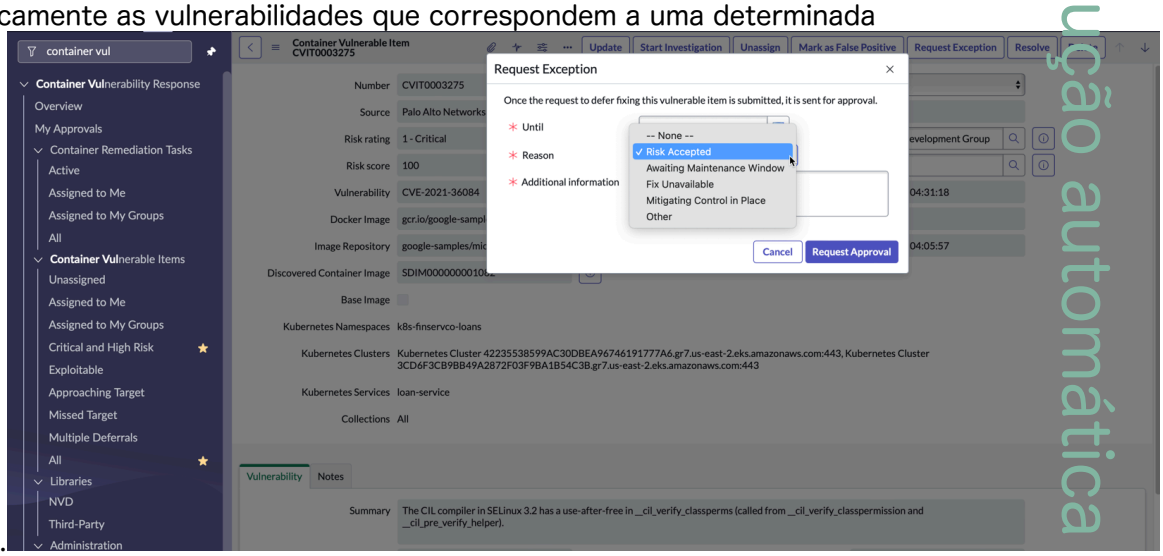
ServiceNow identifica vulnerabilidades que foram relatadas nas versões anteriores das imagens do contêiner, mas resolvidas na versão mais recente da imagem e move automaticamente essas vulnerabilidades para o estado "Encerrado/Corrigido" para que as equipes de segurança sempre tenham visibilidade precisa da postura de risco mais recente.

Gerenciar exceções

As equipes de aplicações ou os responsáveis pela correção das vulnerabilidades podem precisar da capacidade de solicitar uma exceção pelos seguintes motivos.

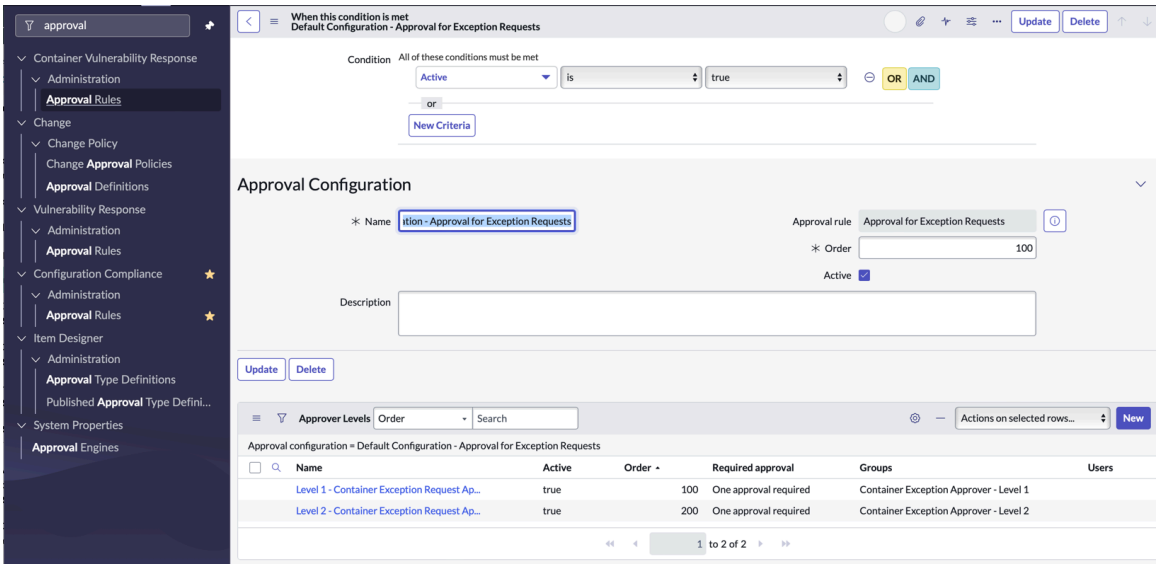
- Um controle de mitigação já está em vigor
- Risco aceito
- Aguardando a janela de manutenção para enviar a correção.

ServiceNow permite que os administradores de segurança definam vários níveis de aprovadores para solicitações de exceção. Você também pode definir regras de exceção automática que podem ser usadas para adiar automaticamente as vulnerabilidades que correspondem a uma determinada condição.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Novidades

Para saber mais sobre o que há de novo e o que mudou em Washington DC, consulte as notas de versão Washington DC.

Iniciar

- Para obter uma visão geral sobre Security Operations na sua instância Now Platform, consulte Noções básicas sobre Security Operations.
- Para obter informações sobre todas as aplicações Security Operations disponíveis para download na ServiceNow Store, consulte Security Operations e ServiceNow Store.

Explorar o Vulnerability Response contêiner

A aplicação Vulnerability Response contêiner importa itens vulneráveis de contêiner (CVITs). De acordo com as regras, o recurso permite corrigir as vulnerabilidades do contêiner. Vulnerability Response contêiner está disponível por meio de uma assinatura separada.

Ao contrário das aplicações tradicionais, os contêineres empacotam todos os códigos de origem da aplicação junto com suas dependências em um arquivo binário chamado de imagem de contêiner. A imagem é publicada em um registro para fornecer uma opção para executar essa imagem como uma aplicação ou uma instância de contêiner em qualquer plataforma. As fases em um ciclo de vida de pré-implantação de contêiner são as seguintes:

1. Compor a imagem do contêiner: a imagem do contêiner é composta e apontada para um código de origem ou uma biblioteca dependente.
2. Criar a imagem do contêiner
3. Publicar a imagem do contêiner: o arquivo de imagem do contêiner é publicado em um registro. Cada imagem tem seu próprio ID exclusivo com base no conteúdo da imagem. Essas imagens são extraídas do registro para o ambiente de tempo de execução no modo de pós-implantação. As imagens são executadas como instâncias de contêiner no host no ambiente de produção.

Verificando imagens de contêiner

Uma imagem de contêiner pode ser verificada quanto a vulnerabilidades antes ou depois da implantação. Se as imagens de contêiner forem verificadas durante a fase de pré-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

implantação, você poderá receber muitos alertas de vulnerabilidade, que podem não precisar de sua atenção imediata. No entanto, a verificação de vulnerabilidades durante a fase de pós-implantação oferece maiores benefícios, como o seguinte:

- Fornecendo visibilidade sobre o risco associado às aplicações implantadas.
- Fornecendo uma exibição focada somente nas imagens no ambiente de produção.
- Identificar e priorizar as vulnerabilidades que devem ser tratadas imediatamente.
- Agrupamento e atribuição de vulnerabilidades com base nos metadados da imagem. Por exemplo, um repositório de imagens, um rótulo de imagem e outros atributos relacionados à imagem do contêiner podem ser usados para regras de agrupamento e atribuição.

Cada imagem de contêiner tem os seguintes componentes principais:

- Repositório de contêiner ou imagem: representa a imagem do docker com um determinado repositório ou nome. Ele hospeda todas as versões da imagem.
- Imagem do Docker: representa uma versão específica da imagem do Docker de compilação.
- Contêiner do Docker: representa uma instância em execução da imagem do Docker. Cada versão tem um ID exclusivo e várias instâncias dos contêineres em execução no ambiente de produção.

Vulnerability Response contêiner módulos

O módulo Vulnerability Response contêiner fornece detalhes sobre o seguinte:

Itens vulneráveis de contêiner

Os itens vulneráveis de contêiner (CVITs) são agrupados e listados com base na atribuição, criticidade, exploração e status de correção.

Bibliotecas

Obtenha acesso ao National Vulnerability Database (NVD) e bibliotecas de terceiros. Enquanto a biblioteca do NVD fornece informações limitadas ao ID do item de vulnerabilidade, a biblioteca de terceiros fornece a maioria dos detalhes de um item de vulnerabilidade. As informações na tela do NVD são preenchidas somente quando a integração do NVD é acionada.

Administração

O módulo Administração fornece informações sobre as regras de atribuição de itens vulneráveis, regras de destino de correção e integrações de vulnerabilidade de contêiner. Além disso, você também pode configurar a duração após a qual um item vulnerável deve ser encerrado automaticamente. Você pode usar a seção Configurar granularidade de IV para configurar a granularidade de CVITs especificando as combinações de chave. Por padrão, um CVIT é criado para uma combinação de um repositório de imagens, um marcador de imagem e uma vulnerabilidade. Você pode adicionar componentes adicionais à chave para maior granularidade. Por exemplo, você pode criar um CVIT para uma combinação de repositório de imagens, marcador de imagem, vulnerabilidade e cluster.

Versões disponíveis

Versão de lançamento	Notas de versão
Vulnerability Response contêiner v2.1 Vulnerability Response contêiner v2.06	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versão de lançamento	Notas de versão
Vulnerability Response contêiner v2.0.4	

Configuração do Vulnerability Response contêiner

Antes de executar Vulnerability Response contêiner em sua instância Now Platform, você deve configurá-lo.

Como instalar Vulnerability Response e Configuration Compliance para contêineres

Antes de executar a aplicação Vulnerability Response e Configuration Compliance para contêineres em sua instância Now Platform, você deve obter o direito e baixar a aplicação do ServiceNow Store. Instale a aplicação na sua instância Now Platform e conclua algumas etapas de instalação no Assistente de configuração.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Tarefas de configuração	Descrição
Verifique se a aplicação está instalada e ativada.	Para verificar se ele está ativado, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Se a aplicação não estiver instalada e ativada, consulte Como instalar Vulnerability Response.
Verifique se você tem as funções ServiceNow necessárias atribuídas à sua instância.	A função de administrador é necessária para a instalação. Se ainda não estiver atribuído, o administrador do sistema [admin] também atribuirá a função de administrador de vulnerabilidade, sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)].

Função necessária: administrador

Procedimento

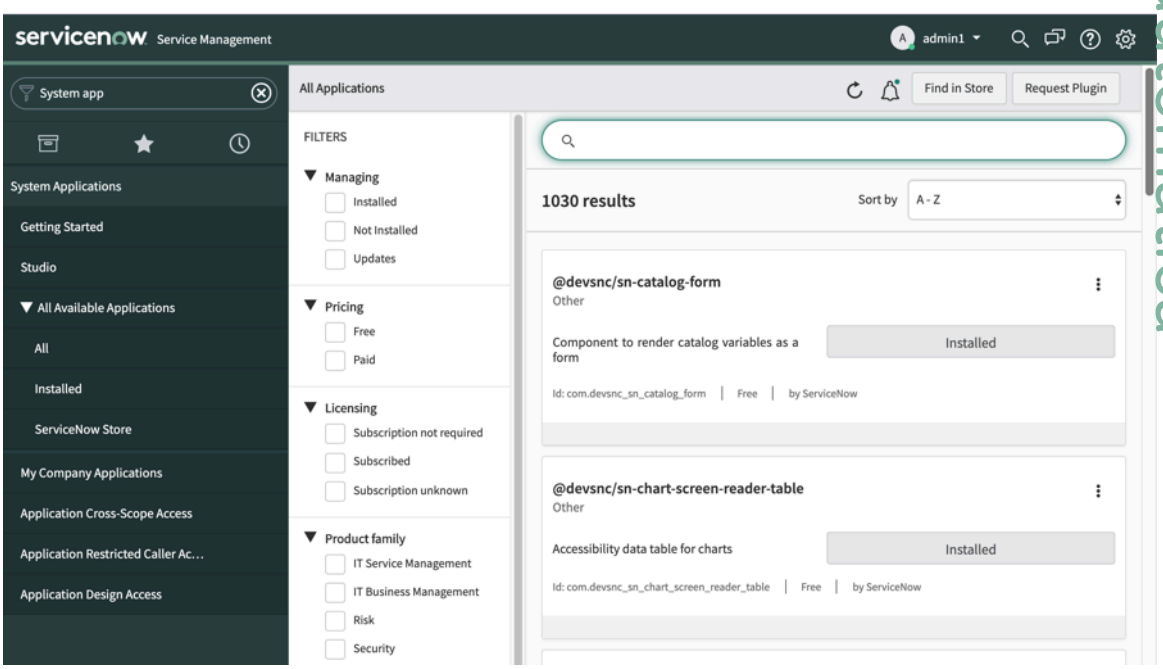
1. Para obter o direito e baixar a aplicação Vulnerability Response e Configuration Compliance para contêineres, navegue até ServiceNow Store.
2. No canto superior direito da página, clique em **Fazer login**.
3. Na barra de pesquisa, digite Vulnerability Response e Configuration Compliance para contêineres.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Em Aplicativos e soluções, clique no bloco Vulnerability Response e Configuration Compliance para contêineres.

5. Clique **em Solicitar instalação**.
6. Faça login na instância da Now Platform em que você deseja instalar a aplicação Vulnerability Response e Configuration Compliance para contêineres.
7. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.



8. Entre as aplicações listadas, localize a aplicação Vulnerability Response e Configuration Compliance para contêineres, selecione uma versão na lista e clique em **Instalar**.
   A caixa de diálogo de instalação da aplicação é exibida. Todas as dependências instaladas são exibidas.
9. Clique em **Fechar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar Gestão de exceções para Vulnerability Response contêiner

Limite a duração de uma exceção solicitada e adicione um questionário à exceção ou à solicitação de falso-positivo usando o módulo Vulnerability Response contêiner. Por padrão, uma exceção é solicitada usando o módulo ServiceNow® Vulnerability Response contêiner. Você também pode solicitar uma exceção usando a integração GRC: Policy and Compliance Management.

Antes de Iniciar

Função necessária: sn_vul_container.manage_exception_configuration

Por Que e Quando Desempenhar Esta Tarefa

Se Vulnerability Response contêiner estiver habilitado, você poderá limitar a duração pela qual uma exceção pode ser solicitada. Da mesma forma, se o módulo GRC: Policy and Compliance Management estiver instalado, você poderá selecionar GRC: Policy and Compliance Management na tela de configuração. Habilitar esta opção permite solicitar uma exceção que especifica a política e o objetivo de controle de GRC.

Se você adicionar um questionário, ele será enviado para a pessoa que gerou a exceção ou a solicitação de falso-positivo. Você pode usar o questionário padrão ou criar um com base em seus requisitos. .

É útil que o aprovador de exceção entenda o motivo da solicitação da exceção.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Administração** > **Gestão de exceção**.
2. No formulário **Configuração de gestão de exceções**, selecione como você deseja gerenciar uma exceção selecionando uma opção na lista **Gerenciar exceções usando**.
   Você pode selecionar Vulnerability Response ou GRC: Policy and Compliance Management.
3. Se você selecionou a opção Vulnerability Response, insira as seguintes informações:

Campos de Vulnerability Response

Campo	Descrição
Duração	Período para o qual uma exceção pode ser solicitada.
Unidade	Unidade de tempo para o período especificado.
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso-positivo que está sendo gerada.
Habilitar questionário para solicitar exceção	Opção para adicionar um questionário à solicitação de exceção que está sendo gerada.
Questionário para solicitar exceção	Exibe o questionário selecionado por você para solicitar uma exceção. Questionário de exceção é exibido por padrão.

Nota:
Quando você seleciona GRC: Policy and Compliance Management, os campos Duração e Unidade desaparecem, já que Governança, risco e conformidade lida com esse fluxo.

4. Selecione **Salvar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar regras de aprovação para Gestão de exceções

A partir da Vulnerability Response v15.0, use o Flow Designer para aprovar solicitações de exceção para gestão de exceções, regras de exceção e gestão de falsos positivos. Se você estiver implantando Vulnerability Response (VR) pela primeira vez, o Flow Designer será habilitado por padrão.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Para usar o Flow Designer, crie regras usando o módulo Regras de aprovação. Usando este módulo, você pode configurar regras de aprovação para cada um dos seguintes fluxos de trabalho de gestão de exceções.

- Solicitação de exceção para tarefas de correção
- Solicitação de exceção para itens vulneráveis de contêiner
- Regra de exceção
- Falso-positivo para tarefas de correção
- Falso positivo para itens vulneráveis de contêiner

Você também pode definir condições que contenham vários níveis de aprovação em uma regra. O Flow Designer herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Administração** > **Regras de aprovação**.
2. Na página Regras de aprovação, selecione o grupo para o qual você deseja definir a regra de aprovação.
3. No formulário, preencha os campos.

Formulário Regra de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Tabela	Tabela na qual a regra é aplicada.
Aplicação	O valor padrão é Vulnerability Response.
Tipo de regra	Especifica o tipo de regra. Por exemplo, gestão de exceções, falso-positivo ou regra de exceção.
Ativo	Habilitado por padrão, o que significa que a regra de aprovação está em uso.
Descrição	Descrição resumida das regras de aprovação.
Expiração da aprovação (dias) A partir da v2.5 de Vulnerability Response contêiner	Data até quando o aprovador pode aprovar a solicitação.
Aprovador do Notify (dias)	Data após a qual o aprovador é notificado para agir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
A partir da v2.5 de Vulnerability Response contêiner	

4. Selecione **Atualizar**.
   Na guia Configurações de aprovação, há dois níveis de aprovadores configurados por padrão. Você pode selecionar uma regra para definir as condições com base em diferentes casos de uso em uma regra. Para obter mais informações, consulte Criar configurações para uma regra de aprovação.

   Nota:
   Em cada página de configuração, você pode criar vários níveis de aprovação. Para obter mais informações, consulte Criar níveis de aprovação para a Gestão de exceções.

Example:
Com base em diferentes casos de uso, você pode definir diferentes processos de aprovação para as mesmas vulnerabilidades encontradas em diferentes itens de configuração.

Testes de início rápido para Vulnerability Response contêiner

Valide se Vulnerability Response contêiner ainda funciona depois de fazer qualquer alteração na configuração, como aplicar um upgrade ou desenvolver um aplicativo. Copie e personalize esses testes de início rápido para aprovar ao usar seus dados específicos da instância.

A propriedade de execução de teste está desabilitada por padrão para impedir a execução de testes em um sistema de produção. Execute testes somente em instâncias de desenvolvimento, teste e outras que não sejam de produção. Se dados de demonstração ou contas de demonstração forem criados, todos os dados de demonstração deverão ser removidos antes de usar a instância em produção ou não produção. Consulte Executar o pacote de testes do Automated Test Framework (ATF) para Vulnerability Response para obter mais informações sobre como configurar e executar o pacote de testes para Vulnerability Response contêiner.

Os testes de início rápido do Vulnerability Response contêiner exigem a ativação da aplicação Vulnerability Response contêiner (sn_vul_container).

Testes Vulnerability Response contêiner

Teste	Descrição	Versão de lançamento
CVR: Regras de atribuição	Determina se um conjunto de regras de atribuição pode atribuir automaticamente itens vulneráveis de contêiner a um grupo de atribuição para correção.	Vancouver
CVR: regra de exceção	Regras de exceção de teste.	Vancouver
CVR: marcar como fluxo falso-positivo	Teste se a opção de marcar como fluxo falso-positivo está funcionando no item vulnerável do contêiner.	Vancouver
CVR: regras de destino de correção	Crie regras de destino de correção.	Vancouver

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Testes Vulnerability Response contêiner

Teste	Descrição	Versão de lançamento
CVR: fluxo de exceção de solicitação	Teste se o fluxo de exceção de solicitação está funcionando conforme o esperado.	Vancouver
CVR: Calculadoras de vulnerabilidade	Testa as calculadoras de vulnerabilidade do contêiner.	Vancouver

Tópicos relacionados

Testes de início rápido

Executar o pacote de testes do Automated Test Framework (ATF) para Vulnerability Response contêiner

Execute o pacote de testes do Automated Test Framework (ATF) depois de instalar ou atualizar a aplicação Vulnerability Response contêiner.

Antes de Iniciar

Confirme uma instalação bem-sucedida e que sua instância funciona conforme projetado.

A propriedade de execução de teste está desabilitada por padrão para impedir a execução de testes em um sistema de produção. Execute testes somente em instâncias de desenvolvimento, teste e outras que não sejam de produção. Se dados de demonstração ou contas de demonstração forem criados, todos os dados de demonstração deverão ser removidos antes de usar a instância em produção ou não produção.

- Para habilitar o teste, siga estas etapas:
  1. Navegar até **Todos** > **Automated Test Framework (ATF)** > **Administração** > **Propriedades**.
  2. Se não estiver selecionado, marque a caixa de seleção **Habilitar execução de teste/pacote de testes**.
  3. Clique em **Salvar**.
  4. Se o escopo não estiver definido como **Container Vulnerability Response** no cabeçalho ou o escopo não for exibido no cabeçalho, clique no ícone de configurações.
  5. Na janela Configurações do sistema, clique em **Desenvolvedor**.
  6. Se não estiver selecionado, clique em **Mostrar seletor de aplicações no cabeçalho** e feche a janela.
  7. Na lista exibida ao lado de Administrador do sistema, clique em **Vulnerability Response de contêiner** para o campo.

Função necessária: admin ou atf_test_admin

Procedimento

1. Navegar até **Todos** > **Automated Test Framework (ATF)** > **Testes**.
2. Na lista Pacote, localize **Vulnerability Response e Configuration Compliance para contêineres**.
3. Selecione um teste para abrir o registro.
4. No registro aberto, marque a caixa de seleção **Ativo**.
5. Na lista relacionada Etapas de teste, selecione verdadeiro na coluna Ativo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Atualizar**.
7. Abra o teste novamente e clique em **Habilitar execução de testes e pacote de testes aqui**.
8. Habilite Propriedades de Pacote de testes/teste e Propriedades de depuração de teste.
9. Clique em **Salvar**.
10. Se o botão **Executar teste** não for exibido, atualize a tela, abra o registro novamente e clique em **Executar teste** para iniciar o teste.
    Após alguns momentos, a caixa de diálogo Executar teste indica um teste bem-sucedido. Clique **em Ir para o resultado** para obter mais informações.

O que Fazer Depois

Parabéns! Você pode continuar com a configuração de Vulnerability Response contêiner.

Para obter mais informações sobre testes automatizados para Vulnerability Response contêiner e testes automatizados, pacotes de testes e criação de testes automatizados, consulte Automated Test Framework (ATF) .

Integração do Vulnerability Response contêiner a outras aplicações

Estenda os recursos de Vulnerability Response contêiner integrando-os a outros aplicativos.

Vulnerability Response contêiner integra-se a produtos de segurança de contêiner para extrair dados de vulnerabilidade das imagens que são implantadas no tempo de execução. Em seguida, ele enriquece os dados de vulnerabilidade com as informações contextuais de tempo de execução, como hosts, clusters do Kubernetes, serviços e namespaces onde essas imagens de contêiner são implantadas. Com a descoberta do Kubernetes da ServiceNow, você pode ver as referências criadas a partir de vulnerabilidades para as entidades relevantes do Kubernetes em seu Configuration Management Database (CMDB). Além de aprimorar os metadados, a ServiceNow também oferece um painel de relatórios abrangente para fornecer informações sobre as tendências de vulnerabilidade e correção.

Vulnerability Response contêiner fornece integrações com os seguintes aplicativos:

- Integração de Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute
- Noções básicas sobre a integração [Atlassian Jira com Vulnerability Response

Anotações adicionais para integrações

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 2.1.2 do Vulnerability Response contêiner, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- *sn_sec_cmn.record_threshold_heartbeat*: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- *sn_sec_cmn.maximum_heartbeat_delay*: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Integração de Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

A integração do Prisma Cloud Compute permite que você verifique imagens de contêiner para detectar vulnerabilidades.

A partir da versão 16.1 do Vulnerability Response, você pode usar o Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute na aplicação Vulnerability Response contêiner para importar dados de vulnerabilidade de imagem de contêiner para contêineres implantados. Você pode exibir relatórios sobre vulnerabilidades e itens vulneráveis nos painéis Vulnerability Response. Essas vulnerabilidades podem ser priorizadas e corrigidas.

Se o produto Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute e sua instância Now Platform não estiverem no mesmo ambiente, você precisará usar um MID Server. Para obter mais informações, consulte Requisitos de sistema do MID Server .

Exibição das integrações

Você pode exibir as integrações que fazem parte do Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Para exibir as integrações, navegue até **Todos** > **Integração do Prisma Cloud Compute** > **Integrações**.

As seguintes integrações estão disponíveis.

Sequência de execução	Programação	Integração	Descrição
1	Diariamente	Integração de imagens de base do Prisma Cloud Compute	Recupera as vulnerabilidades das imagens de base da API do Prisma e relata as vulnerabilidades das imagens de base separadamente. Ele também cria descobertas de imagem e itens vulneráveis, que apontam para as imagens de base.
2	Diariamente	Integração de vulnerabilidades do Prisma Cloud Compute	Recupera vulnerabilidades de contêiner. Cria descobertas, CVITs e imagens de contêiner descobertas.
3	Sob demanda	Prisma Cloud Compute Containers Integration	Recupera contagens de contêiner para cada imagem não básica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuração de imagem base no Prisma

No console do Prisma, você pode configurar o registro e, em seguida, configurar as imagens de base desses registros. Se uma vulnerabilidade estiver presente na imagem base, quando você executar a integração de imagens base do Prisma Cloud Compute, a caixa de seleção **Imagem base** será marcada, indicando que as vulnerabilidades estão presentes na imagem base.

Configurar granularidade de IV

Para configurar a granularidade de CVITs, navegue até **Todos** > **Vulnerability Response do contêiner** > **Configurar granularidade de IV**e especificam as combinações de teclas. Por padrão, um CVIT é criado para uma combinação de repositório de imagens, marcador de imagem e vulnerabilidade. Você pode adicionar componentes adicionais à chave para maior granularidade. Por exemplo, você pode criar um CVIT para uma combinação de repositório de imagens, marcador de imagem, vulnerabilidade e cluster.

Processo de integração do Prisma

Quando o Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute é executado, ele verifica se existe uma vulnerabilidade e exposição comum (CVE) na tabela do banco de dados nacional de vulnerabilidades (NVD). Se já estiver presente, as informações existentes serão usadas. No entanto, se o CVE não for encontrado, os registros de espaço reservado serão gerados na tabela NVD. Ao criar esses registros NVD de espaço reservado, inicialmente somente o CVE e seu nome são preenchidos. Outros detalhes não são preenchidos com a suposição de que a integração do NVD preenche esses detalhes posteriormente. Se o parâmetro de instância de integração *update_nvd* estiver definido como verdadeiro, ele atualizará os registros NVD de espaço reservado. Por padrão, o parâmetro da instância é definido como falso. No entanto, pelo menos até que a integração do NVD seja executada e preencha esses detalhes, é necessário algum conhecimento do CVE, como sua severidade ou algumas informações básicas sobre o problema. Para atender a esse requisito, os campos **Explorar existe** e **Notas** de correção são preenchidos com os detalhes obtidos do Prisma. Além disso, essa configuração é personalizável, permitindo que você especifique outros campos que queira preencher na entrada do NVD com base nas informações fornecidas pelo Prisma.

Preparando para o Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

Você pode se preparar para Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute executando tarefas de configuração.

Antes de começar

Para instalar e configurar a aplicação Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute, você pode imprimir a check-list a seguir. Verifique se os itens listados estão concluídos antes de instalar a aplicação e importar os dados de vulnerabilidade para sua instância Now Platform®.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

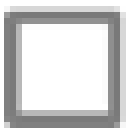
Check-list de preparação da integração

Tarefa	Descrição
☐	Verifique se você tem os seguintes conjuntos de informações: • URL base da API • Nome de usuário e senha. Essas credenciais são usadas para extrair as vulnerabilidades da integração do Prisma Cloud Compute. Para obter mais informações, consulte https://pan.dev/compute/api/ **Nota:** O MID Server é opcional. A credencial do usuário usada para a integração do Prisma Cloud Compute precisa de permissão para monitorar as imagens. Veja o seguinte código: `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	Se ainda não estiver instalado e ativado, instale a aplicação Vulnerability Response antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar a aplicação Vulnerability Response, consulte Como instalar Vulnerability Response. Esta integração requer a versão 16.1 de Vulnerability Response ou posterior.
☐	Obtenha direitos e baixe a aplicação Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute em sua instância Now Platform®.
☐	Estime o número de itens vulneráveis que você espera importar. Verifique se sua instância pode aceitar o número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a longos tempos de carregamento. Se você não souber o tamanho da sua instância ou se precisar de assistência, entre em contato com o ServiceNow Suporte técnico.
☐	Verifique se você tem os seguintes grupos ou usuários para gerenciar as integrações e corrigir os itens vulneráveis: **admin** Instale a aplicação Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidades do contêiner (sn_vul_container.vulnerability_admin) e outras funções. **sn_vul_container.vulnerability_admin** Conclui a configuração da integração do Prisma Cloud Compute. Esta função tem acesso completo à aplicação Vulnerability Response contêiner (CVR) e seus registros. Este administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
	configura integrações e regras em Vulnerability Response contêiner. **Grupo do Vulnerability Response** Por padrão, o grupo Vulnerability Response está disponível. Usuários atribuídos ao grupo Vulnerability Response herdam sn_vul.read_all, sn_vul_container.read_all. **Grupo do responsável pela correção de contêiner** Por padrão, o grupo de proprietários de correção de contêiner está disponível. Os usuários atribuídos a este grupo herdam o sn_vul_container.remediation_owner. O proprietário de correção de contêiner corrige vulnerabilidades de contêiner atribuídas a ele ou a um grupo ao qual pertence. **Analista de vulnerabilidade** Os usuários atribuídos ao grupo Analista de vulnerabilidade do contêiner herdam sn_vul.vulnerability_analyst. O Analista de vulnerabilidade monitora a correção de todos os itens vulneráveis. Se ainda não tiver sido criado, talvez você prefira criar grupos adicionais e adicionar usuários com o módulo Administração de usuários em sua instância. Para obter mais informações, consulte Criar um grupo de usuários .
	Instale a integração Vulnerability Response com o NVD e execute a API do NIST National Vulnerability Database Integration (somente CVE).

Você está pronto para Configurar a aplicação Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.

Instalar o Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

Antes de executar a integração na sua instância, conclua as etapas de instalação e configuração para que o produto Prisma Cloud Compute se integre corretamente ao Vulnerability Response contêiner. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login na instância na qual você deseja instalar o Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.
2. Navegue até o ServiceNow Store.
3. Na aplicação ServiceNow Store, pesquise a aplicação Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.
4. Clique no bloco da aplicação.
   Informações detalhadas sobre a aplicação que você está instalando são exibidas.

   Nota:
   Leia as seções **Outros requisitos** e **Dependências**, se necessário.

5. Clique em **Solicitar app** e insira suas Now Support credenciais de login.
6. Clique **em Obter**.
7. Atualize o **Nome da instância** e **o Motivo dos campos da instância** e clique em **Validar instância**.
8. Clique em **Solicitar**.
   Você receberá um e-mail com instruções detalhadas de instalação.
9. Navegar até **Aplicações do sistema** > **Candidaturas**.
10. Localize a aplicação, selecione-a e clique em **Instalar**.

Resultado
Sua aplicação é instalada automaticamente na sua instância.

O que Fazer Depois
Configure o Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute para o seu ambiente. Consulte Configurar a aplicação Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.

Configurar a aplicação Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

Instale e configure a aplicação Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Importe dados do Prisma Cloud Compute. Você pode usar os dados importados para priorizar e corrigir vulnerabilidades das imagens do Docker.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Abra o e-mail de ServiceNow que você recebeu sobre a integração.
2. Faça login na sua instância como administrador.
3. Siga as instruções no e-mail para obter o Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.
4. Navegar até **Todos** > **Integração do Prisma Cloud Compute** > **Administração** > **Configuração**.
   No formulário de configuração do Prisma Cloud Compute, preencha os campos. Para obter mais informações, consulte Formulário de configuração do Prisma Cloud Compute.
5. Na lista Projetos, selecione **Todos os projetos** ou **Projetos específicos** para configurar todos os projetos ou projetos selecionados, respectivamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você selecionar **Projetos específicos**, poderá selecionar os projetos da lista Disponível.

6. Conclua a configuração clicando em **Concluir** ou em **Salvar e testar credenciais**.
   - Se você configurou um projeto, clique em **Concluir**.
   - Se você não configurou um projeto, clique em **Salvar e testar credenciais**
7. Exiba a instância recém-criada navegando até **Integração do Prisma Cloud Compute** > **Administração** > **Instâncias de Integração**.
8. Exiba os projetos configurados anteriormente clicando em **Parâmetros de instância de integração**.
9. Execute a instância de integração recém-criada para importar os seguintes dados:
   - Imagens do Docker: lista as imagens do Docker, que são criadas usando um mecanismo de identificação e reconciliação (IRE). Cada imagem do Docker também fornece informações sobre o relacionamento entre os repositórios e as versões instaladas.
   - Imagens de contêiner descobertas: o módulo Imagens de contêiner descobertas fornece informações sobre o ID da imagem, a imagem do Docker e o repositório de imagens. Ele também armazena as informações da camada e as associa à imagem descoberta. Você também pode exibir os projetos e a contagem de contêineres aqui. Para uma imagem de contêiner descoberta, você pode exibir metadados de nuvem, como provedor de nuvem, região de nuvem, ID de conta de nuvem e IDs de recurso de nuvem.
   - Pacotes de imagem de contêiner: fornece informações sobre os pacotes em que existem vulnerabilidades. Os detalhes do pacote binário também são fornecidos como um valor separado por vírgulas.
   - Camadas de imagem do contêiner: esta tela exibe o registro de cada camada de imagem.
   - Descobertas da imagem do contêiner: esta tela exibe a lista de descobertas junto com informações sobre as vulnerabilidades associadas, camada de imagem, imagem do docker, repositório de imagens e imagem descoberta. Atualmente, as informações de vulnerabilidade são limitadas apenas ao ID. Informações adicionais são preenchidas quando a integração do NVD é acionada.
   - Itens vulneráveis do contêiner: cada descoberta tem uma vulnerabilidade correspondente. Os CVITs são criados com base na granularidade.
10. Configure a granularidade de um item vulnerável.

    a. Navegar até **Integração do Prisma Cloud Compute** > **Configurar chaves de vulnerabilidade de imagem**

    b. Configure a granularidade dos CVITs marcando as caixas de seleção necessárias.
    Os itens vulneráveis são criados com base nas chaves selecionadas, durante a próxima importação.

    Nota:
    Por padrão, um CVIT é criado para uma combinação de Repositório de imagem, Vulnerabilidade e Marcador de imagem. Você pode adicionar componentes à chave para granularidade adicional. Por exemplo, você pode criar um CVIT para uma combinação de Repositório de imagens, Vulnerabilidade, Marcador de imagem e Cluster. Depois que os itens vulneráveis ou as descobertas do item vulnerável forem criados, as caixas de seleção não serão mais editáveis.

Correção de vulnerabilidades de contêiner

O monitoramento de correção é um processo que começa com a revisão do status e termina com o fechamento de itens vulneráveis de contêiner (CVITs). Vulnerability Response

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

contêiner oferece ferramentas e procedimentos para tornar esse processo mais produtivo e eficiente.

Vulnerability Response contêiner regras da calculadora

As calculadoras de vulnerabilidade automatizam o cálculo dos valores iniciais dos campos nos itens vulneráveis do contêiner. A condição de cada calculadora é avaliada na ordem e a primeira calculadora correspondente é usada.

Para exibir e criar calculadoras de vulnerabilidade, navegue até **Todos** > **Vulnerability Response do contêiner** > **Administração** > **Calculadoras de vulnerabilidade**.

O sistema base Vulnerability Response contêiner inclui duas calculadoras de vulnerabilidade que definem a pontuação de risco base no item vulnerável do contêiner. Os seguintes grupos de calculadoras estão disponíveis no sistema de base:

- Gravidade da vulnerabilidade: calcula a pontuação de risco dos itens vulneráveis usando a severidade da vulnerabilidade normalizada.
- Calculadora de risco padrão: é baseada na regra de risco.

Ponderações de Pontuação de Risco de Vulnerabilidade

Todas as vulnerabilidades são atribuídas a uma pontuação de risco e classificação com base em fatores como severidade, criticidade, informações de exploração e assim por diante. A regra de negócios *`Update Risk Rating from Risk Score`* na tabela de item vulnerável do contêiner é responsável pelo cálculo da classificação de risco. Sempre que a pontuação de risco muda, a classificação de risco é calculada e preenchida nos itens vulneráveis do contêiner. Antes da versão 17.1 da aplicação Vulnerability Response (VR), as classificações de risco a seguir eram fornecidas como parte da inclusão de script VulnerabilityUtils, que eram codificadas.

Valor (classificação de risco)	Peso (pontuação de risco)
1	90–100
2	70–89
3	40–69
4	1 a 39
5	0

Começando com a versão 18.0 de Vulnerability Response,

- Os tipos de classificação de risco são enviados na tabela base Ponderações de pontuação de risco [sn_sec_cmn_risk_scorew_weights] como cvr_risk_rating. Esses tipos são passados como parte das regras de negócios ou inclusões de script em cada tabela em que a classificação de risco é calculada.
- O script foi modificado para que você possa consultar as entradas nos valores da tabela Ponderações de pontuação de risco para o cálculo da classificação de risco.
- Adicione entradas adicionais para um tipo existente ou crie um novo tipo. Ao criar um novo tipo, certifique-se de adicionar os rótulos para a nova classificação de risco e também de modificar os scripts e as regras de negócios relacionados. Você também deve adicionar um novo estilo para a nova pontuação de risco.
- Modifique o script para consultar os registros na tabela base.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode acessar a tabela Ponderações de pontuação de risco inserindo sn_sec_cmn_risk_score_weight no navegador de filtros.

Além disso, a pontuação de risco é recalculada automaticamente nos seguintes cenários:

- Quando um item de configuração (IC) muda de não voltado para a internet para voltado para a internet.
- Quando as Vulnerabilidades e exposições comuns (CVEs) associadas ou as entradas de terceiros (TPEs) nos itens de vulnerabilidade (IVs) estão vinculadas a uma Vulnerabilidade de exploração conhecida (KEV) de CVE.

Para obter mais informações, consulte Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade.

Vulnerability Response contêiner regras de atribuição

Defina os critérios pelos quais os itens vulneráveis de contêiner (CVITs) são atribuídos automaticamente a um grupo de atribuição para correção.

Para criar e exibir regras de atribuição para itens vulneráveis de contêiner. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Administração** > **Regras de atribuição**. Ao criar uma regra de atribuição, você pode definir as condições. Quando essas condições são atendidas, a regra atribui automaticamente os itens vulneráveis do contêiner ao grupo de usuários selecionado. Somente a primeira regra de atribuição com uma condição correspondente é executada em um registro.

Nota:
Itens vulneráveis de contêiner que não estão no estado Aberto ou que foram atribuídos manualmente são sempre excluídos.

Para obter mais informações, consulte Vulnerability Response visão geral de regras de atribuição.

Vulnerability Response contêiner regras de destino de correção

As regras de destino de correção definem o intervalo de tempo esperado para corrigir um item vulnerável de contêiner (CVIT). Essas regras são semelhantes à forma como os SLAs fornecem um intervalo de tempo para corrigir a própria vulnerabilidade.

Para criar e exibir regras de destino de correção para vulnerabilidades de contêiner, navegue até **Todos** > **Vulnerability Response do contêiner** > **Administração** > **Regras de destino de correção**.

As regras de destino de correção definem o tempo de correção de destino dos itens vulneráveis de contêiner (CVITs) selecionados. Defina um prazo para corrigir a vulnerabilidade selecionando o número de dias para a correção. Defina um lembrete para correção e defina os itens vulneráveis de contêiner aos quais a regra se aplica. Você pode definir uma meta de correção para os dias em que ela precisa ser corrigida e também definir um lembrete antes de se aproximar da data de destino. Para obter mais informações, consulte Vulnerability Response regras de destino de correção.

Gestão de exceções no Vulnerability Response contêiner

Quando sua organização não pode estar em conformidade com uma gestão de vulnerabilidades ou política de segurança, padrão ou diretriz publicada, você pode solicitar uma exceção. A gestão de exceções envolve solicitar, revisar, aprovar ou rejeitar exceções a um item vulnerável de contêiner (CVIT) que não pode ser corrigido de acordo com a política.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Algumas vulnerabilidades de contêiner (CVIT) podem não ter um patch, correção ou solução existente. Quando uma exceção é aprovada, isso também significa que você está aceitando um risco porque está reconhecendo e concordando com as consequências de não corrigir a vulnerabilidade.

Ciclo de vida de uma exceção

Definição de uma exceção

Uma exceção é uma solicitação para adiar a correção de um CVIT ou RT por um período especificado. Por exemplo, como proprietário de correção, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Solicitar uma exceção

Como proprietário da correção, você pode solicitar uma isenção para um CVIT ou RT usando o processo de gestão de exceções. Depois que o aprovador de exceção aprova esta solicitação, o **CVIT** ou RT passa para um estado Adiado.

Aprovação de uma solicitação de exceção

CVIT ou RTs que não podem ser corrigidos imediatamente são revisados por analistas de vulnerabilidade, avaliados quanto ao risco e aprovados para adiamento até que possam ser corrigidos. A aprovação de uma solicitação de exceção pode ser um fluxo de trabalho de dois níveis. Se somente o aprovador de primeiro nível estiver presente, a exceção poderá ser solicitada e aprovada. No entanto, se não houver nenhum aprovador de primeiro nível, uma exceção não poderá ser solicitada. Para obter mais informações, consulte Adicionar um aprovador de exceção.

Nota:

A partir de Vulnerability Response v15.0, se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

Depois que uma solicitação de exceção para um CVIT ou RT for aprovada, você poderá executar as seguintes ações:

- Reabrir
- Deletar
- Atualizar os campos **Atribuição a** ou **Grupos** de atribuição

Como rastrear uma solicitação de exceção

Depois de gerar a exceção, você pode rastrear seu status usando a guia **Aprovações de mudança de estado** do CVIT ou RT. Se uma ação for realizada em um RT, você não poderá rastrear o status dos CVITs individuais nesse RT.

Vencimento de uma solicitação de exceção

Quando uma solicitação de exceção para um CVIT ou RT específico expira, o CVIT ou RT afetado é revertido para o estado **Aberto**.

Se um único CVIT ou todos os CVITs em um RT forem aprovados na próxima verificação, os CVITs e, quando aplicável, o campo **Estado** do RT mudarão para **Encerrado** com o subestado **Fixo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar regras de aprovação

Exiba e configure regras de aprovação navegando até **Todos** > **Vulnerability Response do contêiner** > **Administração** > **Regras de aprovação**. Solicite uma exceção para as CVITs que não podem ser corrigidas ou adiadas imediatamente, identificando as vulnerabilidades afetadas, os itens de configuração (ICs) ou as CVITs. Automatize o processo de adiamento de CVIT. Adie as CVITs correspondentes com base nessas regras quando o sistema identificar essas CVITs.

As seguintes regras de aprovação são enviadas por padrão:

- Aprovação de solicitações de exceção: uma configuração padrão com dois níveis de aprovação é fornecida no sistema de base. Sempre que há uma solicitação de exceção em um item vulnerável, a solicitação de aprovação é enviada aos usuários ou grupos presentes no nível 1. Depois de aprovada pelos aprovadores de nível 1, ela é enviada aos aprovadores de nível 2.

  Nota:
  Você pode mudar os níveis padrão e editar conforme necessário. A partir de Vulnerability Response contêiner v2.0.6, você pode usar as propriedades do sistema fornecidas no sistema de base para aprovações de exceção por meio do fluxo de trabalho na tabela Propriedades do sistema [sys_properties]. Portanto, quando uma solicitação de falso-positivo ou exceção é gerada por meio do fluxo de trabalho, ela é enviada para aprovação dos IDs de grupo definidos na propriedade do sistema. Navegar até **Todos** > **Propriedades do sistema** e selecione *sn_vul_container.container_exception_approver_L1*, *sn_vul_container.container_exception_approver_L2*ou *sn_vul_container.container_false_positive_approver_group* para mudar o valor da propriedade.

- Aprovação para regras de exceção: não tem configuração, mas dois níveis de aprovação.
- Aprovação de falso-positivos: tem uma configuração com um nível de aprovação.

Nota:
A partir da v2.5 de Vulnerability Response contêiner, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável do contêiner muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável do contêiner ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Como solicitar e aprovar uma exceção no Vulnerability Response contêiner

Você pode solicitar o adiamento da correção de um item vulnerável de contêiner (CVIT) por um período especificado. Por exemplo, como desenvolvedor, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina. Os aprovadores que têm acesso podem aprovar solicitações de outros usuários.

Para solicitar ou aprovar uma exceção, consulte:

- Solicitar uma exceção para um item vulnerável de contêiner
- Solicitar uma exceção para vulnerabilidades de contêiner usando GRC: Policy and Compliance Management

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Notificações por e-mail são enviadas em todas as fases do gerenciamento de exceções, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma exceção é solicitada, o solicitante recebe um e-mail confirmando que a solicitação foi gerada. O aprovador também recebe um e-mail informando que uma exceção foi solicitada. A partir da v2.5 de Vulnerability Response contêiner, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável do contêiner muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável do contêiner ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Solicitar uma exceção para um item vulnerável de contêiner

Solicite uma exceção para um item vulnerável de contêiner (CVIT) que não possa ser corrigido imediatamente. Por exemplo, como proprietário de correção, você pode solicitar uma exceção se um patch não estiver disponível para uma máquina.

Antes de Iniciar

Função necessária: grupo de desenvolvedores

Procedimento

1. Navegar até **Vulnerability Response do contêiner** > **Itens vulneráveis de contêiner** > **Todos**.
2. Selecione o item para o qual você deseja solicitar uma exceção.
   O item selecionado deve estar no estado Aberto ou Em investigação.
3. No formulário Item vulnerável do contêiner, clique em **Solicitar exceção**.
   [store-future: BEGIN review]

   Nota:
   Dependendo se Vulnerability Response ou GRC: Policy and Compliance Management está selecionado no **Vulnerability Response do contêiner** > **Gestão de exceção** tela, o formulário de Exceção de solicitação muda.

   [End]
4. [store-future: BEGIN review]Se Vulnerability Response for selecionado na tela Gerenciamento de exceções, faça o seguinte.[End]

   a. No formulário, preencha os campos.

Formulário de Exceção de solicitação

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração selecionada no **Todos** > **Vulnerability Response do contêiner** > **Administração** > **Gestão de exceção** tela. Quando a solicitação de exceção expira, o grupo é revertido para o estado Aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: A partir da versão 1.2 do Vulnerability Response contêiner, se um item vulnerável foi adiado para correção usando o recurso de gestão de exceções, caso ele seja reaberto pelo scanner, a data de adiamento definida na vulnerabilidade ainda persistirá. Para habilitar esta funcionalidade, defina o valor da propriedade do sistema `sn_vul.container.auto_defer_cvit_in_active_e` como verdadeiro. Além disso, a data adiada até persiste mesmo depois que o CVIT é encerrado ou a exceção expira. A função necessária é sn_vul_container.manage_exception_configuration para leitura e gravação.
Motivo	Motivo da exceção. Estas são as opções: ▪ Risco aceito ▪ Aguardando janela de manutenção ▪ Correção indisponível ▪ Redução do controle no local ▪ Outro Para ver como adicionar novas opções de motivo, consulte Definir um mapeamento de motivo de política.
Informações adicionais	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

b. Envie a solicitação de exceção clicando em **Solicitar aprovação**.
O estado do item vulnerável do contêiner muda para Em revisão. Use a guia **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

Solicitar uma exceção para uma tarefa de correção de contêiner

Solicite uma exceção para adiar uma tarefa de correção de contêiner por um período especificado se ela não puder ser resolvida imediatamente.

Antes de Iniciar

Você pode solicitar exceções nos espaços Vulnerability Response. Consulte Solicitar uma exceção no Espaço de correção de problemas de TI.

Função necessária:

sn_vul.remediation_owner, sn_vul.app_security_Champion ou sn_vul_container.remediation_owner.

Você também pode solicitar exceções para tarefas de correção de contêiner no ambiente clássico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Tarefas de correção** > **Todos**.
2. Selecione o grupo para o qual você deseja solicitar uma exceção.
   A tarefa selecionada deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
3. No registro da tarefa de correção de contêiner, selecione **Solicitar exceção**.
4. No formulário, preencha os campos.

Formulário de Exceção de solicitação

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração da exceção definida na configuração.
Motivo	Justificativa para solicitar uma exceção.
Informações adicionais	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

5. Clique em **Solicitar Aprovação**.

Solicitar uma exceção para vulnerabilidades de contêiner usando GRC: Policy and Compliance Management

Solicite exceções de política usando o recurso de gestão de exceções de política GRCPolicy and Compliance Management na aplicação [] de dentro de Vulnerability Response contêiner.

Antes de Iniciar

Antes de usar a integração de exceção de política para solicitar exceções de política, você deve baixar a aplicação GRC: Policy and Compliance Management do ServiceNow Store.

Função necessária: sn_vul.remediation_owner

Você também pode solicitar exceções na IU clássica:

Procedimento

1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Itens vulneráveis de contêiner** (ou **Tarefas**de correção)>**Todos**e abra o item ou grupo para o qual você deseja solicitar uma exceção.
   O item ou grupo selecionado deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. No formulário selecionado, clique em **Solicitar exceção**.

Nota:
Se GRC: Policy and Compliance Management for selecionado na tela Gestão de exceções, preencha os campos no formulário Solicitar exceção. Para obter mais informações sobre os campos de formulário, consulte Formulário de Exceção de solicitação.

   a. Envie a solicitação de exceção clicando em **Solicitar aprovação**.
      O estado dos itens vulneráveis muda para Em revisão e uma exceção de política é criada. Use a guia **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

   b. Exiba a exceção de política clicando na lista relacionada Exceções de política.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Clique no número da exceção de política.

d. No campo **Aprovador**, selecione o nome do aprovador.

e. Clique na guia Origem e selecione um objetivo de **controle no campo Objetivo** de controle.

f. Clique na guia Avaliação de risco e selecione a classificação de **risco** no campo Classificação de risco.

g. Salve o formulário.

h. Clique na guia **Controles afetados**.

i. Adicione os controles clicando em **Adicionar**.

j. Salve o formulário.

Nota:
Você pode gerar uma revisão de conformidade clicando em **Solicitar revisão de conformidade**.

O formulário de aprovação é enviado ao aprovador.

O aprovador pode aprovar a solicitação clicando em **Aprovar** ou solicitar aprovação adicional clicando em **Solicitar aprovação adicional**.

O estado do registro muda para Adiado. O motivo declarado é aquele que você selecionou ao gerar a solicitação de exceção. A guia **Adiamento** fornece anotações adicionais sobre o registro.

Nota:
Se a solicitação for rejeitada, o registro será movido para o estado anterior.

3. Clique em **Enviar**.
Para obter mais informações sobre a integração de exceção de política e a transferência entre o proprietário de correção e o gerente de conformidade, consulte Configuração opcional do Policy and Compliance Management .

Definir um mapeamento de motivo de política

Defina as opções de motivo para que estejam disponíveis para qualquer usuário que solicite uma exceção.

Antes de Iniciar

Função necessária: sn_vul.compliance.manager e sn_vul_container.manage_exception_configuration

Procedimento

1. Navegar até **Todos** > **Policy and Compliance** > **Exceções da Política** > **Registro de Integração**.

Nota:
Você pode selecionar um motivo nas opções de motivo disponíveis na tabela Opções de motivo ou adicionar um novo motivo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. Clique no registro de integração do Vulnerability Response - CVIT do contêiner.
3. Na lista de Opções de motivo, clique em **Novo**.
4. Clique no ícone de lupa.
5. Adicione uma opção de motivo existente para criar uma nova.
   - Se você quiser adicionar uma opção de motivo existente, selecione um motivo.
   - Se você quiser adicionar uma nova opção de motivo à tabela Opções de motivo, clique em **Novo** e preencha os campos no formulário.

Formulário Lista de seleção de motivos

Campo	Descrição
Rótulo	Rótulo exclusivo para esta opção.
Valor	Valor exclusivo para esta opção. Este valor é mapeado na tabela Mapeamento do motivo da política para as respectivas aplicações. Para navegar até esta tabela, insira `sn_vul_policy_reason_mapping.LIST` no navegador de filtros.
Ordem	Ordem para esta opção. Os motivos são solicitados com base neste número.
Padrão	Opção para indicar que esta opção de motivo estará disponível sempre que uma exceção de política sob demanda for solicitada. Se o registro de integração não contiver opções específicas da aplicação, todas as opções de motivo que tenham o campo **Padrão** selecionado estarão disponíveis.
Ativo	Opção para exibir a opção na lista de opções de motivo.

6. Clique em **Enviar**.

Resultado
A opção de motivo é adicionada. A opção de motivo estará disponível no campo **Motivo** do formulário de solicitação de exceção de política para a aplicação selecionada.

Aprovar uma solicitação de exceção no Vulnerability Response contêiner

Aprove solicitações de exceção para itens vulneráveis de contêiner ou tarefas de correção que não possam ser corrigidas imediatamente. Você deve avaliar essas solicitações quanto ao risco e aprová-las para adiamento até que possam ser corrigidas.

Antes de Iniciar
Você pode aprovar solicitações de exceção e falso-positivo no espaço Vulnerability Response. Consulte Aprovar solicitações no Vulnerability Manager Workspace.

Função necessária: sn_vul.exception_approver

Você também pode aprovar solicitações de exceção no ambiente clássico:

Procedimento
1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprove ou rejeite a solicitação com os comentários apropriados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adiar um item vulnerável de contêiner no Vulnerability Response contêiner

Se você determinar que o problema associado a um item vulnerável de contêiner (CVIT) é de baixo risco e pode ser adiado imediatamente sem análise adicional, você pode usar o recurso **Adiar**.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Por Que e Quando Desempenhar Esta Tarefa

Um trabalho programado é executado todos os dias na verificação de itens vulneráveis adiados que atingiram a data de reabertura. No dia em que o adiamento do CVIT estiver definido para expirar, o registro será reaberto.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Itens vulneráveis de contêiner**.
2. Abra um item vulnerável.
3. Clique **em Solicitar exceção**.
4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Até	Selecione a data em que o estado Adiado expira e a tarefa de correção é reativada. **Nota:** A partir da versão 18.0 do Vulnerability Response contêiner, se um item vulnerável de contêiner adiado (CVIT) for fechado e reaberto por um scanner antes que a janela de exceção expire, o estado do CVIT será revertido para o estado adiado, respeitando a janela de exceção ativa. Para habilitar esta funcionalidade, defina o valor da propriedade do sistema `sn_vul.container.auto_defer_cvit_in_active_ex` como verdadeiro. Além disso, a data adiada até persiste mesmo depois que o item vulnerável é encerrado ou a exceção expira. A função necessária é sn_vul_container.manage_exception_configuration para leitura e gravação. Depois que o registro for enviado, se as notificações por e-mail forem definidas, os membros do grupo Vulnerability Response contêiner receberão um e-mail quando a

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	data de expiração estiver dentro de uma semana. Quando a data de adiamento expira, o item vulnerável é definido novamente como Aberto e uma segunda notificação por e-mail é enviada.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Falso positivo ○ Correção indisponível ○ Risco aceito ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Clique em **Enviar**.
   O grupo está marcado **em revisão**. Um link relacionado **Reabrir** é exibido. A data e o motivo de reabertura aparecem nas anotações de trabalho na guia **Aprovações de mudança de estado**.

   Começando com Vulnerability Response contêiner v2.3, você pode adicionar informações relevantes no campo Anotações de trabalho na seção Anotações para um item vulnerável de contêiner adiado.

Solicitar uma extensão para um item vulnerável de contêiner adiado

Solicite uma extensão para um item vulnerável de contêiner adiado antes que ele atinja o adiado até a data de vencimento. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Por Que e Quando Desempenhar Esta Tarefa
Você também pode solicitar uma extensão nos espaços Vulnerability Response. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no Espaço do gerenciador de vulnerabilidades.

Procedimento
1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Itens vulneráveis de contêiner**.
2. Abre um item vulnerável de contêiner adiado.
3. Selecione **Solicitar extensão**.

   Nota:
   O botão Solicitar extensão fica visível somente quando o estado do item vulnerável do contêiner é Adiado.

4. Preencha os campos no formulário, conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Prorrogar até	Selecione a data até quando o item vulnerável do contêiner adiado deve ser estendido para correção.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Um e-mail é acionado no envio da solicitação e na ação subsequente do aprovador.

   Nota:
   - A solicitação passa por dois níveis de aprovação.
   - Se um item vulnerável de contêiner adiado for estendido novamente, a contagem de adiamento de extensão aumentará no back-end.

6. Depois que a solicitação é aprovada, as anotações Até, Motivo e Adiamento são atualizadas.

Como trabalhar com uma regra de exceção no Vulnerability Response contêiner

Você pode solicitar uma exceção para itens vulneráveis de contêiner (CVITs) que não podem ser corrigidos ou adiados imediatamente. Ao automatizar o processo de adiamento de IV, você pode adiar os CVITs correspondentes com base na regra quando o sistema os identifica.

Você pode executar as seguintes tarefas para uma regra de exceção:

- Criar uma regra de exceção no Vulnerability Response contêiner
- Aprovar uma solicitação de regra de exceção no Vulnerability Response contêiner
- Ativação de uma regra de exceção no Vulnerability Response contêiner
- Reabrir uma regra de exceção no Vulnerability Response contêiner
- Atualizar uma regra de exceção aprovada no Vulnerability Response contêiner
- Excluir uma regra de exceção no Vulnerability Response contêiner
- Adiar um item vulnerável de contêiner no Vulnerability Response contêiner

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A partir da v2.5 de Vulnerability Response contêiner, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável do contêiner muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável do contêiner ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Criar uma regra de exceção no Vulnerability Response contêiner

Crie uma regra para solicitar automaticamente uma exceção para uma condição específica de um grupo de itens vulneráveis de contêiner (CVITs), como uma regra com uma condição que se baseia na severidade da vulnerabilidade desses CVITs. Com esta regra, você pode adiar CVITs novos e existentes automaticamente se eles corresponderem à condição de regra aprovada.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
A regra é aplicada da data "Válido a partir de" até a data "Válido até". A tarefa de correção (VUL) é criada quando a regra é aprovada. O método de agrupamento para este VUL é conhecido como regras de exceção. O VUL é criado no estado Adiado. Você não pode fechar, reabrir ou excluir este VUL. CVITs novos e reabertos são adiados e adicionados a este VUL a partir da data "Válido a partir de" até o grupo expirar na data "Válido até".

Nota:

As notificações por e-mail são enviadas em todas as fases do fluxo de trabalho da regra de exceção. Esses e-mails fornecem o status e outros detalhes de uma solicitação. Por exemplo, quando uma regra de exceção é solicitada, o solicitante recebe um e-mail que confirma que a solicitação foi enviada.

Nota:
Se a regra for rejeitada, você poderá reabri-la no estado Rascunho, atualizá-la e reenviá-la para aprovação.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Administração** > **Regras de exceção**.
2. Na página de novo registro da regra de exceção, clique em **Novo** para criar uma regra.
3. No formulário Regra de exceção, preencha os campos.

   Nota:
   Para obter mais informações sobre os campos de formulário, consulte Formulário Regra de exceção.

4. Adicione o grupo de atribuição ao criar a regra.
5. Envie o formulário para aprovação.
   O status da solicitação muda para Em revisão. Até que você envie a regra de exceção, ela permanecerá no estado Rascunho.
6. Para exibir e criar um grupo para gerenciar regras de exceção:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Navegar até **Todos** > **Administração de usuários** > **Grupos**.

b. Em uma regra de exceção, clique na guia **Aprovações solicitadas** para exibir o status da solicitação. Um trabalho programado é executado diariamente, que executa as regras de exceção nos dados existentes. Todos os itens vulneráveis que correspondem à condição são movidos para o estado Adiado. Se uma regra de exceção aprovada for excluída, todos os itens vulneráveis adiados serão revertidos para o estado anterior. Para obter mais informações, consulte Trabalhando com uma regra de exceção.

[store-future: BEGIN review]

Aprovar uma solicitação de regra de exceção no Vulnerability Response contêiner

Avalie as solicitações de regra de exceção dos usuários para que você possa aprovar ou rejeitar essas solicitações.

Antes de Iniciar

Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa

Os membros do grupo de usuários de nível 1 do aprovador de exceções podem aprovar as solicitações de regra de exceção de nível 1. Da mesma forma, os membros do grupo de usuários de nível 2 do aprovador de exceções podem aprovar as solicitações de regra de exceção de nível 2. Ambos os grupos de usuários herdam a função de aprovador de exceção por padrão.

Nota:

Se você estiver implantando a aplicação de VR pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho. Para configurar regras de aprovação para gestão de exceções e falso-positivo, consulte Configurar regras de aprovação para Gestão de exceções.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprove ou rejeite a solicitação com e explique por que você aprovou ou rejeitou a solicitação.
   Depois que uma regra de exceção é aprovada, uma tarefa de correção (RT) é criada no estado Adiado por padrão. A partir da data "Válido a partir de", esta regra é executada em todos os CVITs criados e também nos que são movidos do estado Encerrado para Aberto. CVITs que correspondem às condições definidas são adicionados ao RT e adiados pelo período especificado.

   Nota:
   Se a regra for rejeitada, você poderá reabri-la no estado Rascunho, atualizá-la e reenviá-la para aprovação.

[End]

Ativação de uma regra de exceção no Vulnerability Response contêiner

Uma regra é ativada na data "Válido a partir de". Após a ativação, ele automatiza o processo de exceção para itens vulneráveis de contêiner (CVITs).

A regra de exceção segue este ciclo de vida:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Os novos CVITs que você cria ou reabre e que atendem à condição especificada são adiados. Se você habilitar a opção Executar nos dados existentes ao executar a regra de exceção pela primeira vez, todas as CVITs ativas e não adiadas que correspondem à condição da regra de exceção serão movidas para a tarefa de correção (RT) recém-criada e seu estado será alterado para Adiado.
2. Se um CVIT recém-criado corresponder à condição de regra de exceção, ele será movido para o RT adiado que está associado à regra e a regra de grupo não será executada nele.
3. Na data "Válido a partir de", os CVITs existentes serão adicionados se você habilitar a opção Executar nos dados existentes.
4. O RT para de aceitar novos CVITs quando a regra expira na data "Válido até". O RT permanece até a data "Adiado até".
5. A regra de exceção expira na data "Válido até".

Reabrir uma regra de exceção no Vulnerability Response contêiner

Reabra uma regra de exceção que foi rejeitada, mas você deseja reenviar. Reabrir a regra a move para o estado Rascunho.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode atualizar e reenviar a regra para aprovação.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Administração** > **Regras de exceção**.
2. Encontre a regra que você deseja reabrir e clique em **Reabrir**.
3. Atualize o formulário e reenvie-o para aprovação.

Atualizar uma regra de exceção aprovada no Vulnerability Response contêiner

Cancele uma regra aprovada para poder atualizá-la. Por exemplo, antes de modificar datas ou adicionar uma condição a uma regra aprovada, você deve cancelá-la para que a tarefa de correção (VUL) seja excluída e os itens vulneráveis de contêiner (CVITs) sejam movidos para o estado Aberto.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa

As regras do grupo são reaplicadas a esses CVITs. Envie a regra depois de fazer as mudanças para que ela passe pelo processo de aprovação novamente.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Administração** > **Regras de exceção**.
2. Abra a regra de exceção que você deseja cancelar e clique em **Cancelar**.
3. Na caixa de diálogo Cancelar regra, clique em **Cancelar regra**.
   A regra retorna para o estado Rascunho e a VUL associada é excluída. Os CVITs relacionados são reabertos e as regras do grupo são aplicadas aos CVITs individuais.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Excluir uma regra de exceção no Vulnerability Response contêiner

Exclua uma regra de exceção que não seja mais necessária. Por exemplo, você pode excluir uma regra se não quiser adiar um item vulnerável de contêiner (CVIT) durante a ingestão.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
A exclusão de uma regra cancela a tarefa de correção associada (VUL). Os CVITs relacionados são reabertos e as regras do grupo são aplicadas aos CVITs individuais.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Administração** > **Regras de exceção**.
2. Abra a regra de exceção que você deseja excluir e clique em **Excluir**.
3. Na caixa de diálogo Excluir regra, clique em **Excluir regra** para excluir a regra selecionada.
   A tarefa de correção associada também é excluída. Os CVITs relacionados são reabertos e as regras do grupo são aplicadas aos CVITs individuais.

Solicitar uma extensão para uma tarefa de correção adiada no Vulnerability Response contêiner

Solicite uma extensão para uma tarefa de correção adiada (VUL) antes que ela atinja a data de vencimento. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Por Que e Quando Desempenhar Esta Tarefa
Você também pode solicitar uma extensão nos espaços Vulnerability Response. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no Espaço do gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Tarefas de correção**.
2. Abra uma tarefa de correção adiada.
3. Selecione **Solicitar extensão**.
4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Prorrogar até	Selecione a data em que o estado Adiar expira e o item vulnerável do contêiner é reativado.
Motivo	Insira o motivo para adiar o problema. As opções incluem:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Na aprovação da solicitação, as mudanças na tarefa de correção também são revertidas para os itens vulneráveis do contêiner, que fazem parte da tarefa de correção. No entanto, os itens vulneráveis do contêiner devem estar no estado adiado e seus dados atuais até precedem a data até a atualização. Um e-mail também é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma tarefa de correção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Solicitar uma extensão para uma regra de exceção no Vulnerability Response contêiner

Solicite uma extensão para uma regra de exceção adiada antes que ela atinja o adiado até a data de vencimento. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar
Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa
Você também pode solicitar uma extensão nos espaços Vulnerability Response. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no Espaço do gerenciador de vulnerabilidades.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Regras de exceção**.
2. Selecione uma regra de exceção adiada.
3. Selecione **Solicitar extensão**.
4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até quando a regra de exceção deve ser estendida.
Motivo	Insira o motivo para adiar a regra de exceção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	As opções incluem: ○ Risco aceito ○ Aguardando janela de manutenção ○ Correção indisponível ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.
   Na aprovação da solicitação, os campos Adiado até, Motivo e Informações adicionais são atualizados na regra de exceção e nos itens vulneráveis do contêiner. Um e-mail também é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para tarefas de correção criadas como parte de uma regra de exceção.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Marcar e aprovar um item de vulnerabilidade de contêiner com falso-positivo

Itens vulneráveis de contêiner (CVITs) e tarefas de correção (VULs) podem ser marcados como falsos positivos. Aprovadores com acesso de gravação podem aprovar essas solicitações de outros usuários.

- Marcar como falso-positivo em Vulnerability Response contêiner
- Aprovar um falso-positivo

Nota:

Notificações por e-mail são enviadas em todas as fases do fluxo de trabalho de falso-positivo, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma tarefa de correção ou CVIT é marcada como falso-positivo, o solicitante recebe um e-mail de confirmação. Simultaneamente, o aprovador recebe um e-mail informando que um CVIT ou tarefa de correção foi marcado como falso positivo. A partir da v2.5 de Vulnerability Response contêiner, você pode configurar os intervalos de tempo para aprovar falsos positivos e exceções, junto com notificações por e-mail para o aprovador e o solicitante após um número definido de dias. Quando uma solicitação é gerada, o item vulnerável do contêiner muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o item vulnerável do contêiner ou a tarefa de correção será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Marcar como falso-positivo em Vulnerability Response contêiner

Marque um item vulnerável de contêiner (CVIT) ou tarefa de correção como falso positivo se o aviso fornecido pelo scanner não for realmente um problema. Por exemplo, se

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

um CVIT tiver sido desativado, mas o scanner ainda estiver levantando um problema relacionado a ele, marque-o como um falso positivo.

Antes de Iniciar

Função necessária: responsável pela correção

Você pode solicitar falsos positivos nos espaços Vulnerability Response. Consulte Solicitar um falso-positivo no Espaço de correção de problemas de TI.

Você também pode solicitar falsos positivos no ambiente clássico.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response do contêiner (ou Tarefas de correção)** > **Todos**.
2. Abra o CVIT que você deseja marcar como falso-positivo e clique em **Marcar como falso-positivo**.
   O CVIT deve estar em um estado **Aberto**.
3. No formulário de falso positivo, insira os detalhes em **Informações adicionais** e clique em **Solicitar aprovação**.
   A solicitação é enviada para aprovação e o Estado do CVIT muda para **Em revisão**. O solicitante e o aprovador são notificados por e-mail.

Aprovar um falso-positivo

Como aprovador de falso-positivo, você pode aprovar solicitações de falso-positivo de outros usuários.

Antes de Iniciar

Função necessária: false_positive_approver

Você pode aprovar solicitações de exceção e falso-positivo no espaço Vulnerability Response. Consulte Aprovar solicitações no Vulnerability Manager Workspace.

Você também pode aprovar solicitações de exceção e falso-positivo no ambiente clássico:

Procedimento

1. Navegar até **Todos** > **Vulnerability Response do contêiner** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprove ou rejeite a solicitação com os comentários apropriados.

Nota:
Um falso positivo pode ter um limite de tempo. Somente o aprovador pode definir a data de término.

IT Operations Management e descoberta de padrão

Quando a descoberta está habilitada, as informações são recebidas da equipe Information Technology Operations Management (ITOM). Se o ITOM Discovery estiver habilitado, você poderá ver Namespaces do Kubernetes, Clusters do Kubernetes e Serviços do Kubernetes ao abrir um item vulnerável de contêiner (CVIT). Caso contrário, você poderá ver as informações da carga do Prisma.

Os rótulos de imagem das cargas do Prisma são armazenados como pares de chave-valor na imagem do Docker. Os rótulos em uma carga Prisma são armazenados na tabela cmdb_key_value. Para habilitar este recurso, uma regra de identificação é enviada para cmdb_ci_docker_image pela equipe do ITOM. Abra a imagem do Docker para exibir a lista de itens relacionados. A maioria dos itens é preenchida pela equipe ITOM. A entrada de identificação de uma imagem do docker é enviada para mostrar os valores como pares de chave-valor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A criticidade dos negócios é determinada com base nas informações de criticalidade do serviço recebidas da equipe ITOM. Um trabalho programado é executado para extrair dados de todos os serviços associados a uma imagem. Ele calcula a criticidade dos negócios com base no mapeamento de serviços. Como a pontuação de risco pode depender da criticidade dos negócios, a pontuação de risco também é calculada com base nela.

Soluções de análise e relatório para Vulnerability Response contêiner

Este Solução Análise da plataforma contém conteúdo Platform Analytics] pré-empacotado para uso com outros produtos Now Platform. Este Solução Análise da plataforma fornece uma exposição sobre como as vulnerabilidades são gerenciadas por meio de vários gráficos.

Funções necessárias

As seguintes funções e tarefas estão associadas a esta Solução:

- Now Platform administrador (admin): instale e ative esta Solução de análise e relatório e faça as mudanças necessárias nas propriedades do sistema.
- Platform Analytics Administrador (pa_admin): revise os indicadores, detalhamentos, widgets e painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.

Tópicos relacionados

Soluções de análise e relatório

Painel do Vulnerability Response contêiner

As Soluções de análise e relatório contêm conteúdo pré-empacotado de Performance Analytics e Relatórios para uso com outros produtos Now Platform. Este Solução Análise da plataforma permite rastrear o volume, o desempenho e o progresso das vulnerabilidades, desde a análise e detecção iniciais até a contenção ou correção. Você pode filtrar relatórios por grupo de atribuição, explorações, classificação de risco ou estado.

Funções necessárias de Now Platform

- Now Platform administrador (admin): instale e ative esta Solução de análise e relatório e faça as mudanças necessárias nas propriedades do sistema.
- Performance Analytics Administrador (pa_admin): revise os indicadores, detalhamentos, widgets e painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.

Acessar os painéis de Vulnerability Response contêiner

Para abrir o painel, navegue até **Todos** > **Vulnerability Response do contêiner** > **Visão geral**.

A partir da versão 2.2 do Vulnerability Response contêiner, este painel também pode ser exibido na IU da nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e selecione o ícone **Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, selecione o menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Visão geral dos painéis e Visão geral dos painéis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

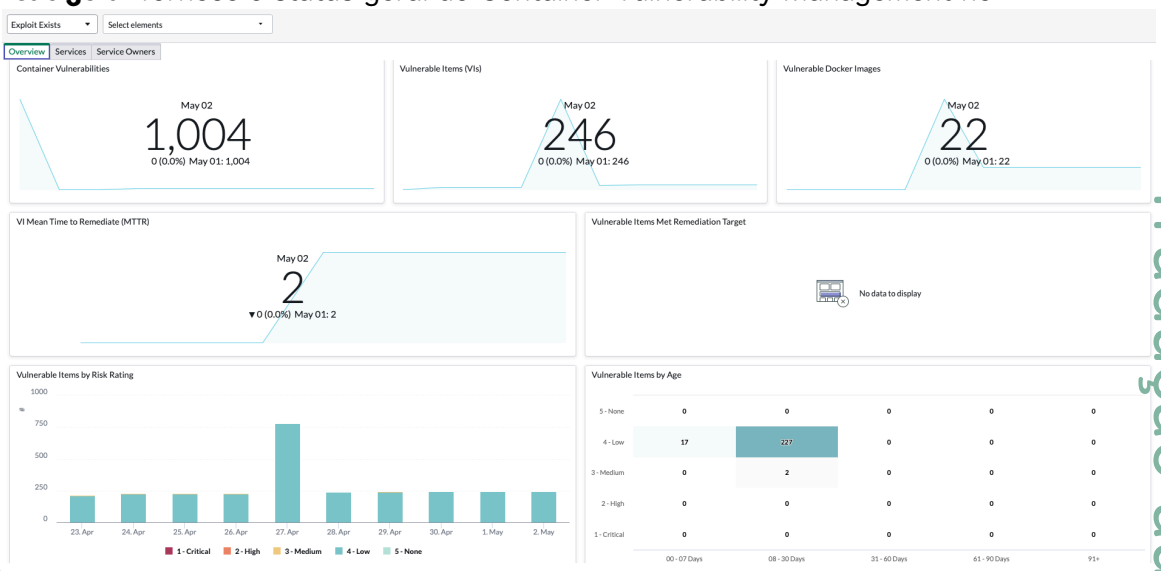
Nota:

- Se você for um novo usuário, poderá exibir os painéis somente nos espaços.
- Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Guias do Container Vulnerability Management

Este painel permite que você veja as vulnerabilidades que estão presentes nos contêineres. Você pode exibir as vulnerabilidades e os dados relacionados por região, idade, serviços e outros detalhamentos.

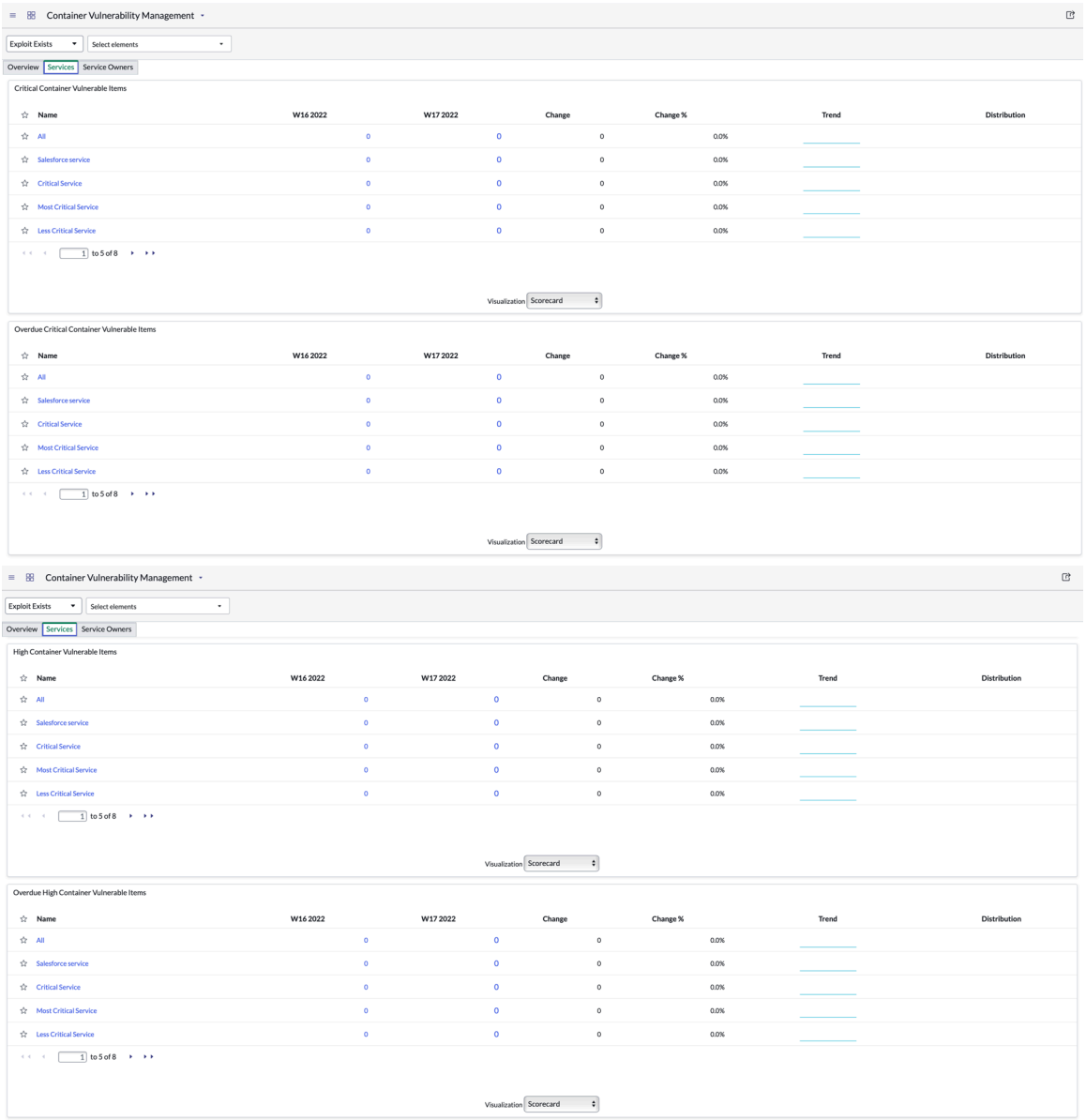
A guia **Visão geral** fornece o status geral do Container Vulnerability Management no sistema.



A guia **Serviços** mostra itens vulneráveis de contêiner que afetam os serviços de aplicações.

Tradução automática

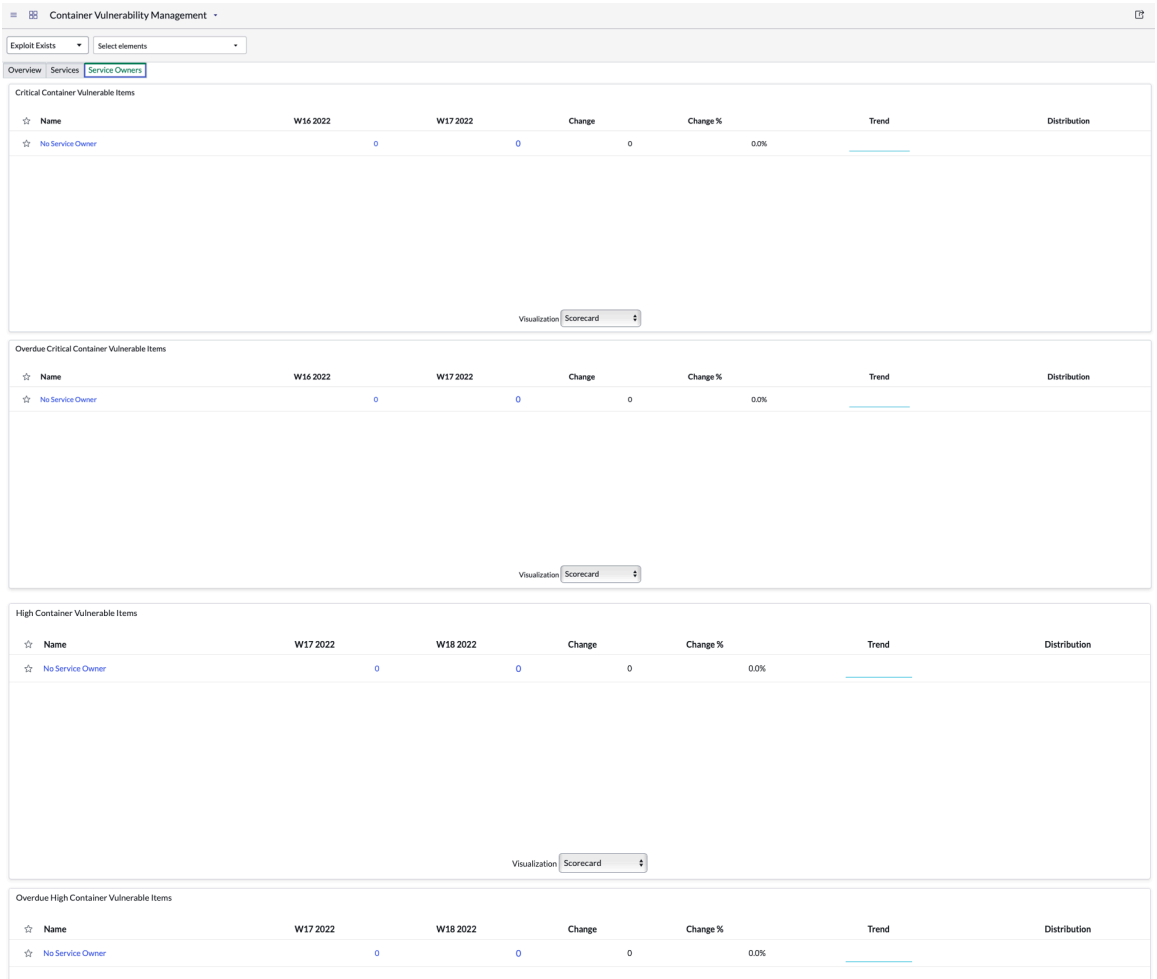
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A guia **Responsáveis pelo serviço** mostra os itens vulneráveis de contêiner que afetam os responsáveis pelo serviço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Detalhamentos

- Explorar Itens Existentes
- Explorar Vetor de Ataque
- Explorar Nível de Habilidade
- Status do Destino de Correção
- Pontuação de risco
- Estado
- Grupo de atribuição

Tradução automática

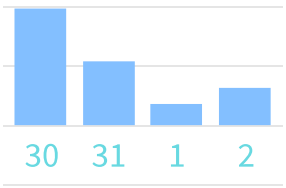
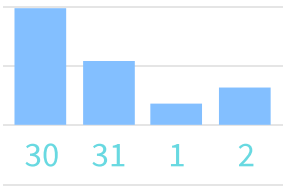
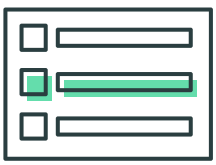
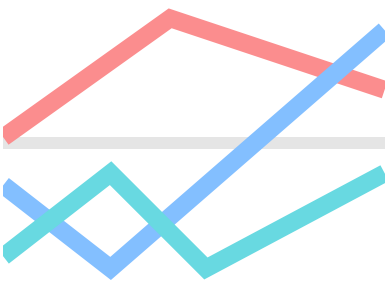
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações de dados

Nome	Tipo	Descrição
Vulnerabilidades do contêiner	Pontuação única	Número de vulnerabilidades de contêiner associadas a um ou mais itens vulneráveis de contêiner ativos.
Itens vulneráveis (IVs)	Pontuação única	Número de itens vulneráveis do contêiner ativos (não encerrados).
Imagens do Docker vulneráveis	Pontuação única	Número de imagens do docker associadas aos itens vulneráveis de contêiner ativos.
Tempo médio de correção (MTTR) do IV	Pontuação única	O tempo médio para corrigir (encerrar) um item vulnerável, exibido como uma média de 30 dias de execução.
Itens vulneráveis que atenderam à meta de correção	Pontuação única	Percentual de itens vulneráveis de contêiner encerrados que atingiram as datas de destino de correção nos trimestres atuais e anteriores. As metas de correção são calculadas a partir da data da última abertura mais o número de dias.

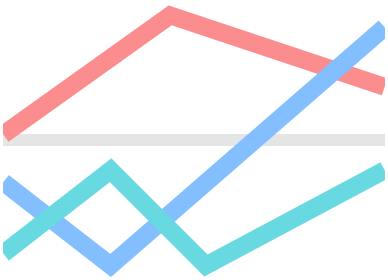
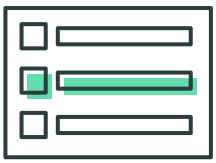
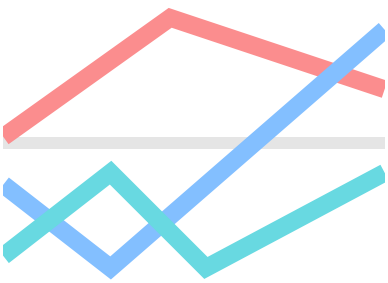
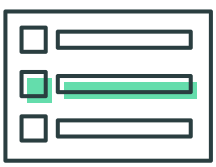
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Itens vulneráveis por classificação de risco	Barra 	Número de itens vulneráveis de contêiner ativo, agrupados por classificação de risco no período selecionado.
Itens vulneráveis conforme o tempo decorrido	Barra 	Número de itens vulneráveis de contêiner ativos agrupados por classificação de risco e idade (em dias).
Itens vulneráveis de contêineres críticos	Lista e   de linhas	Número de itens vulneráveis de contêiner ativos com uma classificação de risco crítica, agrupados por serviço.

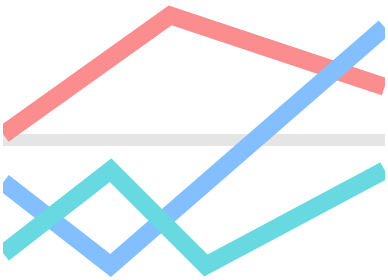
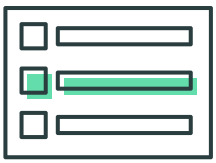
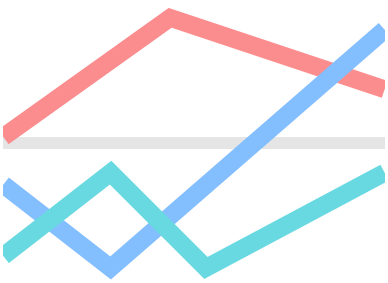
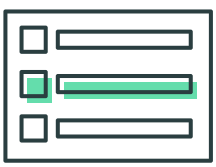
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Itens vulneráveis de contêineres muito atrasados	Lista e linha  de 	Número de itens vulneráveis de contêiner ativos com uma classificação de risco crítica e suas datas de destino de correção, agrupados por serviço.
Itens de alta vulnerabilidade de contêineres	Lista e linha  de 	Número de itens vulneráveis de contêiner ativos com uma classificação de risco alta, agrupados por serviço.

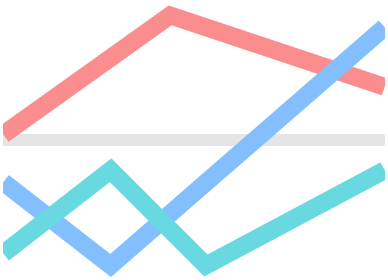
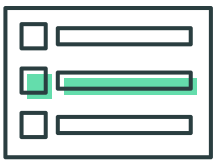
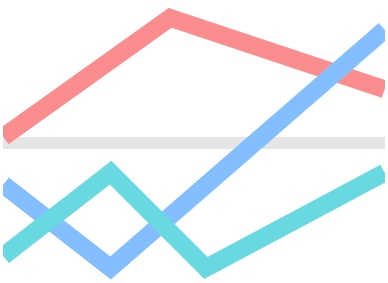
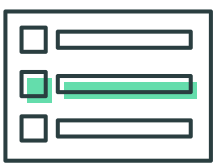
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Itens vulneráveis de contêineres muito atrasados	Lista e linha  de 	Número de itens vulneráveis ativos com uma classificação de risco alta e suas datas de destino de correção, agrupados por serviço.
Itens vulneráveis de contêineres críticos	Lista e linha  de 	Número de itens vulneráveis de contêiner ativos com uma classificação de risco crítica, agrupados por responsável pelo serviço.

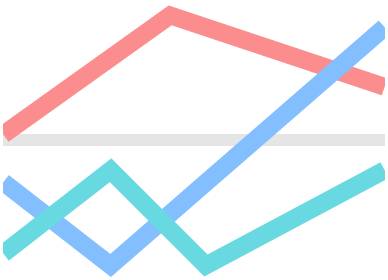
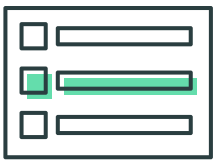
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Itens vulneráveis de contêineres muito atrasados	Lista e linha  de 	Número de itens vulneráveis de contêiner ativos com uma classificação de risco crítica e suas datas de destino de correção, agrupados por responsável pelo serviço.
Itens de alta vulnerabilidade de contêineres	Lista e linha  de 	Número de itens vulneráveis de contêiner ativos com uma classificação de risco alta, agrupados por responsável pelo serviço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Itens vulneráveis de contêineres muito atrasados	Lista e linha  de 	Número de itens vulneráveis ativos com uma classificação de risco alta e suas datas de destino de correção, agrupados por responsável pelo serviço.

Referência do Vulnerability Response contêiner

Tópicos de referência que contêm informações sobre tabelas, funções e propriedades instaladas com o Vulnerability Response contêiner.

Componentes instalados com Vulnerability Response contêiner

Vários tipos de componentes são instalados com a ativação da aplicação Vulnerability Response contêiner, incluindo tabelas, funções de usuário e trabalhos programados.

Nota:
A tabela Arquivos da Aplicação lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

Funções instaladas com Vulnerability Response contêiner

As funções são adicionadas com a ativação de Vulnerability Response contêiner.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que usuários e grupos podem ver e fazer na aplicação Vulnerability Response. Para obter uma atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração. Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Se você for um cliente de atualização, o acesso dos usuários e grupos atribuídos com as permissões sn_vul.vulnerability_read e sn_vul.vulnerability_write anteriores à v10.3 não foi alterado. Usuários e grupos permanecem atribuídos com essas funções até que você os altere. No entanto, a partir da v10.3, você pode preferir atribuir funções granulares para ter mais controle sobre o que usuários e grupos podem fazer e ver na aplicação Vulnerability Response. Para obter uma visão geral e mais informações sobre como gerenciar essas funções, consulte Vulnerability Response personas e funções granulares e Gerenciar persona e funções granulares para Vulnerability Response.

Título da função [nome]	Descrição
sn_vul_container.ci_manager	Gerencia a reclassificação de iten configuração (ICs) incompatíveis
sn_vul_container.configure_integrations	Configura integrações de contêin
sn_vul_container.configure_vi_granularity	Configura a granularidade do iten contêiner.
sn_vul_container.create_vi	Pode criar itens vulneráveis de co manualmente.
sn_vul_container.delete_vi	Pode excluir itens vulneráveis de criados manualmente.
sn_vul_container.exception_approver	Aprova exceções, adiamentos e f itens vulneráveis de contêiner. A partir da v2.3, a função sn_vul_container.read_all, fo desta função para que você acessar os itens vulneráveis contêiner e as tarefas de co atribuídos a você e seu gru todos os itens vulneráveis e tarefas de correção.
sn_vul_container.false_positive_approver	Aprova ou rejeita o fechamento d vulneráveis de contêiner como un
sn_vul_container.manage_assignment_rules	Define e atualiza as regras de atri vulneráveis de contêiner.
sn_vul_container.manage_auto_close_stale_vi	Configurar os itens vulneráveis d obsoleto de fechamento automáti
sn_vul_container.manage_auto_exception_rule	Gerenciar regras de exceção (cria excluir)
sn_vul_container.manage_normalized_severity	Pode atualizar o mapeamento par severidade.
sn_vul_container.manage_permissions	Pode atribuir funções de resposta vulnerabilidade de contêiner a us
sn_vul_container.manage_remediation_targ…	Define e atualiza as regras de des de contêiner.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição
sn_vul_container.manage_risk_score_confi...	Define e atualiza calculadoras de risco, regras de risco e calculador de vulnerabilidade para itens vuln contêiner.
sn_vul_container.read_all	Pode exibir todos os itens vulnera contêiner e informações relaciona
sn_vul_container.read_assigned	Pode exibir itens vulneráveis de c atribuídos a mim ou aos meus gru
sn_vul_container.read_assignment_rules	Pode exibir regras de atribuição c vulneráveis de contêiner.
sn_vul_container.read_auto_exception_rule	Regras de exceção de leitura
sn_vul_container.read_discovered_image	Pode exibir itens descobertos.
sn_vul_container.read_integrations	Pode exibir resultados de execuç integração.
sn_vul_container.read_normalized_severity	Pode exibir o mapeamento de sev normalizado.
sn_vul_container.read_remediation_target...	Pode exibir Regras de destino de
sn_vul_container.read_risk_score_configu...	Pode exibir calculadoras de pontu regras de risco e calculadoras de de vulnerabilidade para itens vuln contêiner.
sn_vul_container.remediation_owner	Lê e grava itens vulneráveis de co atribuídos a eles. Os registros de também podem ser lidos por um função.
sn_vul_container.update_assigned_to	Pode atualizar a atribuição vulneráveis de contêiner. Requer sn_vul_container.wr sn_vul_container.write_assi
sn_vul_container.update_assignment_group	Pode atualizar o grupo de a para itens vulneráveis de co Requer sn_vul_container.wr sn_vul_container.write_assi
sn_vul_container.update_state	Pode atualizar estados de i vulneráveis. Requer sn_vul_container.wr sn_vul_container.write_assi
sn_vul_container.vulnerability_admin	Configura todas as regras, integra por diante para o produto Vulnera contêiner.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição
sn_vul_container.vulnerability_analyst	Monitora a correção de todos os i de contêiner.
sn_vul_container.write_all	Pode atualizar todos os itens vuln contêiner e tarefas de correção.
sn_vul_container.write_assigned	Pode atualizar itens vulneráveis c tarefas de correção atribuídas a m grupos.
sn_vul_container.read_watch_topic	Pode ler tópicos de observação pa vulnerabilidades de contêiner.
sn_vul_container.create_watch_topic	Pode criar tópicos de observação vulnerabilidades de contêiner.
sn_vul_container.edit_watch_topic	Pode editar tópicos de observaçã vulnerabilidades de contêiner.
sn_vul_container.manage_exception_configuration	Pode gerenciar configurações de exceções.

Tabelas instaladas com Vulnerability Response contêiner

As tabelas são adicionadas com a ativação de Vulnerability Response contêiner (CVR).

Tabela	Descrição
Descoberta de imagem do contêiner sn_vul_container_image_findings	Armazena informações sobre as vulnerabilidades associadas, camada de imagem, imagem do docker, repositório de imagens e imagem descoberta.
Camada da imagem do contêiner sn_vul_container_image_layer	Contém as informações de cada camada de imagem. Uma imagem é um arquivo estático com código executável que pode criar um contêiner em um sistema de computação.
Pacote de imagem do contêiner sn_vul_container_image_package	Fornece informações sobre os pacotes em que existem vulnerabilidades. Os detalhes do pacote binário também são fornecidos como um valor separado por vírgulas.
Item vulnerável de contêiner sn_vul_container_image_vulnerable_item	Contém detalhes de cada descoberta e a vulnerabilidade correspondente.
Imagem de contêiner descoberta sn_vul_container_image	Fornece informações sobre o ID da imagem, a imagem do Docker e o repositório de imagens. Ele também armazena as informações da camada e as associa à imagem descoberta.
Encontrando mapeamentos sn_vul_container_finding_m2m_vul_item	Relacionamento M2M das descobertas da imagem do contêiner e dos itens vulneráveis do contêiner (CVITs).
Encerrar automaticamente itens vulneráveis sn_vul_container_image_auto_close_config	Contém as informações sobre como fechar as descobertas de imagem do contêiner obsoletas e acumular o estado para os CVITs.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Chaves de vulnerabilidade da imagem do contêiner sn_vul_container_image_vulnerability_keys	Contém a configuração de granularidade para criação de CVITs a partir das descobertas da imagem do contêiner.
Serviços relacionados ao Docker sn_vul_container_m2m_ci_services	Contém todos os serviços de negócios relacionados a uma imagem de contêiner.
Contagens de contêineres de VR sn_vul_container_vr_container_counts	Contém a média contínua de instâncias de contêiner geradas a partir de uma imagem de contêiner nos últimos 90 dias.
Item de Tarefa de correção de contêiner sn_vul_container_m2m_vul_group_item	Tabela M2M entre CVIT e tarefas de correção de contêiner.
Tarefa de correção de contêiner sn_vul_container_vulnerability	Contém tarefas de correção de contêiner.
Manifesto de tarefa de correção de contêiner sn_vul_container_rt_manifest	Todas as atualizações na tarefa de correção serão feitas usando esta tabela de manifesto por trabalhos programados.

Trabalhos programados instalados com Vulnerability Response contêiner

Trabalhos programados são adicionados com a ativação de Vulnerability Response contêiner.

Trabalho programado	Descrição
Associar IVs de contêiner existentes à regra de exceção automática	Associa automaticamente a regra de exceção automática aos itens vulneráveis de contêiner (CVITs) existentes.
Verificar expiração do adiamento do item vulnerável do contêiner	Envia notificações se os itens vulneráveis do contêiner ou as vulnerabilidades do contêiner expirarem (e se eles expirarem em uma semana).
Contagem de contêineres do Vulnerability Response (aplicação - Vulnerability Response e Configuration Compliance para contêineres)	É executado diariamente para preencher a tabela sn_vul_container_vr_container_counts que calcula a média contínua de 90 dias para contêineres.
CVITs de encerramento automático	Fecha automaticamente os itens de vulnerabilidade do contêiner que correspondem à condição definida na configuração de fechamento automático. O status deles é alterado para "fixo".
Calcular criticalidade dos negócios para CVIT	Processa todos os CVITs ativos e atualiza o campo Criticalidade dos negócios, com base nos serviços afetados da imagem do docker do CVIT.
Fechar e cancelar CVITs que não têm uma imagem do Docker associada	Expira automaticamente os CVITs que não têm um IC associado a. O estado deles é definido como Encerrado e o subestado como Cancelado.
Calcular contagens de IV relacionadas para tarefa de correção de contêiner	Calcula as contagens nos registros da Tarefa de correção de contêiner.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho programado	Descrição
Acumular valores de item vulnerável de contêiner para vulnerabilidade e grupo	Calcula vulnerabilidades e acúmulos de grupo para itens vulneráveis de contêiner.

Vulnerability Response contêiner glossário

Saiba mais sobre termos e conceitos exclusivos de Vulnerability Response contêiner.

Termos-chave

Contêiner

Uma unidade de software que empacota o código e todas as suas dependências para que a aplicação seja executada de forma contínua e confiável de um ambiente de computação para outro.

Imagem do contêiner

Um arquivo estático com código executável que pode criar um contêiner em um sistema de computação. Uma imagem de contêiner não pode ser alterada e, portanto, pode ser implantada de forma consistente em qualquer ambiente.

Cluster

Um conjunto de máquinas de trabalho, chamadas de nós, que executam aplicações em contêineres.

Docker

Software para criar, implantar e gerenciar contêineres de aplicações em servidores e na nuvem.

Imagem do Docker

Um arquivo de modelo que contém código, bibliotecas necessárias, configurações e assim por diante. O arquivo é usado para iniciar instâncias de contêiner. Ele consiste em uma união de sistemas de arquivos em camadas.

Dockerfile

Um arquivo de texto que contém instruções para criar imagens de contêiner adicionando várias camadas. Por exemplo, camadas de código base do Ubuntu, Nginx e do aplicativo.

Composição do Docker

Uma ferramenta para definir e executar aplicações complexas com o Docker. Com o Compose, você pode definir uma aplicação de vários contêineres em um único arquivo.

Contêiner do Docker

Um contêiner do Docker é uma instância de tempo de execução iniciada a partir de uma imagem do Docker.

Camada de imagem

Uma camada é uma modificação de uma imagem. É representado por uma instrução no Dockerfile. As camadas são aplicadas em sequência à imagem base para criar a imagem final.

Repositório de imagem

Uma coleção de imagens do Docker com diferentes marcadores ou versões.

Rótulos de imagem

Um conjunto de pares de chave-valor armazenados com a imagem como metadados.

Namespace

Uma abstração usada pelo Kubernetes para oferecer suporte ao isolamento de grupos de recursos em um único cluster.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pod

Um conjunto de contêineres em execução (outra abstração além de um contêiner).

Registro

Um serviço hospedado que contém repositórios de imagens.

Serviço

Uma maneira abstrata de expor uma aplicação em execução em um conjunto de pods como um serviço de rede.

Marcador

Um marcador é um rótulo aplicado a uma imagem do Docker em um determinado repositório de imagens. As tags são como várias imagens em um repositório são diferenciadas umas das outras.

Formulário de configuração do Prisma Cloud Compute

O formulário de configuração do Prisma Cloud Compute é acessado no módulo Prisma Cloud Compute Integration.

Para exibir o formulário de configuração do Prisma Cloud Compute, navegue até **Todos** > **Integração do Prisma Cloud Compute** > **Administração** > **Configuração**.

Configuração do Prisma Cloud Compute

Campo	Descrição
Instância de Integração	Nome da nova instância de integração. Você pode criar uma instância ou clicar no ícone de pesquisa para selecionar uma instância existente.
URL Base da API	URL para integração com o Prisma Cloud Compute.
Nome do usuário	Nome de usuário para acessar o Prisma Cloud Compute.
Senha	Senha para acessar o Prisma Cloud Compute.
MID Server	Uma aplicação Java que é executada como um serviço do Windows ou daemon do UNIX em um servidor em sua rede local. O MID Server permite a comunicação e a movimentação de dados entre uma instância ServiceNow e aplicações externas, fontes de dados e serviços.
Usar projetos	Opção para configurar os projetos. Ao marcar a caixa de seleção, você pode selecionar projetos na página de configuração e executar as integrações com base nos projetos configurados para preencher os detalhes específicos do projeto. **Nota:** Se esta caixa de seleção estiver marcada, a guia **Configurar projetos** será habilitada. Clique em **Avançar** para prosseguir com a configuração dos projetos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de Exceção de solicitação

Solicite exceções de política usando o recurso de gestão de exceções de política GRCPolicy and Compliance Management na aplicação [] de dentro de Vulnerability Response contêiner.

Para exibir o formulário de configuração do Prisma Cloud Compute, navegue até **Todos** > **Vulnerability Response do contêiner** > **Itens vulneráveis de contêiner** (ou **Tarefas**de correção)>**Todos**e abra o item ou grupo para o qual você deseja solicitar uma exceção.

Formulário de Exceção de solicitação

Campo	Descrição
Política	Política de gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válido de	Data em que a exceção será iniciada. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até	Data em que a exceção de política expira e quando o estado do item ou grupo vulnerável muda de Adiado para Aberto. **Nota:** O número de dias em que a exceção de política é válida não pode exceder a **Duração máxima da exceção (dias)** que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Criar uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser preenchido pelo responsável pela correção.

Formulário Regra de exceção

Crie uma regra para solicitar automaticamente uma exceção para uma condição específica de um grupo de itens vulneráveis de contêiner (CVITs), como uma regra com uma condição que se baseia na severidade da vulnerabilidade desses CVITs. Com esta regra, você pode adiar CVITs novos e existentes automaticamente se eles corresponderem à condição de regra aprovada.

Para exibir o formulário Regra de exceção, navegue até **Todos** > **Vulnerability Response do contêiner** > **Administração** > **Regras de exceção**.

Formulário Regra de exceção

Campo	Descrição
Nome	Nome da regra de exceção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Regra de exceção

Campo	Descrição
Válido de	Data a partir da qual esta regra está ativa para adiar os CVITs.
Válido até	Data a partir da qual a tarefa de correção para de aceitar novos CVITs.
Motivo	Motivo para criar esta regra de exceção.
Grupo de atribuição	Grupo ao qual a tarefa de correção criada para rastrear as CVITs adiadas é atribuída.
Informações adicionais	Informações adicionais que o solicitante deseja fornecer ao aprovador. Essas informações são preenchidas no campo de descrição da tarefa de correção.
Condição	Condição de filtro para os CVITs que podem ser definidos durante o processamento dos CVITs.
Executar em dados existentes	Opção que permite executar esta regra em dados existentes na primeira vez em que esta regra é executada.
Fase do fluxo de trabalho	Status de aprovação atual da regra de exceção.
Estado	Estado da regra de exceção.
Ordem de execução	Ordem exclusiva para cada regra de exceção.
Adiado até	Data até quando as VULs e CVITs são adiadas. Nesta data, o VUL criado é encerrado, todos os CVITs são movidos para fora do grupo e as regras do grupo são reaplicadas.

Tradução automática

Configuration Compliance

A aplicação ServiceNow® Configuration Compliance é uma aplicação de avaliação de configuração segura (SCA) que agrega resultados de verificação de integrações com aplicações de verificação de configuração de terceiros. Você pode priorizar problemas de conformidade de configuração usando seu Configuration Management Database (CMDB). O Configuration Compliance se integra totalmente ao processo de gerenciamento de mudanças de TI para corrigir suas configurações fora de conformidade.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

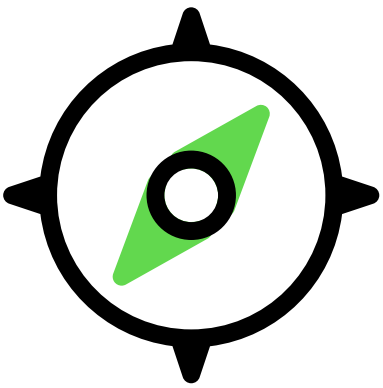
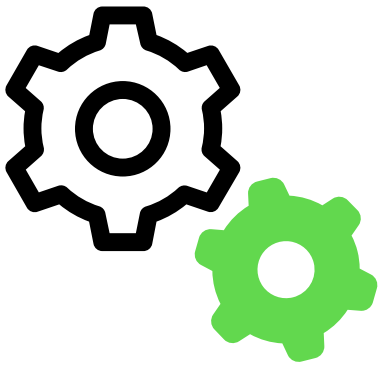
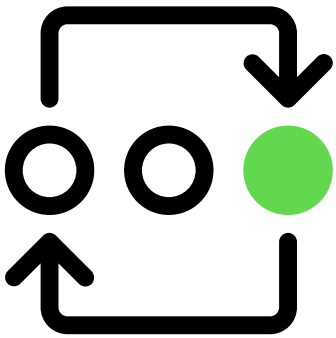
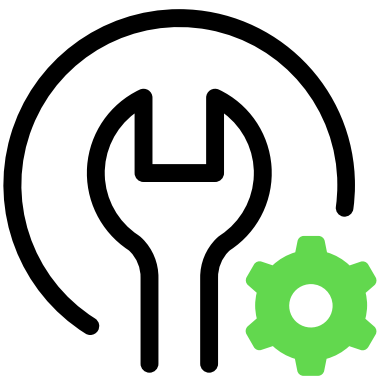
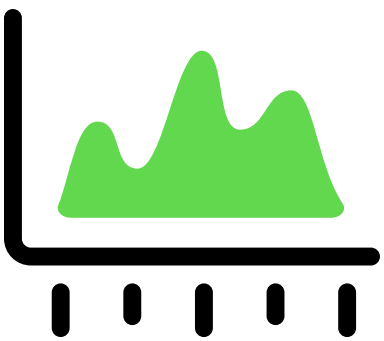
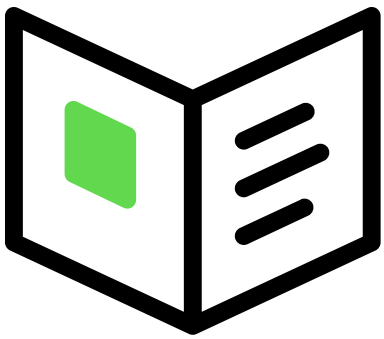
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A partir da versão 18.0 do Vulnerability Response, é possível monitorar e corrigir problemas de configuração no Vulnerability Manager Workspace e no IT Remediation Workspace, respectivamente. Para obter mais informações, consulte Explorando o Vulnerability Manager Workspace e Explorando o Espaço de correção de problemas de TI.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Configuration Compliance

Explorar	Configurar	Integrar
		
Saiba mais sobre os conceitos e recursos do Configuration Compliance	Configurar o Configuration Compliance	Estenda o Configuration Compliance integrando-o a outros aplicativos
Corrigir	**Análise e Relatórios**	**Referência**
		
Saiba como corrigir seus ativos fora de conformidade com o Configuration Compliance	Exibir análise do Configuration Compliance	Veja os detalhes sobre os componentes do Configuration Compliance, como campos, tabelas e propriedades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorar o Configuration Compliance

Use os resultados de testes obtidos de integrações de avaliação de configuração segura (SCA) de terceiros para verificar a conformidade com as políticas corporativas ou de segurança. Identifique, priorize e corrija itens de configuração fora de conformidade.

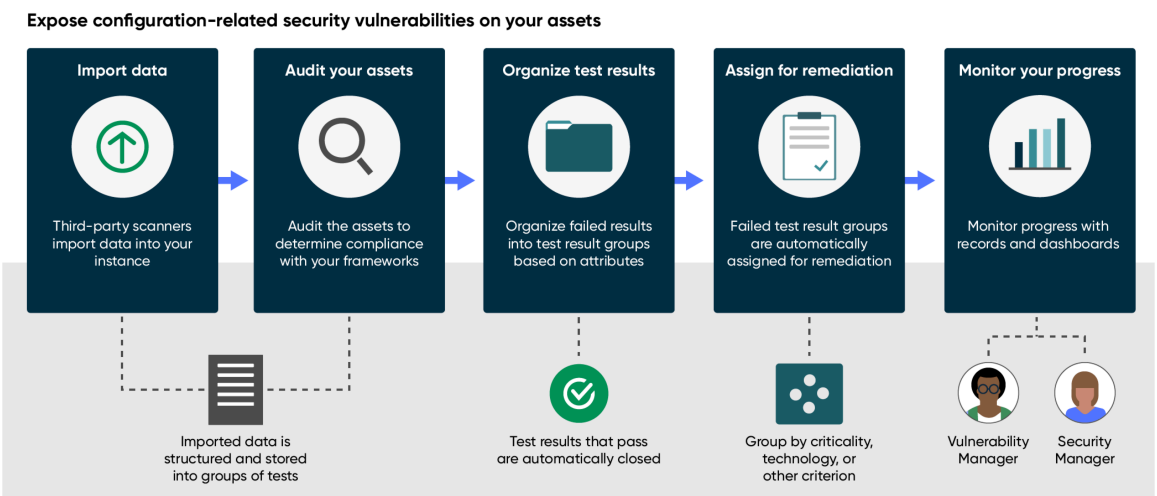
Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

O que é Configuration Compliance

A aplicação ServiceNow® Configuration Compliance permite que você priorize e corrija as vulnerabilidades relacionadas à configuração mais críticas em seu ambiente de forma rápida e eficiente. Configuration Compliance está disponível por assinatura no ServiceNow® Store.



Principais recursos do Configuration Compliance

Use o Configuration Management Database (CMDB) em seu Now Platform® para ajudá-lo a expor e corrigir suas vulnerabilidades de segurança relacionadas à configuração mais críticas. Concentre seus recursos de correção em atividades com a maior redução de risco. Simplifique o processo de correção na segurança, na TI e nas partes interessadas do processo de negócios. A aplicação Configuration Compliance inclui os seguintes recursos principais:

- Com integrações de terceiros compatíveis, importe automaticamente políticas, testes, fontes autorizadas e tecnologias. Consulte Integrações do Configuration Compliance para obter mais informações sobre integrações compatíveis.
- Correlacione políticas e testes a itens de configuração (ativos) para identificar vulnerabilidades relacionadas à configuração e ajudá-lo a verificar se seus ativos estão em conformidade com suas políticas e controles.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Unifique a avaliação de configuração, a atribuição e a correção em todos os seus ativos.
- O conteúdo de verificação de configuração pode ser importado das principais aplicações de integração do ecossistema de avaliação de configuração segura (SCA).
- As descobertas de configuração, falhas de teste, podem ser agrupadas e roteadas automaticamente com base nos conjuntos de habilidades do especialista em correção e áreas de responsabilidade. Fluxos de trabalho inteligentes e integração estreita com a gestão de mudanças fornecem transferências de tarefas suaves entre os grupos.
- Quando usados com a aplicação ServiceNow Governança, risco e conformidade (GRC), os testes de configuração em Configuration Compliance podem ser acumulados em seus controles GRC correspondentes.
- Com a gestão de mudanças aprimorada, crie solicitações de mudança preenchidas previamente para TI diretamente de Configuration Compliance para ajudá-lo com suas tarefas de correção que exigem recursos adicionais.
- Com os painéis, exiba as métricas de status de correção no grupo de resultados de testes, no teste de conformidade e nos registros de política.

Quem usa Configuration Compliance

Configuration Compliance As atividades do podem envolver muitos níveis de gestão.

- Administradores do sistema
- Administradores de vulnerabilidade
- Gerenciadores de vulnerabilidade
- Analistas de vulnerabilidade
- Administradores de conformidade

Configuration Compliance As tarefas do envolvem as funções a seguir.

- sn_vulc.admin — pode ler, gravar e excluir
- sn_vulc.write — pode ler e gravar
- sn_vulc.remediation_owner — Pode ler e atualizar registros atribuídos

> **Nota:**
> A função sn_vulc.remediation_owner também é atribuída automaticamente quando qualquer usuário é atribuído à função itil.

- sn_vulc.read — pode ler

Configuration Compliance e Security Operations

Quando o Qualys Vulnerability Integration e o Tenable Vulnerability Integration estão instalados, o acesso a Vulnerability Response se torna disponível. Você pode ter várias implantações dessas integrações. Os dados provenientes de cada implantação são identificados e disponíveis em uma única instância de GRC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Versões disponíveis para Washington DC

Versão de lançamento	Notas de versão
Configuration Compliance v14.7, v14.8, v14.9	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Configuration Compliance dados importados

A aplicação Configuration Compliance importa políticas, testes, fontes autorizadas e resultados de testes de integrações de terceiros e os armazena em módulos para exibição.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Integrações compatíveis

As integrações de terceiros importam descobertas de avaliação de configuração, políticas, testes, tecnologias, fontes autorizadas e resultados de testes para a aplicação Configuration Compliance. Os gerentes de vulnerabilidade ou analistas de vulnerabilidade podem usar esses dados para identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos.

Para obter mais informações sobre integrações compatíveis, consulte Integrações do Configuration Compliance.

Políticas

As políticas estão relacionadas a documentos oficiais e registros de teste. Um grupo de testes de configuração define as políticas. As políticas normalmente se alinham a uma classe de tecnologia, por exemplo, Windows, bancos de dados Oracle, Cisco IOS e geralmente são derivadas do padrão primário do setor. As políticas podem ser modificadas para atender às necessidades da organização. Um único teste de configuração pode pertencer a várias políticas.

Testes

Testes são bibliotecas de registros de dados que organizam verificações de ativos de computação. Os testes de configuração definem como uma classe de ativos de tecnologia deve ser controlada.

Um teste Configuration Compliance é o mecanismo que as aplicações de integração de terceiros usam para agrupar ativos por tipo de vulnerabilidade. Algumas soluções de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

verificação de VA de terceiros, como a Qualys, têm bibliotecas muito grandes de testes (até 8.000) que são mapeadas para políticas e "estruturas" de fontes autorizadas.

Um Teste pode ter vários valores, um para muitos, esperado versus real e assim por diante. Um teste é qualquer coisa que possa ser usada para identificar uma classe de ativo de software ou hardware que está fora de conformidade. Por exemplo, uma versão ou número de hardware.

Integração	Descrição
Qualys Vulnerability Integration	O trabalho programado, **Qualys PC Controls**, recupera os testes. Você pode exibir o trabalho programado navegando até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** > **Controles de PC da Qualys**. **Nota:** Se você optar por executar a integração manualmente, execute os **Controles de PC** da **Qualys após as Políticas de PC**da Qualys.
Tenable Vulnerability Integration	O trabalho programado Tenable.io Compliance Results Integration importa testes de configuração (Testes). Se você optar por executar as integrações manualmente, execute as integrações na seguinte ordem até reconciliar todos os ativos ignorados com os dados de avaliação: • Tenable.io Integração de ativos • Tenable.io Integração de resultados de conformidade • Tenable.io Compliance Results Backfill Integration • Tenable.io Integração de ativos • Tenable.io Compliance Results Backfill Integration Para exibir o registro de teste de configuração, navegue até **Configuration Compliance** > **Testes**. No registro, os dados importados são exibidos no campo **Descrição resumida** e nas guias Status da correção, Descrição e Correção. Os dados também são exibidos nos links relacionados **Citações**, **Políticas**e **Resultados de testes**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tecnologias

Uma das técnicas usadas por scanners de vulnerabilidade de terceiros para criar grupos de teste de itens de configuração de software e hardware para análise é organizá-los por tecnologia. As tecnologias são uma biblioteca importada de sistemas operacionais, dispositivos de rede, bancos de dados e aplicativos associados a políticas. Os testes têm várias implementações para diferentes tecnologias. A correção também é específica da tecnologia.

Você pode exibir as tecnologias aplicáveis a um teste para entender melhor a quais tipos de ativos de software ou hardware o controle pode ser aplicado. Exemplos de tecnologias que podem ser aplicadas aos controles incluem CentOS 7.x, Windows 8.1, Windows 2016 Server e assim por diante. A lista de tecnologias é somente leitura e corresponde às tecnologias definidas na aplicação Qualys Cloud Platform.

As tecnologias são importadas somente para avaliações de configuração relacionadas ao banco de dados. O *db_type* (se não estiver vazio) na importação é usado para criar uma tecnologia. Exibir tecnologias preenchidas na seção Tecnologias em registros de teste de configuração, registros de resultado de testes, registros de política e em **Configuration Compliance** > **Dados de suporte** > **Tecnologias**.

Fontes autorizadas

Configuration Compliance O usa Fontes autorizadas e citações ao gerar alertas de vulnerabilidade para testes. As fontes autorizadas geralmente mapeiam para seções de padrões do setor publicados, como "NIST 800-53 versão 3 (2009) 3: 2009, SA-4".

Nota:
No Qualys Vulnerability Integration, esta combinação é chamada de estrutura.

Fontes autorizadas e citações (também conhecidas como mandatos) são importadas dos scanners de vulnerabilidade de terceiros.

Os registros de origem autorizados contêm referências a informações sobre problemas conhecidos de configuração de software e hardware de especialistas no campo de segurança do computador. Eles definem requisitos para políticas e procedimentos de segurança. Os testes de configuração podem fazer referência a várias fontes autorizadas por meio de citações. Fontes autorizadas podem relatar a conformidade de um determinado padrão em preparação para uma auditoria.

Integração	Descrição
Qualys Vulnerability Integration	O trabalho programado, **Qualys PC Policies Detail**, recupera as fontes autorizadas e as citações. Você pode exibir este trabalho programado navegando até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** > **Detalhe das políticas de PC da Qualys**. **Nota:** Se você optar por executar a integração manualmente, execute **Qualys PC Policies Detail** após **Qualys PC Policies**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
Tenable Vulnerability Integration	O trabalho programado Tenable.io Compliance Results Integration importa fontes autorizadas como parte dos dados de citações. Se você optar por executar as integrações manualmente, execute as integrações na seguinte ordem até reconciliar todos os ativos ignorados com os dados de avaliação: • Tenable.io Integração de ativos • Tenable.io Integração de resultados de conformidade • Tenable.io Compliance Results Backfill Integration • Tenable.io Integração de ativos • Tenable.io Compliance Results Backfill Integration Os dados são exibidos no link relacionado **Citações** nos registros de teste de configuração.

Resultados de testes

Configuration Compliance não calcula os resultados do teste, mas os importa como parte de uma integração de terceiros. Quando estiverem visíveis em Configuration Compliance, eles serão corrigidos usando **Tarefas**de correção. Para obter mais informações, consulte Configuration Compliance correlação.

Integração	Descrição
Qualys Vulnerability Integration	Você pode recuperar os resultados do teste de uma das seguintes maneiras: • O trabalho programado, **Qualys PC Results**, recupera os resultados do teste. Você pode exibir este trabalho programado navegando até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** > **Resultados de PC da Qualys**. **Nota:** Se você optar por executar a integração manualmente, execute **Resultados de PC** da **Qualys após Políticas de PC** da **Qualys e Detalhe**de políticas de PC da Qualys . A importação de **Resultados de PC da Qualys** usa o parâmetro `Start Time`

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração	Descrição
	na guia **Detalhes de integração**. Todas as outras importações de Configuration Compliance trarão todos os dados disponíveis, independentemente de *`Start Time`*. Quando a importação dos **resultados de PC da Qualys** estiver concluída, um evento será acionado para acionar os cálculos de fim de importação. Para obter mais informações, consulte Configuration Compliance estados. • Como alternativa, a partir da V14.5, você também pode executar as seguintes integrações para recuperar os resultados do teste:
Tenable Vulnerability Integration	O trabalho programado Tenable.io Compliance Results Integration importa resultados de testes. Se você optar por executar as integrações manualmente, execute as integrações na seguinte ordem até reconciliar todos os ativos ignorados com os dados de avaliação: • Tenable.io Integração de ativos • Tenable.io Integração de resultados de conformidade • Tenable.io Compliance Results Backfill Integration • Tenable.io Integração de ativos • Tenable.io Compliance Results Backfill Integration Para exibir o registro de teste de configuração, navegue até **Configuration Compliance** > **Resultados de testes**. No registro, os dados importados são exibidos nos campos**Teste**e **Item de configuração**. Os dados também são exibidos nas guias **Valores esperados, Valoresreais**e **Correção**. Os **grupos de resultados** de **testes e os links relacionados ao histórico de resultados de testes** são preenchidos.

Descoberta de Configuration Compliance

Configuration Compliance os dados são importados de aplicações de scanner SCA de terceiros. Eles estruturam grupos de testes de software e hardware em registros de dados para agilizar a realização de avaliações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Quando uma importação é concluída, um evento é enviado para indicar ações de fim de importação. Para cada grupo de resultados de testes ativo, as seguintes ações são realizadas:

- Grupos resolvidos com resultados com falha retornam ao estado **Aguardando implementação**.
- Os grupos de resultados de testes em que todos os resultados foram aprovados estão **Encerrados**.
- O estado dos resultados de testes que estão em grupos ativos é atualizado.
- O sinalizador que indica se um resultado faz parte de um grupo ativo é atualizado.

Configuration Compliance correlação

Configuration Compliance fornece priorização e agrupamento de resultados de testes para ajudar na correção de problemas de não conformidade.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Priorização centrada em ativos

As verificações de configuração podem produzir um grande número de descobertas. Priorize as descobertas para obter a maior redução de risco. A prioridade inclui a criticidade do teste de configuração e a criticidade do ativo. A prioridade do resultado do teste de configuração é expressa como uma pontuação de risco na escala de 0 a 100. Os grupos de calculadoras calculam a pontuação de risco e podem ser personalizados.

Quando a importação de terceiros é concluída, Configuration Compliance envia um evento para indicar ações de fim de importação. Para cada grupo de resultados ativo, as seguintes ações são realizadas:

- Grupos resolvidos com resultados com falha retornam ao estado **Aguardando implementação**.
- Grupos em que todos os resultados aprovados são **Encerrados**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- O estado dos resultados de testes que estão em grupos ativos é atualizado.
- O sinalizador que indica se um resultado faz parte de um grupo ativo é atualizado.

Ordem de precedência das Tarefas de correção

Quando os resultados de testes pertencem a mais de um grupo, o **Estado** de um resultado de teste é derivado de acordo com uma ordem de precedência.

Os campos **Estado** e **Resolução** no formulário **Teste de configuração** e o campo **Resultado** no formulário **Resultado do teste** são calculados seguindo esta ordem de precedência.

Nota:

A precedência de associação de grupo se aplica somente a itens em que o item não foi aprovado no teste de configuração. Os itens**aprovados** estão sempre no estado **Encerrado-Corrigido**.

O valor do **resultado** determina o estado. Ignoramos os grupos no estado **Encerrado-Corrigido** e **Encerrado-Cancelado**. O estado do item é calculado a partir dos estados de todas as outras tarefas de correção às quais ele pertence ou está definido como **Aberto**, se não houver outro grupo para o item.

Order of Precedence for Test Results belonging to multiple Test Result Groups						
Group A	**Group B**					
	Open	**Under Investigation**	**Awaiting Implementation**	**Resolved**	**Deferred**	**Closed-Invalid**
Open	Open	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Under Investigation	Under Investigation	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Resolved	Resolved	Resolved	Resolved	Resolved	Deferred	Closed-Invalid
Deferred	Deferred	Deferred	Deferred	Deferred	Deferred	Closed-Invalid
Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid

Criação de tarefas de correção

Configuration Compliance Tarefas de correção são criadas manualmente.

Existem duas maneiras de criar e preencher **Tarefas**de correção.

- No módulo **Tarefas** de correção e usando filtros que preenchem automaticamente a guia **Resultados de testes**.

  Essa maneira é boa para quando você sabe qual filtragem deseja usar. Por exemplo, capturar todos os resultados de testes com falha que são de criticalidade moderada e alta, afetam a infraestrutura baseada em Windows e se aplicam somente à aplicação de cadeia de suprimentos SAP.

- Selecionando resultados de testes na lista **Resultados** de testes e criando um grupo no menu **Ações em linhas selecionadas...**

  Este método é bom para resultados que não são filtrados facilmente ou situações em que você deseja especificar resultados de testes para correção. Por exemplo, valores atípicos que não têm nada em comum.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Se você criar um grupo a partir da lista **Resultados de testes** e, posteriormente, decidir usar um filtro para esse grupo, suas entradas originais serão removidas e substituídas pelos resultados do filtro.

Resultados de testes não agrupados

Os Resultados de testes não agrupados contêm todos os resultados de testes não aprovados que não são membros de um grupo ativo (não**Encerrado**). Este módulo é atualizado após cada importação e sempre que os resultados de testes são adicionados ou removidos de um grupo.

Itens Descobertos para Configuration Compliance

Os ativos são correspondidos automaticamente aos itens de configuração (ICs) usando regras de pesquisa de IC, quando eles são importados usando o host e as integrações de resultados de testes. Os itens descobertos fornecem visibilidade de como a identificação de ativo é mapeada para ICs no CMDB.

Os itens descobertos são considerados **correspondentes**, não **correspondentes**ou **reclassificados**. Os ICs identificados estão no estado **Correspondido**.

Para facilitar a localização de possíveis problemas de correspondência, a regra de pesquisa de IC que correspondeu ao IC aparece no campo **de regra de correspondência de IC**.

Nota:
O suporte ao campo**de regra de correspondência de IC** está disponível somente para a integração Qualys.

Se uma correspondência não for encontrada, um IC será criado na classe de *IC*incompatível [sn_sec_cmn_unmatched_ci], [cmdb_ci_unclassed_hardware]ou [cmdb_ci_incomplete_ip] do CMDB. Se o IC original sem correspondência foi reclassificado, os registros de item descoberto serão atualizados para refletir esse estado. Para obter mais informações, consulte ICs incompatíveis e Exibir e reclassificar itens de configuração incompatíveis.

Por padrão, o **Security Operations** > **CMDB** > **Itens Descobertos** O módulo lista itens de configuração incompatíveis. Você pode exibir todos os itens descobertos de uma importação removendo o filtro.

Para obter uma descrição dos campos em Itens descobertos, consulte Campos de formuláriode itens descobertos.

Mudanças de IC para itens descobertos para Configuration Compliance

O valor padrão da propriedade sn_sec_cmn.update_on_ci_change é verdadeiro. Portanto, quando o item de configuração (IC) de um item descoberto é atualizado, os resultados do teste também são atualizados.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O ID externo do resultado do teste é atualizado e a pontuação de risco, as regras de atribuição, as regras de grupo e a regra de destino de correção são reavaliadas. Se houver um resultado de teste com o mesmo teste e IC, os resultados do teste serão atualizados com o resultado do teste existente e o resultado do teste atual será encerrado com o subestado inválidoCI. As anotações de trabalho são adicionadas de acordo.

Se você não quiser atualizar o IC para o resultado do teste existente, defina a propriedade como falsa. Nesse caso, se um IC mudar, um novo resultado de teste será criado e o existente será encerrado como um IC inválido.

Reconciliar itens descobertos incompatíveis para Configuration Compliance

Crie um trabalho programado para reconciliar itens descobertos incompatíveis. Quando um resultado de teste é criado, o item de configuração (IC) adicionado a ele no momento da criação pode estar desatualizado.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Se as informações no CMDB forem alteradas, as informações de IC incompatíveis não serão reconciliadas. Para reconciliar, aplique regras de pesquisa de IC nos resultados de testes que estão em um estado incompatível quando o CMDB for atualizado com os ICs mais recentes.
Um trabalho programado é executado sob demanda para reaplicar a regra de correspondência de IC para os itens descobertos em um estado incompatível. Se o IC mudar após a reaplicação das regras de pesquisa, os itens descobertos serão atualizados com o novo IC. Os resultados de testes afetados também são atualizados. Para obter detalhes, consulte Mudanças de IC para itens descobertos para Configuration Compliance.

Procedimento

1. Navegar até **Todos** > **Security Operations > Reconciliar itens descobertos incompatíveis**.
2. Na página Trabalhos em segundo plano, clique em **Criar trabalho de reconciliação**.
3. No formulário, preencha os campos.

> **Nota:**
> Você só pode editar o campo Parâmetros.

Trabalho em segundo plano

Campo	Descrição
Número	Número do trabalho exclusivo.
Criado por	Usuário que criou o trabalho.
Parâmetros	Parâmetros para reconciliar os itens descobertos incompatíveis: ○ limit: o número máximo de itens descobertos a serem reconciliados. Se você não inserir um valor, 10.000 itens descobertos serão reconciliados. ○ firstDiscovereditem: primeiro item descoberto que deve ser reconciliado. Se você não inserir um valor, o processo de reconciliação será iniciado a partir do primeiro item descoberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Estado	Estado atual do trabalho em segundo plano.
Descrição do estado	Descrição do estado atual do trabalho em segundo plano.
Tipo de trabalho	Tipo de trabalho. O valor é **Reconciliar itens descobertos incompatíveis**.
Iniciada em	Hora em que o trabalho foi iniciado.
Finalizado às	Hora em que o trabalho foi concluído.
Duração do trabalho	Tempo total para concluir o trabalho.
Subestado	Subestado para o estado selecionado.
Anotações	Número de registros processados.

4. Clique em **Enviar**.

Nota:

- Para parar de executar o trabalho, clique em **Cancelar**.
- Você não pode reconciliar ICs incompatíveis ou reaplicar regras de pesquisa de IC ao importar hosts ou resultados de testes.

Reaplicar regras de pesquisa de IC em itens descobertos selecionados para Configuration Compliance

Reaplicar regras de pesquisa de item de configuração (IC) em itens descobertos selecionados das ações de seleção de exibição de lista de itens descobertos. O administrador pode precisar editar ou atualizar uma regra de pesquisa por vários motivos. Se a regra de pesquisa for alterada, eles poderão reaplicá-la aos itens descobertos.

Antes de Iniciar

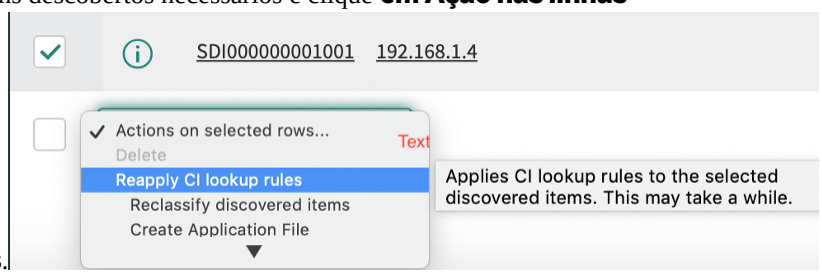
Funções necessárias:

Por Que e Quando Desempenhar Esta Tarefa

Se o IC mudar após a reaplicação das regras de pesquisa de IC, os itens descobertos serão atualizados com o novo IC e os resultados de testes. Para obter mais informações, consulte Mudanças de IC para itens descobertos para Configuration Compliance.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **CMDB** > **Itens Descobertos**.
2. Selecione os itens descobertos necessários e clique **em Ação nas linhas selecionadas**.



3. Selecione **Reaplicar regras de pesquisa de IC** na lista.

As regras são reaplicadas nesses itens descobertos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O Tenable Vulnerability Integration com Configuration Compliance

O produto Tenable.io de Tenable Vulnerability Integration importa políticas, controles (resultados de testes) e testes de configuração para processamento na aplicação Configuration Compliance.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Tenable.io

O Tenable Vulnerability Integration é compatível.

Você pode usar dados importados para:

- Identifique vulnerabilidades relacionadas à configuração em seus ativos listados em Configuration Management Database (CMDB)
- Verifique se seus ativos estão em conformidade com suas políticas e controles.

Dados de ativos, políticas, controles (resultados de testes) e testes de configuração são importados com as seguintes integrações:

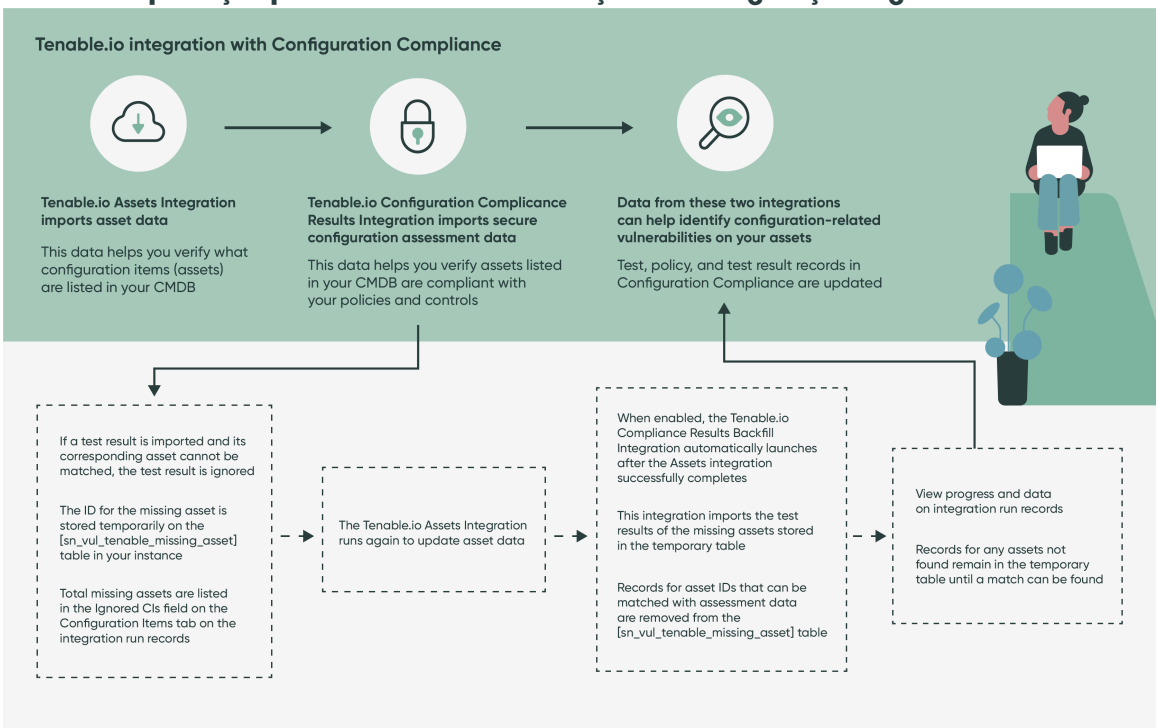
- Tenable.io Integração de ativos
- Tenable.io Integração de resultados de conformidade
- Tenable.io Compliance Results Backfill Integration

A imagem a seguir ilustra como as integrações funcionam juntas para importar dados de avaliação de ativo e configuração e reconciliar todos os ICs ignorados durante uma importação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de importação para resultados de avaliação de configuração segura



Os dados são importados, atualizados e exibidos no resultado do teste, na política e nos registros de teste de configuração na aplicação Configuration Compliance.

Em alguns casos, o número de itens de configuração (ICs) importados é diferente para a integração de ativos Tenable.io e a integração de resultados de conformidade Tenable.io. Quando isso ocorre, registros temporários são criados e armazenados para os IDs de ativo ignorados. Esses registros podem ser correspondidos posteriormente com dados de avaliação importados por importações da integração de preenchimento de resultados de conformidade.

Por exemplo, digamos que a integração de ativos importe 80 ativos em uma execução de integração, mas a integração de resultados de conformidade importe 100.

Nota:
Você pode verificar o número de ICs ignorados nas execuções de integração navegando até **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**. Clique no nome de uma integração para abrir o registro. No link relacionado **Execuções de integração de vulnerabilidade**, abra um registro de execução de integração e selecione a guia **Itens** para ver o valor no campo **ICs ignorados**. Este campo rastreia o total de ativos ignorados (ausentes) da importação.

Ao comparar os valores nos campos de **ICs ignorados** em cada registro de execução de integração, há uma diferença de 20 ICs ignorados. Como resultado, a integração de preenchimento é executada automaticamente, conforme mostrado na imagem anterior. Esta integração importa as informações de avaliação de configuração dos 20 ativos extras encontrados pela integração de resultados de conformidade, mas ausentes pela integração de ativos. Como os dados de avaliação de ativos ausentes não são importados, a integração de preenchimento de resultados de conformidade Tenable.io importa até 200 IDs de ativo por execução de integração para reconciliar os ativos ausentes com os dados de avaliação correspondentes. Todos os registros criados para ativos ausentes ou ignorados e listados na tabela temporária são excluídos depois que esses ativos e seus dados são correspondidos.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Pode levar várias execuções dessas integrações para importar todos os ativos ignorados.

Para obter mais informações sobre como habilitar e configurar o Tenable.io Asset Integration, consulte Configurar a integração de vulnerabilidade da Tenable usando o assistente de configuração. Consulte Noções básicas sobre a integração de vulnerabilidade da Tenable para obter mais informações sobre a integração.

A integração de resultados de conformidade Tenable.io e a integração de backfill de resultados de conformidade Tenable.io estão inativas por padrão.

Para ativá-los:

1. Navegar até **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
2. Na lista Integrações da Tenable, clique em um nome de integração para abrir o registro e marque a caixa de seleção **Ativo** para habilitá-lo. Você pode preferir deixar as configurações de programação em seus valores padrão para que essas integrações sejam iniciadas.

Regras de Pesquisa de IC para identificar itens de configuração a partir de integrações de vulnerabilidade de terceiros do Configuration Compliance

Quando os dados são importados de uma integração de terceiros, o Configuration Compliance usa automaticamente os dados do host para pesquisar correspondências no Configuration Management Database (CMDB). Ele faz isso usando **Regras de Pesquisa de IC**. Essas regras são usadas para identificar itens de configuração (ICs) e adicioná-los ao registro de resultado de testes para ajudar na correção.

Conforme os ativos são importados, uma pesquisa é realizada primeiro na lista de **itens descobertos** usando IDs de terceiros para encontrar correspondências com os itens de configuração (ICs) de importações anteriores. Quando uma correspondência de ID de host é encontrada, ela é usada como o campo **Item de configuração** no registro de resultado de testes.

Você pode ver como os ativos importados são mapeados para ICs usando a lista de **Itens descobertos**. Se uma correspondência não for encontrada ou o campo cmdb_ci estiver vazio, as regras usarão as outras informações do host para tentar identificar corretamente o IC. Se uma correspondência ainda não for encontrada, um IC de espaço reservado será criado e designado como **IC incompatível**. Consulte ICs incompatíveis para obter mais informações sobre como esses ICs são tratados.

Um novo item descoberto é criado e mapeado para este IC.

Nota:
As regras de pesquisa de IC estão disponíveis somente para a integração Qualys para Security Operations.

As regras de pesquisa de IC podem ser separadas por domínio e são específicas da origem. Cada origem pode ter várias implantações. A Qualys pode ter várias implantações da integração da Qualys. Cada implantação tem seu próprio conjunto de regras de pesquisa de IC.

Nota:
As regras de pesquisa de IC são compartilhadas por todas as implantações da integração de vulnerabilidade. Se uma regra for excluída ou modificada, a exclusão ou as mudanças afetarão todas as implantações da integração de vulnerabilidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ao tentar uma correspondência, a primeira etapa é uma pesquisa de ID de fornecedor para uma correspondência exata entre origem, source_instance e ID de fornecedor. Em seguida, as regras de pesquisa são executadas em ordem, da menor para a maior, e param quando uma regra retorna apenas um único IC como uma correspondência. Se uma regra for criada de forma a retornar mais de um IC, somente a primeira correspondência será usada.

Nota:
Para evitar a correspondência em elementos de network de baixo nível, se um IC correspondente for dscy_switchport, cmdb_ci_network_adapter, cmdb_ci_nic ou cmdb_ci_ip_address, o IC primário será retornado.

Uma propriedade do sistema para excluir classes de IC está disponível. Esta propriedade não está disponível com atualização. Consulte Ignorar classes de IC para obter informações de atualização e instruções sobre como definir a propriedade.

Para facilitar a localização de problemas de correspondência, quando uma correspondência for encontrada, a regra de pesquisa de IC usada para localizá-la será adicionada ao registro de item descoberto no campo **Regra de correspondência de IC**. As regras de pesquisa são avaliadas primeiro pelo menor valor de **Pedido**.

Essas regras Qualys de pesquisa de IC são enviadas com o sistema de base.

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

Essas regras de pesquisa de IC do Microsoft Defender são enviadas com o sistema de base.

- Bucket S3
- Nome
- ID do recurso

Essas regras de pesquisa de IC do Palo Alto Prisma Cloud são enviadas com o sistema de base.

- Bucket S3
- Nome
- ID do recurso

Importar dados de resultados de testes pode sobrecarregar uma instância e podem ocorrer problemas de desempenho com recursos se as regras não forem construídas com cuidado. A lógica usada para iterar e executar a correspondência dentro do CMDB pode resultar em longos tempos de processamento. Para evitar qualquer degradação potencial de recursos ou complicações de desempenho, teste todas as regras de pesquisa de IC personalizadas ou modificações nas **regras de pesquisa de IC** predefinidas. Consulte Etapas para ajudar a evitar registros duplicados ou órfãos após a execução de Vulnerability Response regras de pesquisa de IC para obter mais informações sobre como evitar registros órfãos duplicados, excluir dados e limpar dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicar novamente as regras de pesquisa de IC atualizadas

Ao alterar uma regra de pesquisa de IC, clique em **Aplicar mudanças** na página da lista Regras de pesquisa de IC para executar novamente todas as regras nos itens descobertos que:

- Foram correspondidos pelas regras atualizadas
- Não são correspondidos por nenhuma regra

Se o item de configuração (IC) mudar após a reaplicação das regras de pesquisa, os itens descobertos serão atualizados com o novo IC. Os resultados do teste também são atualizados. Para obter mais informações, consulte Mudanças de IC para itens descobertos para Configuration Compliance.

Desduplicando itens de configuração existentes para Configuration Compliance

O Remediador de ICs duplicados para tarefas de desduplicação é atualizado com a propriedade `sn_sec_cmn_src_ci.cmdb_ci`.

Sempre que uma tarefa de desduplicação é usada para atualizar os itens de configuração (ICs), ela também atualiza os itens descobertos relacionados a esses ICs. Portanto, os resultados do teste são atualizados com o IC. Para obter detalhes, consulte Mudanças de IC para itens descobertos para Configuration Compliance.

Criando ICs para Configuration Compliance usando o Mecanismo de Identificação e Reconciliação

A partir do Configuration Compliance 11.1, você pode criar itens de configuração (ICs) no Configuration Management Database (CMDB) usando a API do mecanismo de Identificação e Reconciliação (IRE). Ao usar a API do IRE para criar ICs, você pode impedir a criação de ICs duplicados e reconciliar atributos de IC, permitindo que somente fontes de dados autorizadas gravem em CMDB.

Uma classe de IC (tabela) é o nome da tabela original no banco de dados da instância. CMDB contém classes do sistema de base que armazenam dados sobre ICs.

Uso de IRE para criação de IC

Antes da versão 11.1, se um IC correspondente não fosse encontrado na lista de itens descobertos ou CMDB, um IC era criado na classe de IC incompatível (`sn_sec_cmn_unmatched_ci`).

Para obter mais informações, consulte ICs incompatíveis.

A partir da versão 11.1, você pode usar a API IRE para criar ICs em CMDB. Em vez de usar a classe de IC incompatível, um IC é criado na classe Hardware sem classificação ou na classe de dispositivo identificado por IP incompleto.

CMDB Classes de IC

Nota:
Para usar as novas classes, ative o plug-in CMDB CI Class Models. Caso contrário, os ICs serão criados na classe de IC incompatível.

A partir da versão 11.1, se o host que você importou de um scanner de terceiros não puder ser encontrado na lista de itens descobertos ou CMDB, ele será armazenado em uma das seguintes novas CMDB classes de IC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

CMDB Classes de IC

CMDB Classe de IC	Descrição
Dispositivo identificado por IP incompleto (cmdb_ci_incomplete_ip)	O IC será criado nesta tabela se somente o endereço IP estiver disponível nas informações de host recebidas do scanner.
Hardware não classificado (cmdb_unclassed_hardware_ci)	O IC será criado nesta tabela se qualquer uma das seguintes informações estiver disponível nas informações do host recebidas do scanner: • Nome do host • Endereço IP • DNS • NETBIOS • Endereço MAC **Nota:** Se o endereço MAC estiver disponível, a entrada do adaptador de rede será criada e relacionada ao IC de hardware não classificado. Se os endereços IP e MAC estiverem disponíveis, o IC de endereço IP também será criado e relacionado ao IC de hardware não classificado.

O sistema usará automaticamente uma classe de IC incompatível se ocorrer um dos seguintes:

- O plug-in CMDB Classe de IC não está ativado.
- O IRE gera uma exceção ao criar um novo IC.

Tópicos relacionados

Aplicação da Store do CMDB CI Class Models

Mecanismo de Identificação e Reconciliação (IRE)

Configuration Compliance visão geral de regras de atribuição

Defina os critérios pelos quais os resultados de testes são atribuídos automaticamente a um grupo de atribuição para correção.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma regra de atribuição padrão, **Atribuir ao grupo de suporte de IC**, está incluída no sistema de base que atribui resultados de testes **ao Grupo de suporte de IC**. Inativo por padrão.

Os grupos de atribuição definidos pelas Regras de atribuição são usados pelas **Regras de grupo** para atribuir proprietários a tarefas de correção (RTs).

Atribuir resultados de testes automaticamente

Existem três maneiras diferentes de atribuir resultados de testes usando **Atribuir usando**:

- Grupo de atribuição: esta opção permite selecionar qualquer um dos grupos de usuários Now Platform® existentes.
- Campo de grupo de atribuição: esta opção permite escolher qualquer campo de grupo de atribuição disponível usando a tabela cmdb_ci. Por padrão, você vê os três campos de grupo a seguir:
  - Nenhum: indica que não há valor padrão para este campo obrigatório
  - Item de configuração: grupo de aprovação
  - Item de configuração: grupo de atribuição
  - Item de configuração: grupo de suporte
- Script: esta opção permite definir as condições usando um script. Esta opção requer codificação ou conhecimento avançado ServiceNow®.

Consulte Criar ou editar Configuration Compliance regras de atribuição para obter mais informações sobre como criar regras de atribuição.

Com a função sn_vulc.remediation_owner, você pode exibir e atualizar resultados de testes e tarefas de correção que são atribuídos a eles ou aos grupos de atribuição. Para exibir os módulos, navegue até **Todos** > **Configuration Compliance** > **Resultados de testes** > **Meus Resultados de testes em Aberto**ou **Configuration Compliance** > **Tarefas de correção** > **Minhas tarefas em aberto**.

A função sn_vulc.remediation_owner pode ser atribuída diretamente a um usuário ou é atribuída automaticamente quando você atribui a função itil a um usuário.

Processo de avaliação da regra de atribuição

Quando um novo resultado de teste é importado ou reaberto após ser fechado, as regras de atribuição são avaliadas em relação a ele. As regras de atribuição são avaliadas após a correspondência de IC e os cálculos de pontuação de risco. Um resultado de teste só é avaliado automaticamente na importação inicial e quando uma regra é alterada, a menos que seja reaberto após ser fechado. Você pode reaplicar as regras manualmente após as mudanças.

O processo a seguir é usado para cada resultado de teste novo ou reaberto:

- Para cada regra de atribuição de resultado de teste, o resultado do teste é comparado ao filtro de atribuição, a regra de ordem mais baixa primeiro.
- Onde a condição corresponde, o resultado do teste é atribuído a um grupo de atribuição. A pesquisa é interrompida.
- Quando as condições não encontrarem uma correspondência entre todas as regras, o resultado do teste permanecerá não atribuído.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Reaplicar regras de atribuição

Ao mudar uma regra de atribuição, use o botão **Aplicar mudanças** na página da lista Regras de atribuição para executar novamente todas as regras alteradas em todos os resultados de teste Aberto ativos, exceto aqueles que foram atribuídos manualmente.

Nota:
As regras de atribuição não reavaliam as atribuições criadas manualmente.

O trabalho programado [*Reapply all assignment rules*] está inativo, por padrão. Quando ativado, ele avalia todos os resultados de testes abertos em relação a todas as regras ativas, exceto aquelas atribuídas manualmente. Ele pode ser executado diariamente, semanalmente, mensalmente, periodicamente, uma vez ou sob demanda.

Regras de atribuição e atribuição de tarefa de correção

Normalmente, você atribuiria sua tarefa de correção (RT) ao mesmo grupo de atribuição que os resultados de teste nele. É isso que as regras de tarefa de correção fazem, por padrão.

Por exemplo, se o seu RT agrupar por classe de item de configuração, a tarefa de correção criada poderá ser dividida pelos diferentes grupos de atribuição. Um Oracle Database TRG pode ser atribuído ao Grupo 1 e um Oracle Database TRG atribuído ao Grupo 2.

Quando o grupo de atribuição é alterado no nível da tarefa de correção, todos os resultados de testes nesse grupo que têm o mesmo grupo de atribuição são atualizados para o novo grupo de atribuição. Os resultados do teste são marcados como atribuídos manualmente e não são qualificados para avaliação de regra adicional.

Removendo atribuições de Configuration Compliance tarefas de correção

Você pode limpar os campos **Atribuído a** e **Grupo de atribuição** nas tarefas de correção (RT) e nos resultados de testes associados diretamente dos registros do TRG que você determina que podem ter sido atribuídos incorretamente a você ou aos seus grupos.

Visão geral

A partir da v14.3 da aplicação Configuration Compliance, os responsáveis pela correção podem atualizar registros para reatribuição com o botão Cancelar **atribuição**.

Caso de uso para sn_vulc.remediation_owner

Se você determinar que os RTs e seus resultados de testes associados não estão dentro do seu escopo de correção, ou se você achar que os registros foram atribuídos incorretamente a você ou aos seus grupos, remova a si mesmo ou seus grupos de **Atribuído a** e Campos de **grupo de atribuição** nesses registros de tarefa de correção.

Desatribuir módulo

O botão **Cancelar atribuição** é exibido nos registros RT em qualquer estado diferente dos estados Encerrado ou Resolvido.

Se você selecionar **Desatribuir**, será solicitado que todos os resultados de testes associados ao grupo sejam reatribuídos e façam a transição para o tipo de atribuição **Não atribuído**.

Todos os registros que você atualiza com o botão de IU ou manualmente são exibidos no módulo Não atribuído em Configuration Compliance.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para saber como reatribuir registros usando a ação de IU *Unassigned*, consulte Remover atribuições de grupos de resultados de testes para você ou seus grupos.

Propriedades e notificações do sistema

Se você for um administrador com a função **sn_vulc.vulnerability_admin**, ao selecionar Cancelar atribuição em um registro, por padrão, a propriedade do sistema, *sn_vulc.unassign_test_result_group.approval_required* aciona o registro de Aprovação de mudança de estado e o registro de Aprovação solicitada. Além disso, a solicitação é exibida na lista Minhas aprovações do aprovador.

Nota:
Como administrador de vulnerabilidade, você pode definir a propriedade do sistema *sn_vulc.unassign_test_result_group.approval_required* como **falsa** para desabilitar o processo de aprovação.

- Se o aprovador aprovar sua solicitação, por padrão, a propriedade do sistema, *sn_vulc.default_assignment_group* limpa os campos Atribuído a e Grupo de atribuição e preenche o campo Tipo de atribuição com **Não atribuído**. Como administrador de vulnerabilidade, você pode alterar o valor na propriedade do sistema *sn_vulc.default_assignment_group* para que os campos de atribuição sejam limpos e um grupo específico seja atribuído. Por exemplo, se um usuário selecionar **Cancelar atribuição** em um registro e você quiser redirecioná-lo para um grupo específico para revisão, será possível adicionar um ID de sistema para o grupo de sua escolha no campo de valor da propriedade do sistema.
- Se o aprovador rejeitar sua solicitação, o motivo da rejeição será exibido na guia **Anotações**.

Como alternativa, se *sn_vulc.default_assignment_group* não estiver configurado para um grupo específico, por padrão, os usuários que você adicionar ao grupo de usuários de notificação de cancelamento de atribuição serão alertados quando os registros não forem atribuídos. A propriedade do sistema, *sn_vulc.default_notification_group* determina as notificações para este grupo.

O tipo de atribuição, seja **Manual**, **Regra**ou **Não atribuído**, está disponível nos registros RT e na exibição de lista. O tipo de atribuição **Não atribuído** é exibido depois que os campos **Atribuído a** e **Grupo de atribuição** são limpos pela propriedade do sistema do recurso.

Monitorar suas regras de atribuição com o trabalho programado para este recurso

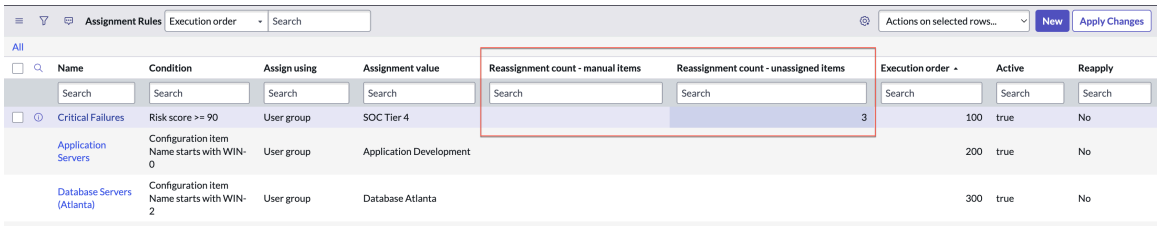
Um trabalho programado diário conta os registros quando eles fazem a transição para o tipo de atribuição **Não atribuída**. Com essa contagem, os analistas de vulnerabilidade podem monitorar e ajustar quaisquer regras de atribuição que possam não estar funcionando bem com base em quaisquer regras de atribuição que tenham contagens mais altas de RTs não atribuídos.

O trabalho programado *Reassignment count for assignment rules* é executado diariamente e publica o número total de RTs não atribuídos por este recurso para uma regra de atribuição específica.

O trabalho também conta todos os registros que são desatribuídos manualmente. As contagens manuais e as contagens que são coletadas por este recurso são publicadas na lista Regras de atribuição de vulnerabilidade em duas colunas: *Reassignment count - manual items* e *Reassignment count - unassigned items*.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



1. Como administrador de vulnerabilidades, você pode exibir essas contagens navegando até **Configuration Compliance** > **Administração** > **Regras de atribuição**.
2. Selecione o ícone de engrenagem no canto superior direito da lista e selecione a **Contagem de reatribuições - itens manuais**e a **Contagem de reatribuições - itens não atribuídos** para exibição.
3. Qualquer RT que foi originalmente atribuído por uma regra, mas depois foi reatribuído automaticamente ou manualmente, contém uma referência à regra original na exibição de lista.

Configuration Compliance tarefas de correção e visão geral de regras de grupo

Crie automaticamente Tarefas de correção (RTs) para analisar os resultados em massa usando regras de tarefa de correção. Os critérios pelos quais os grupos são formados são configurados para que você não precise atribuir manualmente os resultados de testes em grupos.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Noções básicas sobre tarefas de correção

As tarefas de correção representam um conjunto de resultados de testes a serem corrigidos. O agrupamento de resultados de testes tem muitas vantagens. Você pode mover os resultados de testes pelos estados de correção, marcá-los como sob investigação, adiá-los e marcá-los como resolvidos em massa usando grupos. Você pode criar condições para agrupar automaticamente todos os resultados com resultados especificados, tecnologias, pontuações de risco e quaisquer outros dados relacionados aos resultados do teste. Os resultados de testes podem pertencer a mais de uma tarefa de correção, dando a você a flexibilidade de trabalhar ativamente com um grupo e monitorar outro. Tudo depende das necessidades organizacionais. Por exemplo, você pode agrupar por atribuição e também criar um grupo que contenha tecnologias.

As tarefas de correção são criadas da seguinte forma.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Manualmente, usando uma das duas opções, para adicionar itens vulneráveis ao grupo.
  - **Manual**: cria um grupo sem entradas. Os resultados de testes devem ser adicionados manualmente.
  - **Filtro**: cria um grupo e usa condições para adicionar automaticamente resultados de testes a esse grupo.

  Nota:
  Os resultados de testes adicionados manualmente não são removidos automaticamente das tarefas de correção por regras de tarefa de correção ou condições de grupo.

- Automaticamente, usando regras de tarefa de correção. Esta é a opção mais fácil. Depois de configuradas, as regras de tarefa de correção criam todas as tarefas de correção desejadas.

Em uma tarefa de correção, o grupo de resultados de testes pode ser atribuído a um usuário, adiado até mais tarde, usado para criar uma **solicitação de mudança**e assim por diante.

Nota:

Com a função sn_vulc.remediation_owner, você pode exibir e atualizar resultados de testes e tarefas de correção que são atribuídos a você ou aos seus grupos de atribuição. Para exibir os módulos, navegue até **Todos** > **Configuration Compliance** > **Resultados de testes** > **Meus Resultados de testes em Aberto**ou **Configuration Compliance** > **Tarefas de correção** > **Minhas tarefas em aberto**.

Quando é determinado que um novo resultado de teste pode ser adicionado a um grupo, o resultado do teste é incluído na lista relacionada **Resultados de testes** da tarefa de correção.

Ao atualizar o estado de uma tarefa de correção, os resultados de testes associados podem ter seu estado atualizado para corresponder a essa tarefa de correção. Para obter mais informações sobre mudanças de estado, consulte Configuration Compliance estados.

Noções básicas sobre regras de tarefa de correção

As regras de tarefa de correção permitem que você defina como os resultados de testes são automaticamente agrupados e atribuídos. Uma regra padrão, **Grupo de atribuição, Teste**, está incluída no sistema de base que agrupa os resultados do teste com base em um **grupo de atribuição** de resultado de teste e no campo **Teste**. Esta regra está desabilitada, por padrão. Você pode agrupar por qualquer outro conjunto de valores em colunas acessíveis a partir do resultado do teste. Você pode usar até seis chaves e qualquer número de condições. Para obter mais informações, consulte Criar ou editar Configuration Compliance regras de grupo de resultados de testes.

Por exemplo, você pode agrupar seus resultados de testes por grupo de atribuição ou tecnologia e item de configuração (IC). Um conjunto diferente de regras pode ser usado para resultados de testes que expõem a empresa a mais riscos. Você pode ter uma regra de grupo para ICs de baixa severidade ou baixo risco. Consulte Campos de resultados de testes para obter mais informações sobre os campos disponíveis.

Quando um novo resultado de teste é importado ou reaberto após ser fechado, as regras da tarefa de correção são avaliadas em relação a ele. Um resultado de teste é avaliado apenas uma vez, a menos que seja reaberto após ser fechado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As regras de grupo são avaliadas após a correspondência de IC, os cálculos de pontuação de risco e as regras de atribuição.

O processo a seguir é usado para cada resultado de teste novo ou reaberto:

- Para cada regra de tarefa de correção, o resultado do teste é comparado ao filtro de condição.
- Para cada regra em que a condição da regra corresponde, ele extrai os dados das colunas de chave do grupo no resultado do teste. A regra verifica se há uma tarefa de correção em **aberto** correspondente que seja atribuída ao mesmo grupo de atribuição que o resultado do teste.

  Se o grupo for encontrado, o resultado do teste será adicionado ao grupo existente no estado **Aberto**.

- Se nenhum grupo no estado **Aberto** for encontrado, a regra criará um grupo, o atribuirá com base no valor de **Grupo de usuários** ou **Chave** na regra e colocará o resultado do teste nele.

Mais de uma regra de resultado de teste pode ser definida para agrupar diferentes tipos de resultados. Como cada resultado é comparado com as condições da regra antes de ser colocado em um grupo, muitas regras podem afetar o desempenho.

Quando uma regra de grupo é excluída, você tem a opção de excluir todos os grupos abertos criados pela regra. Isso se aplica à exibição de formulário de regra e à exibição de lista.

Quando uma atribuição de tarefa de correção é feita ou alterada, os campos **Grupo de atribuição** e **Atribuído a** são transferidos para todos os resultados de testes, exceto para aqueles em que o resultado do teste tem um grupo de atribuição diferente do RT. Para obter mais informações sobre regras de atribuição, consulte Configuration Compliance visão geral de regras de atribuição. Essas atribuições são usadas automaticamente para este grupo na próxima importação.

Rastrear contagens de adiamento para resultados de testes e tarefas de correção

A partir da v14.3, rastreie o número de vezes que um resultado de teste ou uma tarefa de correção é adiado no módulo Vários adiamentos. Um trabalho programado, **definir contagens de adiamento**, é executado diariamente para publicar contagens de registros que são adiados mais de uma vez na coluna Contagem de adiamento nos registros listados no módulo Vários adiamentos.

Configuração de grupos de calculadoras e calculadoras para Configuration Compliance

As calculadoras do Configuration Compliance são usadas para atualizar valores de registro quando condições predefinidas são atendidas. As calculadoras são agrupadas com base nos critérios usados para determinar como os registros são atualizados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Calculadoras do Configuration Compliance

A aplicação Configuration Compliance inclui dois tipos de calculadoras, Calculadoras de risco e Calculadoras de acúmulo de pontuação de risco. Esses grupos de calculadoras são habilitados por padrão.

O grupo de calculadoras de Pontuação de Risco foi renomeado para Calculadoras de Risco.

As Calculadoras de Rollup de Pontuação de Risco incluem calculadoras de rollup para testes de configuração e tarefas de correção.

A configuração de calculadoras de risco e de acúmulo para correção de resultados de testes e tarefas de correção inclui as seguintes tarefas:

- Criar uma calculadora de risco
- Criar uma calculadora de acúmulo de pontuação de risco

Depois de criar uma calculadora de risco, ela fica disponível para cálculos com a próxima ingestão de dados. Depois de criá-lo, você também pode aplicá-lo sob demanda.

Para obter mais informações sobre calculadoras e grupos de calculadoras, consulte Configuration Compliance grupos de calculadoras.

Configuration Compliance Visão geral da Gestão de exceções

Quando sua organização não pode estar em conformidade com uma gestão de vulnerabilidades ou política de segurança, padrão ou diretriz publicada, você pode solicitar uma exceção. A gestão de exceções envolve solicitar, revisar, aprovar ou rejeitar exceções para uma tarefa de correção que não pode ser corrigida de acordo com a política.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Algumas vulnerabilidades podem não ter um patch, correção ou solução existente. Quando uma exceção é aprovada, isso também significa que você está aceitando um risco porque

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

está reconhecendo e concordando com as consequências de não corrigir a vulnerabilidade relacionada à configuração.

Ciclo de vida de uma exceção

Uma exceção é uma solicitação para adiar a correção de uma tarefa de correção por um período especificado.

O ciclo de vida de uma exceção é o seguinte:

- Solicitar uma exceção
- Aprovação de uma solicitação de exceção
- Como rastrear uma solicitação de exceção
- Vencimento de uma solicitação de exceção

Solicitar uma exceção

Como responsável pela correção, você pode solicitar uma isenção para uma tarefa de correção usando o processo de gestão de exceções. Durante o processo de aprovação, a tarefa de correção permanece no estado **Em revisão**. Depois que o aprovador de exceção aprova essa solicitação, a tarefa de correção é movida para um estado **Adiado**.

Aprovação de uma solicitação de exceção

As tarefas de correção que não podem ser corrigidas imediatamente são revisadas, avaliadas quanto ao risco e aprovadas para adiamento até que possam ser corrigidas. A aprovação de uma solicitação de exceção pode ser um fluxo de trabalho de dois níveis. Se somente o aprovador de primeiro nível estiver presente, a exceção poderá ser solicitada e aprovada. No entanto, se não houver nenhum aprovador de primeiro nível, uma exceção não poderá ser solicitada. Para obter mais informações, consulte Adicionar um aprovador de exceção para Configuration Compliance.

Nota:

A partir de Configuration Compliance v13.0, se você estiver implantando a aplicação CC pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho.

Depois que uma solicitação de exceção para uma tarefa de correção for aprovada, você poderá executar as seguintes ações:

- Reabrir
- Fechar
- Excluir

Nota:

Os comentários de rejeição são mostrados nas Anotações de trabalho para uma tarefa de correção. Se uma solicitação de exceção for rejeitada, essa tarefa de correção será revertida para o estado anterior.

Como rastrear uma solicitação de exceção

Depois de gerar a exceção, você pode rastrear seu status usando a guia **Aprovações de mudança de estado** da tarefa de correção. Se uma ação for realizada em um grupo, você não poderá rastrear o status dos resultados de testes individuais nesse grupo.

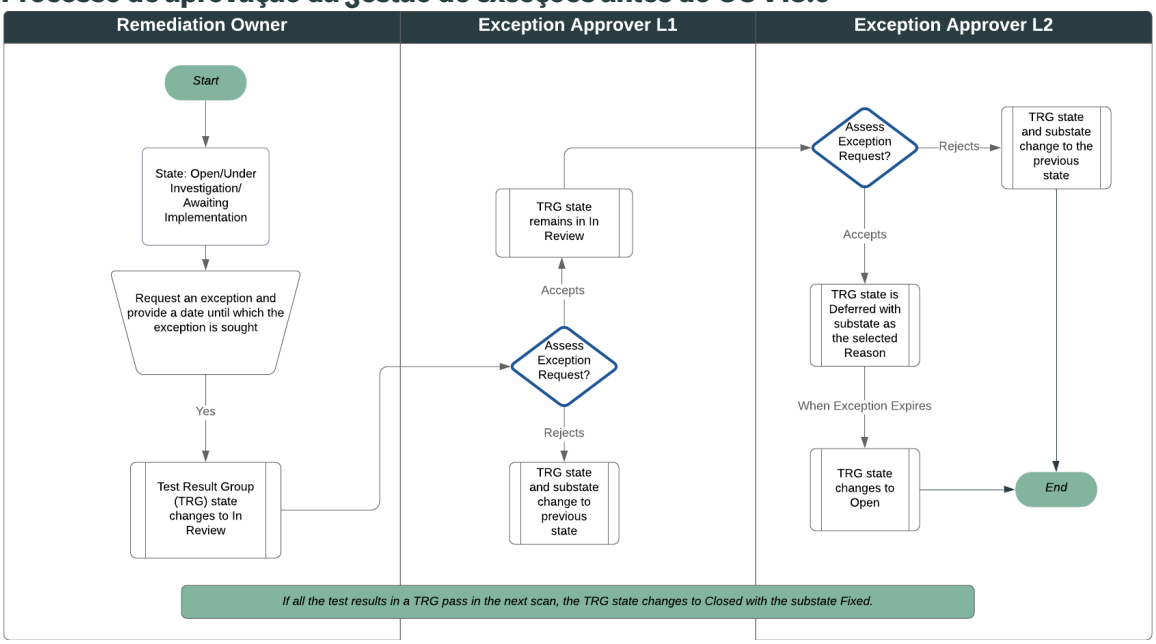
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Vencimento de uma solicitação de exceção

Quando uma solicitação de exceção para uma tarefa de correção expira, o grupo é revertido para o estado **Aberto**.

Processo de aprovação da gestão de exceções antes do CC v13.0



Configuration Compliance gestão de mudanças

Como proprietário de correção de TI, você pode criar e gerenciar solicitações de mudança (CHG) diretamente de grupos de resultados de testes (TRGs) na aplicação Configuration Compliance.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Solicitações de mudança e o fluxo de trabalho Configuration Compliance

As solicitações de mudança e o gerenciamento de mudanças fazem parte do processo de correção do fluxo de trabalho Configuration Compliance. Durante essa fase de correção, você pode usar solicitações de mudança para ajudá-lo a priorizar, rastrear e corrigir os resultados de testes.

A aplicação Configuration Compliance funciona com o processo de gestão de mudanças de TI Now Platform® para ajudá-lo a corrigir software e tecnologias fora de conformidade em seu ambiente.

Com o gerenciamento de mudanças na aplicação Configuration Compliance, você pode associar resultados de testes a solicitações de mudança existentes ou dividir um grupo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de resultados de testes e criar um novo grupo de resultados de testes somente para resultados de testes selecionados.

Para obter mais informações, consulte Como criar uma solicitação de mudança no Configuration Compliance.

Termos-chave

Testes

Testes são bibliotecas de registros de dados que organizam verificações de ativos de computação. Os testes de configuração definem como uma classe de ativos de tecnologia deve ser controlada. Um teste é qualquer coisa que possa ser usada para identificar uma classe de software ou um ativo de hardware que está fora de conformidade.

Resultados de testes

Os resultados de testes são importados por integrações de terceiros. Quando estiverem visíveis em Configuration Compliance, eles serão corrigidos usando **Grupos de resultados de testes**. Os grupos são atribuídos para correção de acordo com as regras de atribuição.

Nota:
A partir da versão 14.9 do Configuration Compliance, o resultado do teste é rotulado como *Descoberta*.

Grupo de resultado do teste

Os resultados de testes são agrupados em grupos de resultados de testes de acordo com as regras de atribuição e atribuídos automaticamente aos responsáveis pela correção.

Nota:
A partir da versão 14.9 do Configuration Compliance, o resultado do teste é rotulado como *Tarefa*de correção.

Políticas

As políticas estão relacionadas a documentos oficiais e registros de teste. Um grupo de testes de configuração define as políticas.

Solicitações de mudança

As solicitações de mudança ajudam a implementar processos controlados para correção. Você pode usar solicitações de mudança com grupos de resultados de testes em Configuration Compliance para ajudá-lo a identificar, rastrear e resolver ativos fora de conformidade (itens de configuração) que exigem recursos adicionais ou que você pode direcionar para adiamento.

Para obter mais informações sobre resultados de testes e grupos de resultados de testes, consulte Configuration Compliance tarefas de correção e visão geral de regras de grupo.

Quando usar solicitações de mudança no Configuration Compliance

As solicitações de mudança ajudam a iniciar e rastrear atividades de correção nos resultados de testes. Quando os proprietários de correção têm um grande número de resultados de testes não corrigidos ou itens de configuração, eles podem usar solicitações de mudança para identificar os resultados de testes para adiamento. Como alternativa, eles podem identificar e reagrupar resultados de testes e itens de configuração que exigem mais recursos do que os inicialmente identificados no grupo de resultados de testes original.

Criar solicitações de mudança a partir de um grupo de resultados de testes

Crie uma solicitação de mudança diretamente de um grupo de resultados de testes para todos os resultados de testes do grupo ou use a filtragem para identificar somente os resultados de testes

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

que correspondam a critérios específicos. Crie uma solicitação de mudança com informações preenchidas previamente para agilizar sua investigação de resultados de testes que exigem intervenção manual.

Dividir grupo

Em um grupo de resultados de testes existente, identifique um subconjunto de resultados de testes que você deseja mover para um novo grupo de resultados de testes. Ao criar um novo TRG, você pode trabalhar com um grupo específico de resultados de testes sem afetar o grupo de resultados de testes original.

Associar resultados de testes a uma solicitação de mudança existente

Associe resultados de testes a tarefas existentes para evitar a criação de solicitações de mudança duplicadas enquanto você trabalha para resolver seus grupos de resultados de testes. Ao associar um grupo de resultados de testes a uma solicitação de mudança que já está disponível em sua instância, você pode usar listas de tarefas existentes.

Tipos de solicitações de mudança para um grupo de resultados de testes

Você pode criar, aprovar, implementar, revisar e fechar solicitações de mudança diretamente dos grupos de resultados de testes atribuídos a você. Você pode criar três tipos de solicitações de mudança com informações preenchidas previamente de um grupo de resultados de testes:

- Padrão. Uma mudança pré-autorizada de baixo risco, relativamente comum e que segue um procedimento especificado ou instrução de trabalho.
- Normal. As solicitações de mudança normais seguem um processo prescritivo que requer dois níveis de aprovação antes de ser implementado, revisado e encerrado.
- Emergência. Uma mudança para resolver um incidente grave.

Instalando, instalando e configurando a aplicação Configuration Compliance

Antes de executar a aplicação em sua instância Now Platform®, você deve primeiro baixar e instalar a aplicação Configuration Compliance da ServiceNow® Store. Esta aplicação está disponível como uma assinatura separada.

Conclua as etapas da check-list de configuração listadas na tabela a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Para obter mais informações sobre as versões lançadas da aplicação Configuration Compliance, bem como aplicações de terceiros e ServiceNow que são compatíveis com ela, consulte o artigo Matriz de compatibilidade do Vulnerability Response e Mudanças de esquema de versão [KB0856498] na Base de conhecimento HI.

Para obter mais informações sobre como obter direitos para aplicações da Store, consulte Security Operations e o ServiceNow Store.

Configurar tarefas de check-list

Tarefas de configuração	Descrição
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar tarefas de check-list

Tarefas de configuração	Descrição
	• Se ainda não estiver atribuído, o administrador do sistema [admin] instalará a aplicação e atribuirá a função de administrador do Configuration Compliance [sn_vulc.admin]. • O administrador do Configuration Compliance [sn_vulc.admin] supervisiona a configuração e verifica os resultados esperados. • O proprietário de correção [sn_vulc.remediation_owner] lê e atualiza os registros atribuídos. A função sn_vulc.remediation_owner também é atribuída automaticamente quando qualquer usuário é atribuído à função itil.
Integrações compatíveis	Antes de usar Configuration Compliance para corrigir itens de configuração, você deve instalar uma integração de scanner de terceiros e executar pelo menos uma verificação de rede. Verifique se a aplicação Vulnerability Response está instalada e ativada antes de configurar integrações de terceiros compatíveis. Consulte Como instalar Vulnerability Response. Para verificar se as aplicações de integração estão instaladas e ativadas, navegue até **Gestão de assinaturas** > **Assinaturas** em sua instância. A lista exibe as assinaturas que sua organização comprou. Para obter mais informações sobre integrações de terceiros e uma lista de produtos compatíveis, consulte Integrações do Configuration Compliance.

Qualys Vulnerability Integration

- Se o Qualys Vulnerability Integration já estiver instalado no seu sistema e suas credenciais de API forem diferentes daquelas que você deseja usar para Configuration Compliance, vá para o Assistente de configuração (em Vulnerability Response) e atribua-as a cada integração de **PC da Qualys**.
- Navegar até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** e edite o campo **Credenciais de API** da **Qualys na guia Detalhes de REST** da Qualys.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter informações mais detalhadas sobre Qualys Vulnerability Integration, consulte Noções básicas sobre o Qualys Vulnerability Integration.

Agora você está pronto para instalar a aplicação Configuration Compliance. Consulte Como instalar Configuration Compliance.

Como instalar Configuration Compliance

Antes de executar Configuration Compliance em sua instância Now Platform®, você deve primeiro baixar e instalar a aplicação Configuration Compliance do ServiceNow Store. Esta aplicação está disponível como uma assinatura separada.

Antes de Iniciar

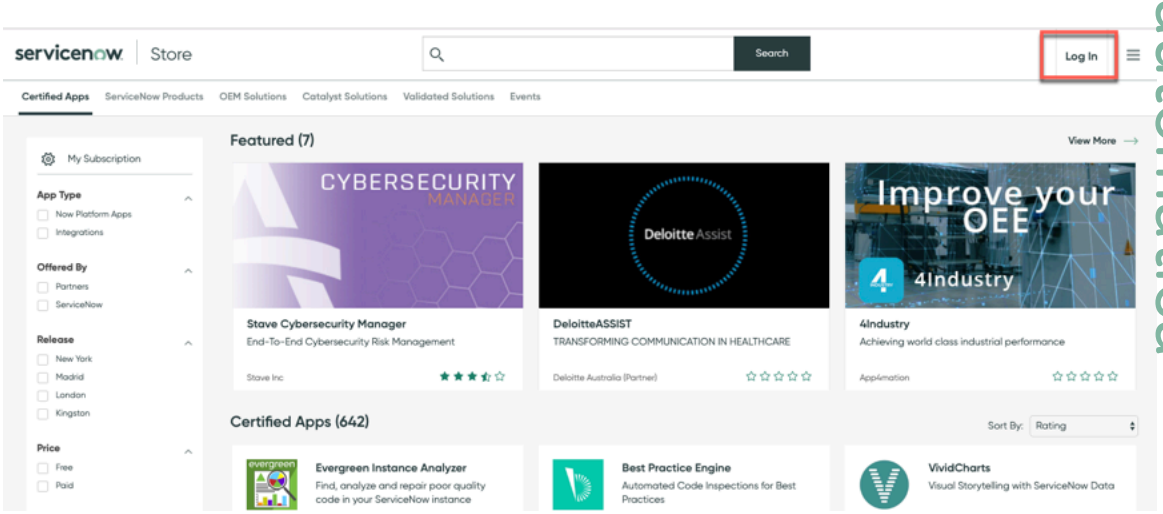
Conclua a check-list de configuração a seguir antes da instalação. Consulte Instalando, instalando e configurando a aplicação Configuration Compliance para tarefas de configuração. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Função necessária: administrador

Procedimento

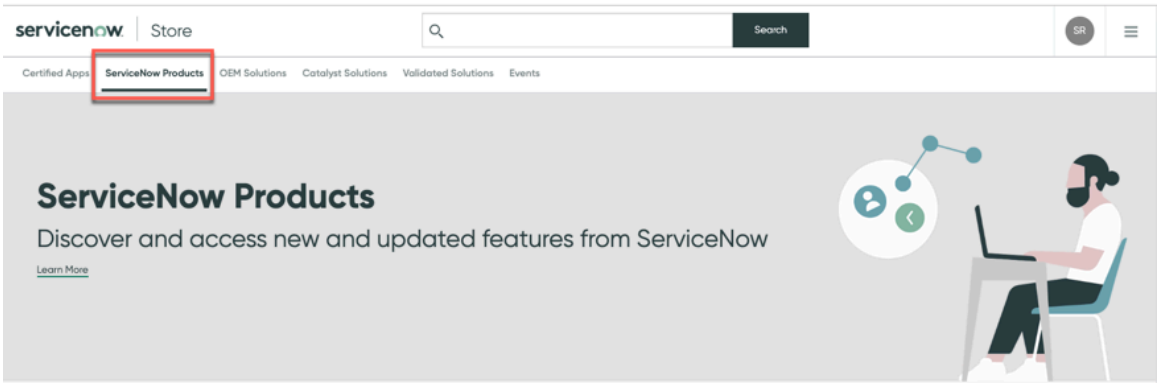
1. Para obter o direito e baixar a aplicação principal Configuration Compliance, navegue até ServiceNow Store.
2. No canto superior direito da página, clique em **Fazer login**.



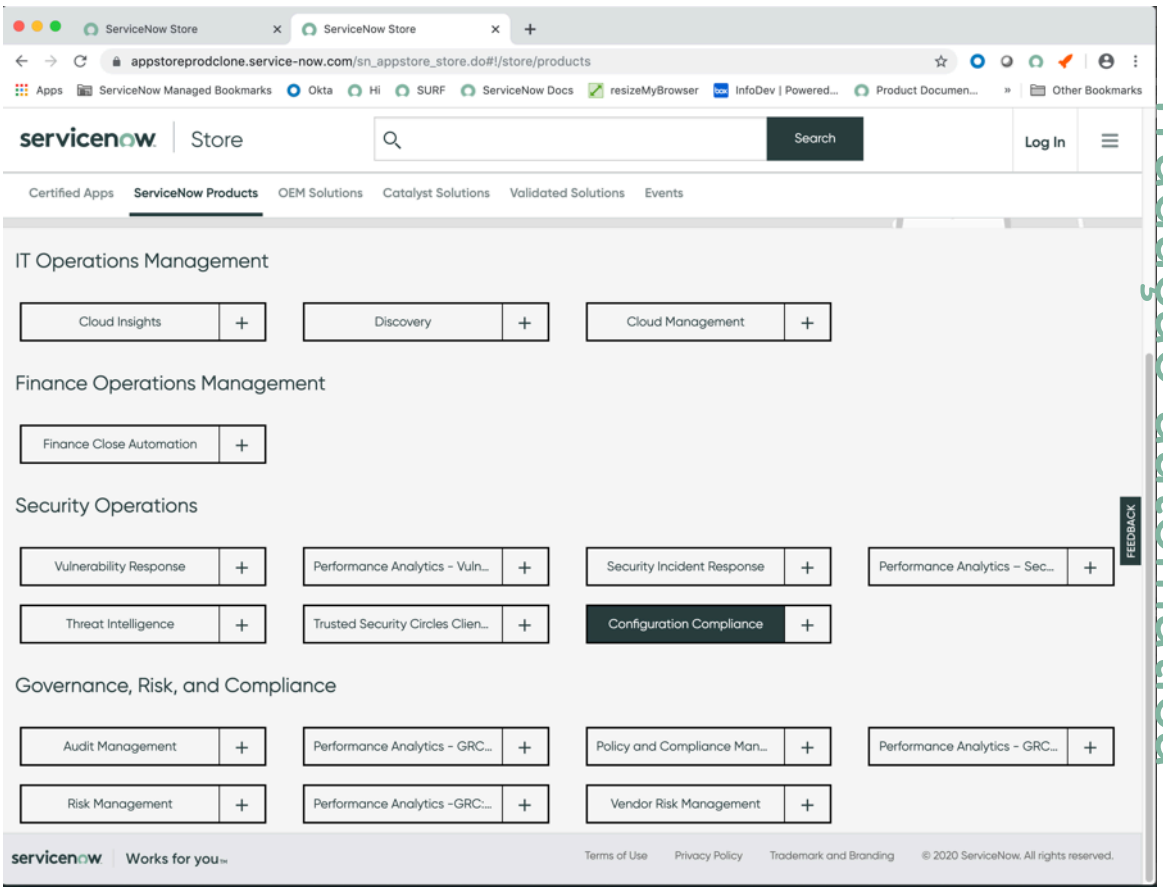
3. Na caixa de diálogo exibida, insira suas credenciais HI e clique em **Login**.
4. Na página exibida, se não estiver selecionada, clique na guia **Produtos da ServiceNow**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



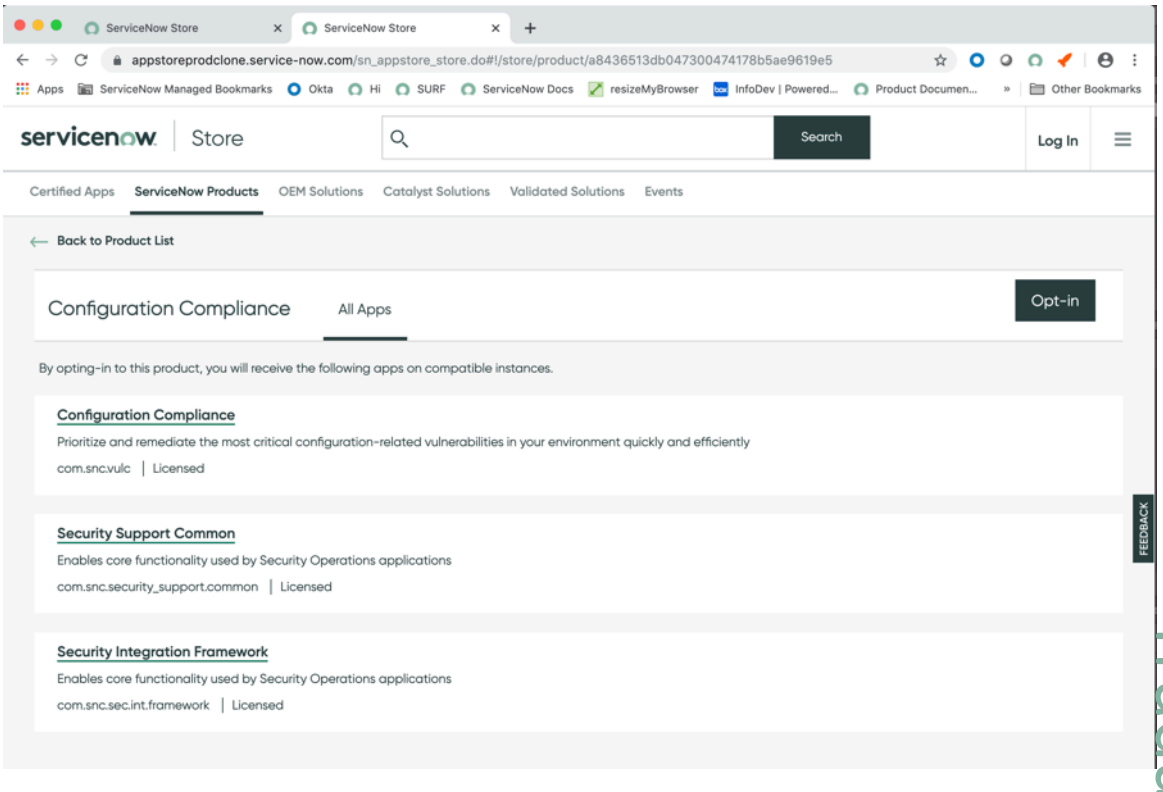
5. Para exibir as aplicações associadas para as quais você está qualificado com a aplicação Configuration Compliance, na página da lista de produtos, clique no produto **Configuration Compliance**.



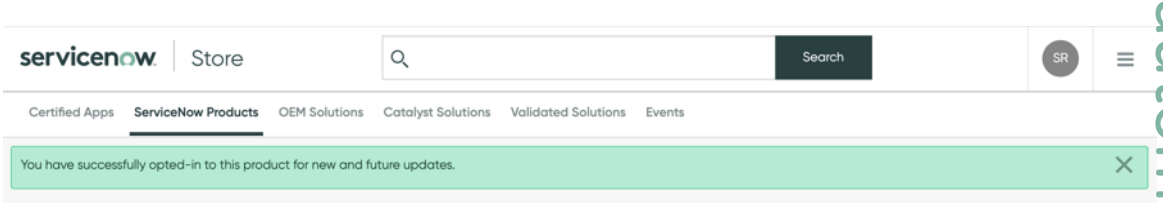
A página exibida lista todas as aplicações para as quais você está qualificado se aceitar. Para obter mais informações sobre uma aplicação, clique em um link.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Para obter a aplicação Configuration Compliance, clique em **Aceitar**.
7. Para concordar com os termos e condições, no prompt, marque a caixa de seleção e clique em **Aceitar**.
   Uma mensagem é exibida indicando que você aceitou a aplicação com sucesso.



Com a guia Produtos ServiceNow selecionada na Lista de produtos, uma marca de seleção verde substitui o sinal de mais à direita da aplicação Configuration Compliance, conforme mostrado na figura a seguir.

Depois de aceitar os termos e condições e os direitos gerenciados de qualquer uma das aplicações na guia **Produtos da ServiceNow**, na página Lista de produtos, você pode clicar no sinal de mais (+) para obter o direito e aceitar as outras aplicações nesta página com um único clique.

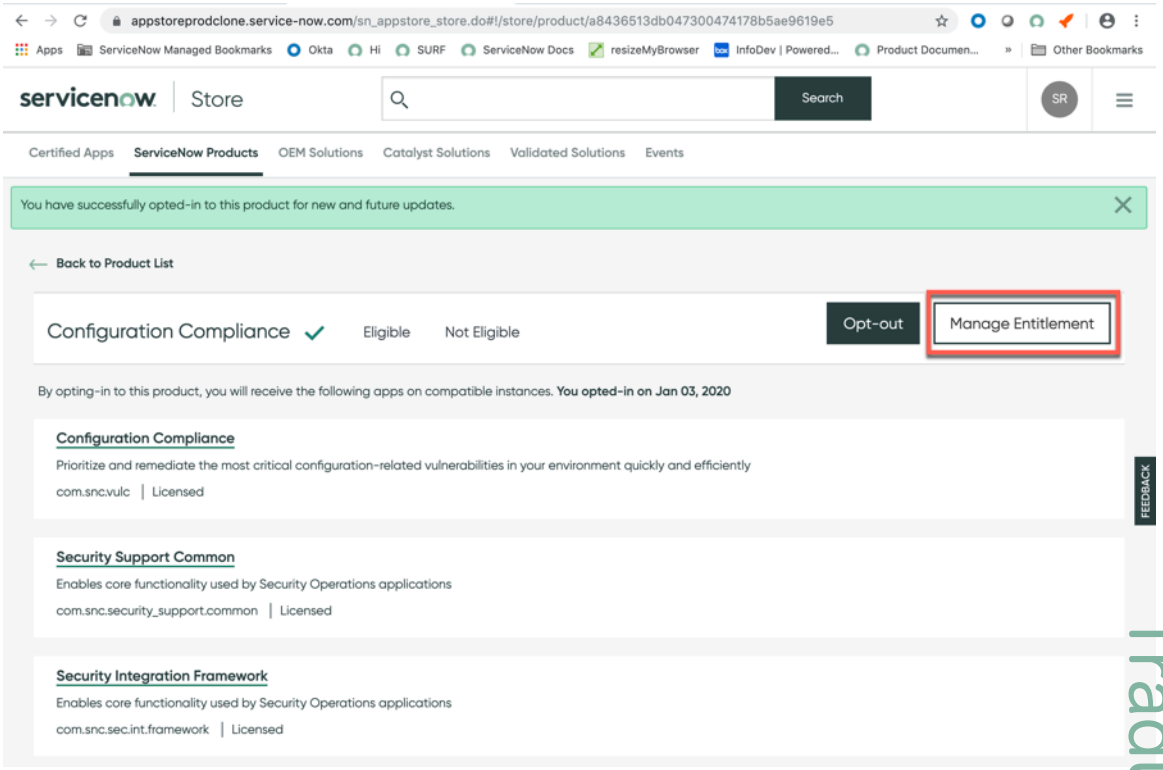
8. Pule para a etapa 10 para instalar a aplicação na sua instância Now Platform.
9. **Opcional:** Como alternativa, se você quiser gerenciar seu direito da aplicação Configuration Compliance em outras instâncias Now Platform, siga estas etapas.

   a. Se o botão Gerenciar direito não for exibido, clique na aplicação Configuration Compliance na lista de produtos para exibi-lo.

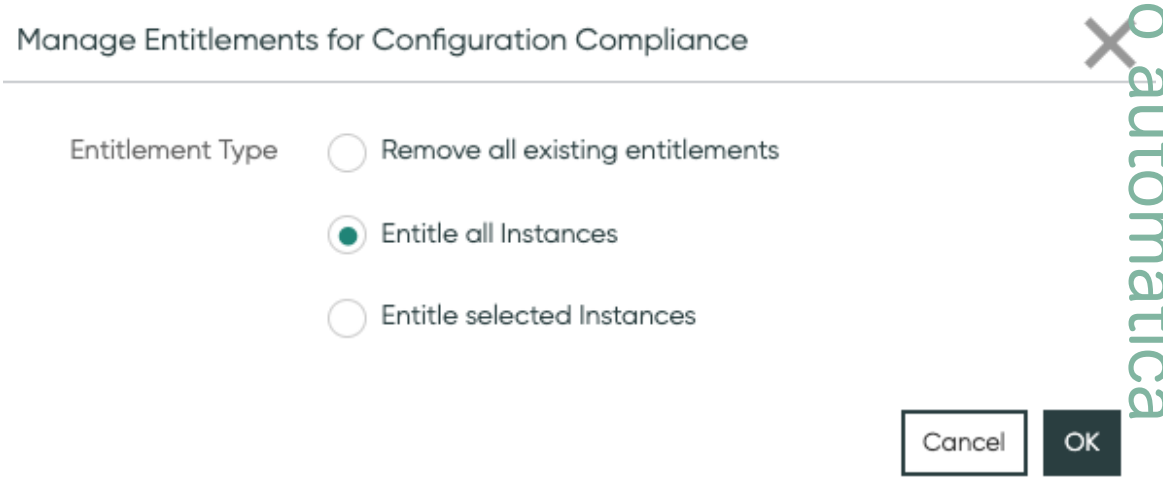
   b. Clique **em Gerenciar direito**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



c. Na caixa de diálogo Gerenciar direitos do Configuration Compliance exibida, escolha uma:



d. Clique em **OK** ou em **Cancelar** para continuar.

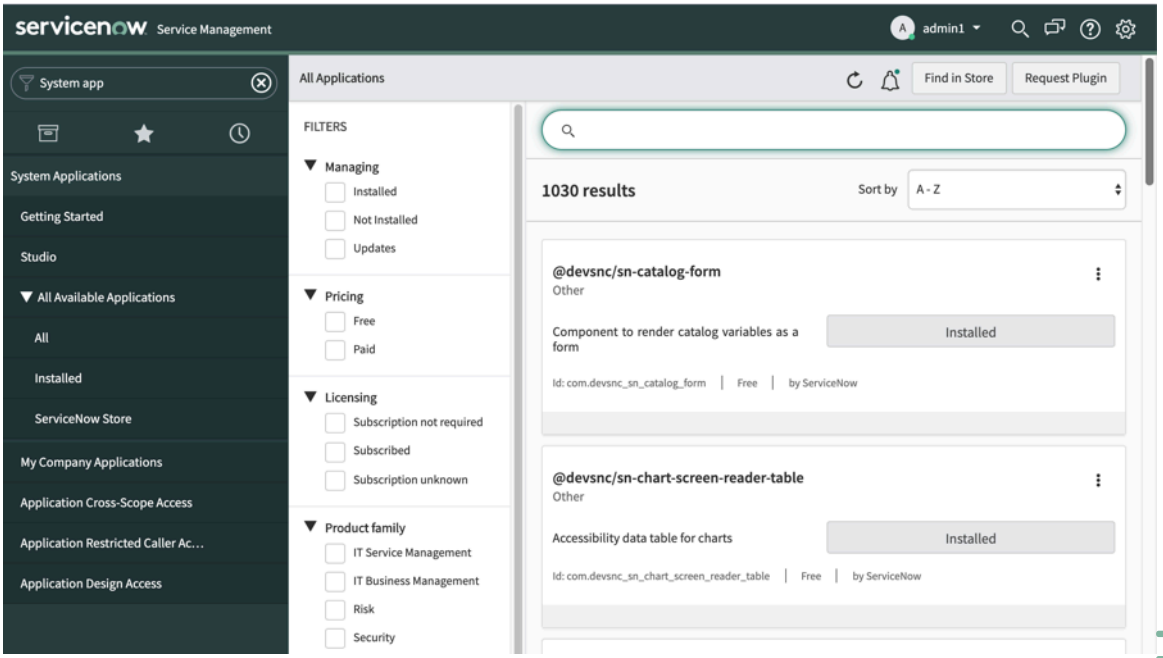
Você está pronto para ativar plug-ins e instalar a aplicação em suas Now Platform instância(s).

10. Faça login na instância Now Platform na qual você deseja instalar a aplicação Configuration Compliance.

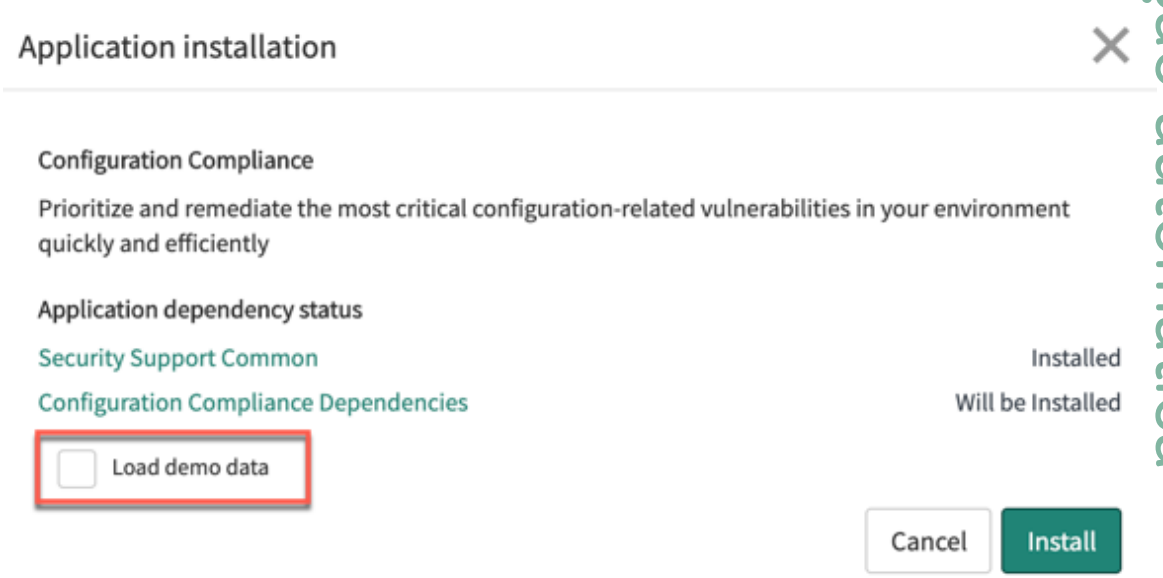
11. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



12. Entre as aplicações listadas, localize a aplicação Configuration Compliance (sn_vulc) e clique em **Instalar**. A caixa de diálogo de instalação da aplicação é exibida. Todas as dependências que serão instaladas serão exibidas.



13. Se você quiser dados de demonstração, marque a caixa de seleção Carregar dados de demonstração e clique em **Instalar**.

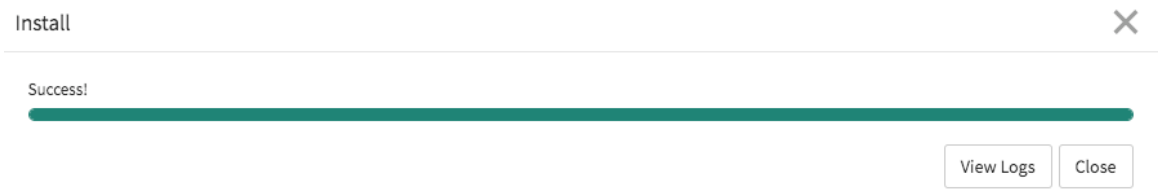
Nota:

Se você não marcar a caixa de seleção **Carregar dados** de demonstração, os dados de demonstração não ficarão disponíveis para instalação no **Gerenciador de aplicações** posteriormente. Para obter informações sobre como instalar ou reinstalar os dados de demonstração após a instalação inicial, consulte o artigo Solução alternativa para instalar dados de demonstração se a aplicação já estiver instalada [KB0722909] na Base de conhecimento Now Support.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta instalação pode levar algum tempo. Uma mensagem é exibida na caixa de diálogo Instalar depois que a aplicação e suas dependências são instaladas com sucesso.



14. Clique em **Fechar**.

Plug-ins SCA de terceiros separados adquirem e transformam dados em Configuration Compliance. Antes de usar Configuration Compliance para corrigir itens de configuração, você deve instalar uma integração de scanner de terceiros e executar pelo menos uma verificação de rede.

Para obter informações sobre como instalar integrações de terceiros para Configuration Compliance, consulte Integrações do Configuration Compliance.

Componentes instalados com Configuration Compliance

Vários tipos de componentes são instalados com a ativação do plug-in Configuration Compliance, incluindo tabelas e funções do usuário.

Nota:
A tabela Arquivos da Aplicação lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Exibir listas filtradas de componentes instalados com uma aplicação

Filtre a tabela Arquivos de aplicações para que somente as funções, os trabalhos programados e as tabelas que são instaladas com uma aplicação sejam exibidos. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.
2. Selecione o construtor de condição (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação. Por exemplo, **Aplicação** > **é** > **Vulnerability Response**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No construtor de condição, para adicionar um segundo filtro, selecione **E e**, em seguida, selecione, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função**, **Trabalho programado**ou **Tabela**.
4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
Administrador do Configuration Compliance [sn_vulc.admin]	Capaz de modificar a propriedade da aplicação, configuração, regras de atualização, integrações da aplicação Configuration Compliance.	sn_vulc.write **Nota:** Herda as funções necessárias para a administração dos registros da aplicação Configuration Compliance.
ler [sn_vulc.read]	Ler listas e registros no Configuration Compliance.	sn_sec_cmn.calcul_read
gravar [sn_vulc.write]	Grave listas e registros no Configuration Compliance.	• sn_vulc.read • sn_vulc.remediation_owner
escrever atribuição [sn_vulc.write_assignment]	Grave nos campos de atribuição de resultado de testes.	Contido na função sn_vulc.remediation_owner.
responsável pela correção sn_vulc.remediation_owner	Exiba e atualize a permissão para resultados de testes atribuídos a você ou seu grupo.	Contido na função itil. Contém: • sn_sec_cmn.read • sn_vulc.write_assignment
CC.Sistema sn_vulc.import_admin	Executa todos os trabalhos programados na aplicação Configuration Compliance.	• sn_vulc.write • import_admin • sn_vul_tenable.read_integration

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
	Nota: Este usuário é o padrão para executar como usuário para cada trabalho programado no Configuration Compliance.	
VRCommon.Sistema sn_vul_cmn.admin	Executar como usuário padrão para todos os trabalhos programados na aplicação comum do Vulnerability Response.	• sn_vul_cmn.write • sn_sec_cmn.admin • report_admin
SecCommon.Sistema sn_sec_cmn.admin	Padrão para executar como usuário para todos os trabalhos programados que são usados para a capacidade de trabalhos em segundo plano na aplicação comum de suporte de segurança	• sn_sec_cmn.int_write • sn_sec_cmn.write • workflow_admin • sn_sec_cmn.calcul_write • sn_sec_core.read_dictionary • sn_sec_cmn.manage_approval_rules • sn_sec_int.admin • sn_sec_cmn.cap_email_write • sn_sec_cmn.manage_classification_rules • sn_sec_cmn.manage_background_job
V14.7: sn_vulc.edit_watch_topic	Edite os tópicos de observação do Configuration Compliance.	sn_vulc.read_watch_topic
V14.7: sn_vulc.read_watch_topic	Leia os tópicos de observação do Configuration Compliance.	cmdb_read
V14.7: sn_vulc.create_watch_topic	Crie tópicos de observação para o Configuration Compliance.	sn_vulc.read_watch_topic

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalhos programados instalados

Trabalho programado	Descrição
Versão 12.0 Calcular métricas de correção para todos os grupos de resultados de testes	Calcula e atualiza valores para métricas de status em registros de tarefa de correção.
Versão 12.0: Calcular métricas de correção para todos os resultados de testes	Calcula e atualiza valores para métricas de status em registros de resultados de testes.
Versão 12.0: Sincronização de estado da solicitação de mudança	Trabalho sob demanda que sincroniza os estados de todas as tarefas de correção (RTs) existentes com solicitações de mudança (CHGs). Conforme uma solicitação de mudança passa por seu ciclo de vida, ela também move os estados de todas as tarefas de correção relacionadas automaticamente. Habilita a sincronização de estado daqui para frente.
Versão 11.1: Verificar adiamento de grupos de resultados de testes Vencimento	Envia notificações se as tarefas de correção expirarem (e se elas expirarem em uma semana).
Contagem de IC do Configuration Compliance	Preenche a contagem de itens de configuração (IC) distintos e a média de 90 dias consecutivos na tabela Contagem de itens de configuração [sn_vulc_cc_configuration_item_count].
Versão 11.1: Avalie e notifique os destinos de correção	Define ou atualiza datas de destino de correção em todos os resultados de testes. Determina o status das datas de destino da correção em relação às regras. Envia notificações
V14.7: Inserir grupos de resultados de testes na Tarefa de correção unificada	Trabalho programado único para inserir todas as tarefas de correção criadas na IU clássica na tarefa de correção unificada (sn_vul_remediation_task).
Versão 12.0: Preencher CR-TRG m2m para CR e CR-Primário	Preenche solicitações de mudança em tarefas de correção.
Removido em v11.1: reabrir grupos de resultados de testes adiados **Nota:** Descontinuado para versões anteriores a 11.1. Não use.	Reabre grupos adiados quando o prazo passa.
Reaplicar todas as regras de atribuição	Reaplica todas as regras de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho programado	Descrição
Versão 14.3: contagem de reatribuições para regras de atribuição	É executado diariamente e publica o número total de resultados de testes e tarefas de correção que não estão atribuídos por este recurso para uma regra de atribuição específica.
Reavaliar o estado dos grupos de resultados de testes	Reavalia o estado das tarefas de correção para entradas em que **assessment_state** é falso. É executado a cada 15 minutos.
Acumular pontuação de risco do resultado de testes para o grupo de resultados de teste e teste de configuração	É executado por hora e calcula as pontuações de acúmulo para os testes de configuração alterados e as tarefas de correção. • Calcula a pontuação de risco de acúmulo para todos os testes em sn_vulc_test_manifest e exclui o registro de manifesto após a conclusão. • Calcula a pontuação de risco de acúmulo para todos os testes em sn_vulc_result_group_manifest e exclui o manifesto após a conclusão.
Versão 12.0: Atualizar métricas de correção de política	Calcula e atualiza valores para métricas de status em registros de política.
Versão 14.3: definir contagens de adiamento	Coleta o número de vezes que um resultado de teste ou uma tarefa de correção é adiado.
Atualizar classificação de risco para resultados de testes	Atualiza a classificação de risco dos resultados de testes.
Atualize a pontuação de risco de acúmulo para todos os grupos de resultados e testes de configuração não encerrados.	Atualiza a pontuação de risco de acúmulo para todos os grupos de resultados não encerrados e testes Configuration Compliance.

Tabelas instaladas

Tabela	Descrição
Regra de atribuição [sn_vulc_assignment_rule]	Contém o conjunto de regras avaliadas para definir o grupo de atribuição nos resultados de testes.
Fonte Autorizada [sn_vulc_auth_src]	Armazene fontes autorizadas importadas.
Calculadora [sn_vulc_calculator_risk_score]	Contém a calculadora que define determinados campos de resultado de testes quando determinadas condições são atendidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Contagem de Itens de Configuração do CC [sn_vulc_cc_configuration_item_count]	Contém o número total de itens de configuração.
Versão 12.0: associação de solicitação de mudança [sn_vulc_action_associate_cr]	Tabela de preparação usada para associar solicitações de mudança a tarefas de correção.
Versão 12.0: criação de solicitação de mudança [sn_vulc_action_create_cr]	Tabela de preparação usada para criar formulários de solicitação de mudança.
Versão 12.0: formulário de solicitação de mudança [sn_vulc_cr_form]	Tabela base para gestão de solicitações de mudança.
Citação [sn_vulc_citation]	Contém citações importadas
Teste de configuração [sn_vulc_test]	Contém dados de teste de configuração importados.
Manifesto de teste de configuração [sn_vulc_test_manifest]	Contém os testes de configuração para os quais a pontuação de risco de acúmulo precisa ser calculada.
Tabela de ativos ausentes da versão 12.2 [sn_vul_missing_asset]	Contém registros de ativo temporário para dados de avaliação de conformidade de configuração importados com ativos incompatíveis.
Tecnologia de Teste de Configuração [sn_vulc_test_tecnologia]	Contém tecnologias de teste de configuração importadas.
Regra de Grupo [sn_vulc_grouping_rule]	Contém as regras que definem os critérios com os quais os grupos são criados automaticamente para um conjunto de resultados de testes.
Política [sn_vulc_policy]	Contém políticas importadas.
Teste de Configuração de Política [sn_vulc_policy_test]	Contém dados de teste de configuração de política importados.
Regra de destino de correção	Define o intervalo de tempo esperado para corrigir um resultado de teste.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_vulc_ttr_rule]	
Calculadoras de Risco [sn_vulc_calculator_group]	Contém o agrupamento de calculadoras Configuration Compliance. A ordem do grupo de calculadoras determina qual grupo é avaliado primeiro e, em cada grupo, uma calculadora é usada no máximo.
Calculadora de acúmulo de pontuação de risco [sn_vulc_risk_score_rollup]	Contém configurações da calculadora de acúmulo.
Grupo de resultados do teste de divisão [sn_vulc_action_split_trg]	Tabela de preparação usada para dividir tarefas de correção.
Aprovação de mudança de estado [sn_vulc_state_change_approval]	Contém dados de processo de estado de aprovação.
Tecnologia [sn_vulc_tecnologia]	Contém tecnologias importadas.
Mapa de Criticidade de Teste [sn_vulc_test_criticality_map]	Contém dados de mapa de criticalidade.
Resultado do Teste [sn_vulc_result]	Contém resultados de testes importados.
Grupo de resultados de testes [sn_vulc_result_group]	Contém tarefas de correção importadas.
Versão 12.0: Solicitações de Mudança de Grupo de Resultado de testes	Contém solicitações de mudança para tarefas de correção.
Manifesto de grupo de resultados de testes [sn_vulc_result_group_manifest]	Contém as tarefas de correção para as quais a pontuação de risco de acúmulo precisa ser calculada.
Grupos de resultados de testes [sn_vulc_m2m_result_result_group]	Contém dados da tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Histórico de Resultado de testes [sn_vulc_result_history]	Contém histórico de resultados de testes importados.
Status de correção do resultado de testes	Status do resultado do teste em relação à regra de destino de correção aplicada mais próxima.
V14.7: Contagens de teste de tópico de observação [sn_vulc_wt_test_counts]	Tabela de cache da guia Testes de configuração distinta no Espaço do gerenciador de vulnerabilidades.

Criar ou editar Configuration Compliance regras de atribuição

Crie regras para atribuir automaticamente resultados de testes com base nas condições do filtro. Essas regras atribuem resultados de testes conforme eles são importados.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

O sistema de base é fornecido com uma regra de atribuição Configuration Compliance, **Atribuir ao grupo de suporte de IC**, que atribui resultados de testes ao mesmo grupo de atribuição que o grupo de suporte de IC. Esta regra está inativa por padrão. Você pode modificar usando condições de filtro. Com as regras de atribuição, você define uma ou mais condições de atribuição e a ordem de execução. Quando um resultado de teste corresponde a uma condição de regra, a pesquisa de atribuição é interrompida.

Nota:
Regras novas ou atualizadas são avaliadas automaticamente na próxima importação ou manualmente usando o botão **Aplicar mudanças** na lista Regras de atribuição.

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Regras de atribuição**.
2. Abra a regra **Atribuir ao grupo de suporte de IC** ou clique em **Novo**.
3. Edite a regra **Atribuir ao grupo de suporte de IC** ou, se for **Novo**, preencha os campos no formulário, conforme apropriado.

Regra de atribuição do Configuration Compliance

Campo	Descrição
Nome	Nome da regra de grupo.
Ordem de execução	Ordem na qual as regras são avaliadas. O número mais baixo é avaliado primeiro. Regras de alta prioridade, resultados de testes que precisam de tratamento especial, onde o risco é crítico, ou um resultado de teste que deve ser tratado pela conformidade regulatória, deve ser executado primeiro. Em seguida, execute suas regras gerais, onde nenhum tratamento especial é necessário, e você saberá quem deve ser responsável por elas. Por fim, crie uma regra padrão para atribuir resultados de testes ao grupo que descobre a qual grupo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	de atribuição ele deve pertencer. Este grupo pode adicionar outra regra para cobrir suas decisões. Esta regra padrão seria executada por último.
Ativo	Indica se a regra de atribuição está ativa.
Condição	
Campos de condição	Condições que devem ser atendidas. A diferenciação de maiúsculas e minúsculas para o texto de pesquisa inserido no construtor de condição não é compatível com este registro ou formulário.
Novos critérios	Adiciona mais campos de filtro de condição para você escolher.
Descrição	Texto que descreve a regra de atribuição.
Atribuir usando	Para automatizar a atribuição de grupos criados com base nesta regra, escolha uma das opções disponíveis. ○ Grupo de usuários: selecione um grupo de usuários na tabela de pesquisa ○ Campo de grupo de usuários: selecione um campo de grupo de usuários no menu suspenso. ○ Script: crie ou edite um script. **Nota:** Criar ou editar um script requer experiência em ServiceNow.
Campo de grupo de usuários	Selecione o grupo de usuários responsável pela correção dos testes que correspondem às condições das regras de atribuição.

4. Clique em **Enviar**.

Configuration Compliance regras de destino de correção

Com as regras de destino de correção, você pode definir os intervalos de tempo esperados para corrigir os resultados do teste. Você pode enviar notificações para usuários e grupos quando as datas de destino estiverem se aproximando e quando elas estiverem atrasadas.

Funções necessárias: administrador do Configuration Compliance (sn_vulc_admin) ou um gerente com a função sn_vulc.manage_remediation_target_rules.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

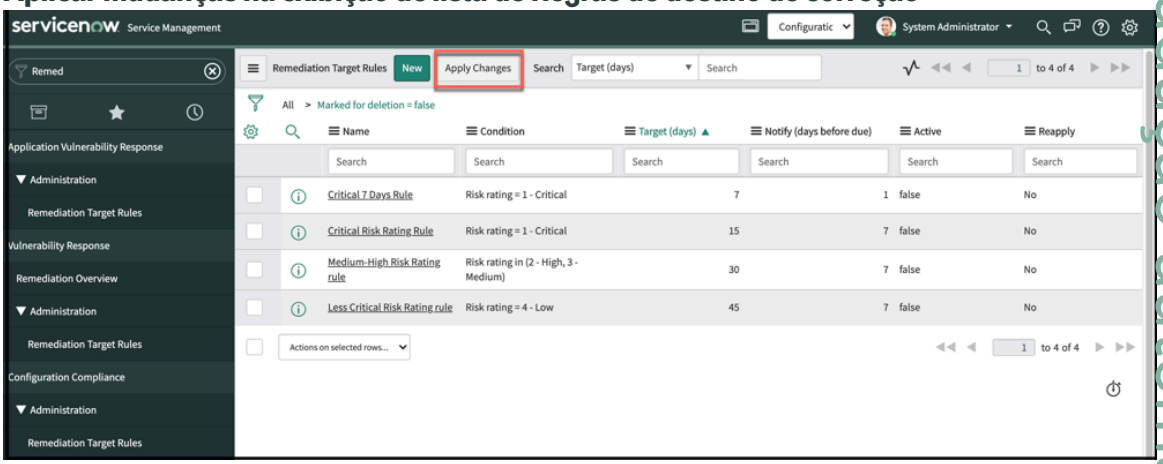
Regras de destino de correção

Um trabalho programado, *Evaluate and notify remediation targets*, é executado diariamente e usa regras de destino de correção ativas para avaliar registros de resultado de testes ativos. Sempre que os registros de resultado de testes associados aos grupos de resultados de testes são atualizados ou alterados, os valores modificados são avaliados pelas regras de destino e as mudanças são acumuladas e exibidas nos grupos de resultados de testes associados.

Você pode editar, desabilitar ou excluir regras de destino de correção existentes e criar novas. Ao mudar, desabilitar ou criar uma nova regra, você tem a opção de clicar em **Aplicar mudanças** na exibição da lista Regras de destino de correção e aplicar manualmente as mudanças introduzidas antes do próximo trabalho programado. Com esta opção, você pode reavaliar seus registros de resultado de testes sem precisar esperar. Se você optar por não aplicar as mudanças manualmente, o próximo trabalho programado diário selecionará as mudanças e as aplicará.

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Regras de destino de correção** para exibir regras de destino de correção.

Aplicar mudanças na exibição de lista de Regras de destino de correção



2. Clique em uma regra na coluna Nome para abrir seu registro.
3. Marque a caixa de seleção **Ativa** no registro Regra de destino de correção para habilitar (verdadeiro) quaisquer regras desabilitadas (falso).

Sempre que você altera ou adiciona uma regra de destino, independentemente de optar por aplicar as mudanças manualmente ou aguardar o próximo trabalho programado, suas mudanças são usadas para avaliar todos os resultados de testes ativos junto com quaisquer outras regras de destino afetadas por suas mudanças. Quando você opta por aplicar as mudanças manualmente, essa avaliação pode levar algum tempo se você tiver um grande volume de resultados de testes ativos, porque todas as regras afetadas pelas mudanças são usadas para uma avaliação.

Por exemplo, o valor padrão para dias de correção direcionados é 30. Se você criar uma nova regra que também tenha 30 para Dias de correção direcionados, esta regra e quaisquer regras de destino com 30 dias ou mais como datas de destino serão aplicadas aos resultados de testes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regras de destino desativadas e excluídas

Quando uma regra está ativa, verdadeiro é exibido na coluna Ativa na exibição da lista Regras de destino de correção. Depois que uma regra é desativada (falso), ela não é mais aplicada a novos resultados de testes. No entanto, o trabalho programado continua rastreando todos os resultados de testes existentes aos quais a regra foi aplicada. Se a regra ou regras desativadas forem reativadas posteriormente, qualquer resultado de teste com um campo **Data de destino de correção** vazio será avaliado em relação às regras reativadas. Isso inclui resultados de testes criados enquanto as regras foram desativadas.

Quando as regras são excluídas, a **Data de destino** da correção e os campos relacionados nos resultados de testes encerrados são preservados. A **Data de destino** da correção e os campos relacionados em resultados de testes não encerrados são apagados e todas as regras dependentes são reaplicadas.

Para desativar uma regra, no registro de regra de destino de correção, desabilite a caixa de seleção ativa e clique em **Atualizar**. Falso é exibido na coluna Ativo na exibição de lista de Regras de destino de correção.

Para excluir uma regra, clique em **Excluir** no formulário ou, como alternativa, na exibição de lista, selecione a regra ou as regras e clique em **Excluir** na lista **Ações nas linhas**. A regra não é mais exibida na lista e a próxima regra na ordem de operação substitui a regra excluída.

Se você desativar ou excluir uma regra e optar por aplicar as mudanças antes do próximo trabalho programado, a referência da regra será apagada do campo, mas a data de correção e os dados de status serão preservados. Se você não aplicar as mudanças manualmente, a referência da regra será apagada do campo com o próximo trabalho programado.

Sobre as Regras de destino e o trabalho programado Avaliar e notificar os destinos de correção

O trabalho programado *`Evaluate and notify remediation targets`* é executado uma vez às 4:30:00 diariamente. Ele seleciona todas as regras de destino de correção ativas e avalia todos os resultados de testes ativos, começando com os resultados de testes com a data de destino de correção mais antiga. Ele avalia todos os resultados de testes que atendem aos seguintes critérios:

- Não estão em um estado **Encerrado**.
- Não tem data de meta de correção.
- Têm datas de destino de correção posteriores às datas nas regras de destino de correção.
- São criados após a conclusão de uma importação de scanner. O trabalho programado seleciona e avalia todos os novos resultados de testes criados como resultado de uma importação.

Depois que uma regra de destino é definida, as datas de destino da correção são calculadas pelo trabalho programado *`Evaluate and notify remediation targets`*. O trabalho programado adiciona uma data de destino de correção, se não houver uma, ou, se esta regra contiver uma data anterior à do registro, ela atualizará a data de destino existente.

Todos os registros expirados e as datas de lembrete que correspondem às regras de destino são selecionados pelo trabalho e as notificações são enviadas. Para regras

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

desabilitadas, o trabalho limpa os campos de correção nos registros de resultado de testes e para de enviar notificações.

Exibir datas de destino e status nas exibições de lista e formulário

Configuration Compliance Os gerentes podem ver a data de destino da correção no formulário de resultado de testes e nas exibições de lista. As regras de destino de correção também são executadas após uma importação de scanner e executadas novamente se um resultado de teste for reaberto.

O trabalho programado atualiza o **Destino** de correção e o **Status** de correção na exibição da lista de resultados de testes e os campos **Regra de destinode correção**, Destino de **correção e Status** de correção no formulário de resultado de testes.

Nota:

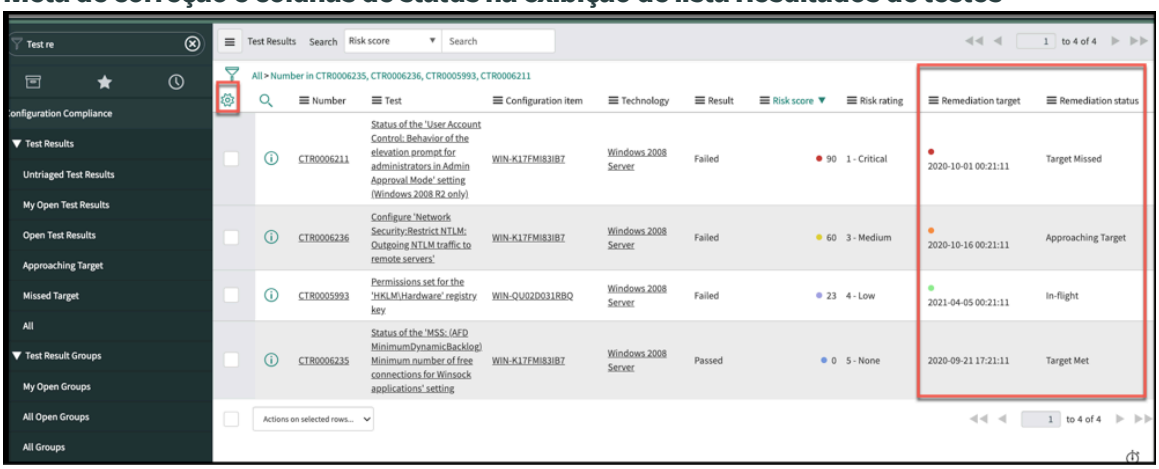
Por padrão, as colunas Destino de **correção** e **Status** de correção não são exibidas na exibição da lista Resultados de testes. Para exibir essas colunas, você também deve adicioná-las à exibição de lista. Da mesma forma, adicione os campos **Regra de destinode correção**, Destino de **correção e Status** da correção ao formulário de resultado de testes.

Use os slushbuckets nos menus Configurações e Ação adicional, respectivamente, conforme mostrado nas imagens a seguir para exibir essas colunas e campos. Para o menu Ação adicional no registro de resultado do teste, clique no ícone do menu, seguido por **Configurar** e **Layout do formulário** para exibir a interface de caixa de listagem dupla e mover os campos de **Disponível** para **Selecionado**.

A data de destino da correção é codificada na exibição de lista Resultados de testes como pontos coloridos:

- Os resultados de testes que não atingiram a data de notificação são mostrados em verde.
- Os resultados de testes que se aproximam da data de destino da correção são mostrados em laranja.
- Os resultados de testes após a data de destino da correção são mostrados em vermelho.

Meta de correção e colunas de status na exibição de lista Resultados de testes

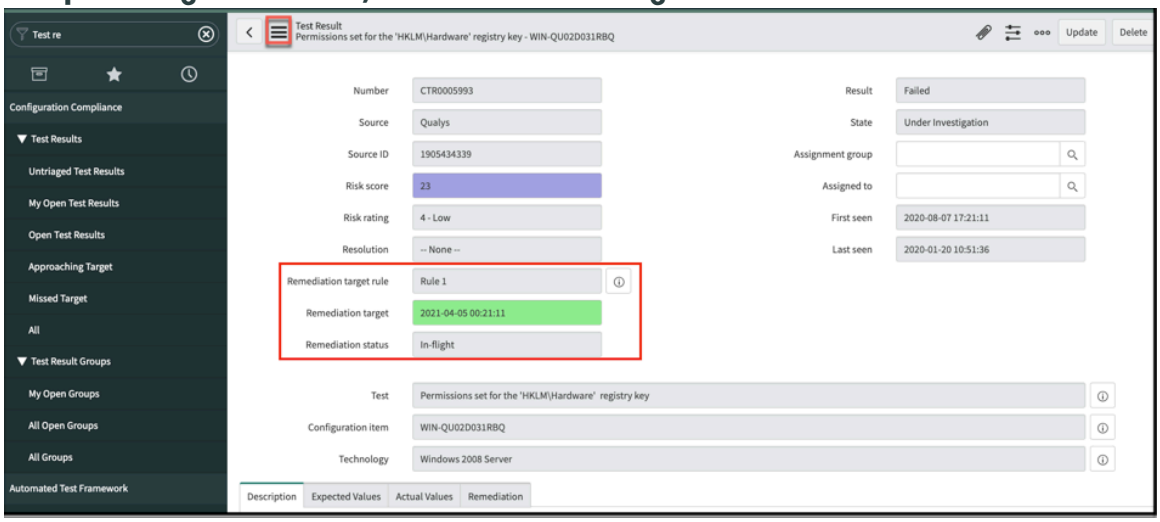


- Meta não atingida: a data de meta está vencida
- Emandamento : o resultado do teste está em andamento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos de regra de destino, destino e status no registro de resultado de testes



Os registros de resultado de testes também são exibidos visualmente no painel Configuration Compliance. Navegar até **Todos** > **Configuration Compliance** > **Visão geral** e verifique o painel para o status. A visão geral inclui widgets existentes e status de correção. As cores dos gráficos correspondem às cores exibidas na exibição da lista Resultados de testes e no registro do Resultado de testes.

Cenário de regra de destino de correção

Quando várias regras de destino de correção são aplicadas ao mesmo resultado de testes, a regra mais restritiva é aplicada.

Por exemplo, se um resultado de teste identificado pela primeira vez em 01/03/2018 atender às condições para duas regras de destino de correção:

- Regra de destino de correção 1: definida em 03/07/2018; a meta de correção é de 15 dias desde a primeira vista; A data de destino da correção calculada é 16/03/2018 10:00:00.
- Regra de destino de correção 2: definida em 10/03/2018; a meta de correção é de 10 dias desde a primeira vista; A data de destino da correção calculada é 11/03/2018 10:00:00.

Nota:

Os destinos de correção são calculados a partir da data da **última exibição** mais o número de dias (medidos como incrementos de 24 horas).

A partir da V14.5, as metas de correção são calculadas a partir da **meta de (data)**. O valor padrão permanece **Última Visto**.

Neste cenário, a Regra de destino de correção 2 se aplica ao resultado do teste, porque tem a data mais restritiva: 10 dias desde que o resultado do teste foi identificado pela primeira vez versus 15 dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar ou modificar regras de destino e reaplicar as mudanças

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Regras de destino de correção** para exibir, editar e criar novas regras de destino de correção.
2. Na coluna Nome, clique em uma regra para abrir uma regra de destino e editar o registro ou, como alternativa, clique em **Novo** para criar uma nova regra de destino.
3. Preencha o formulário para definir o intervalo de tempo de correção esperado, especifique a quais resultados de testes esta regra se aplica com condições e determine quando enviar lembretes para usuários ou grupos, ou ambos.
4. Clique em **Enviar**. Como alternativa, para salvar regras editadas, clique em **Atualizar**.

   A exibição de lista é exibida com sua regra atualizada ou nova. As regras na lista são ordenadas e executadas começando com a regra com a data de meta de correção mais baixa. Se você desabilitar ou excluir uma regra, a próxima regra na sequência de ordem substituirá a regra inativa ou excluída.
5. Para aplicar as novas mudanças agora, clique em **Aplicar mudanças**.

Configuration Compliance grupos de calculadoras

Configuration Compliance calculadoras são usadas para atualizar valores de registro quando condições predefinidas são atendidas. As calculadoras são agrupadas com base nos critérios usados para determinar como os registros são atualizados.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Configuration Compliance grupos de calculadoras

No registro Calculadora de risco padrão, as regras da calculadora podem ser aplicadas a todos os resultados de testes afetados e coleções sob demanda. Os gerentes de vulnerabilidade podem usar este recurso para ajustar a configuração da calculadora de risco. Eles podem experimentar vários esquemas de priorização no início da implantação e aplicar essas mudanças sob demanda para ver como elas afetam as descobertas de importação.

O grupo de calculadoras de Pontuação de Risco foi renomeado para Calculadoras de Risco.

As calculadoras de acúmulo de pontuação de risco estão incluídas com Configuration Compliance. Existem dois tipos de calculadoras de acúmulo individuais:

Acúmulo de risco de teste de configuração

Calculadoras que acumulam pontuações de risco para todos os Resultados de testes com o mesmo Teste de configuração para fornecer uma pontuação de risco geral para o Teste de configuração. O valor acumulado é exibido nos campos de Pontuação de risco.

Acúmulo de pontuação de risco do grupo do resultado de testes

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Essas calculadoras acumulam pontuações de risco para todos os resultados de testes em uma tarefa de correção para fornecer uma pontuação de risco geral para esse grupo. O valor acumulado é exibido nos campos de Pontuação de risco.

O grupo de calculadoras de pontuação de risco e o grupo de calculadoras de acúmulo de pontuação de risco estão habilitados por padrão.

Para obter mais informações, consulte os seguintes termos-chave para calculadoras Configuration Compliance :

Resultado do teste

Um resultado de teste é o resultado do teste de configuração em um item de configuração (IC) e a tecnologia associada. Os resultados de testes nos estados Falha, erro e Desconhecido identificam o hardware, o software e os ativos que estão fora de conformidade com suas políticas.

Grupo de resultado do teste

Os resultados do teste são agrupados no momento da importação de dados com base nas regras de grupo predefinidas. Essas tarefas de correção são semelhantes aos grupos de vulnerabilidades em Vulnerability Response. As Tarefas de correção organizam os resultados de testes em grupos para análise em massa e representam um conjunto de itens a serem corrigidos.

Pontuação de risco em um resultado de teste

Um valor calculado por calculadoras de pontuação de risco que se baseia no contexto de negócios de um ativo e na severidade do teste associado. É a média da criticidade dos negócios do ativo afetado, conforme definido no CMDB, e a severidade do teste, conforme comunicado pelo scanner.

Cada ativo pode ter vários serviços associados a ele. A criticidade dos negócios de um ativo é determinada pelo serviço com a criticidade mais alta.

O valor calculado é exibido nos campos de pontuação de risco dos resultados de testes. As pontuações exibem valores que variam de 0 a 100. Os campos também são codificados por cores para fornecer uma visão geral da severidade.

Pontuação de risco no grupo de resultados de testes

Essa pontuação é exibida no registro da tarefa de correção e é o valor acumulado das pontuações de risco de todos os resultados de testes ativos em uma tarefa de correção. Essa pontuação muda conforme os resultados de testes são corrigidos na Tarefa de correção.

Pontuação de risco no teste de configuração

Essa pontuação é exibida em testes de configuração e é o valor acumulado das pontuações de risco para todos os resultados de testes ativos com esse teste de configuração. Essa pontuação muda conforme os resultados de testes associados a este teste de configuração são corrigidos.

Pontuação de risco

A quantidade de risco que um resultado de teste com falha representa para o seu sistema. Ele se baseia em um intervalo de pontuações de risco em uma escala numérica de 1 a 5 que classifica os riscos como Críticos (1) a Nenhum (5). A pontuação é baseada em um intervalo de pontuações de risco e é exibida nos campos de Classificação de Risco.

Intervalos de classificação de risco

Pontuação de risco	Pontuação de risco
1- Crítico	90 a 100
2- Alto	70 a 89

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Intervalos de classificação de risco

Pontuação de risco	Pontuação de risco
3- Média	40 a 69
4- Baixo	1 a 39
5- Nenhum	0

Calculadoras de acúmulo de pontuação de risco

Existem dois tipos de calculadoras de acúmulo:

- Acúmulo de risco de teste de configuração: essas calculadoras acumulam pontuações de risco para todos os resultados de testes com o mesmo teste de configuração para fornecer uma pontuação de risco geral para o teste de configuração. O valor acumulado é exibido nos campos de Pontuação de risco. Você pode editar os valores de script para peso e pontuação dessas calculadoras.
- Acúmulo de pontuação de risco do grupo do resultado de testes: essas calculadoras acumulam pontuações de risco para todos os Resultados de testes em uma tarefa de correção para fornecer uma pontuação de risco geral para esse grupo. O valor acumulado é exibido nos campos de Pontuação de risco. Você pode editar os valores de script para peso e pontuação dessas calculadoras. Para obter um exemplo de uma calculadora de acúmulo de pontuação de risco e como ela calcula as pontuações, consulte Exemplo de cálculo de acúmulo de risco para Configuration Compliance.

Pontuação de risco histórico

A pontuação de risco inerente em todos os resultados de testes aprovados em uma tarefa de correção. Este campo exibe a quantidade de risco que foi corrigida por um grupo de teste e só é exibido depois que um grupo de teste está no estado "Encerrado" e a pontuação de risco é zero.

As pontuações são calculadas sempre que a pontuação de risco muda ou quando os resultados de testes são adicionados ou removidos de uma tarefa de correção.

Nota:
Para funcionar corretamente, este script requer o plug-in Mapeamento de serviços. Mapeamento de serviços está disponível como uma assinatura separada e requer ativação pela equipe ServiceNow.

Criar um grupo de calculadoras Configuration Compliance

Configuration Compliance grupos de calculadoras são usados para agrupar calculadoras com base em como você deseja usá-las.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
O sistema de base Configuration Compliance inclui um grupo de calculadoras: **Pontuação de risco**. Ao criar outras calculadoras, você pode adicioná-las a este grupo ou criar outros grupos e calculadoras. Em cada grupo, a primeira calculadora que corresponde ao resultado do teste é executada.

Há dois grupos de calculadoras incluídos com a aplicação Configuration Compliance:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Calculadoras de Risco
- Calculadoras de acúmulo de pontuação de risco

As calculadoras de risco calculam a pontuação e a classificação de risco de um resultado de teste.

As calculadoras de acúmulo de pontuação de risco acumulam pontuações de risco para todos os resultados de testes e tarefas de correção com o mesmo teste de configuração para fornecer uma pontuação de risco geral.

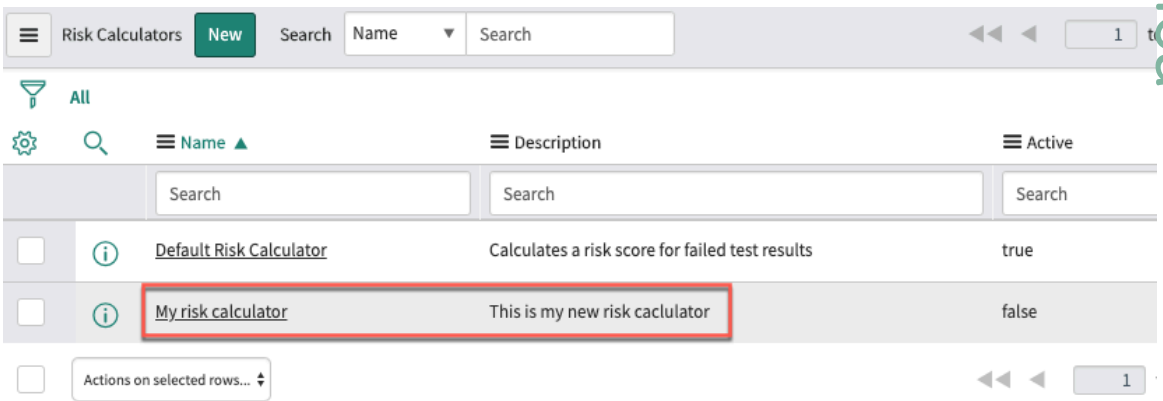
Você também cria novas calculadoras diretamente desses grupos.

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Grupos de Calculadoras**.
2. Navegar até **Todos** > **Configuration Compliance** > **Administração** e selecione Calculadoras de risco ou **Calculadoras** de acúmulo de **pontuação**de risco .
3. Clique em **Nova**.
4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Nome	O nome da calculadora.
Descrição	Uma descrição deste grupo de calculadoras.
Ativo	Habilite ou desabilite o grupo de calculadoras.

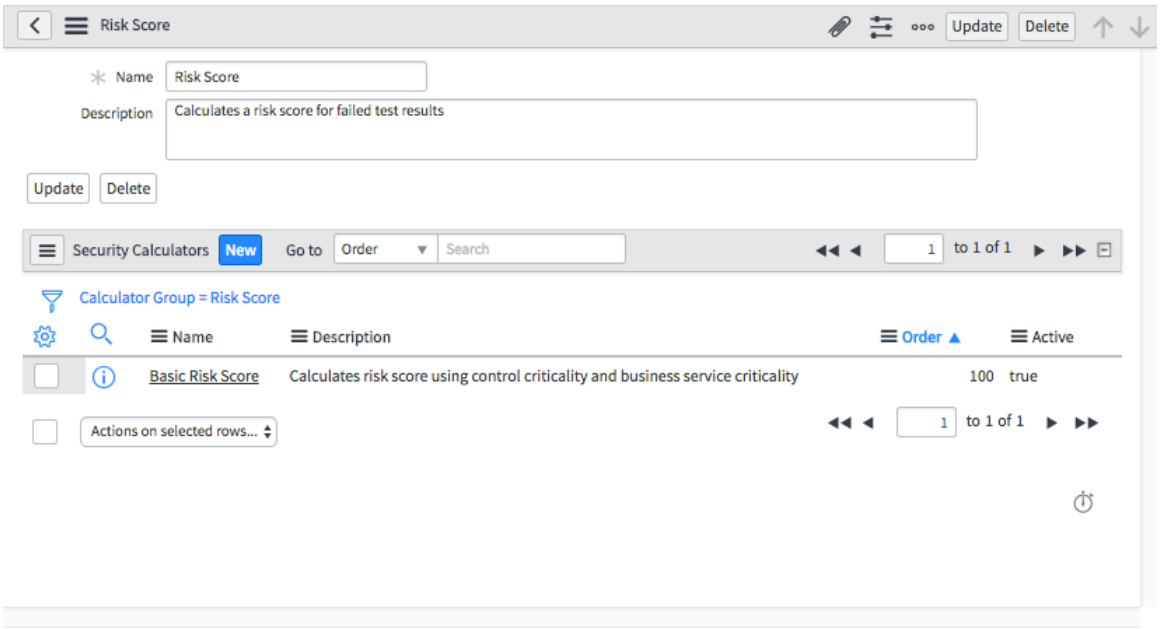
5. Clique com o botão direito do mouse em **Salvar** no cabeçalho do formulário ou clique em **Enviar**.
O novo grupo de calculadoras é exibido na lista de grupos com as outras calculadoras. Clique no nome do novo grupo de calculadoras para abrir o registro. Consulte Criar, editar e reaplicar calculadoras de risco para Configuration Compliance para obter mais informações sobre como definir condições e valores exibidos e reaplicar calculadoras.



A lista relacionada **Calculadoras de segurança** é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Clique em **Novo** para adicionar calculadoras junto com suas condições ao grupo.

   A diferenciação de maiúsculas e minúsculas para o texto de pesquisa inserido no construtor de condição não é compatível com este registro ou formulário.

Configuration Compliance calculadoras e regras da calculadora

Configuration Compliance automatize o cálculo de valores iniciais para os campos nos resultados de testes. A condição de cada calculadora é avaliada na ordem e a primeira calculadora correspondente é usada.

Configuration Compliance calculadoras

O sistema de base do Configuration Compliance inclui uma calculadora de conformidade de configuração (**Calculadora de risco padrão**) que define a **pontuação de risco** básica no resultado do teste. As calculadoras do Configuration Compliance podem ser criadas para priorizar e classificar o impacto dos resultados de testes com base em qualquer critério usando filtros de condição. Seja o impacto nos negócios da vulnerabilidade, a classe do item de configuração (IC), você pode criar calculadoras de conformidade de configuração adicionais para definir outros campos nos resultados de testes ou personalizar as calculadoras de conformidade de configuração existentes. Uma calculadora pode ser escrita para refletir qualquer conjunto de prioridades.

Cada calculadora contém uma lista de regras da calculadora, com uma condição que determina quando aplicá-la. Quando a calculadora é executada, a condição de cada regra da calculadora é avaliada na ordem e a primeira regra da calculadora correspondente é usada.

Todas as calculadoras de conformidade de configuração habilitadas definem os campos selecionados sempre que um resultado de teste é criado, quando um IC associado ou teste de configuração muda ou quando o link relacionado **Calcular pontuação de risco** em um resultado de teste é usado. Por exemplo, a pontuação de risco é atualizada automaticamente nos registros de resultado de testes quando o valor de control.criticality é atualizado em um resultado de teste importado. Depois que uma importação de resultado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de teste tiver atualizado uma pontuação de resultado de teste, o usuário poderá recalcular a pontuação de risco dos resultados de teste clicando no botão **Reaplicar Calculadora**.

Em um resultado de teste existente, se você clicar no link relacionado Calcular pontuação de risco e uma das calculadoras estiver habilitada, o campo Pontuação de risco no resultado do teste será atualizado.

Nota:
O link relacionado **Calcular pontuação de risco** só fica visível quando pelo menos uma calculadora de conformidade de configuração está habilitada.

Configuration Compliance regras da calculadora

Por padrão, uma **calculadora de risco padrão** do sistema básico é fornecida. Se você quiser criar uma regra de risco para esta calculadora, defina o campo de destino da **Calculadora de risco padrão** como **Pontuação**de risco. Clique no botão **Nova regra de risco** para criar uma nova regra de risco . Isso cria uma regra de calculadora de resultado de teste especializada chamada **Regra de Risco** que, por sua vez, calcula a **Pontuação de Risco** com base em vários valores. Por padrão, os seguintes valores para calcular a pontuação de risco são considerados:

- Criticidade dos negócios
- Criticidade

Você pode ajustar os valores a serem usados na **Regra de risco padrão** e quanto peso atribuir a cada um desses valores. Os pesos são usados para ajustar o quanto cada elemento conta ao definir a **Pontuação de risco**base.

A partir da Configuration Compliance versão 13.0, você pode personalizar os critérios para a regra de risco padrão. Para obter mais informações, consulte Definir campos e pesos para a regra de risco .

Atribuição de uma porcentagem de ponderação

Você também pode atribuir porcentagem de ponderação (0-100) no nível de valor do campo. Por exemplo, você pode atribuir uma porcentagem de ponderação a cada nível de Severidade (de Nenhum a Crítico). Se a ponderação de criticalidade for 50 para a regra de risco, os seguintes valores de ponderação forem atribuídos para o nível de criticalidade:

Atribuir percentual de ponderação

Criticidade	Pontuação de risco
Crítico	100
Alto(a)	50
Média	20
Nenhum(a)	0

Se a criticidade for crítica, a ponderação correspondente será 50. Se a criticidade for alta, o peso será 25 e, se o valor for médio, o peso será 10. Se a criticidade for nenhuma, o peso correspondente será 0. Para obter mais informações, consulte Exemplo de cálculo de pontuação de risco para Configuration Compliance.

Cada regra tem uma configuração de **Ordem**. No entanto, a primeira a corresponder às condições atualiza o campo **Pontuação de risco** no resultado do teste. Regras de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

calculadora sem script normalmente criam menos impacto no desempenho do que regras de calculadora com script.

A calculadora do sistema de base Configuration Compliance contém regras de calculadora que atribuem a cada nível de criticidade (de Nenhum a Crítico) um valor (0-100) para a **Pontuação de Risco** com base na severidade. A severidade desconhecida é atribuída automaticamente a uma pontuação de risco de 100. Esses valores podem ser ajustados, como Calculadora de risco padrão, novas regras de calculadora ou novas regras de risco podem ser criadas.

Ponderações de Pontuação de Risco de Vulnerabilidade

Todas as vulnerabilidades são atribuídas a uma pontuação de risco e classificação com base em fatores como severidade, criticidade, informações de exploração e assim por diante. A regra de negócios `Update Risk Rating from Risk Score` na tabela de item vulnerável é responsável pelo cálculo da classificação de risco. Sempre que a pontuação de risco muda, a classificação de risco é calculada e preenchida nos itens vulneráveis. Antes da versão 17.1 da aplicação Vulnerability Response (VR), as classificações de risco a seguir eram fornecidas como parte da inclusão de script VulnerabilityUtils, que eram codificadas.

Valor (classificação de risco)	Peso (pontuação de risco)
1	90–100
2	70–89
3	40–69
4	1 a 39
5	0

Começando com a versão 18.0 de Vulnerability Response,

- Os tipos de classificação de risco são enviados na tabela base como cc_risk_rating. Esses tipos são passados como parte da regra de negócios em cada tabela em que a classificação de risco é calculada.
- O script foi modificado para que você possa consultar as entradas nos valores da tabela Ponderações de pontuação de risco para o cálculo da classificação de risco.
- Adicione entradas adicionais para um tipo existente ou crie um novo tipo. Ao criar um novo tipo, certifique-se de adicionar os rótulos para a nova classificação de risco e também de modificar os scripts e as regras de negócios relacionados. Você também deve adicionar um novo estilo para a nova pontuação de risco.
- Modifique o script para consultar os registros na tabela base.

Você pode acessar a tabela Ponderações de pontuação de risco inserindo sn_sec_cmn_risk_score_weight no navegador de filtros.

Além disso, a pontuação de risco é recalculada automaticamente nos seguintes cenários:

- Quando um item de configuração (IC) muda de não voltado para a internet para voltado para a internet.
- Quando as Vulnerabilidades e exposições comuns (CVEs) associadas ou as entradas de terceiros (TPEs) nos itens de vulnerabilidade (IVs) estão vinculadas a uma Vulnerabilidade de exploração conhecida (KEV) de CVE.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir campos e pesos para a regra de risco

Personalize os parâmetros e pesos da regra de risco para que você possa gerar pontuações de risco que usam os dados de teste e ativo exclusivos da sua organização. Ao selecionar os campos incluídos na regra de risco, você pode definir uma estrutura de pontuação de risco eficaz.

Antes de Iniciar

Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Calculadoras de Risco**.
2. Clique **em Calculadora de risco padrão**.
3. Selecione o campo de destino como **Pontuação de risco**.
   O botão **Nova regra de risco é** exibido na tabela Regra da calculadora.
4. Clique no botão **Nova regra de risco** para navegar até o formulário **Regra de risco do Configuration Compliance**.
5. Na seção Critérios da calculadora de risco, defina o peso de cada critério de acordo com sua importância no cálculo de pontuação de risco geral.
6. Desmarque a caixa de seleção **Ativa** para desativar a regra.
7. Clique em **Adicionar critérios** para adicionar campos de regra de risco aos Critérios da calculadora de risco.
8. No formulário, preencha os campos.

Formulário de campo de regra de risco

Campo	Descrição
Escolher tabela de referência	A tabela que você usa para definir a ponderação da pontuação de risco. Selecione uma das seguintes opções: ○ Resultado do teste: adicione campos para os quais você pode fazer referência com pontos diretamente do resultado do teste (TR). ○ Resultado de testes - Item de configuração: adicione campos de referência com pontos que fazem parte das extensões da tabela base, como a tabela Hardware. Esses campos não fazem parte da tabela cmdb_ci base. ○ Resultado de testes - Teste: adicione campos de referência com pontos que fazem parte das tabelas que estendem a tabela base, por exemplo, Entrada de terceiros. Esses campos não fazem parte da tabela base de teste de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Tabela de referência do resultado de testes: adicione campos que fazem parte das tabelas relacionadas (m2m) ou tabelas que têm uma referência ao resultado do teste. Esses campos não podem ser usados como referência com pontos diretamente do Resultado do teste. ○ Tabela de referência do item de configuração: adicione campos que fazem parte das tabelas relacionadas (m2m) de cmdb_ci ou tabelas que têm uma referência a cmdb_ci. Esses campos não podem ser usados como referência com pontos diretamente do TR. ○ Tabela de referência de teste: adicione campos que fazem parte das tabelas relacionadas (m2m) de sn_vulc_test ou tabelas que têm uma referência a sn_vulc_test. Esses campos não podem ser usados como referência com pontos diretamente do TR. ○ Condições personalizadas: use esta opção para atribuir pesos à regra avaliando a condição. Por exemplo, o filtro voltado para a Internet determina se um item de configuração (IC) é externo ou interno.
Campo	O campo usado para cálculo de pontuação de risco para esta regra.
Ponderação	Ponderação deste campo na regra de risco. O valor deve ser um número inteiro de 0 a 100.
Tabela	○ Resultado de testes > Item de configuração ○ Resultado de testes > Teste ○ Tabela de referência do resultado de testes ○ Tabela de referência do item de configuração ○ Tabela de referência do teste Este campo é exibido somente quando qualquer uma das opções listadas é selecionada no campo Escolher tabela de referência.
Agregação	Selecione o valor mínimo ou máximo a ser considerado para cálculos quando o campo for selecionado nas Tabelas relacionadas (m2m).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Este campo é exibido somente quando uma tabela de referência é selecionada no campo Escolher tabela de referência.
Definir ponderação do valor	Componente para atribuir pesos a cada valor de campo. Para campos numéricos, defina os valores de campo como um intervalo (por exemplo, 1 a 5). O valor deve ser um número inteiro entre 0 e 100. Este campo não será exibido se a opção Condições personalizadas for selecionada no campo Escolher tabela de referência.
Tabela de condição	Selecione uma condição na lista. Este campo é exibido somente quando a opção Condições personalizadas é selecionada no campo Escolher tabela de referência.
Nome do campo	Insira um nome para os critérios de risco. Este campo é exibido somente quando Condições personalizadas são selecionadas no campo Escolher tabela de referência.
Condição	Visualize os itens nesta tabela que correspondem às condições definidas. Este campo é exibido somente quando Condições personalizadas são selecionadas no campo Escolher tabela de referência.

9. Clique em **Enviar**.

O que Fazer Depois

Na página Regra, ative e reaplique a regra para reavaliar a pontuação de risco no resultado do teste ativo.

Criar ou editar calculadoras de acúmulo de risco para Configuration Compliance

Crie uma nova calculadora de risco ou edite uma existente.

Antes de Iniciar

Função necessária: Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** e selecione **Calculadoras de acúmulo de pontuação de risco**.
2. Com a lista de Calculadoras de acúmulo de pontuação de risco exibida, clique em uma calculadora para abrir o registro e editar o formulário.
3. Como alternativa, para criar uma nova calculadora, clique em **Nova** e preencha o formulário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	O nome da calculadora de rollup do Teste de Configuração ou do Grupo de Resultados de Testes.
Descrição	Uma descrição da calculadora de acúmulo de risco.
Valores de Script	Edite os valores no script conforme necessário. **Nota:** A edição de script requer conhecimento avançado da aplicação Now Platform e Configuration Compliance.

4. Clique em **Atualizar** para salvar suas edições.

Calculadoras de acúmulo são trabalhos programados que são executados por hora para selecionar mudanças. Esses trabalhos programados também têm pontuações de risco gerais para testes de configuração e tarefa de correção. Os valores acumulados são exibidos nos campos de Pontuação de risco.

Para obter um exemplo de como uma calculadora de acúmulo de risco determina as pontuações, consulte Exemplo de cálculo de acúmulo de risco para Configuration Compliance.

Criar, editar e reaplicar calculadoras de risco para Configuration Compliance

As regras da calculadora podem ser aplicadas a todos os resultados de testes afetados e coleções sob demanda. Os gerentes de vulnerabilidade podem usar este recurso para ajustar a configuração da calculadora de risco e aplicar mudanças sob demanda para importar descobertas.

Antes de Iniciar

Função necessária: sn_vulc.admin

Procedimento

1. Para criar uma nova calculadora de risco, siga estas etapas.

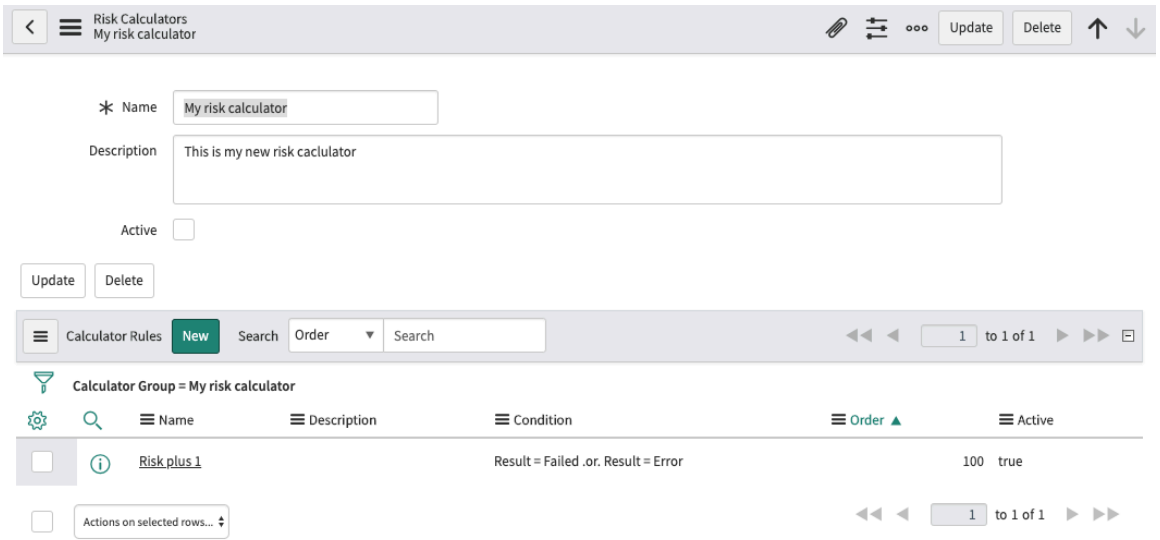
   a. Navegar até **Todos** > **Configuration Compliance** > **Administração** e selecione **Calculadoras de risco**.

   b. Na lista Calculadora de risco, clique em **Novo**.

   c. Insira um nome e uma descrição para sua nova calculadora e clique em **Enviar**.
   A nova calculadora é exibida na lista Calculadora de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



d. Na lista, clique na nova calculadora para criar as condições sob as quais a calculadora é executada e especifique os campos e valores que você deseja exibir nos registros de resultado de testes e nas tarefas de correção.

e. No registro exibido, clique em **Novo**.

f. Preencha os campos nas guias conforme apropriado.

Guia	Descrição
Quando esta condição for atendida	Use o construtor de condições para criar as condições sob as quais a calculadora é executada. Um exemplo é: O resultado é falha ou o resultado é erro.
Definir estes valores	Use o modelo para selecionar os campos e valores que você deseja exibir.

g. Clique em **Enviar**.
O registro é exibido com as novas regras da calculadora e o grupo ao qual ele pertence.

2. Para reaplicar uma calculadora existente para testar resultados ou editar as regras e os valores exibidos para uma calculadora de risco existente, siga estas etapas.

a. Nas listas Calculadoras de risco ou Calculadora de acúmulo de risco, selecione a calculadora que você deseja editar.

b. Para reaplicar uma calculadora de risco aos dados de resultado de testes existentes do registro, clique em **Reaplicar calculadora**.
Todos os resultados de testes que atendem às condições da calculadora são atualizados.

Nota:
Dependendo do número de resultados de testes, esta atualização pode levar algum tempo.

c. Para editar as condições e os valores, no canto inferior esquerdo da coluna Nome, clique no nome da calculadora.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para calculadoras de risco, as guias de registro e **Quando esta condição for atendida** e **Definir esses valores** são exibidas.

d. Preencha o formulário conforme apropriado.

Guia	Descrição do campo
Quando esta condição for atendida	Use o construtor de condições de filtro para criar as condições sob as quais você deseja que a calculadora seja executada.
Definir estes valores	Escolha um para continuar. ▪ Tipo de valor: modelo. Escolha os campos na lista e os valores correspondentes. ▪ Script - Insira suas mudanças usando o editor. **Nota:** A edição de script requer conhecimento avançado da aplicação Now Platform e Configuration Compliance.

3. Opcional: Para aplicar as novas regras sob demanda aos dados de resultado de testes existentes, siga estas etapas.

a. Com a lista Calculadoras de risco exibida, clique em uma calculadora que você deseja aplicar. O registro é exibido.

b. Clique em **Reaplicar calculadora** para testar e aplicar suas mudanças sob demanda às descobertas de importação.

4. Exiba suas mudanças nos resultados de testes e continue editando suas calculadoras conforme necessário.

Exemplos de cálculo de pontuação de risco Configuration Compliance

A partir da v13.0 de Configuration Compliance, você pode personalizar os critérios para a regra de risco padrão. Use pontuações de risco fornecidas por fornecedores terceirizados, como Qualys e Tenable, para cálculos de pontuação de risco.

Fornecedores de terceiros, como Qualys e Tenable, fornecem suas próprias pontuações. Essas pontuações são preenchidas no campo Criticalidade na tabela sn_vulc_test. Use este campo para cálculos de pontuação de risco. Para usar essa pontuação para calcular a pontuação de risco, siga o procedimento:

Adicionar criticalidade de origem como critério para uma regra de risco

Use pontuações com base na criticidade fornecida por fornecedores terceirizados para calcular pontuações de risco.

Antes de Iniciar
Função necessária: sn_vulc.admin

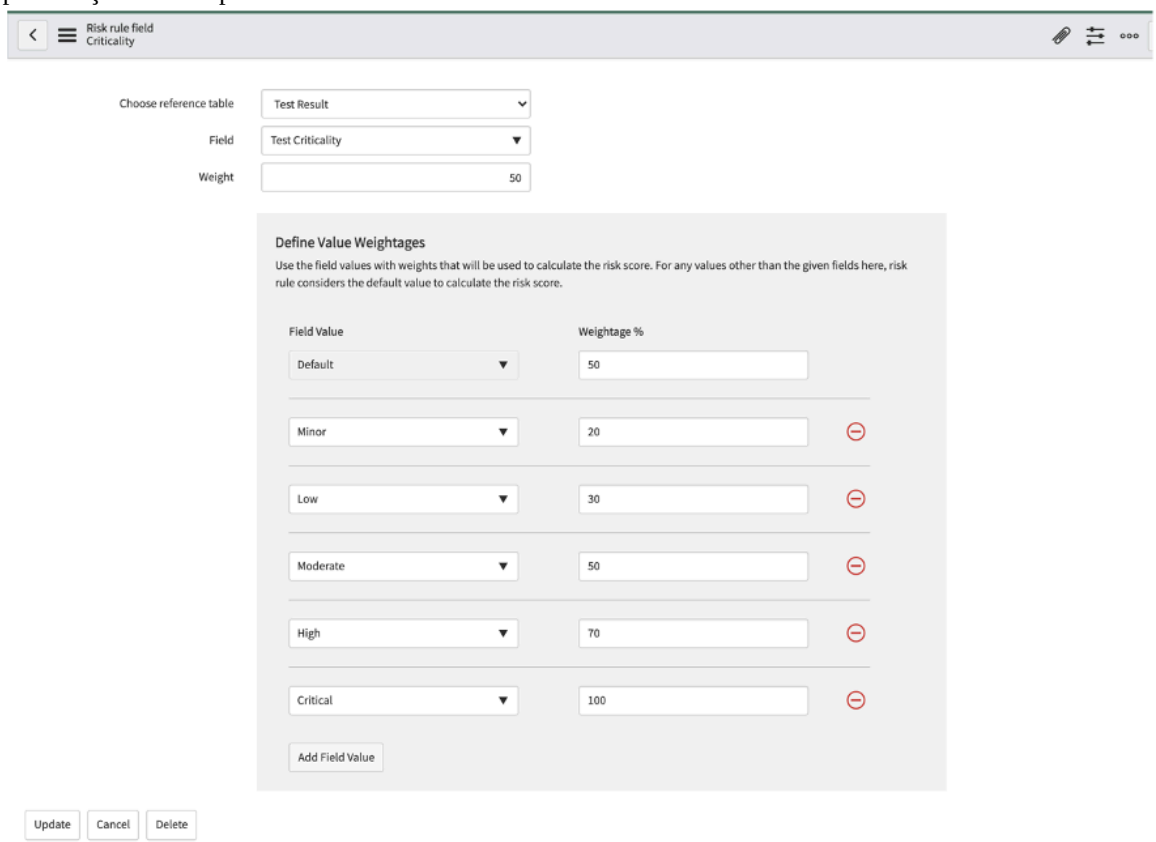
Por Que e Quando Desempenhar Esta Tarefa
Fornecedores terceirizados, como Qualys e Tenable, fornecem suas próprias pontuações de risco. Essas pontuações são preenchidas no campo Criticalidade na tabela sn_vulc_test. Use este campo para cálculos de pontuação de risco e cálculo da pontuação de risco.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Calculadoras de Risco**.
2. Navegue até o formulário Regra de risco.
3. Desmarque a caixa de seleção **Ativa** para desativar a regra.
4. Clique **em Adicionar critérios**.
5. Na lista **Escolher tabela de referência**, selecione **Resultado do teste**.
6. Na lista **Campo**, selecione **Test.Criticality**.
7. No campo **Peso**, especifique a importância relativa deste campo.
   O valor deve ser um número inteiro de 0 a 100.
8. Na seção **Definir Ponderações de Valor**, adicione valores de campo e atribua uma porcentagem de ponderação aos campos.



9. Clique em **Enviar**.

Adicionar criticalidade dos negócios como critério para uma regra de risco

Especifique um valor de criticalidade para serviços de negócios e use a criticalidade de negócios para calcular as pontuações de risco.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Supondo que sua organização tenha muitos serviços de negócios e um item de configuração (IC) esteja sendo usado pelos seguintes serviços:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criticidade dos serviços de negócios

Serviço de negócio	Criticidade
Gestão de nuvem	1 - Mais crítico
Comércio eletrônico	2 - Um pouco crítico
Serviços ao cliente	3 - Menos crítico
Viagem e despesa	4 - Não crítico

O mapeamento entre o IC e os serviços é armazenado na tabela Serviços [cmdb_ci_services]. Quando um IC não passa em um teste de configuração, um resultado de teste (TR) é criado. Você pode usar o valor da criticidade dos serviços afetados para calcular a pontuação de risco para este TR. Siga o procedimento para usar o valor de criticalidade desses serviços para calcular a pontuação de risco.

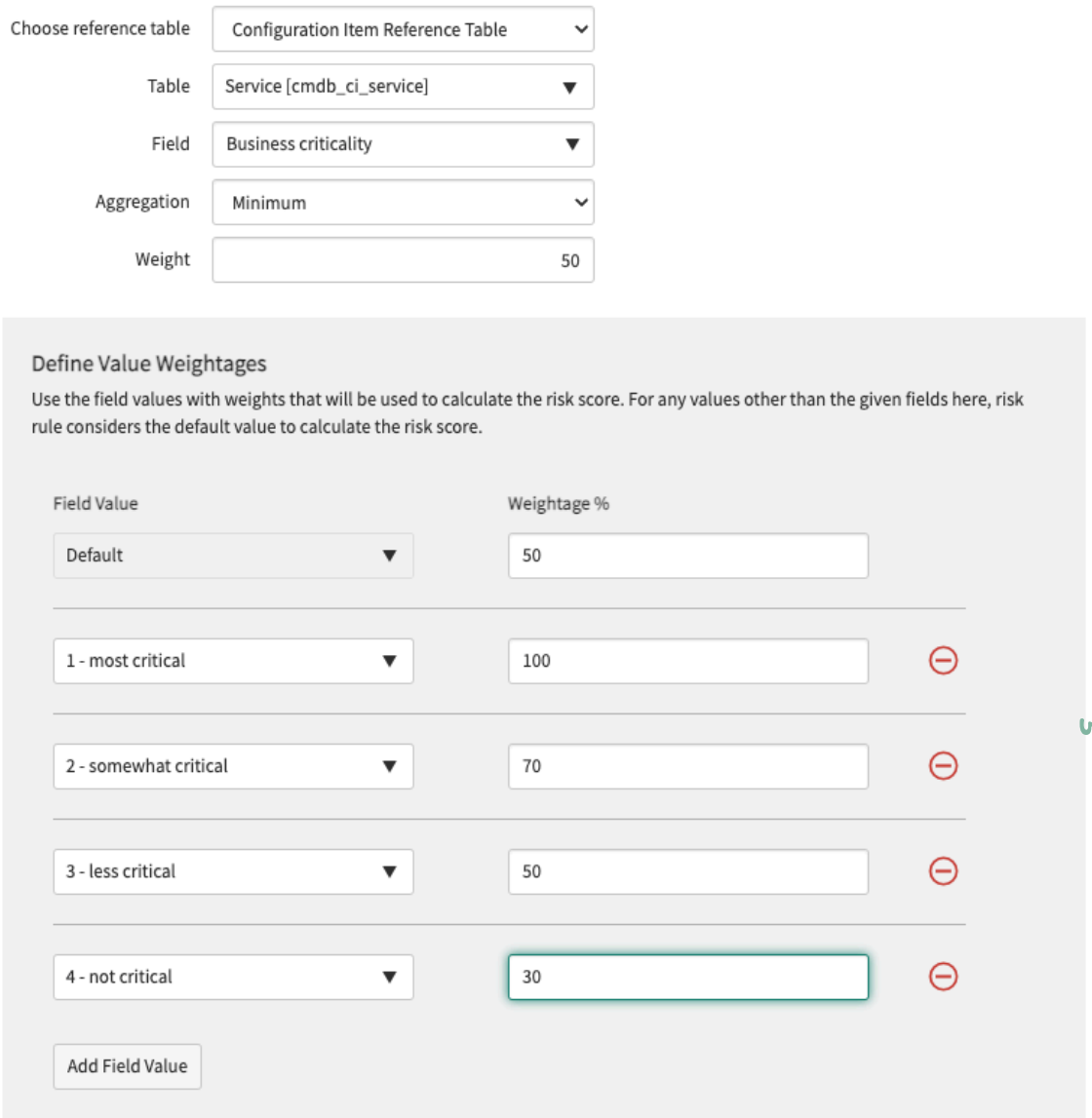
Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Calculadoras de Risco**.
2. Navegue até o formulário Regra de risco na seção **Regras da calculadora**.
3. Desmarque a caixa de seleção **Ativa** para desativar a regra.
4. Clique **em Adicionar critérios**.
5. Na lista **Escolher tabela de referência**, selecione **Tabela de referência do item de configuração**.
6. Na lista **Tabela**, selecione **Serviço [cmdb_ci_service]**.
7. Na lista **Campo**, selecione **Criticalidade dos negócios**.
8. No campo **Agregação**, selecione **Mínimo** para recuperar o serviço mais crítico para este caso de uso (1- Valor mais crítico) ou **Máximo** para recuperar o serviço menos crítico para este caso de uso (4 – Valor não crítico).
9. No campo **Peso**, especifique a importância relativa deste campo.
   O valor deve ser um número inteiro de 0 a 100.
10. Na seção **Definir ponderações de valor**, adicione valores de campo e atribua ponderações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ponderação da regra de risco de criticalidade dos negócios personalizada



Tradução automática

11. Clique em **Enviar**.

Adicionar critério condicional à calculadora de risco

Use condições personalizadas para a regra de risco para o cálculo da pontuação de risco.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
Supondo que sua organização tenha vários itens de configuração (ICs), dos quais apenas alguns podem ser acessados por um usuário externo. Os usuários podem adicionar ponderações de pontuação de risco para esses ICs externos.

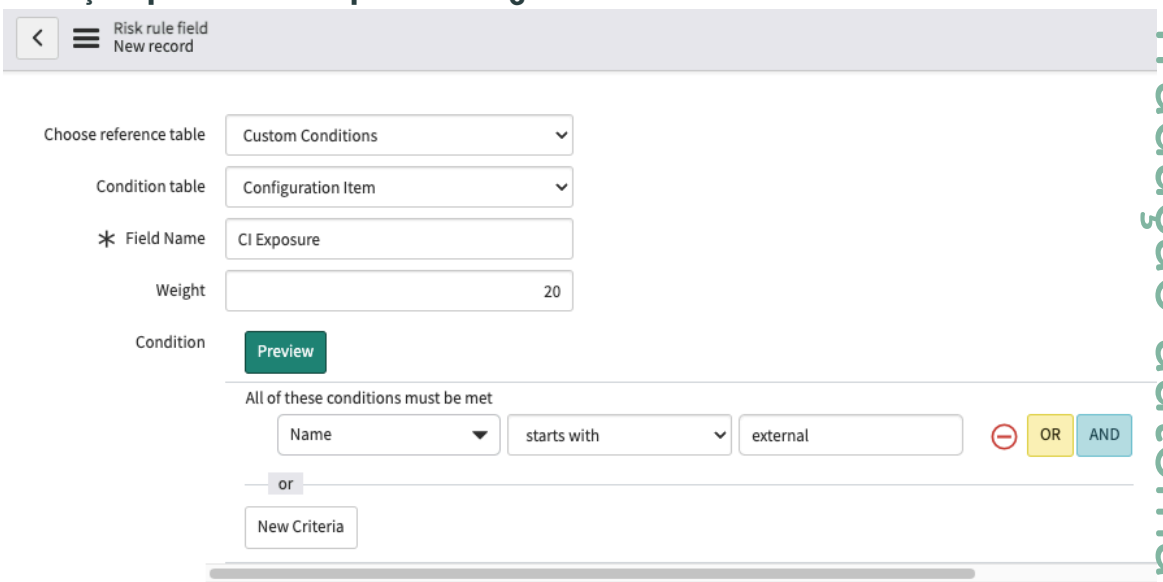
Nota:
Você pode identificar esses ICs pelo nome. Os nomes começam com "externo".

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Calculadoras de Risco**.
2. Navegue até o formulário Regra de risco.
3. Desmarque a caixa de seleção **Ativa** para desativar a regra.
4. Clique **em Adicionar critérios**.
5. Na lista **Escolher tabela de referência**, selecione **Condições personalizadas**.
6. Na lista **Tabela de condições**, selecione **Item de configuração**.
7. No **campo Nome do** campo, insira `Exposição de IC`.
8. No campo **Peso**, especifique a importância relativa deste campo.
   O valor deve ser um número inteiro de 0 a 100.
9. No campo **Condição**, selecione **Nome > começa com**e especifique o valor como `externo`.

Condições personalizadas para nova regra de risco



10. Clique em **Enviar**.

Tópicos relacionados

Grupos de calculadoras do Configuration Compliance

Exemplo de cálculo de pontuação de risco para Configuration Compliance

Determine as calculadoras de pontuação de risco para gerar pontuações de risco que usam os dados de teste e ativo específicos da sua organização.

Exemplo de determinação de pontuações de calculadoras de regra de risco

O exemplo a seguir demonstra como as pontuações das calculadoras de regra de risco são determinadas. Suponha que uma calculadora de regra de risco esteja configurada com os campos nesta tabela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Determinar pontuações da calculadora de regra de risco

Campo	Ponderação	Detalhamento de peso
Criticalidade.Controle	50	Padrão: 0 Secundário: 20 Baixo: 30 Moderado: 50 Alto: 70 Crítico: 100
Criticidade_do_Negócios	50	Padrão: 0 Secundário: 20 Baixo: 30 Moderado: 50 Altura: 70 Crítico: 100

Suponha que os resultados de testes mostrados nesta tabela estejam presentes no sistema.

Mapeamento de resultados de testes

ID	Criticidade dos negócios	Criticalidade do controle
CTR0000001	1 - Mais crítico	Secundário(a)
CTR0000002	1 - Mais crítico	Baixa
CTR0000003	2 - Um pouco crítico	Secundário(a)
CTR0000004	2 - Um pouco crítico	Moderado(a)
CTR0000005	3 - Menos crítico	Baixa

O cálculo da pontuação de risco para o resultado do teste é calculado com base na fórmula:

Pontuação de risco = (W(control.criticality) * FV (control.criticality). + W(business_criticality) * FV(business_criticality)) / 100, em que W é o peso e FV é a porcentagem de peso do valor do campo.

A pontuação de risco resultante para esses resultados de testes é conforme descrita nesta tabela:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pontuação de risco com base nos resultados de testes

ID	Criticalidade dos negócios (50%)	Criticidade do controle (50%)	Pontuação de risco resultante
CTR0000001	1 - Mais crítico (50% x100)	Secundário (50% x 20)	60
CTR0000002	1 - Mais crítico (50% x100)	Baixo (50% x 30)	65
CTR0000003	2 - Um pouco crítico (50% x 70)	Secundário (50% x 30)	45
CTR0000004	2 - Um pouco crítico (50% x 70)	Moderado (50% x 50)	60
CTR0000005	3 - Menos crítico (50% x 50)	Baixo (50% x 30)	40

Se a porcentagem de ponderação for alterada para um dos valores de campo, consulte esta tabela para obter os resultados:

Resultados para porcentagem de ponderação alterada

Campo	Ponderação	Detalhamento de peso
Criticalidade.Controle	50	Padrão: 0 Secundário: 20 Baixo: 30 Moderado: 60 Altura: 70 Crítico: 100
Criticidade_do_Negócios	50	Padrão: 50 1 - Mais crítico: 100 2 - Um pouco crítico: 70 3 - Menos crítico: 20 4 - Não crítico: 30

A pontuação de risco dos resultados do teste após a reaplicação da calculadora é mostrada nesta tabela:

Pontuação de risco para TR ao reaplicar a calculadora

ID	Criticalidade dos negócios (50%)	Criticidade do controle (50%)	Pontuação de risco resultante
CTR0000001	1 - Mais crítico (50% x100)	Secundário (50% x 20)	60
CTR0000002	1 - Mais crítico (50% x100)	Baixo (50% x 30)	65

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pontuação de risco para TR ao reaplicar a calculadora

ID	Criticalidade dos negócios (50%)	Criticidade do controle (50%)	Pontuação de risco resultante
CTR0000003	2 - Um pouco crítico (50% x 70)	Secundário (50% x 30)	45
CTR0000004	2 - Um pouco crítico (50% x 70)	Moderado (50% x 60) *Valor revisado	65 *Valor revisado
CTR0000005	3 - Menos crítico (50% x 20) *Valor revisado	Baixo (50% x 30)	25 *Valor revisado

Exemplo de cálculo de acúmulo de risco para Configuration Compliance

O exemplo a seguir demonstra como as pontuações das calculadoras de acúmulo de risco são determinadas.

Para a seguinte calculadora de acúmulo de grupo de resultados de testes, a fórmula para calcular a Pontuação de risco do grupo do resultado do teste é:

(Pontuação de risco máximo/100) * 85 + (fator * 15).

O fator na equação anterior é determinado pelo número de resultados de testes, conforme mostrado na tabela a seguir.

Contagem de Resultado de testes	Fator
< 10	0,2
1 a 99	0,4
100–1000	0,6
1001-9999	0,8
> 1000	1

Para a Tarefa de correção a seguir, TRG0003066, com três pontuações de risco de resultados de testes, a pontuação máxima é 90.

Número	Pontuação de risco	Grupo	Resultado	Status
CTR000123	90	TRG0003066	Reprovado	Em aberto
CTR000124	70	TRG0003066	Reprovado	Em aberto
CTR000125	40	TRG0003066	Reprovado	Em aberto

Para a tarefa de correção, TRG0003066, a pontuação de risco é 79, (90/100) * 85 + 0,2 * 15 = Math.year (76,5 +3) = 79.

A pontuação de risco histórico é nula porque o grupo ainda está "Aberto".

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Após a ingestão de dados, os resultados do teste são "Aprovados" e o grupo muda para "Encerrado", conforme mostrado na tabela a seguir.

Número	Pontuação de risco	Grupo	Resultado	Status
CTR000123	0	TRG0003066	Aprovado	Encerrado
CTR000124	0	TRG0003066	Aprovado	Encerrado
CTR000125	0	TRG0003066	Aprovado	Encerrado

Resultados de testes O histórico é exibido na tabela a seguir.

Número	Pontuação de risco	Último resultado	Resultado
CTRH000111	90	CTR000123	Reprovado
CTRH000112	70	CTR000124	Reprovado
CTRH000113	40	CTR000125	Reprovado

A pontuação de risco é zero, porque não há resultados de testes abertos no grupo.

A pontuação de risco máximo dos resultados aprovados + a pontuação de risco máximo do histórico - 90.

Para o grupo de resultados de testes TRG0003066, a Pontuação de Risco Histórico é 79.

(90/100) * 85 + 0,2 * 15 = Piso superior (76,5 + 3) = 79.

Criar ou editar Configuration Compliance regras de grupo de resultados de testes

Você pode criar regras para agrupar automaticamente os resultados de testes com base nas condições do filtro. Essas regras agrupam automaticamente os resultados de testes conforme eles são importados. Use o filtro para limitar os resultados de testes agrupados por esta regra, como a seleção de todos os resultados de testes com explorações.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

O sistema de base é fornecido com uma regra de grupo de resultados de teste, **Grupo de atribuição, Teste**, que agrupa os resultados de teste por grupo de atribuição (preenchido previamente em **Regras de atribuição**) e o campo **Teste** de resultado de teste. Esta regra pode ser modificada usando condições de filtro e chaves de grupo. As chaves de grupo são colunas na tabela de resultados de testes. Selecione até seis chaves para indicar quais valores devem ser usados para agrupar os resultados de testes.

A partir da versão 14.7 do Configuration Compliance, a regra Grupo **de atribuição e Grupo de teste** foi desativada para novas implementações.

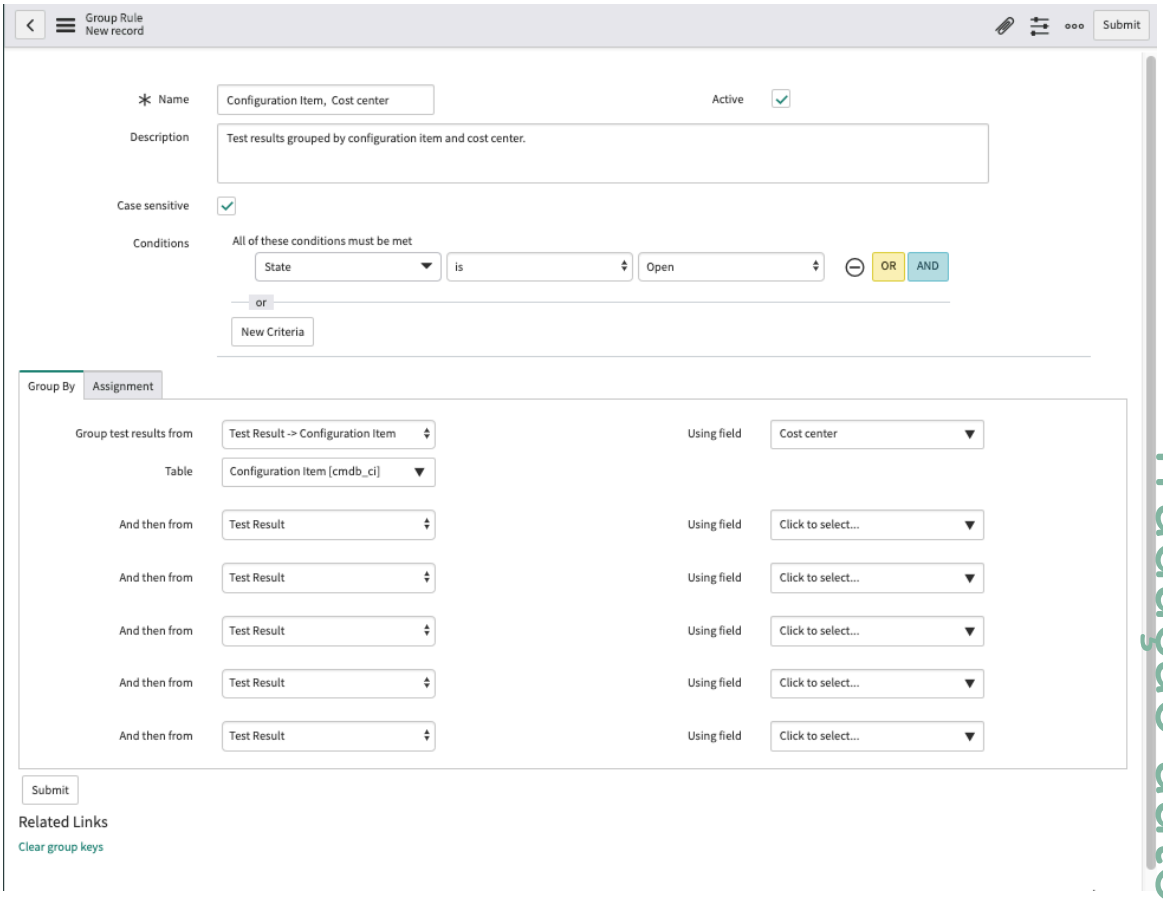
Nota:
Regras novas ou atualizadas são avaliadas automaticamente na próxima importação ou manualmente usando o botão **Reaplicar** no formulário Regra de grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Regras de Grupo**.
2. Abra o **Grupo de atribuição, Regra de teste** ou clique em **Novo**.



3. Se **Novo**, preencha os campos no formulário, conforme apropriado.

Configuration Compliance Regra de Grupo de Resultado de testes

Campo	Descrição
Nome	Nome da regra de grupo.
Ativo	Indica se o grupo está ativo.
Descrição	Descrição de texto desta regra de grupo de resultados de testes.
Diferenciação entre maiúsculas e minúsculas	Determina se a correspondência de regra faz distinção entre maiúsculas e minúsculas ou não. **Nota:** O valor padrão não faz distinção entre maiúsculas e minúsculas.
Condições	Condições que devem ser atendidas. Por padrão, (caixa de seleção**Diferenciar maiúsculas de minúsculas** desabilitada), o texto de pesquisa inserido no construtor de condição em registros e formulários de regras de grupo não faz distinção entre

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	maiúsculas e minúsculas. Você tem a opção de habilitar pesquisas que diferenciam maiúsculas de minúsculas em registros e formulários de grupo.
Agrupar por	
Agrupar resultados de testes de	Automatize a criação de grupos com base nesta regra. Escolha uma das opções disponíveis. ○ Resultado de testes | Usando o campo ○ Resultado do teste->Item de configuração | Tabela | Usando o campo Se um campo **Tabela** estendida for selecionado, os resultados de testes que não usam a tabela estendida correspondente serão agrupados em uma tarefa de correção separada.
Atribuição	
Atribuir grupos de resultados de testes por	Automatize a atribuição de grupos criados com base nesta regra. Escolha uma das opções disponíveis. ○ Chave do grupo Quando selecionado, um campo de valor de chave é exibido, os campos disponíveis são listados em um menu suspenso. ○ Grupo de usuários Quando selecionado, um campo de pesquisa de grupo de usuários é exibido.

4. Clique em **Enviar**.

Nota:
O link relacionado Limpar grupo por chaves remove as chaves de grupo da guia Agrupar por no formulário.

Especificar a duração de uma exceção solicitada para uma tarefa de correção

Use as propriedades do sistema para limitar a duração da solicitação de uma exceção para uma tarefa de correção. A correção da tarefa de correção é adiada pelo período especificado.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
A propriedade `sn_vulc.exception_max_request_days` é usada para especificar o número máximo de dias para os quais uma exceção para uma tarefa de correção pode ser solicitada. O valor padrão é 365 dias.

Nota:
Você pode usar a propriedade `sn_vulc.exception_approval_required` para desabilitar o fluxo de trabalho de aprovação de exceção para a tarefa de correção se ele não for necessário. Por padrão, esta propriedade está habilitada e seu valor é `verdadeiro`.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Propriedades do sistema** > **Todas as Propriedades**.
2. Na página Propriedades do sistema, pesquise por sn_vulc.exception_max_request_days.
3. Clique no nome da propriedade para abrir o registro de propriedade do sistema.
4. Para poder editar este registro, certifique-se de que Configuration Compliance esteja selecionado como a aplicação atual.
5. Insira um **valor** positivo e clique em **Atualizar**.
   O registro é atualizado e salvo.

Configurar Gestão de exceções para Configuration Compliance

Limite a duração de uma exceção solicitada e adicione um questionário à exceção usando o módulo Configuration Compliance. Por padrão, uma exceção é solicitada usando o módulo ServiceNow® Vulnerability Response. Você também pode solicitar uma exceção usando a integração GRC: Policy and Compliance Management.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Se Vulnerability Response estiver habilitado, você poderá limitar a duração pela qual uma exceção pode ser solicitada. Da mesma forma, se o módulo GRC: Policy and Compliance Management estiver instalado, você poderá selecionar GRC: Policy and Compliance Management na tela de configuração. Habilitar esta opção permite solicitar uma exceção que especifica a política e o objetivo de controle de GRC.

Se você adicionar um questionário, ele será enviado para a pessoa que gerou a exceção ou a solicitação de falso-positivo. Você pode usar o questionário padrão ou criar um com base em seus requisitos.

É útil que o aprovador de exceção entenda o motivo da solicitação da exceção.

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Gestão de exceção**.
2. No formulário Configuração de gestão de exceções, selecione como você deseja gerenciar uma exceção selecionando uma opção na lista Gerenciar exceções usando.

   Nota:
   A partir da Vulnerability Response versão 17.1, você pode selecionar Vulnerability Response ou GRC: Policy and Compliance Management. Você deve ativar o plug-in GRC para usar GRC: Policy and Compliance Management para solicitar uma exceção. Alterar a configuração não afeta os dados existentes.

3. Preencha os campos no formulário com base na opção selecionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se você selecionou a opção Vulnerability Response, preencha os campos no formulário.

Configurações do formulário de gestão de exceções de VR

Campo	Descrição
Duração	Período para o qual uma exceção pode ser solicitada.
Unidade	Unidade de tempo para o período especificado.
Habilitar questionário para solicitar exceção	Opção para adicionar um questionário à solicitação de exceção que está sendo gerada.
Questionário para solicitar exceção	Opção para exibir o questionário selecionado por você para solicitar uma exceção. O Questionário de exceção é exibido por padrão.

- Se você selecionou a opção GRC: Policy and Compliance Management, preencha os campos no formulário.

Configurações do formulário de gestão de exceções de VR

Campo	Descrição
Habilitar questionário para marcar como falso-positivo	Opção para adicionar um questionário à solicitação de falso-positivo que está sendo gerada.
Questionário para marcar como falso-positivo	Opção para exibir o questionário selecionado por você para marcar como falso positivo. O questionário para uma solicitação de falso-positivo é exibido por padrão.

4. Selecione **Salvar**.

Adicionar um aprovador de exceção para Configuration Compliance

Adicione usuários aos grupos de aprovadores para que você possa solicitar uma exceção para uma tarefa de correção em Configuration Compliance.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Uma solicitação de exceção para uma tarefa de correção é aprovada usando o fluxo de trabalho de aprovação de dois níveis padrão. Adicionar usuários ao grupo de primeiro nível é obrigatório. Se não houver usuários no segundo nível, a solicitação será aprovada automaticamente após a aprovação de primeiro nível.

Nota:
Se não houver nenhum aprovador de primeiro nível, uma exceção não poderá ser solicitada.

Nota:
Até Configuration Compliance v13.0, se não houver nenhum aprovador de primeiro nível, uma exceção não poderá ser solicitada. No entanto, a partir de Configuration Compliance v13.0, se você estiver implantando a aplicação CC pela primeira vez, o Flow Designer para gestão de exceções será habilitado por padrão. Se você já estiver usando o fluxo de trabalho, poderá atualizar para o Flow Designer. Em ambos os casos, você não pode alterá-lo de volta para o fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Segurança do sistema** > **Usuários e Grupos** > **Grupos**.
2. Na coluna Nome, pesquise por **Exceção**e clique em **Aprovador de exceção - Nível 1 CC**.

> **Nota:**
> A partir de Configuration Compliance v14.7.5, você pode usar as propriedades do sistema fornecidas no sistema de base para aprovações de exceção por meio do fluxo de trabalho na tabela Propriedades do sistema [sys_properties]. Portanto, quando uma solicitação de exceção é gerada por meio de fluxo de trabalho, ela é enviada para aprovação para os IDs de grupo definidos na propriedade do sistema. Navegar até **Todos** > **Propriedades do sistema** e selecione `sn_vulc.exception_approver_L1_CC` ou `sn_vulc.exception_approver_L2_CC` para mudar o valor da propriedade.

3. No formulário Aprovador de exceção do grupo - CC de nível 1, navegue até **Membros do Grupo** > **Novo** (ou **Editar**).
4. No formulário, preencha os campos.

Formulário do usuário

Campo	Descrição
ID do usuário	Identificador exclusivo do usuário.
Nome	Nome do usuário.
Sobrenome	Sobrenome do usuário.
Título	Cargo do usuário. Insira um título ou descrição do trabalho ou selecione um na lista.
Departamento	Departamento do usuário.
Senha	Senha atribuída ao usuário. Esta senha pode ser permanente ou temporária.
A senha precisa ser redefinida	Opção para permitir que o usuário redefina a senha para garantir a segurança.
Bloqueado	Opção para bloquear a saída do usuário da instância e encerrar todas as sessões ativas do usuário. O sistema evita que usuários com a função de administrador se bloqueiem.
Ativo	Opção para tornar este usuário ativo. Somente você pode ver um usuário inativo nestas áreas: ○ Listas de usuários ○ Lista de seleção nos campos de referência (ícone de lupa) ○ Lista de preenchimento automático que aparece quando você digita em um campo de referência
Acesso somente ao serviço Web	Opção para designar este usuário como um usuário não interativo.
Usuário de integração interna	Opção para designar este usuário como um usuário de integração interna.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
E-mail	Endereço de e-mail do usuário.
Idioma	Idioma preferencial do usuário.
Integração de calendário	Calendário usado para gerenciar a programação de trabalho. Por exemplo, Outlook.
Fuso horário	Fuso horário para a localização deste usuário.
Formato de data	Formato preferencial do usuário para datas.
Telefone comercial	Telefone comercial do usuário.
Telefone celular	Telefone celular do usuário.
Foto	Foto que você pode carregar clicando em **Clique para adicionar...**.

5. Clique em **Enviar**.
6. **Opcional:** Repita as etapas 1 a 5 para criar um Aprovador de exceção - Nível 2 CC.

Nota:
Ao criar um aprovador de segundo nível, selecione **Aprovador de exceção - CC de nível 2**

7. **Opcional:** Se você selecionar **Editar**, mova os usuários da **Coleção** para o painel **Membros do grupo** e clique em **Salvar**.
O aprovador deve navegar até **Todos** > **Configuration Compliance** > **Minhas aprovações** e aprova solicitações.

Criar um mapa de criticalidade Configuration Compliance

O mapeamento de criticalidadeConfiguration Compliance fornece um mapa de transformação para campos de criticalidade de origem de terceiros em campos reconhecíveis na severidade Configuration Compliance.

Antes de Iniciar
Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Mapeamento de Criticalidade**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Mapeamento de campo

Campo	Descrição
Fonte	O nome da origem do mapeamento de criticalidade.
Valor de origem	O valor de criticalidade de origem.
Valor de meta	O valor de meta. As opções são: **Crítico**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	O problema de configuração associado ao controle está causando uma interrupção em um ou mais ICs críticos para os negócios. **Alto(a)** O problema de configuração associado ao controle é uma ameaça, mas não está causando o desligamento de recursos críticos de rede. **Moderado(a)** O problema de configuração associado ao controle é um risco, mas não é uma ameaça imediata. **Baixa** O problema de configuração associado ao controle é uma ameaça de baixo nível e pode ser ignorado em favor de ICs que correm maior risco. **Secundário(a)** O problema de configuração associado ao controle é um risco menor e pode ser ignorado, se necessário.

4. Clique em **Enviar**.

Criar notificações por e-mail

Os administradores de vulnerabilidade podem editar a notificação ou adicionar novas, especificando quando enviar a notificação, quem recebe a notificação e qual conteúdo está na notificação.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode criar modelos de e-mail para diferentes tipos de notificações por e-mail. Para obter mais informações sobre como criar modelos de e-mail, consulte Definir modelos de e-mail do Vulnerability Response.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Notificações**.
2. Selecione o registro de notificação de destino de correção ou selecione **Novo**.
3. Preencha os campos no formulário, conforme apropriado.
   Para obter mais informações sobre os campos de formulário, consulte Create an email notification .
4. Selecione **Visualizar notificação** para exibir a mensagem.

Resultado

A partir da v14.11 de Configuration Compliance, quando um destinatário clica nos links em uma notificação por e-mail, os registros são abertos no Vulnerability Manager Workspace ou Espaço de correção de problemas de TI com base em sua função.

- Links abertos no Vulnerability Manager Workspace para os usuários com a função sn_vulc.admin.
- Links abertos no Espaço de correção de problemas de TI para os usuários com a função sn_vulc.remediation_owner.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se o destinatário não tiver nenhuma das funções anteriores, os links em uma notificação por e-mail serão abertos na IU clássica.

Configurar regras de aprovação para o Exception Management no Configuration Compliance

Começando com Configuration Compliance v13.0, use o Flow Designer para aprovar solicitações de exceção para gerenciamento de exceções e regras de exceção. Se você estiver implantando o CC pela primeira vez, o Flow Designer será habilitado por padrão.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Se você for um usuário existente Configuration Compliance, a opção padrão será fluxo de trabalho.

Se você implantou Configuration Compliance v13.0 ou posterior, o valor da propriedade do sistema *sn_vulc.flow_designer_activation* será definido como verdadeiro. Isso significa que o Flow Designer está habilitado por padrão.

Se você já estiver usando Configuration Compliance antes da v13.0, o valor desta propriedade do sistema será definido como falso. Você pode ativar o Flow Designer alterando o valor para verdadeiro.

Nota:
Você não pode reverter para usando o fluxo de trabalho depois de ativar o Flow Designer. Para obter uma comparação detalhada entre o fluxo de trabalho e o Flow Designer, consulte Fluxo de trabalho de gestão de exceções versus Flow Designer no Configuration Compliance.

Para usar o Flow Designer, crie regras usando o módulo Regras de aprovação. Usando este módulo, você pode configurar regras de aprovação para cada um dos seguintes fluxos de trabalho de gestão de exceções.

- Regras de aprovação de exceção para grupos de resultados de testes
- Regra de aprovação para regras de exceção automática

Nota:
Você também pode definir condições que contenham vários níveis de aprovação em uma regra. O Flow Designer herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente. Para obter informações sobre como configurar níveis de aprovação, consulte Como criar níveis de aprovação para o Exception Management no Configuration Compliance.

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Regras de aprovação** > **Regras de aprovação de exceção para o grupo de resultados de testes**.
2. Na página Regras de aprovação, selecione o grupo para o qual você deseja definir a regra de aprovação.
3. No formulário, preencha os campos.

Formulário Regra de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Tabela	Tabela na qual a regra é aplicada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aplicação	O valor padrão é Configuration Compliance.
Tipo de regra	Especifica o tipo de regra. Por exemplo, gerenciamento de exceções ou regra de exceção.
Ativo	Habilitado por padrão, o que significa que a regra de aprovação está em uso.
Descrição	Descrição resumida das regras de aprovação.
Expiração da aprovação (dias) A partir da v14.11 de Configuration Compliance	Data até quando o aprovador pode aprovar a solicitação.
Aprovador do Notify (dias) A partir da v14.11 de Configuration Compliance	Data após a qual o aprovador é notificado para agir.

4. Selecione **Atualizar**.
   Na guia Configurações de aprovação, há dois níveis de aprovadores configurados por padrão. Você pode selecionar uma regra para definir as condições com base em diferentes casos de uso em uma regra. Para obter mais informações, consulte Como criar configurações para uma regra de aprovação no Configuration Compliance.

   Nota:
   Em cada página de configuração, você pode criar vários níveis de aprovação. Para obter mais informações, consulte Como criar níveis de aprovação para o Exception Management no Configuration Compliance.

Example:
Com base em diferentes casos de uso, você pode definir diferentes processos de aprovação para os mesmos resultados de testes encontrados em diferentes grupos de resultados de testes.

Como criar configurações para uma regra de aprovação no Configuration Compliance

Defina as condições para filtrar grupos de resultados de testes correspondentes para um nível de aprovação.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
No módulo Configurações de aprovação, você pode configurar vários níveis de aprovação para diferentes configurações. Defina regras baseadas em condição, com cada regra contendo vários níveis de aprovação.

Nota:
Use o módulo Regras de aprovação para configurar regras de aprovação para os fluxos de trabalho de gestão de exceções. Para obter informações sobre como configurar regras de aprovação, consulte Como criar níveis de aprovação para o Exception Management no Configuration Compliance.

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Regras de aprovação**.
2. Selecione uma regra de aprovação e navegue até a guia **Configurações de aprovação**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Selecione uma configuração.
4. No formulário, preencha os campos.

Formulário Configuração de aprovação

Campo	Descrição
Nome	Nome da configuração de aprovação.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação.
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Ativo	Habilitado por padrão, o que significa que a configuração de aprovação está em uso.
Descrição	Descrição resumida dos níveis de configuração de aprovação.
Condição	Identifica os grupos de resultados de testes correspondentes.

5. Selecione **Atualizar**.
   Você pode definir condições que contêm vários níveis de aprovação em uma regra. O Flow Designer herda automaticamente as regras criadas neste módulo e processa o fluxo de trabalho de aprovação correspondente. Para obter informações sobre como configurar níveis de aprovação, consulte Como criar níveis de aprovação para o Exception Management no Configuration Compliance.

Example:
Você pode definir diferentes caminhos de aprovação para diferentes tipos de grupos de resultados de testes.

Como criar níveis de aprovação para o Exception Management no Configuration Compliance

Defina os níveis de usuários e grupos de usuários que aprovarão as solicitações de exceção.

Antes de Iniciar
Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Regras de aprovação**.
2. Selecione uma regra de aprovação e navegue até a guia **Configurações de aprovação**.
3. Selecione uma configuração.
4. Na seção **Níveis** de aprovador, selecione um nível de aprovador.
5. No formulário, preencha os campos.

Formulário de nível de aprovação

Campo	Descrição
Nome	Nome do nível de aprovação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Aprovação obrigatória	Selecione quantas aprovações são necessárias para o nível selecionado: ○ Um aprovador necessário ○ Todos os usuários devem aprovar
Ativo	Habilitado por padrão, o que significa que o nível de aprovação está em uso.
Ordem	Ordem de execução de várias configurações em uma regra. Por exemplo, uma configuração com uma entrada de pedido de 100 é executada antes de uma configuração com uma entrada de pedido de 200.
Regra de aprovação	Contém a tabela e os detalhes do tipo da regra de aprovação. Este campo é somente leitura.
Configuração de aprovação	Contém as configurações de aprovação. Este campo é somente leitura.
Atribuir usando	Selecione uma opção de: ○ Usuário e grupo de usuários ○ Campo da tabela de aprovação ○ Script
Grupos	Grupo de nível de aprovador que consiste em vários usuários. O usuário deve ter uma das seguintes funções para gestão de exceções e regras de exceção: ○ sn_vulc.exception_approver ○ sn_vulc.read ○ sn_vulc.read_auto_exception_rule
Usuários	Edite os usuários listados nos grupos.

6. Para salvar as mudanças, selecione **Atualizar**.

Nota:
Antes da v13.0, o processo de fluxo de trabalho é funcional se houver usuários somente no nível de exceção 1. No entanto, a partir da v13.0, deve haver pelo menos um usuário em cada nível.

Antes da v13.0, no fluxo de trabalho, se não houvesse nenhum usuário no segundo nível, o grupo de resultados de testes era adiado. No entanto, da v13.0 em diante, se não houver usuário no segundo nível, a solicitação de aprovação será rejeitada automaticamente.

Example:
Pode haver diferentes níveis de aprovação para grupos de resultados de testes para servidores Linux e Windows.

Fluxo de trabalho de gestão de exceções versus Flow Designer no Configuration Compliance

A partir do Configuration Compliance (CC) v13.0, se você estiver implantando o CC pela primeira vez, o Flow Designer para aprovar solicitações de exceção na gestão de exceções será habilitado por padrão. Se você for um usuário existente do CC, a opção padrão será fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho versus designer de fluxo

Considerações	Fluxo de trabalho	Flow Designer
Versão	Antes da v13.0 do CC.	A partir da v13.0 do CC.
Opção padrão	Opção padrão se você for um usuário de CC existente.	Opção padrão para novos usuários de CC a partir da v13.0.
Configuração do processo de aprovação	O gerenciamento de exceções inclui solicitações de exceção junto com regras de exceção.	Inclui a definição de vários níveis e a adição de diferentes aprovadores para diferentes casos de uso. Mais fácil de implementar do que o fluxo de trabalho. O gerenciamento de exceções inclui solicitações de exceção junto com regras de exceção.
Atualizando para o Flow Designer	Você pode atualizar para o Flow Designer a partir do fluxo de trabalho. No entanto, as solicitações existentes só podem ser aprovadas usando o fluxo de trabalho.	O Flow Designer está habilitado por padrão.
Propriedade do sistema `sn_vulc.flow_designer_activation`	Se você estiver usando o fluxo de trabalho para gerenciamento de exceções antes da v13.0, a propriedade do sistema será definida como falsa. Para ativar o Flow Designer, defina esta propriedade como verdadeira. **Nota:** Você não pode reverter para usando o fluxo de trabalho depois de ativar o Flow Designer.	Se você estiver usando o CC pela primeira vez para v13.0 ou posterior, o valor da propriedade do sistema será definido como verdadeiro por padrão.
Módulo de regras de aprovação	Depois de definir a propriedade do sistema como verdadeira, o trabalho programado **Habilitar regras de aprovação do módulo** é executado em 24 horas. Este trabalho programado habilita o módulo **Regras de aprovação**. Para ativar este módulo instantaneamente, execute este trabalho manualmente.	Se você implantou o CC pela primeira vez a partir do CC v13.0, este módulo está disponível por padrão.
Níveis de aprovação	Fornece a opção de definir apenas dois níveis de aprovadores.	Fornece várias opções, como definir qualquer número de configurações, níveis de aprovador e adicionar dinamicamente aprovadores para cada regra.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Configuration Compliance

As integrações de terceiros importam descobertas de avaliação de configuração, políticas, testes, tecnologias, fontes autorizadas e resultados de testes junto com outros dados de vulnerabilidade para a aplicação Configuration Compliance.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

A aplicação Configuration Compliance oferece suporte às seguintes integrações de terceiros:

- A partir da v14.11, dirija a correção de lacunas de segurança em seus ativos empresariais identificados pela aplicação Security Posture Control publicando descobertas como resultados de testes na aplicação Configuration Compliance. A aplicação Security Posture Control e suas aplicações compatíveis estão disponíveis com assinaturas separadas da ServiceNow® Store. Para obter mais informações, consulte Controle de posturas de segurança.
- Microsoft Defender for Cloud Integration para Security Operations
- Palo Alto Prisma Cloud Vulnerability Integration
- Qualys integração com Configuration Compliance
- O produto Tenable.io da integração de vulnerabilidade da Tenable

Anotações adicionais para integrações

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 14.8.5 do Configuration Compliance, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- `sn_sec_cmn.record_threshold_heartbeat`: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- `sn_sec_cmn.maximum_heartbeat_delay`: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Microsoft Defender for Cloud Integration para Security Operations

O produto Microsoft Defender for Cloud Integration é um sistema de gestão de segurança de infraestrutura que aprimora a postura de segurança de seus ambientes de nuvem.

Microsoft Defender for Cloud Integration para Security Operations integra-se com a aplicação Configuration Compliance para mapear testes para itens de configuração (ICs) para criar resultados de testes. Ele descobre continuamente novos recursos de nuvem implantados em cargas de trabalho e determina se eles estão configurados de acordo com padrões de segurança, como o Center for Internet Security (CIS).

A partir da versão 2.2, o Microsoft Azure Security Center foi renomeado para Microsoft Defender for Cloud Integration para Security Operations.

Versões disponíveis

Aplicação	Versão
Microsoft Defender for Cloud Integration para Security Operations	2,3
Configuration Compliance	14,3
Security Support Common	13,2
Vulnerability Response	16,2

Várias implantações da plataforma Microsoft Defender for Cloud

Se você tiver várias implantações da aplicação da plataforma Microsoft Defender for Cloud, poderá adicionar uma integração para cada implantação. Os recursos que são identificados por várias implantações de terceiros são consolidados e reconciliados com seu Configuration Management Database (CMDB). Essa consolidação ocorre mesmo quando os processos de verificação se sobrepõem entre as várias implantações.

ServiceNow Microsoft Defender for Cloud Integrações

O Microsoft Defender for Cloud Integration para Security Operations enriquece os dados de conformidade em sua instância recuperando dados de Microsoft Defender for Cloud. Uma série de trabalhos programados invoca as integrações automaticamente. Você também pode executar esses trabalhos programados manualmente. Os trabalhos programados simplificam o ciclo de vida de correção dos resultados de testes, mantendo a instância sincronizada com Microsoft Defender for Cloud.

Há um usuário executado configurado para cada registro de integração, com o valor padrão **VR.System**. Este valor deve permanecer o mesmo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Se você não definir um usuário executar como válido, anexos de recuperação de dados duplicados ou múltiplos serão criados para os registros de fonte de dados. O número de anexos aumenta cada vez que a integração é executada. Isso aumenta o tempo de processamento, resultando em resultados de transformação inconsistentes.

Microsoft Defender for Cloud As tarefas de integração da plataforma envolvem as funções a seguir.

- sn_vul_asc.configure_integration: capacidade de ler, gravar e excluir registros.
- sn_vul_asc.read_integration: capacidade de ler registros.

Exibindo as integrações Microsoft Defender for Cloud

Exiba as integrações navegando até **Todos** > **Integração com Microsoft Defender para Nuvem** > **Integrações**.

As integrações a seguir estão incluídas no sistema de base.

Integração	Descrição
Integração de definição de política	Recupera políticas e cria entradas de política em sua instância.
Integração de metadados de avaliação	Recupera metadados de avaliação e cria testes em sua instância.
Compliance Standards & Controls Integration	Recupera padrões e controles e cria a fonte de autorização e as citações. Em seguida, ele os vincula aos testes criados.
Integração de avaliação	Recupera avaliações e as processa em sua instância. A saída desta integração são os resultados de testes.

Criar ICs usando o Mecanismo de Identificação e Reconciliação

Use o Mecanismo de Identificação e Reconciliação (IRE) para criar ICs quando um IC existente não puder ser correspondido com um host importado de um scanner de terceiros.

Se um IC não for correspondido no CMDB, um IC será criado na classe `cmdb_ci_cmp_resource`. Posteriormente, quando uma descoberta encontrar o mesmo IC, ela aprimorará o IC ou criará outro.

Nota:
A reconciliação automática não acontece para recursos de nuvem.

Instalar e configurar Microsoft Defender for Cloud Integration para Security Operations

Instale e configure o Microsoft Defender for Cloud Integration para Security Operations, para que você possa usar os dados importados de Microsoft Defender for Cloud para priorizar e corrigir quaisquer configurações incorretas em seus ativos.

Antes de Iniciar
Crie um novo registro de app no Azure Active Directory. Para obter mais informações sobre como registrar uma nova aplicação no Azure Active Directory, pesquise por Registrar uma aplicação cliente no Azure Active Directory no site de documentação da Microsoft. Atribua a função de **leitor de segurança** para o registro do app recém-criado no escopo relevante com o qual você deseja se conectar a ServiceNow. Pode ser em um grupo de gestão ou nível de assinatura.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Todos** > **Definição do Sistema** > **Plug-ins**.
2. Na barra de pesquisa, pesquise por Microsoft Defender for Cloud Integration for Security Operations.
3. Selecione **Instalar**.

   Todas as dependências que serão instaladas serão exibidas.
4. Navegar até **Todos** > **Integração com Microsoft Defender para Nuvem** > **Administração** > **Configuração** > **Configuração do Microsoft Defender para Nuvem**.
5. No formulário, preencha os campos.

Microsoft Defender for Cloud Formulário de configuração

Campo	Descrição
URL da API	URL do recurso da instância. Exemplo: https://management.azure.com (nuvem pública do Azure)
ID de locatário	Identidade de locatário da sua organização.
Instância de integração	Instância padrão. Você também pode criar uma instância para trazer os dados de vários locatários ou assinaturas do Microsoft Defender.
ID de cliente	Identidade do cliente gerada depois que a aplicação Microsoft Defender for Cloud Integration é registrada.
Segredo do cliente	Segredo do cliente que é gerado depois que a aplicação Microsoft Defender for Cloud Integration é registrada.
Importar descobertas de	Recursos e avaliações que correspondem aos IDs de grupo de gestão e IDs de assinatura selecionados que serão recuperados.
IDs do grupo de gestão	Recursos e avaliações que correspondem aos IDs de grupo de gestão que serão recuperados. **Nota:** Este campo é exibido somente quando você seleciona **Grupos de gestão específicos** no campo **Importar descobertas de**.
IDs de Assinatura	Números de identificação das assinaturas para as quais os recursos e as avaliações serão recuperados. **Nota:** Este campo aparece somente quando você seleciona **Assinaturas específicas** no campo **Importar descobertas de**.
Status de validação	Se as credenciais e o ID de assinatura fornecidos são válidos.

6. Configure ou execute as integrações selecionando **Salvar e testar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuration Compliance dados importados para Microsoft Defender for Cloud Integration

Configuration Compliance O importa políticas, testes, fontes autorizadas e resultados de testes de integrações de terceiros e os armazena em módulos para exibição.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Grupos de teste

Um grupo de testes de configuração constitui um grupo de teste. Os grupos de teste estão relacionados a documentos oficiais e registros de teste e podem ser modificados para atender às necessidades da sua organização. Um teste de configuração pode pertencer a vários grupos de teste.

Se o Microsoft Defender for Cloud Integration estiver instalado, os grupos de teste serão recuperados e preenchidos pelo trabalho programado, **Integração de definições de política**. Você pode exibir o trabalho programado navegando até **Todos** > **Integração com Microsoft Defender para Nuvem** > **Administração** > **Integrações** > **Integração de definições de política**.

Nota:
Se você optar por executar a integração manualmente, execute a **integração de definições de política** primeiro.

Testes

Testes são bibliotecas de registros de dados que organizam verificações de ativos de computação. Os testes de configuração definem como os ativos devem ser controlados.

Um teste Configuration Compliance é o mecanismo que as aplicações de integração de terceiros usam para agrupar ativos por tipo de resultados de teste.

Se o Microsoft Defender for Cloud Integration estiver instalado, o trabalho programado, **Assessment Metadata Integration**, recuperará os testes. Você pode exibir o trabalho programado navegando até **Integração** > **Integrações Primárias** > **Integração de metadados de avaliação**.

Nota:
Se você optar por executar a integração manualmente, execute a integração de **metadados de avaliação** após a **integração de definições de política**.

Fontes autorizadas

Configuration Compliance usa fontes autorizadas e citações ao gerar alertas de vulnerabilidade para testes. As fontes autorizadas geralmente são mapeadas para seções de padrões do setor publicados, como **ISO 27001** e **PCI DSS 3.2.1**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esses registros de origem contêm referências a informações sobre problemas conhecidos de configuração de software e hardware de especialistas no campo de segurança do computador. Eles definem requisitos para políticas e procedimentos de segurança.

Se o Microsoft Defender for Cloud Integration estiver instalado, o trabalho programado, **Compliance Standards & Controls**, recuperará as fontes autorizadas e as citações. Você pode exibir este trabalho programado navegando até **Todos** > **Integração com Microsoft Defender para Nuvem** > **Integrações** > **Compliance Standards & Controls Integration**.

Nota:
Se você optar por executar a integração manualmente, execute a **integração de controles e padrões de conformidade** após a **integração de metadados de avaliação**.

Ativos

A **integração de avaliação** fornece informações vitais, como marcadores de recurso e atributos de nuvem. Essas informações são exibidas no formulário Item descoberto. Ele é usado principalmente para filtragem em Configuration Compliance Regras de atribuição e grupo.

- Marcadores de recurso: todos os marcadores de recurso de nuvem são importados como marcadores de host como parte da **integração de avaliação**. Os marcadores de nuvem para qualquer tipo de recurso de nuvem são armazenados aqui, seja o recurso um host ou não.
  - O armazenamento de marcador não faz distinção entre maiúsculas e minúsculas. Se um marcador Tokyo for criado, um marcador **TOKYO**não poderá ser armazenado na tabela de marcadores do host. **Tokyo** e **TOKYO** são considerados o mesmo marcador de host. Qualquer marcador que tenha sido importado primeiro vencerá.
  - Usar marcadores de host como chave de grupo em uma regra de grupo pode ter resultados inesperados. Os marcadores de host devem ser usados somente no construtor de condição.
- Atributos de nuvem para ativos: a seguir estão os atributos de nuvem que as integrações recuperam de Microsoft Defender for Cloud:
  - Conta de nuvem
  - Região da nuvem
  - Tipo de Recurso de Nuvem
  - Provedor de serviço de nuvem

Resultados de testes

Configuration Compliance não calcula os resultados do teste, mas os importa como parte de uma integração de terceiros. Quando estiverem visíveis em Configuration Compliance, eles serão corrigidos usando **Grupos de resultados de testes**.

Se a integração Microsoft Defender for Cloud estiver instalada, o trabalho programado, **integração de avaliação**, recuperará os resultados do teste. Você pode exibir este trabalho programado navegando até **Todos** > **Integração com Microsoft Defender para Nuvem** > **Integrações** > **Integração de avaliação**.

A importação **de integração de avaliação** é a única integração que usa o parâmetro *`Start Time`* na guia **Detalhes da integração**. Todas as outras importações de Configuration Compliance trarão todos os dados disponíveis, independentemente de *`Start Time`*.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando a importação da **integração de avaliação** estiver concluída, um evento será iniciado para acionar cálculos de fim de importação.

A **integração de avaliação** extrai as avaliações de dados somente se houver uma mudança de status da última integração bem-sucedida executada no último dia por padrão. Portanto, se a avaliação falhar continuamente nos últimos dias, a integração não buscará a avaliação, pois não há mudança de status para a avaliação. Para manter os resultados do teste atualizados com as avaliações do Defender, uma nova **integração de avaliação abrangente** é adicionada, que extrai os dados dos últimos sete dias. Ele é executado semanalmente e extrai todos os resultados de testes, que não são aprovados.

Regras de pesquisa de IC para identificar ICs de Microsoft Defender for Cloud integrações

Quando os dados são importados de uma integração de terceiros, Configuration Compliance usa automaticamente os dados de recursos para pesquisar correspondências no Configuration Management Database (CMDB), usando Regras de pesquisa de IC. Essas regras são usadas para identificar os itens de configuração (ICs) e adicioná-los ao registro de resultado de testes para ajudar na correção. As regras de pesquisa de IC do sistema básico estão disponíveis para ID de recurso, Nome e Bucket S3. Para obter mais informações sobre regras de pesquisa de IC, consulte Regras de bloqueio de IC para Microsoft Defender for Cloud Integration for Security Operations.

Noções básicas sobre o Vulnerability Response Integration with Palo Alto Prisma Cloud

O Prisma Cloud é uma solução de segurança de infraestrutura em nuvem baseada em API. Ele se conecta ao seu ambiente de nuvem e monitora os recursos implantados nos ambientes de nuvem pública, como Amazon Web Services (AWS), Microsoft Azuree assim por diante. Você obtém visibilidade e controle completos sobre os riscos em sua infraestrutura de nuvem pública.

A aplicação Vulnerability Response Integration with Palo Alto Prisma Cloud facilita a ingestão de políticas e alertas do Prisma Cloud, como testes e resultados de testes, respectivamente, na aplicação Configuration Compliance. Com a configuração correta, os resultados do teste podem ser gerenciados sem problemas, atribuindo-se pontuações de risco apropriadas e agrupando-as e atribuindo-as a usuários e grupos relevantes.

Versões disponíveis

A tabela lista as aplicações das quais Vulnerability Response Integration with Palo Alto Prisma Cloud depende, junto com a versão da aplicação.

Aplicação	Versão
Prisma Cloud integration for Security Operations	2,3
Configuration Compliance	14,7
Security Support Common	13,5
Vulnerability Response	18,0

ServiceNow Prisma Cloud Integrations

A aplicação Vulnerability Response Integration with Palo Alto Prisma Cloud ajuda a importar os dados do Prisma para sua instância ServiceNow para enriquecer sua instância para um

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

melhor gerenciamento. Uma série de trabalhos programados invoca as integrações automaticamente. Você também pode executar esses trabalhos programados manualmente. Os trabalhos programados simplificam o ciclo de vida de correção dos resultados de testes, mantendo a instância atualizada, recuperando dados periodicamente do Prisma Cloud.

As tarefas de integração do Prisma Cloud envolvem as seguintes funções.

- sn_vul_prismacloud.configure_integration: capacidade de ler, gravar e excluir registros.
- sn_vul_prismacloud.read_integration: capacidade de ler registros.

Exibição das integrações

Você pode exibir as integrações que fazem parte de Vulnerability Response Integration with Palo Alto Prisma Cloud navegando até **Integração na nuvem do Prisma** > **Integrações**.

As seguintes integrações estão disponíveis no sistema de base.

Sequência de execução	Programação	Integração	Descrição
1	Semanalmente	Prisma Policy Integration	• Recupera políticas do Prisma Cloud e cria entradas de teste na sua instância. • Ele não fornece suporte incremental. Se você executar a integração nos últimos 10 dias, ele mostrará o resultado das execuções de integração anteriores também.
2	Diariamente	Prisma Alerts Integration	• Recupera alertas do Prisma Cloud e cria entradas de resultados de testes na sua instância. • Fornece suporte incremental. A integração é executada diariamente após o último tempo de execução de integração.

Preparando para instalar o Vulnerability Response Integration with Palo Alto Prisma Cloud

Prepare-se para instalar o Vulnerability Response Integration with Palo Alto Prisma Cloud executando tarefas de configuração.

Antes de começar

Para integrar o Vulnerability Response ao Palo Alto Prisma Cloud, você deve ser atribuído a um grupo de permissões no Prisma que forneça acesso somente leitura aos dados de política e alertas. Você pode encontrar mais informações sobre grupos de permissão em https://docs.prismacloud.io/en/classic/cspm-admin-guide/manage-prisma-cloud-administrators/prisma-cloud-administrator-roles#id437b5c4a-3dfa-4c70-8fc7-b6d074f5dffc .

Para obter informações detalhadas sobre as funções atribuídas a diferentes grupos de permissão, consulte a página https://docs.prismacloud.io/en/classic/cspm-admin-guide/manage-prisma-cloud-administrators/prisma-cloud-admin-permissions .

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Além disso, as chaves de acesso devem ser criadas para permitir a leitura dos alertas. Para obter mais informações sobre como criar chaves de acesso, consulte https://docs.prismacloud.io/en/classic/cspm-admin-guide/manage-prisma-cloud-administrators/create-access-keys .

Para instalar e configurar o Vulnerability Response Integration with Palo Alto Prisma Cloud, use a check-list a seguir. Antes de instalar a aplicação, verifique se os itens listados foram concluídos.

Check-list de preparação da integração

Tarefa	Descrição
☐	Verifique se você tem os seguintes conjuntos de informações: • URL base da API • ID da chave de acesso • Chave secreta • Nome de usuário e senha para acessar o Prisma Cloud. Essas credenciais são usadas para se conectar à instância do Prisma Cloud a partir da instância Now Platform®. O ID da chave de acesso e a chave secreta devem ser gerados no portal do Prisma Cloud após o registro.
☐	Se ainda não estiver instalado e ativado, instale a aplicação Vulnerability Response antes de instalar a aplicação Vulnerability Response Integration with Palo Alto Prisma Cloud. Para obter mais informações sobre como instalar e ativar a aplicação Vulnerability Response, consulte Como instalar Vulnerability Response. Esta integração requer a versão 15.2.0 de Vulnerability Response ou posterior.
☐	Se você ainda não tiver a aplicação em sua instância, obtenha direitos e baixe a aplicação Vulnerability Response Integration with Palo Alto Prisma Cloud para sua instância Now Platform®. Consulte .
☐	Certifique-se de ter instalado os seguintes plug-ins para uma execução de integração sem problemas: • Vulnerability Response • Configuration Compliance • Vulnerability Response Integration with Palo Alto Prisma Cloud Os plug-ins a seguir são opcionais, mas podem ser úteis: • Cloud Provisioning and Governance • Padrões de descoberta e mapeamento de serviços

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list de preparação da integração

Tarefa	Descrição
☐	Estime o número de resultados de testes que você espera importar. Verifique se sua instância pode aceitar o número de resultados de testes que você espera importar. Uma instância subdimensionada pode levar a longos tempos de carregamento. Se você não souber o tamanho da sua instância ou se precisar de assistência, entre em contato com o ServiceNow Suporte técnico.
☐	Verifique se você tem um administrador para gerenciar as integrações e corrigir os resultados de testes: O administrador instala a aplicação Vulnerability Response Integration with Palo Alto Prisma Cloud. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidade (sn_vul.vulnerability_admin) e outras funções.

Você está pronto para Instalar e configurar a aplicação Vulnerability Response Integration with Palo Alto Prisma Cloud.

Instalar e configurar a aplicação Vulnerability Response Integration with Palo Alto Prisma Cloud

Instale a aplicação Vulnerability Response Integration with Palo Alto Prisma Cloud para usar os dados importados do Prisma Cloud. Use esses dados para priorizar e corrigir configurações incorretas em seus ativos.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Definição do Sistema** > **Plug-ins**.
2. Na barra de pesquisa, pesquise por Vulnerability Response Integration with Palo Alto Prisma Cloud.
3. Clique em **Instalar**.

   Todas as dependências que serão instaladas serão exibidas.
4. Navegar até **Todos** > **Integração na nuvem do Prisma** > **Administração** > **Configuração** > **Configuração do Prisma Cloud**.
5. No formulário, preencha os campos.

Campo	Descrição
Instância de Integração	Nome da nova instância de integração. Você pode criar uma instância ou clicar no ícone de pesquisa para selecionar uma instância existente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
URL da API	URL para integração com o Prisma Cloud.
ID da chave de acesso	Chave exclusiva para autenticar a solicitação de acesso ao Prisma Cloud. **Nota:** Você deve gerar a chave após fazer login no portal do Prisma Cloud.
Chave secreta	Chave privada para autenticar a solicitação de acesso ao Prisma Cloud. **Nota:** Você deve gerar a chave secreta após fazer login no portal do Prisma Cloud.

6. Clique **em Salvar e testar**.

O que Fazer Depois

Depois de concluir a instalação, navegue até **Integração na nuvem do Prisma** > **Configuração** para continuar com a configuração.

Configurar a aplicação Vulnerability Response Integration with Palo Alto Prisma Cloud

Configure a aplicação Vulnerability Response Integration with Palo Alto Prisma Cloud. Use os dados importados do Prisma Cloud para priorizar e corrigir configurações incorretas em seus ativos.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Integração na nuvem do Prisma** > **Configuração**.
2. No formulário, preencha os campos.

Configuração do Prisma Cloud

Campo	Descrição
Instância de Integração	Nome da nova instância de integração. Você pode criar uma instância ou clicar no ícone de pesquisa para selecionar uma instância existente.
URL da API	URL para integração com o Prisma Cloud.
ID da chave de acesso	Uma chave exclusiva para autenticar a solicitação de acesso ao Prisma Cloud. Você deve gerar a chave após fazer login no portal do Prisma Cloud.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Chave secreta	Uma chave privada para autenticar a solicitação de acesso ao Prisma Cloud. Você deve gerar a chave secreta após fazer login no portal do Prisma Cloud.

3. Clique **em Salvar e testar**.

O que Fazer Depois
Depois de concluir a configuração, navegue até **Integração na nuvem do Prisma** > **Integrações** para verificar se a execução da integração foi bem-sucedida.

Verificar o status de execução de importação Vulnerability Response Integration with Palo Alto Prisma Cloud

Use o status de execução de importação Vulnerability Response Integration with Palo Alto Prisma Cloud para verificar o sucesso das execuções de integração e para identificar quaisquer problemas.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 14.8.5 do Configuration Compliance, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- `sn_sec_cmn.record_threshold_heartbeat`: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- `sn_sec_cmn.maximum_heartbeat_delay`: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento
1. Navegar até **Integração na nuvem do Prisma** > **Integrações**.
2. Clique **em Integração de políticas do Prisma**.
3. Clique em **Executar agora**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando esta integração é executada, as seguintes tabelas são preenchidas nesta ordem:

a. sn_vulc_test.list (Testes de configuração)

b. sn_vulc_auth_src (Origem autorizada

c. sn_vulc_citation (Citações)

4. Na guia **Itens**, exiba o número de novos testes criados, atualizados e ignorados clicando na execução da integração de vulnerabilidade.

> **Nota:**
> As políticas são definidas no Prisma Cloud para a instância de nuvem selecionada. A instância é verificada com base nas políticas definidas.

5. Clique **em Prisma Alerts Integration**.
6. Clique em **Executar agora**.
   As tabelas a seguir são preenchidas com base na integração:
   - Resultados de testes
   - Itens descobertos: se os itens de configuração não estiverem disponíveis no sistema, eles serão criados. A classe é sempre Recurso de Nuvem. Na página Item descoberto, três novos campos são criados: **Tipo de recurso denuvem , Provedor de serviço de nuvem**e **Categoria de ativo**.

     Na guia **Itens**, clique na execução da integração de vulnerabilidade para exibir o número de novos resultados de testes importados, atualizados e ignorados. A guia **Itens de configuração** também é preenchida com base no número de resultados de testes criados.

Mapeamento de dados

Os dados do Prisma Cloud são importados no módulo Configuration ComplianceServiceNow da instância [].

> **Nota:**
> A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Os dados do Prisma Cloud são importados com um nome diferente em Configuration Compliance, conforme mencionado na tabela.

Mapeamento de dados do Prisma Cloud no Configuration Compliance

Prisma Cloud	Configuration Compliance
Política	Testar
Alerta	Resultado do teste

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de dados do Prisma Cloud no Configuration Compliance

Prisma Cloud	Configuration Compliance
Padrão de conformidade	Fonte autorizada
Seções	Citação
Ativo	Item de descoberta/item de configuração (IC)

Testes

Uma política no Prisma Cloud é importada como um teste em Configuration Compliance. As políticas estão relacionadas a documentos oficiais e registros de teste e podem ser modificadas para atender às necessidades da sua organização. Você pode exibir os testes navegando até **Configuration Compliance** > **Testes**.

Se **o Vulnerability Response Integration with Palo Alto Prisma Cloud** estiver instalado, o trabalho de integração *`Prisma Policy Integration`* recuperará os testes. Você pode exibir o trabalho de integração navegando até **Todos** > **Prisma Cloud Integrations** > **Prisma Policy Integration**.

Resultados de testes

Um alerta no Prisma Cloud é importado como um resultado de teste em Configuration Compliance. Os alertas são corrigidos usando **Grupos de resultados de testes**. Você pode exibir os resultados do teste navegando até **Configuration Compliance** > **Resultados de testes**.

O Configuration Compliance importa resultados de testes como parte de uma integração de terceiros. Depois que estiverem visíveis na aplicação Configuration Compliance, eles serão corrigidos usando Grupos de resultados de testes.

Se **o Vulnerability Response Integration with Palo Alto Prisma Cloud** estiver instalado, o trabalho de integração do **Prisma Alert Integration** recuperará os resultados do teste. Você pode exibir este trabalho de integração navegando até **Todos** > **Integração na nuvem do Prisma** > **Integrações** > **Prisma Alert Integration**.

O **Prisma Alert Integration** é um trabalho de integração que é executado diariamente e extrai os resultados de testes com mudança de status após a hora definida no campo **Hora** de início na guia **Integração**.

Nota:
Se você executar o trabalho de integração, **Prisma Alert Integration** manualmente, execute-o depois de executar o trabalho de integração, **Prisma Policy Integration**.

Quando o **Prisma Alert Integration** conclui importando os dados, um evento é iniciado para acionar cálculos de fim de importação. Se o alerta falhar continuamente nos últimos dias, a integração não buscará os alertas, pois não há mudança de status para o alerta. Portanto, para manter os dados dos resultados de testes atualizados com os alertas do Prisma, um novo trabalho de integração, **Integração de alerta abrangente do Prisma**, foi adicionado, o que extrai os alertas atualizados nos últimos sete dias. Ele é executado semanalmente e extrai todos os resultados de testes, que não são aprovados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fontes Autorizadas

Configuration Compliance usa fontes autorizadas e citações ao gerar alertas de vulnerabilidade para testes. As fontes autorizadas geralmente são mapeadas para seções de padrões do setor publicados, como ISO 27001 e PCI DSS 3.2.1.

Esses registros de origem contêm referências a informações sobre problemas conhecidos de configuração de software e hardware de especialistas no campo de segurança do computador. As referências definem requisitos para políticas e procedimentos de segurança. Navegar até **Configuration Compliance** > **Fontes Autorizadas** para exibir as fontes autorizadas.

Ativos

Se o Vulnerability Response Integration with Palo Alto Prisma Cloud estiver instalado, o trabalho programado *`Prisma Alerts Integration`* capturará as informações relacionadas ao alerta no módulo ou na tabela Itens descobertos. Você pode exibir este trabalho programado navegando até **Integração na nuvem do Prisma** > **Integrações**.

A integração do Prisma Alerts importa tipos adicionais de informações, como marcadores de recurso e atributos de nuvem que são armazenados em tabelas. Essas informações são exibidas no formulário de itens descobertos.

- Marcadores de host: um recurso pode ter vários marcadores. As tags de host estão disponíveis no formato de par de chave-valor. Por exemplo, o sistema operacional é o Windows 10 e a versão do Java é 1.8.
- Atributos de nuvem para ativos: os seguintes atributos de nuvem estão disponíveis:
  - Conta de nuvem: fornece o ID da conta da integração. As informações são preenchidas a partir da tabela Contas de nuvem [sn_sec_cmn_cloud_account.LIST].
  - Região da nuvem: fornece o local onde o recurso foi hospedado. As informações são preenchidas a partir da tabela Regiões de nuvem [sn_sec_cmn_region.LIST].
  - Tipo de recurso de nuvem: fornece informações sobre o tipo de recurso, por exemplo, se é uma máquina virtual ou uma instância de banco de dados e assim por diante. As informações são preenchidas a partir da tabela Tipo de recurso de nuvem [sn_sec_cmn_cloud_resource_type.LIST].
  - Provedor de serviços em nuvem: fornece informações sobre o provedor de serviços em nuvem, seja Amazon Web Services (AWS), Oracle Cloud e assim por diante. As informações são preenchidas a partir da tabela Cloud Service Provider [sn_sec_cmn_cloud_service_provider.LIST].
  - Grupos de contas de nuvem: fornece informações sobre os grupos de contas. As informações são preenchidas a partir da tabela Grupos de contas de nuvem [sn_vul_prismacloud_account_group.list].

Nota:
O atributo Grupos de contas em nuvem está disponível somente para Prisma.

Regras de pesquisa de IC

As regras de pesquisa de IC do sistema básico estão disponíveis para ID de recurso, Nome e Bucket S3. Para obter mais informações sobre regras de pesquisa de IC, consulte Regras de pesquisa de IC para Microsoft Defender for Cloud Integration para Security Operations e Palo Alto Prisma Cloud.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagens REST do Prisma Cloud

As mensagens REST do Prisma são usadas para fazer chamadas para a Interface de programação da aplicação (API) do Prisma para buscar os dados de conformidade.

As mensagens REST a seguir são enviadas com o sistema de base.

Prisma Cloud integrations

Todas as integrações do Prisma Cloud usam o JSON Web Token (JWT) para autenticação e autorização.

Mensagem REST de login do Prisma

Endpoint	Descrição	Método	Corpo	Link da documentação da API
/login	Obtém o token JWT para uso em todas as integrações subsequentes.	*POST*	{ "username": <<access key id >>, "password": <<secret access key>>}	https://pan.dev/prisma-cloud/api/cspm/app-login/

Mensagem REST de token de atualização do Prisma

Endpoint	Descrição	Método	Corpo	Link da documentação da API
/auth_token/extend	Renova automaticamente o token JWT na expiração. A duração padrão da expiração do token é de 60 minutos.	*OBTER*	N/D	https://pan.dev/prisma-cloud/api/cspm/extend-session/

Mensagem REST da política do Prisma

Endpoint	Descrição	Método	Corpo	Link da documentação da API
/v2/policy	Recupera todos os dados de política do Prisma.	*OBTER*	N/D	https://pan.dev/prisma-cloud/api/cspm/get-policies/

Mensagem REST de alerta do Prisma

Endpoint	Descrição	Método	Corpo	Link da documentação da API
/v2/alert	Recupera todos os alertas do Prisma.	*POST*	{ "detailed": "false", "filters": [{ "name": "timeRange.type", "operator": "=", "value": "ALERT_STATUS_UPDATED"	https://pan.dev/prisma-cloud/api/cspm/post-alerts/

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mensagem REST de alerta do Prisma

Endpoint	Descrição	Método	Corpo	Link da documentação da API

			}
			],
			"sortBy": [
			"resource.id"
			],
			"pageToken": "",
			"offset": 0,
			"limit": 2000,
			"timeRange": {
			"type": "absolute",
			"value": {
			"startTime": <<Import since at integration level>>,
			"endTime": << Current integration run time>>
			}
			}
			}	

Para a integração do Alerta de compreensão do Prisma, os filtros no corpo do POST acima devem ser substituídos da seguinte forma:

```
"filters": [
 {
                "name": "alert.status",
                "operator": "=",
                "value": "open"
            },
            {
                "name": "alert.status",
                "operator": "=",
                "value": "dismissed"
            },
            {
                "name": "alert.status",
                "operator": "=",
                "value": "snoozed"
            },
            {
                "name": "alert.status",
                "operator": "=",
                "value": "pending_resolution"
            },
            {
                "name": "timeRange.type",
                "operator": "=",
                "value": "ALERT_UPDATED"
            }

  ],
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Qualys integração com Configuration Compliance

O Qualys Policy Compliance coleta os dados e os envia automaticamente para a aplicação Qualys, que analisa e correlaciona continuamente as informações. Ele se integra facilmente como Qualys Integration for Security Operations para mapear descobertas de configuração para ICs e serviços de negócios para determinar o impacto e a prioridade de possíveis configurações incorretas.

Se você tiver várias implantações da aplicação Qualys Cloud Platform, poderá adicionar uma integração para cada implantação. Os ativos, identificados por várias implantações de terceiros e suas vulnerabilidades, são consolidados e reconciliados com o seu CMDB. Essa consolidação acontece mesmo quando os processos de verificação se sobrepõem entre as várias implantações. Os dados provenientes de cada implantação são identificados e disponíveis em uma única instância de Vulnerability Response.

Nota:
Você não pode excluir a integração de vulnerabilidade original, mas pode desabilitá-la. As integrações criadas a partir de modelos inativos são desabilitadas por padrão.

Marcadores de host

Todos os marcadores de host são importados como parte da integração da lista de hosts Qualys. Os marcadores de host são usados principalmente para filtragem em Vulnerability Response Regras de Grupo de Atribuição e Vulnerabilidade. Eles são exibidos no formulário Item descoberto.

Nota:
A integração da lista de hosts Qualys deve ser executada antes de criar as Regras de atribuição ou de tarefa de correção em Vulnerability Response para que todos os marcadores possam estar presentes nas regras e antes que os itens vulneráveis sejam importados e agrupados.

- O armazenamento de marcador não faz distinção entre maiúsculas e minúsculas. Se um marcador **San Diego** for criado, um marcador **SAN DIEGO** não poderá ser armazenado na tabela de marcadores do host. "San Diego" e "SAN DIEGO" são considerados o mesmo marcador de host. Qualquer marcador que tenha sido importado primeiro vencerá.
- Usar marcadores de host como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. Os marcadores de host devem ser usados somente no construtor de condição.
- Os marcadores de host são controlados pela propriedade do sistema global **sn_vul.import_host_tags**. Esta propriedade é definida como verdadeira por padrão. Desativar os marcadores os desativa em todas as instâncias.

Marcadores de host (também chamados de marcadores de ativo) são usados para organizar e rastrear os ativos em sua organização. Você pode atribuir marcadores aos ativos de host. Em seguida, ao iniciar as verificações, você pode selecionar marcadores associados aos hosts que deseja verificar. O módulo Marcadores de host permite que você baixe dados de marcador de host de Qualys para sua instância de forma programada.

Integrando Qualys com a aplicação ServiceNow® Configuration Compliance

Se o Qualys Vulnerability Integration já estiver instalado no seu sistema e suas credenciais de API forem diferentes daquelas que você deseja usar para Configuration Compliance, vá para o Assistente de configuração (em Vulnerability Response) e atribua-as a cada integração de **PC da Qualys**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** e edite o campo **Credenciais de API** da **Qualys na guia Detalhes de REST** da Qualys.

Configurar os parâmetros de PCRS

A partir da v12.6.3 de Integração Qualys para Security Operations, é possível usar a Integração de host de política Qualys PCRS e a Integração de resultados de testes Qualys PCRS para importar resultados de testes com novos conjuntos de APIs Qualys. Essas integrações precisam de um URL de gateway para buscar informações de Qualys.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Ao instalar o Integração Qualys para Security Operations para Vulnerability Response, você pode configurar o **gateway_url** para as novas integrações de PCRS em Configuration Compliance. Para obter mais informações sobre como encontrar o URL do gateway para o URL da API, consulte Identificar sua plataforma Qualys .

O URL do gateway deve ser adicionado à sua instância ServiceNow.

Procedimento

1. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Instâncias de Integração**.

   Nota:
   Certifique-se de que o escopo em que você está seja Qualys for Security Operations.

2. Abra a instância usada pelas integrações de PCRS.
3. Na guia Parâmetros de instância de integração, adicione a URL do gateway para a configuração **gateway_url**.

   Nota:
   A integração de resultados de testes de PCRS da Qualys depende da integração de host de política de PCRS da Qualys. Portanto, se você retroceder os Resultados de testes de PCRS da Qualys da integração, talvez precise executá-los na mesma ordem novamente.

Componentes instalados com o Qualys Integration for Security Operations

As funções, os trabalhos programados e as tabelas a seguir são instalados com o Qualys Integration for Security Operations.

Nota:
A tabela Arquivos da Aplicação lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Exibir listas filtradas de componentes instalados com uma aplicação

Filtre a tabela Arquivos de aplicações para que somente as funções, os trabalhos programados e as tabelas que são instaladas com uma aplicação sejam exibidos. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.
2. Selecione o construtor de condição (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação. Por exemplo, **Aplicação** > **é** > **Vulnerability Response**.
3. No construtor de condição, para adicionar um segundo filtro, selecione **E e**, em seguida, selecione, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função**, **Trabalho programado**ou **Tabela**.
4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
sn_vul_qualys.read	Tem acesso de leitura aos registros Qualys Vulnerability Integration.	
sn_vul_qualys.usuário	Usuário para Qualys Vulnerability Integration. Pode ler e gravar registros	sn_vul_qualys.read
sn_vul_qualys.admin	Administrador paraQualys Vulnerability Integration. Por exemplo, você pode modificar as datas de início da integração e executar algumas definições de configuração avançadas.	• sn_vul_qualys.usuário • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	Pode configurar o Qualys Vulnerability Integration	sn_vul_qualys.admin

Integração trabalhos instalado

Trabalho programado	Descrição
Qualys Políticas de PC	Recupera políticas de Qualys. A saída é armazenada na tabela sn_vulc_policy. A API usada nesta integração não oferece suporte à paginação, portanto, todas as políticas são baixadas em uma única página.
Qualys Detalhe das políticas do PC	Recupera os detalhes completos da política, como tecnologias e seções, por exemplo.
Qualys Controles do PC	Recupera informações de controles de conformidade para diferentes IDs de controle de Qualys.
Qualys Resultados de PC	Recupera registros de postura de conformidade de Qualys. A saída desta integração são Resultados de testes. Por padrão, os detalhes do parâmetro são passados para importar informações do host, datas/horas da última verificação, ID de controle e informações de evidência.
Qualys Resultados abrangentes de PC	Recupera registros de postura de conformidade de Qualys com base na última

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho programado	Descrição
	data de avaliação dos resultados de testes que não foram aprovados. Este trabalho é executado uma vez por semana. A saída desta integração são os resultados de testes. Por padrão, os detalhes do parâmetro são passados para importar as informações do host, datas/horas da última verificação, ID de controle e informações de evidência.
Qualys Integração de Host de Política de PCRS	Recupera dados de host de Qualys e os processa em sua instância. A saída desta integração é IDs de host de política. Os dados Qualys do host são importados nesta integração. **Nota:** • Este trabalho programado aparece somente quando Configuration Compliance está instalado. • Configure os parâmetros de instância de integração gateway_url e pcrs_page_size antes de executar esta integração. Essas duas integrações ficarão OOB inativas. Se você ativar qualquer uma dessas integrações, as integrações de Resultados de PC serão desativadas. Essas duas integrações são adicionadas com base nas novas APIs de streaming da Qualys.
Qualys Integração de resultados de testes de PCRS	Recupera os resultados de testes para cada ID de host. Esta integração usa o parâmetro Hora de início na guia Detalhes da integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Trabalho programado	Descrição
	Nota: • Este trabalho programado aparece somente quando Configuration Compliance está instalado. • Configure os parâmetros de instância de integração gateway_url e pcrs_page_size antes de executar esta integração. • Se você optar por executar a integração manualmente, execute Qualys Integração de resultados de testes de PCRS após Qualys Políticas de PC, Qualys Detalhe de políticas de PC e Qualys Integração de host de política de PCRS.

Nota:
As integrações Qualys Host de política de PCRS e Resultados de testes de Qualys PCRS estão inativas por padrão. Essas duas integrações são baseadas nas novas APIs de streaming da Qualys. Se você ativar qualquer uma dessas integrações, a integração Resultados de PC será desativada e vice-versa.

Tabelas instaladas

Tabela	Descrição
Qualys Importação de resultados de PC sn_vul_qualys_pc_result_import	Tabela que estende a linha do conjunto de importação. A transformação de mapas de campo é ignorada e o anexo de resposta é processado diretamente com o script onComplete.
Id de host de política sn_vul_qualys_policy_host_id	Tabela que armazena o mapeamento entre a política e o host para o qual esta política foi verificada. Esta tabela é usada na nova integração Qualys de PCRS. **Nota:** Esta tabela é exibida somente quando Configuration Compliance está instalado.
Qualys Importação de host de política de PCRS sn_vul_qualys_pcrs_policy_host_import	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o anexo da resposta é processado diretamente com o script onComplete. **Nota:** Esta tabela aparece somente quando Configuration Compliance está instalado.
Qualys Importação de política de PC sn_vul_qualys_pc_policy_import	Tabela que estende a linha do conjunto de importação. A transformação do mapa de campo é ignorada e o

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
	anexo da resposta é processado diretamente com o script onComplete.

Atualizar itens de configuração com o identificador de partição de rede para a integração do Qualys

Crie itens de configuração (ICs) exclusivos para ativos em seu ambiente que compartilham endereços IP. Identifique os ativos distintos em seu ambiente e atualize automaticamente os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Por padrão na aplicação Vulnerability Response, uma maneira de identificar seus ativos é por endereço IP. Em determinados casos, os ativos podem compartilhar endereços IP, mas eles são armazenados como um IC no seu CMDB.

Por exemplo, conforme mostrado nas tabelas a seguir, vários ativos (IC) em seu ambiente podem compartilhar endereços IP, mas têm IDs de rede e repositório exclusivos. No entanto, por padrão, esses ativos são normalmente identificados e armazenados como um único IC (IC 1) durante a pesquisa de endereço IP.

Pesquisa de IP padrão e criação de IC

Origem	Endereço IP	NETWORK_Identificador	Item de configuração
Qualys Vulnerability Integration: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1
	123.12.12.141	03713	IC 1

Origem	Endereço IP	REPOSITÓRIO_ID	Item de configuração
Qualys Vulnerability Integration: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1
	123.12.12.141	13	IC 1

Você pode criar ICs individuais para ativos que têm o mesmo endereço IP para que possa identificá-los como ativos distintos. Iniciando de uma importação de dados recente, você pode atualizar seus ICs existentes com mais granularidade que inclua o identificador de partição de rede [network_partition_identifier] executando o trabalho programado, *`Update existing discovered items with network partition identifier`*.

Este trabalho programado está desabilitado por padrão. Ative este recurso para as integrações de ativos e vulnerabilidades fixas e abertas para Qualys Vulnerability Integration no Assistente de configuração para exibir este identificador em seus registros.

Tradução automática

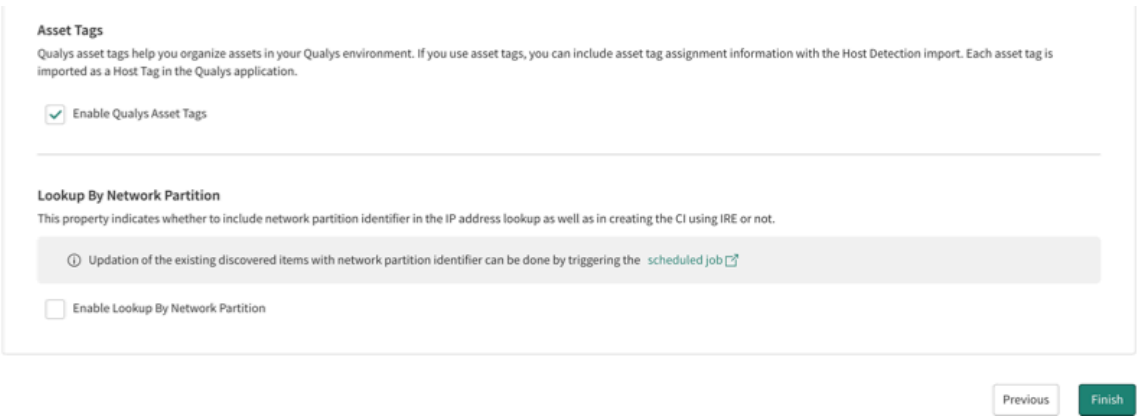
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Quando ativado, este trabalho programado adiciona o identificador de partição de rede [network_partition_identifier] aos registros de IC existentes a partir de dados importados. Os ICs existentes criados pelo IRE também são atualizados. O trabalho programado também cria ICs que incluem o identificador da partição de rede que começa com a próxima importação. Como alternativa, você pode iniciar o trabalho sob demanda para atualizar os dados existentes.

A partir da v14.0 de Vulnerability Response e v12.1 da Qualys Vulnerability Integration Integração de vulnerabilidade, os CMDB CI Class Models (1.0.21.) são compatíveis. Os modelos de classe têm o identificador de partição de rede [network_partition_identifier] nas regras de identificação de Identificação e Reconciliação (IRE).

Procedimento

1. Navegar até **Vulnerability Response** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
2. Escolha Qualys Vulnerability Integration.
3. **Edite** a integração necessária.
4. Escolher **Configuração de Detecção de Host**.
5. Escolher **Habilitar pesquisa por partição de rede** caixa de seleção do **Pesquisa por partição de rede**



seção.

6. Clique em **Concluir**.

Identificadores de partição de rede NETWORK_ID e REPOSITORY _ID incluídos na pesquisa de IP e na criação de IC

Origem	Endereço IP	NETWORK_Identifi	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Qualys Vulnerability Integration: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1	IC 1
	123.12.12.141	03713	IC 1	IC 2

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Origem	Endereço IP	REPOSITÓRIO_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Qualys: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1	IC 1
	123.12.12.141	13	IC 1	IC 2

As regras de pesquisa de identificação de IC de endereço IP e endereço IP incompleto incluem o atributo do identificador de partição de rede automaticamente para uma importação de dados das integrações de ativos e vulnerabilidades fixas e abertas para Qualys Vulnerability Integration.

Depois de ativar o trabalho programado e salvar os registros, você pode atualizar os itens descobertos existentes com ICs que incluem o identificador de partição de rede iniciando trabalhos programados sob demanda. Os ICs no item descoberto existente, no item vulnerável e nos registros de detecção são atualizados automaticamente.

Definir parâmetros de filtro adicionais para importações de Qualys

Personalize os parâmetros de filtragem das suas consultas programadas com Qualys Vulnerability Integration para ajudar a refinar ainda mais os dados de vulnerabilidade importados com as integrações Qualys compatíveis.

Antes de Iniciar

Casos de uso: como gerente ou analista de vulnerabilidade, convém filtrar os dados de suas consultas para que você possa revisar somente os detalhes específicos da vulnerabilidade. Por exemplo, digamos que você queira exibir vulnerabilidades importadas que são filtradas por IPs ou intervalos de IP específicos. Ou você deseja importar somente máquinas que estão no seu escopo, por exemplo, somente máquinas em sua rede corporativa que não sejam dispositivos externos.

Para ajudá-lo a coletar esses dados, você pode adicionar parâmetros Qualys para ajudá-lo a importar os detalhes da vulnerabilidade específica de que precisa.

Sem adicionar chamadas de API ou codificação adicionais, este recurso permite que você personalize suas informações de solicitação HTTP com parâmetros Qualys em seu Now Platform. Você modifica ou adiciona esses valores ao registro do método HTTP no método REST para as integrações Qualys compatíveis do Qualys Vulnerability Integration.

Função necessária: sn_vul.vulnerability_admin

Procedimento

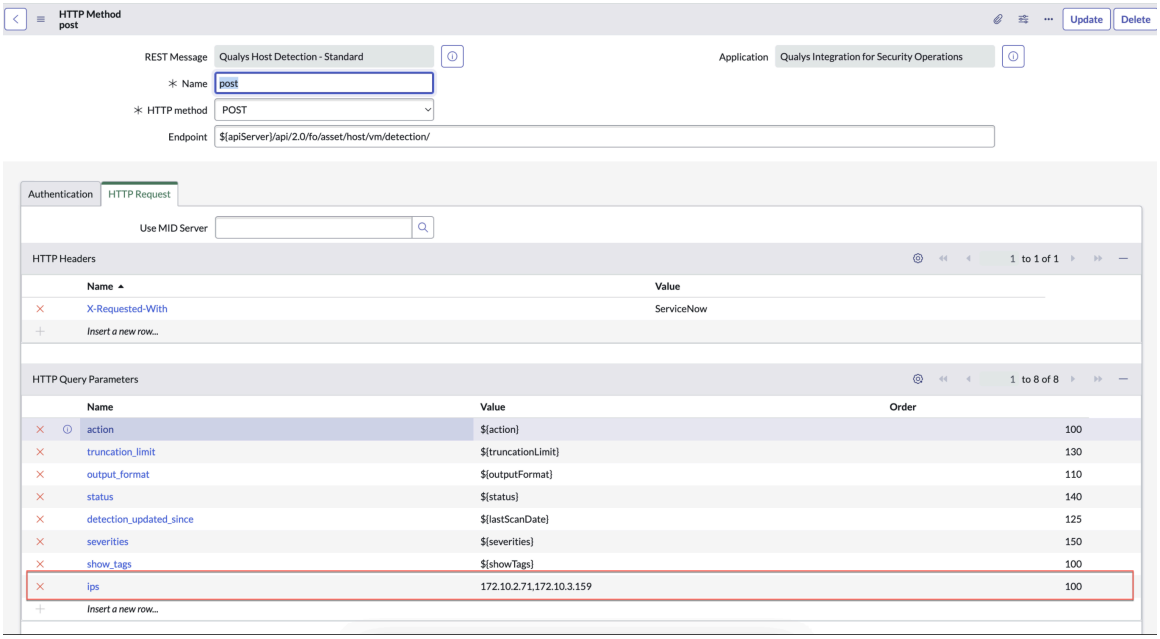
1. Localize os parâmetros compatíveis com o produto Qualys no site do desenvolvedor que você deseja usar para sua filtragem.
   Os parâmetros e valores inseridos no produto Qualys são compatíveis somente no nível da instância de integração em seu Now Platform. Todas as integrações Qualys são compatíveis com filtragem usando parâmetros de consulta.
2. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
3. Na página da lista de integrações Qualys, clique no registro da integração que você deseja abrir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Com a guia Qualys Detalhes REST selecionada, localize e clique no ícone de informações (I) do método REST, seguido por **Abrir registro** para abrir o registro do método HTTP.
5. Selecione a guia **Solicitação HTTP**.
6. Nos Parâmetros de consulta HTTP do corpo da solicitação, adicione os valores obtidos do site do desenvolvedor Qualys.

   Na imagem a seguir, como exemplo, o parâmetro que ingere somente determinados endereços IP/intervalos, *`ips={value}`* foi adicionado. Nesse caso, o **valor** é um ou mais IPs/intervalos que você especificar. Várias entradas são separadas por vírgulas, 172.10.2.71, 172.10.3.159e um intervalo é especificado com um hífen, 10.10.10.1-10.10.10.100. Consulte o site do desenvolvedor Qualys para obter mais informações.



   Se você quiser inserir mais de um parâmetro, consulte a documentação Qualys para obter mais informações sobre como separar cada valor.

   Nota:
   Você deve estar ciente de seus requisitos de API. Talvez você precise adicionar essas propriedades de API aos Parâmetros de consulta ou ao conteúdo do corpo.

   Alguns outros parâmetros que você pode achar úteis no site do desenvolvedor Qualys :

   - *`ag_ids`* - IDs da lista do grupo de ativos a serem recuperados. Este parâmetro garante que somente máquinas no seu escopo sejam trazidas.
   - *`qids`* - Este parâmetro limita os resultados a somente determinadas vulnerabilidades (QID na tabela de entrada de terceiros). Esta configuração evita a sobrecarga do sistema com registros informativos.
7. Clique em **Atualizar**.

Resolvendo Qualys problemas de integração de vulnerabilidade

Alguns problemas comumente encontrados, junto com soluções alternativas, são discutidos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Anexos não exibidos após a importação

Se os anexos não estiverem aparecendo conforme o esperado para as fontes de dados ou em um incidente de segurança após as importações de integração de terceiros, verifique as restrições de IP.

As restrições de acesso IP podem impedir que os anexos sejam vistos, a menos que você esteja conectado a partir de um IP seguro. Como um novo anexo é adicionado a cada importação, isso pode resultar em duplicatas que você precisa remover.

Por exemplo, ao executar uma integração de importação de host de terceiros, se você não vir nenhum anexo em suas fontes de dados, verifique as restrições de IP e adicione usuários à lista segura antes da importação.

Modificar mapas de transformação

Os mapas de transformação são fornecidos com configurações de base e geralmente são suficientes. Você pode modificar os mapeamentos de transformação, dependendo das necessidades da sua organização.

Antes de Iniciar

Função necessária: sn_vul_qualys.admin + import_admin

Procedimento

1. Navegar até **Todos** > **Conjuntos de importação do sistema** > **Administração** > **Mapas de transformação** para exibir as mensagens REST.
2. Filtre a lista resultante por aplicação e limite a lista à aplicação **Qualys Vulnerability Integration**.
3. Modifique os mapas de transformação de acordo com os requisitos do cliente.

   Para obter detalhes sobre os dados fornecidos pela API Qualys, consulte a documentação da API Qualys .

Verificar o tamanho da propriedade do anexo XML

Verifica se a propriedade de anexo XML é suficiente para arquivos grandes.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Propriedades do sistema** > **Importação/Exportação**.
2. Rolar para baixo até **Propriedades de importação** > **Formato XML** na parte inferior da página.

3. Se necessário, altere o valor para 250 e clique em **Salvar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Propriedades do sistema disponíveis

Limitações de recuperação de dados

Por padrão, não há restrições sobre como os dados são recuperados do Qualys. Muitos registros podem estar relacionados a vulnerabilidades de baixa severidade que um cliente não está disposto a corrigir usando seu processo de resposta de vulnerabilidade. Atualizar os parâmetros de mensagem/método REST correspondentes pode modificar esse comportamento.

A mensagem/método REST responsável por esta atualização é **Qualys Host Detection – Standard/post**. Para atualizar os valores, adicione um novo parâmetro de consulta HTTP ao método post com os seguintes valores:

- Nome: severities
- Valor: 3-5 (ou quaisquer gravidades apropriadas desejadas)

A Integração da Base de Conhecimento da Qualys está falhando

Resolver Qualys falha de integração da base de conhecimento reduzindo o tamanho do anexo da carga recebida de Qualys para o limite especificado.

Antes de Iniciar

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Certifique-se de que o tamanho do anexo da carga esteja dentro do limite especificado.
   a. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração**.
   b. Selecione a guia **Parâmetros de instância de integração**.
   c. Selecione **max_delta_days** e modifique o valor padrão para 3.
2. Se a integração ainda falhar, execute as seguintes etapas:
   a. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias**.
   b. Selecione **Base de conhecimento da Qualys**.
   c. Selecione a guia **Detalhes da integração**.
   d. No campo **Hora** de início, selecione a data atual para ignorar a execução da execução desse dia.
   e. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Instâncias de Integração**.
   f. Selecione a guia **Parâmetros de instância de integração**.
   g. Selecione **kb_backfill_full_import** e modifique o valor padrão para verdadeiro.

Resultado

Executar a integração do Qualys Knowledge Base Backfill atualiza todas as entradas de terceiros (TPEs) no sistema. Enquanto a integração de detecção de host da Qualys cria uma entrada de espaço reservado, a integração de preenchimento da base de conhecimento da Qualys a atualiza.

Qualys gráfico de status de execução de integração

O módulo Qualys Status de execução de integração é uma exibição gráfica do status de Qualys execuções de integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para exibir o status das execuções de integração, navegue até **Integração de Vulnerabilidade da Qualys** > **Status da Execução da Integração**.

A partir da versão 19.0 do Vulnerability Response, este painel está disponível na IU da nova experiência.

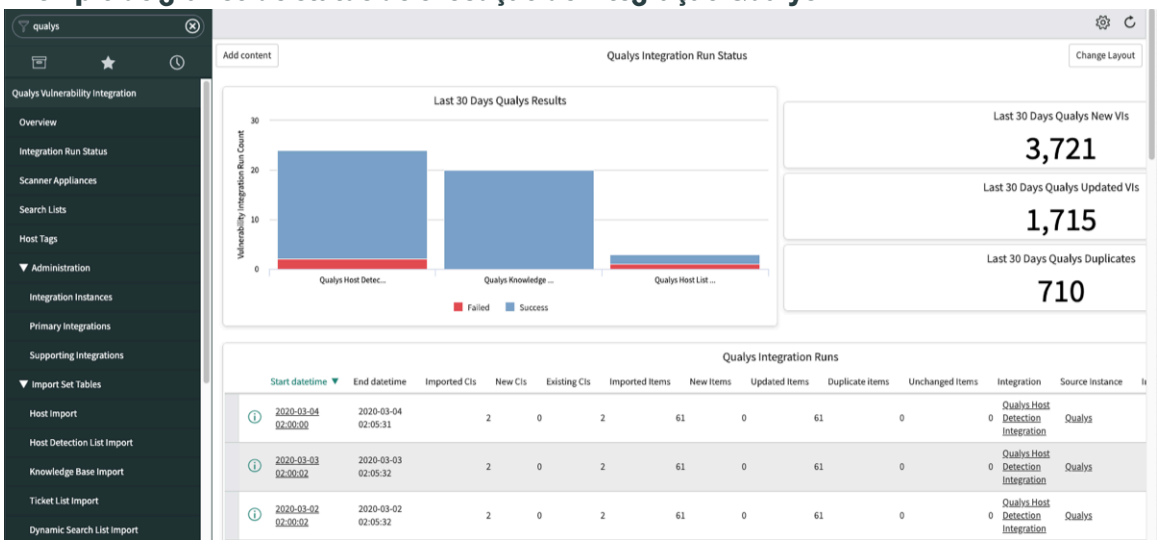
Nota:
Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

No gráfico, aponte para qualquer parte (barra, pizza, ponto de dados e assim por diante) para exibir dados gerais específicos dessa parte. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

O Qualys Status de execução de integração exibe o status de execução da integração de vulnerabilidade nos últimos 30 dias. A contagem de IVs atualizados da Qualys[qualys] indica a contagem de detecções exclusivas no mesmo ativo. O IV é atualizado com a nova detecção.

Nota:
A contagem de execuções de integração de vulnerabilidade é exibida somente para as integrações, que estão definidas para o estado ativo. Navegar até **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias** e defina o estado como ativo.

Exemplo de gráfico de status de execução de integração Qualys



- Os valores na coluna Itens importados representam o número total de registros que são criados a partir de uma execução de integração.
- A coluna Novos itens exibe o número de registros que são criados a partir de uma execução de integração.
- A coluna Itens duplicados não está mais preenchida. Você pode preferir remover esta coluna da exibição.
- A coluna Itens atualizados exibe o número de vezes que os registros são atualizados durante uma execução de integração. Este valor não é o número de registros exclusivos que são atualizados. Se, por exemplo, um registro for atualizado duas vezes durante

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a execução da integração, ele será contado duas vezes e exibido como dois itens atualizados.

- A coluna Itens inalterados exibe registros encontrados durante a execução da integração que já existem no banco de dados, mas não foram atualizados, porque nenhum dos valores de campo relevantes foi alterado.

Nota:
A integração é executada com resultados zero para todos os quatro valores a seguir: **Novos ICs**, **ICs existentes**, **Novos itens**e **Itens atualizados** são filtrados da lista de execuções de **integração da Qualys**.

Qualys relatórios de gráfico de status de execução de integração

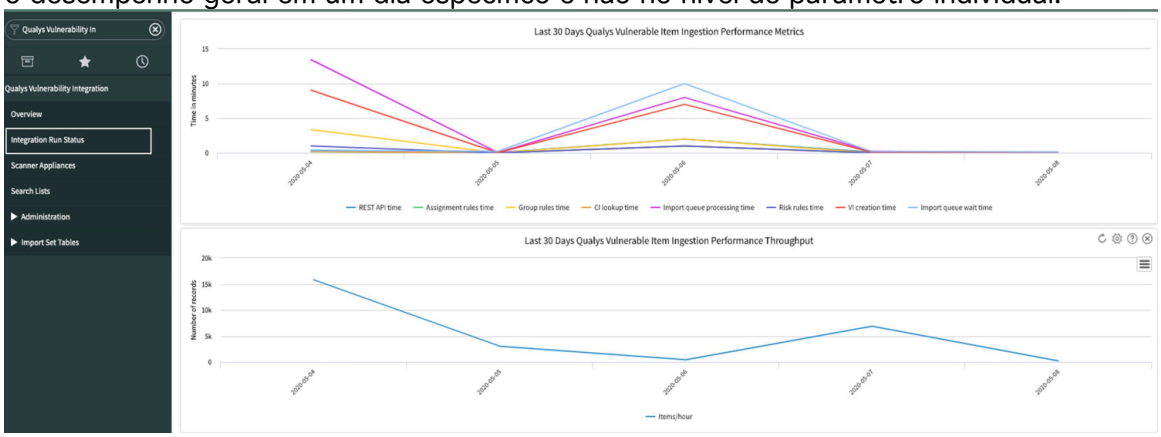
Nome	Descrição
Resultados dos últimos 30 dias Qualys	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Executar em um visual de barra.
Últimos 30 dias Qualys Novos IVs	O número de novos registros importados nos últimos 30 dias. Mostrado como um número inteiro.
IVs atualizados nos últimos 30 dias Qualys	O número de registros atualizados importados nos últimos 30 dias. Mostrado como um número inteiro.
Últimos 30 dias Qualys Duplicatas	O número de registros duplicados importados nos últimos 30 dias. Mostrado como um número inteiro.
Qualys Execuções de integração	Os registros de execução de integração em uma lista. **Nota:** **V16.1:** para verificar as detecções para esta integração, compare as detecções ou descobertas com os dados de detecção ServiceNow`sn_vul_detection`] na tabela . Enquanto a integração está em andamento, pode haver uma mudança na detecção ou na contagem de descobertas. Este relatório exibe a contagem de detecções na coluna "Contagem até a data" na instância, após a conclusão da execução da integração.
Últimos 30 dias Qualys Métricas de desempenho de ingestão de item vulnerável	Métricas de desempenho diárias para itens vulneráveis comparadas nos últimos 30 dias.
Últimos 30 dias Qualys Rendimento do desempenho de ingestão de item vulnerável	Rendimento diário de ingestão de item vulnerável medido para a integração de detecção de host Qualys nos últimos 30 dias.

Vários fatores podem afetar o desempenho da execução da integração, como a quantidade de dados e o tempo necessário para processar esses dados. Dois gráficos comparam as métricas de desempenho:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Qualys Métricas de desempenho de ingestão de item vulnerável: compare as métricas de desempenho diárias para regras de atribuição, regras de grupo, regras de risco, tempo de espera da fila, tempo de processamento da fila e outras estatísticas de itens vulneráveis nos últimos 30 dias para identificar a causa de quaisquer desvios no desempenho. O desempenho é calculado com base no tempo gasto em cada atividade. Esses parâmetros são calculados e associados no nível de execução da integração. Cada parâmetro é codificado por cor para facilitar a identificação.
- Qualys Rendimento de desempenho de ingestão de item vulnerável: compare o rendimento de ingestão de item vulnerável diário para a integração de detecção de host Qualys. O rendimento é medido em itens por hora. Este relatório mostra o desempenho geral em um dia específico e não no nível de parâmetro individual.



Mensagens REST da Qualys

As mensagens REST da Qualys são usadas para fazer chamadas para a API Qualys para buscar os dados de conformidade.

As mensagens REST a seguir são enviadas com o sistema de base.

Mensagem REST de políticas de PC da Qualys

A mensagem REST de Políticas de PC da Qualys recupera dados de política da Qualys. As mudanças no registro do método de mensagem REST afetam a solicitação feita à Qualys para recuperar informações de política.

Parâmetros de mensagem REST de políticas de PC da Qualys

Nome do parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório.
detalhes	Todos	Indica o nível de detalhe mostrado para as políticas recuperadas. É seguro modificar de acordo com seus requisitos.

Mensagem REST de controles de PC da Qualys

A mensagem REST de controles de PC da Qualys recupera informações de controles de conformidade para diferentes IDs de controle da Qualys.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros de mensagem REST de controles de PC da Qualys

Nome do parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório.
detalhes	Todos	Indica o nível de detalhe mostrado para os controles recuperados. É seguro modificar de acordo com seus requisitos.

Mensagem REST de detalhes das políticas de PC da Qualys

A mensagem REST de detalhes de políticas de PC da Qualys recupera os detalhes completos da política, como tecnologias e seções.

Parâmetros de mensagem REST de detalhe de políticas de PC da Qualys

Parâmetro	Valor	Descrição
ação	lista	Indica o tipo de operação que está sendo solicitada. Parâmetro obrigatório.
mostrar_usuário_controles	Booliano	• Defina como 1 para incluir controles definidos pelo usuário (UDCs) na saída XML. • Quando não especificado, os UDCs não são incluídos. Este é um parâmetro opcional. É seguro modificar de acordo com seus requisitos.
mostrar_apêndice	Booliano	(Opcional) Defina como 1 para mostrar a seção do apêndice na saída XML. Quando não especificado.

Mensagem REST de resultados de PC da Qualys

A mensagem REST Resultados de PC da Qualys recupera registros de postura de conformidade da Qualys.

Parâmetros da mensagem REST de resultados de PC da Qualys

Campo de origem	Valor	Descrição
ação	lista	Indica o tipo de operação solicitada. Parâmetro obrigatório. Mudanças não são recomendadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Parâmetros da mensagem REST de resultados de PC da Qualys

Campo de origem	Valor	Descrição
show_extended_evidence	Booliano	• Defina como 1 para mostrar as informações de evidência estendidas na saída. • Definido como 0 ou quando não especificado, as informações de evidência estendida não são mostradas na saída. **Nota:** • Você não pode especificar `show_extended_evidence=1` na mesma solicitação que `hide_evidence=1`. Isso resulta em um erro. A evidência estendida faz parte dos dados de evidência e é mostrada somente quando os dados de evidência são mostrados. • Este parâmetro não é enviado com o sistema de base.
cause_of_failure	Booliano	Se você passar "1", o Qualys retornará a causa da falha. Se você passar "0", o Qualys não retornará esses atributos. **Nota:** Este parâmetro não é enviado com o sistema de base.
policy_id		Mostra registros de informações de postura de conformidade para uma política especificada. É necessário um ID de política válido.
detalhes	Todos	Indica o nível de detalhe mostrado para posturas recuperadas. É seguro modificar de acordo com seus requisitos.
show_remediation_info		(Opcional) Defina como 1 para mostrar informações de correção na saída XML ou CSV. Por padrão, a saída não inclui as informações de correção. Quando não especificadas, as informações de correção não são incluídas na saída.

Mensagem REST de integração de host de política de PCRS da Qualys

A integração de host de política Qualys PCRS recupera dados de host da Qualys e os processa em sua instância.

Parâmetros de mensagem REST de integração de host de política de PCRS da Qualys

Nome do parâmetro	Valor	Descrição
policyId	${lastRunDatetime}	IDs de política para avaliação de conformidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integração de resultados de testes de PCRS da Qualys

A tabela mostra os parâmetros de solicitação enviados.

Parâmetros da mensagem REST de integração de resultados de testes de PCRS da Qualys

Nome do parâmetro	Valor	Descrição
evidência necessária	${lastRunDatetime}	• O valor padrão é 0, o que indica que os dados de evidência não serão recuperados para a postura do host. • Defina o valor como 1 para recuperar os dados de evidência. **Nota:** Alterar o valor para 1 aumenta o tempo necessário para buscar dados de postura.
compactação necessária		• O valor padrão é 1, o que indica que a saída será compactada. • Defina o valor como 0 se você não quiser que os dados sejam compactados. **Nota:** Não compactar os dados aumenta o tempo necessário para buscar dados de postura.

Noções básicas sobre a integração de vulnerabilidade da Tenable

A aplicação Integração do Vulnerability Response com Tenable desenvolvida pela engenharia ServiceNow para o Tenable Vulnerability Integration usa dados importados dos produtos Tenable.io e Tenable.sc para ajudar você a priorizar e corrigir vulnerabilidades de seus ativos. A aplicação está disponível com uma assinatura separada do ServiceNow® Store.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

A integração de vulnerabilidade da Tenable emprega duas integrações da Tenable, Tenable.io e Tenable.sc, para importar dados do scanner de terceiros sobre seus ativos e vulnerabilidades. A aplicação Integração do Vulnerability Response com Tenable oferece suporte ao produto Tenable.sc a partir da versão 5.13.

Tradução automática

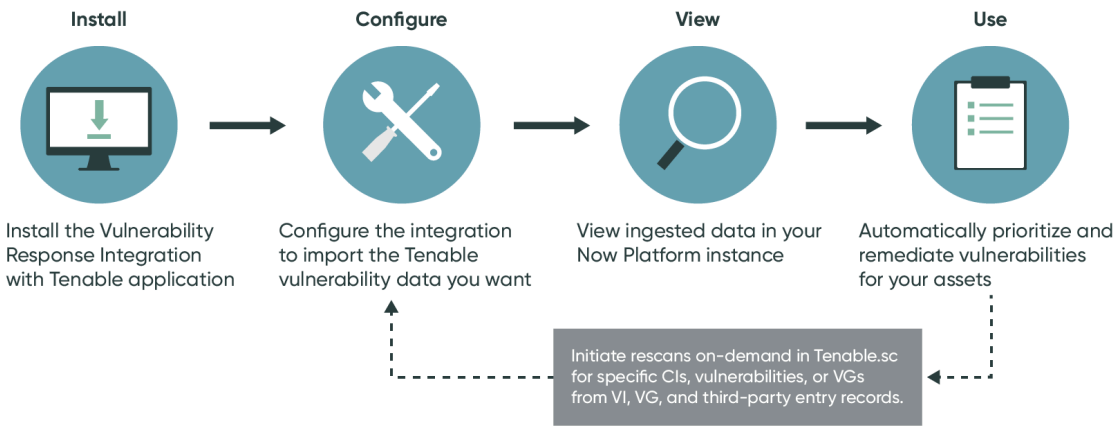
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Tenable.io é uma integração empresarial baseada em nuvem.
- Tenable.sc é uma integração no local que oferece a opção de usar um MID Server se o produto Tenable.sc e sua instância Now Platform estiverem no mesmo ambiente.
- Se o produto Tenable.sc e sua instância Now Platform não estiverem no mesmo ambiente, você precisará usar um MID Server.

A aplicação Integração do Vulnerability Response com Tenable está disponível no ServiceNow Store com uma assinatura separada.

Para obter listas e descrições das integrações no Tenable Vulnerability Integration, consulte Tenable.io integrações com as aplicações Vulnerability Response e Configuration Compliance e Tenable.sc integrações com a aplicação Vulnerability Response.

Integração de vulnerabilidade Tenable



Versões disponíveis para Washington DC

Versão de lançamento	Notas de versão
Integração do Vulnerability Response com Tenable v3.5, v3.6	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão

Termos e principais recursos das integrações

Itens vulneráveis e vulnerabilidades

Um item vulnerável é criado na sua instância Now Platform quando:

- Uma vulnerabilidade importada de um scanner de terceiros é correspondida a um ativo existente (um item de configuração em CMDB). O produto Tenable se refere a essas correspondências como **vulnerabilidades**.
- Uma vulnerabilidade importada de um scanner de terceiros não corresponde a um ativo existente no seu CMDB. Nesse caso, um IC incompatível também é criado junto com um item vulnerável.

  Para ICs incompatíveis, você também pode usar o Mecanismo de Identificação e Reconciliação (IRE) para criar ICs em duas novas classes

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

quando um IC existente não puder ser correspondido com um host. Caso contrário, ICs incompatíveis serão criados nas classes de IC incompatíveis. Para obter mais informações, consulte Criando ICs para Vulnerability Response usando o mecanismo de Identificação e Reconciliação.

Entradas de vulnerabilidade de terceiros e plug-ins

As entradas de vulnerabilidade de terceiros são importadas de scanners de terceiros e listadas na tabela Entradas de vulnerabilidade de terceiros na sua instância Now Platform. As entradas de vulnerabilidade de terceiros da Tenable são ingeridas em Vulnerability Response e correspondidas aos ativos existentes listados em CMDB. A Tenable se refere às entradas de vulnerabilidade de terceiros como plug- **ins**.

IC (Configuration Item, item de configuração)

Itens de configuração são os ativos existentes listados em seu CMDB.

Item descoberto

Os ativos ingeridos da importação de ativos da Tenable são correspondidos aos itens de configuração existentes em seu CMDB. Os ativos importados são atualizados.

Se uma correspondência não for encontrada, um IC será criado na classe de IC incompatível do CMDB. Se o plug-in CMDB CI Class Models estiver habilitado, o Mecanismo de Identificação e Reconciliação (IRE) criará novos ICs usando novas classes. Para obter mais informações, consulte Criando ICs para Vulnerability Response usando o mecanismo de Identificação e Reconciliação. Se o IC original incompatível for reclassificado, os registros de item descoberto serão atualizados para refletir o estado. Os itens descobertos fornecem visibilidade de como os ativos são identificados e mapeados para ICs no CMDB.

Regras de pesquisa de IC

Quando os dados são importados de uma integração de terceiros, o Vulnerability Response usa automaticamente os dados do host (ativo) para pesquisar correspondências no Configuration Management Database (CMDB). As regras de pesquisa de IC são usadas para identificar ICs e adicioná-los aos registros de IV quando os IVs são criados para ajudá-lo na correção.

Nova verificação e verificação de correção

Você pode iniciar um comando de nova verificação direcionado em um item de configuração específico, grupo de vulnerabilidade ou entrada de terceiros diretamente do item vulnerável, tarefa de correção e registros de entrada de vulnerabilidade de terceiros em sua instância Now Platform. A Tenable se refere a esta nova verificação como uma **verificação de correção**.

Fechar automaticamente IVs mais antigos

Com o módulo Fechar automaticamente itens vulneráveis obsoletos no seu Now Platform, você pode limpar itens vulneráveis (IV) obsoletos que não foram encontrados recentemente por suas integrações de terceiros. Mover esses IVs para **Encerrado** ajuda a reduzir o número de itens vulneráveis ativos e tarefas de correção e reconciliar ativos em seu CMDB. Você pode usar todas as integrações com Integração do Vulnerability Response com Tenable para fechar automaticamente IVs obsoletos.

Instância

Este termo se refere a uma ocorrência distinta da sua aplicação Now Platform®.

Integração

Uma integração é uma referência específica de produto para uma integração, como a Tenable.io Integração de ativos ou a Tenable.sc Integração de plug-in. Essas são as integrações separadas que pertencem a produtos específicos da Tenable na integração de vulnerabilidade da Tenable em sua instância.

Instância de integração

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este termo se refere às integrações separadas da Tenable listadas por seus produtos Tenable.io e Tenable.sc.

Implantação

Quando uma integração oferece suporte a várias origens, uma existência de integração única e distinta é chamada de implantação da sua integração. O termo é usado para se referir às integrações e produtos em seu ambiente. Por exemplo, você pode ter várias implantações de várias integrações dos produtos Tenable.io e Tenable.sc em seu ambiente.

As integrações Tenable.io e Tenable.sc também incluem os seguintes recursos principais:

- As descobertas da avaliação de configuração, ou seja, resultados de testes junto com políticas, testes de configuração (controles) e citações com fontes autorizadas podem ser importados para a aplicação Configuration Compliance com o produto Tenable.io. Consulte Tenable.io integrações com as aplicações Vulnerability Response e Configuration Compliance e Explorar o Configuration Compliance para obter mais informações sobre como esta integração funciona com a aplicação Configuration Compliance.
- A partir da v2.1 do Tenable Vulnerability Integration, crie itens de configuração (ICs) exclusivos que incluem diferentes identificadores de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. Identifique os ativos distintos em seu ambiente e atualize os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.
- Você pode programar quando deseja que os trabalhos sejam executados para todas as integrações Tenable.io e Tenable.sc. Você também pode executar trabalhos programados manualmente sob demanda.
- Para importações de ativo com Tenable.io, você pode habilitar etiquetas do ativo para organizar e rastrear os ativos listados em CMDB no ambiente Tenable.io.
- As integrações Tenable.io e Tenable.sc permitem que você configure Regras de pesquisa de IC para definir como os dados de ativo de fontes de terceiros são usados para identificar itens de configuração (ICs) em seu Now Platform CMDB.
- As integrações Tenable.io e Tenable.sc permitem que você defina filtros de importação na importação de vulnerabilidades para que você importe somente as vulnerabilidades desejadas da Tenable. Para Tenable.io, você tem a opção de importar vulnerabilidades **fixas** da Tenable com a importação de vulnerabilidades.
- Para Tenable.sc, você tem a opção de iniciar novas verificações sob demanda diretamente do item vulnerável, da tarefa de correção e dos registros de entrada de terceiros na sua instância Now Platform. Se os IVs tiverem sido transicionados para **Encerrado/Corrigido**, mas ainda não estiverem atualizados em sua instância, você poderá verificar se as vulnerabilidades em itens de configuração específicos foram corrigidas. Consulte Iniciar nova verificação para a integração Tenable.sc.

As seções a seguir listam mais detalhes sobre as integrações da Tenable.

Funções necessárias de Now Platform

As tarefas de integração exigem as seguintes funções na sua instância Now Platform.

admin

O administrador do sistema usa o Assistente de configuração para instalar a aplicação Integração do Vulnerability Response com Tenable. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração.

sn_vul.vulnerability_admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois de atribuído, o administrador de vulnerabilidade conclui a configuração das integrações da Tenable no Assistente de configuração. Esta função tem acesso completo à aplicação Vulnerability Response (VR) e seus registros. O administrador de vulnerabilidades configura todas as aplicações de VR e regras para integrações de terceiros instaladas.

sn_vul_tenable.configure_integration

Esta função contém a função granular sn_vul_tenable.read_integration e os usuários com esta função podem configurar a aplicação Integração do Vulnerability Response com Tenable.

sn_vul_tenable.read_integration

Usuários com essas funções podem exibir (ler), mas não editar registros da aplicação Integração do Vulnerability Response com Tenable.

Grupo do Vulnerability Response

Por padrão, o grupo do Vulnerability Response está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Vulnerability Response herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente.

Itens vulneráveis

Os itens vulneráveis são agrupados em tarefas de correção de acordo com as regras do grupo e atribuídos para correção com base nas regras de atribuição. Para obter mais informações, consulte Vulnerability Response tarefas de correção e regras de tarefa visão geral e Vulnerability Response visão geral de regras de atribuição.

Regras de pesquisa de item de configuração (IC)

As Regras de Pesquisa de IC identificam ICs e determinam quando adicioná-los a um item vulnerável. Para obter mais informações sobre como funcionam as regras de pesquisa de IC, consulte Regras de pesquisa de IC para identificar itens de configuração de Vulnerability Response integrações de vulnerabilidade de terceiros.

Nota:
As regras, depois de removidas, não podem ser recuperadas. Em vez de remover as regras existentes, desabilite-as ao criar novas.

As regras de pesquisa Tenable.io a seguir são enviadas com o sistema de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- Nome do host
- DNS
- IP

As regras de pesquisa Tenable.sc a seguir são enviadas com o sistema de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Vários valores para ip_address, mac_address, fqdns e network_interfaces são usados para um ativo. Todos os valores são considerados nas regras de pesquisa de IC para correspondência. Todos os valores são usados para criar vários adaptadores de rede usando IRE.

Para obter mais informações sobre como configurar a categorização de recursos de nuvem incompatíveis em sua classe de IC preferencial, consulte Atualizando classe de IC para ativos de nuvem incompatíveis.

Novas propriedades para ignorar endereços IP

Em Tenable.io, há duas propriedades disponíveis se você quiser ignorar vários endereços IP ou vários endereços Mac como parte de suas regras de pesquisa de IC:

ignoreIPAddress

Uma lista de endereços IP a serem ignorados para pesquisa de IC e criação de IC.

ignoreMacAddress

Uma lista de endereços MAC a serem ignorados para pesquisa de IC ou criação de IC.

Itens descobertos

Este módulo lista os itens de configuração detectados durante a importação das integrações de item vulnerável da Tenable e das integrações de ativo da Tenable.

Nota:
O filtro padrão desta lista é definido como Incompatível. Você pode exibir todos os itens descobertos de uma importação removendo o filtro.

Para obter mais informações sobre o módulo Itens descobertos, consulte Itens Descobertos.

Etiquetas do ativo

As etiquetas do ativo (também conhecidas como etiquetas do host) são usadas para organizar e rastrear os ativos em sua organização. Você pode atribuir marcadores aos seus ativos. Em seguida, ao iniciar as verificações, você pode selecionar marcadores associados aos ativos que deseja verificar. O módulo Etiquetas do ativo permite que você baixe dados de etiqueta do ativo de Tenable.io para sua instância de forma programada. Os dados de ativo que incluem marcadores de ativo são extraídos de Tenable.io e transformados usando os mapas de transformação de integração Tenable.io Asset Transform.

Todas as etiquetas do ativo são importadas como parte da integração do ativo Tenable.io. As etiquetas do ativo geralmente são usadas para filtragem em regras de atribuição Vulnerability Response e regras de tarefa de correção. Os marcadores são exibidos no formulário Item descoberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Execute a integração de ativo Tenable.io antes de criar regras de atribuição Vulnerability Response ou regras de tarefa de correção na aplicação Vulnerability Response para que todos os marcadores estejam disponíveis para essas regras antes que os itens vulneráveis sejam importados e agrupados. Observe também os seguintes pontos sobre marcadores:

- O armazenamento de marcador não faz distinção entre maiúsculas e minúsculas. Por exemplo, se você criar um marcador para descrever ativos em seu local de San Diego e criar o marcador San Diego, também não poderá criar um marcador SAN DIEGO e armazená-lo na tabela Etiqueta do ativo. San Diego e SAN DIEGO são considerados a mesma etiqueta do ativo pelo sistema. O marcador que for importado primeiro será o marcador armazenado e reconhecido daqui em diante.
- Usar etiquetas do ativo como uma chave de grupo em uma regra de tarefa de correção pode ter resultados inesperados. As etiquetas do ativo devem ser usadas somente no Construtor de condição.
- As etiquetas do ativo são controladas pela propriedade do sistema global sn_vul.import_asset_tags. Esta propriedade é definida como verdadeira por padrão. Desabilitar os marcadores os desabilita em todas as Now Platform® instâncias.

Filtros de recuperação de dados

As configurações de recuperação de dados ajudam a determinar especificamente o tipo e o escopo dos dados que você deseja importar da aplicação Tenable para sua instância Now Platform®. Para obter uma lista das configurações usadas com mais frequência, consulte Configurações de recuperação de dados para a integração de vulnerabilidade da Tenable.

Classificação de prioridade de vulnerabilidade (VPR)

A classificação de prioridade de vulnerabilidade (VPR) é um atributo do produto Tenable que é importado e usado com uma nova calculadora de risco padrão em Vulnerability Response. A Regra de risco da Tenable é instalada com a aplicação Integração do Vulnerability Response com Tenable como parte da Calculadora de risco padrão nas Calculadoras de vulnerabilidade da Vulnerability Response.

Esta regra de risco está desabilitada por padrão.

Ao habilitar a regra da calculadora de risco da Tenable, os valores de VPR importados são usados para calcular a pontuação de risco dos itens vulneráveis. A distribuição de peso padrão para esta calculadora de risco: VPR = 70%, Ativo = 15% e Criticalidade dos negócios = 15%. Habilitar esta regra da Calculadora de risco da Tenable pode afetar o desempenho da ingestão de dados. Para obter mais informações sobre calculadoras Vulnerability Response e a regra da calculadora de risco da Tenable, consulte Vulnerability Response calculadoras e regras da calculadora de vulnerabilidade.

Instalação e configuração

Depois de baixar o Integração do Vulnerability Response com Tenable do ServiceNow® Store, a instalação e a configuração serão compatíveis com o Assistente de configuração em Vulnerability Response. Para obter mais informações, consulte Configuração de Vulnerability Response usando o Assistente de configuração.

Tenable.io integrações com as aplicações Vulnerability Response e Configuration Compliance

As integrações Integração do Vulnerability Response com TenableTenable.io na aplicação [] estão disponíveis nas aplicações Vulnerability Response e Configuration Compliance.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lista de Tenable.io integrações

Várias origens são compatíveis com todas as integrações Tenable.io e Tenable.sc. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente do Assistente de configuração em Vulnerability Response. Você também instala e configura a aplicação Integração do Vulnerability Response com Tenable no Assistente de configuração.

Tenable.io é uma integração empresarial baseada em nuvem. Consulte a tabela a seguir para obter os nomes e as descrições das integrações compatíveis com o produto Tenable.io.

A integração de resultados de conformidade Tenable.io e a integração de backfill de resultados de conformidade Tenable.io estão inativas por padrão.

Para ativá-los:

1. Navegar até **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
2. Na lista Integrações da Tenable, clique em um nome de integração para abrir o registro e marque a caixa de seleção **Ativo** para habilitá-lo. Você pode preferir deixar as configurações de programação em seus valores padrão para que essas integrações sejam iniciadas.

Integrações do Tenable.io

Integração	Descrição
Tenable.io Integração de ativos	• Recupera todos os dados do ativo, incluindo etiquetas do ativo, do produto Tenable.io e os processa em sua instância. • A partir da v3.0, se a integração de resultados de conformidade Tenable.io estiver ativada, você poderá importar dados de avaliação de configuração segura junto com os dados de ativos importados. Esses dados podem ajudar a identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API do ativo. • A saída desta integração são itens descobertos. • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. • A partir da v2.2, `Last Scan Time` é importado e atualizado somente para ativos que têm vulnerabilidades.
Tenable.io Integração de resultados de conformidade	• A partir da v3.0, os dados de avaliação de configuração segura importados da Integração de resultados de conformidade junto com os dados importados

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	da Integração de ativos podem ajudar a identificar e responder às vulnerabilidades relacionadas à configuração em seus ativos. • Se habilitado, recupera dados de avaliação de configuração segura de alto nível e os processa em sua instância Now Platform. Os dados importados incluem resultados de testes junto com políticas, testes de configuração (controles) e citações com fontes autorizadas. • Os dados de avaliação para ativos ausentes ou ativos sem IDs de ativo não são importados. • Se um resultado de teste for importado e o ativo correspondente não puder ser correspondido em sua instância, o resultado do teste será ignorado e o ID do ativo ausente será armazenado em um registro temporário na tabela [sn_vul_tenable_missing_asset]. • O valor total de ativos ignorados (ausentes) está listado no campo **ICs ignorados** na guia **Configuração** no registro de execução da integração para esta integração.
Tenable.io Compliance Results Backfill Integration	• Quando ativada, essa integração é executada automaticamente depois que a integração de ativos é concluída com sucesso como parte de uma execução de integração encadeada. Esta integração corresponde aos dados de avaliação de configuração com os ativos ausentes listados na tabela [sn_vul_tenable_missing_asset]. • Importa até 200 IDs de ativo para todos os ativos ausentes descobertos ou presentes na instância após a conclusão bem-sucedida da importação de integração de ativos. • Remove os registros temporários da tabela [sn_vul_tenable_missing_asset] quando os ativos podem ser correspondidos com os dados de avaliação de configuração correspondentes.
Tenable.io Integração de credencial de verificação	• Esta integração recupera as credenciais de verificação configuradas em Tenable.io. • Coordena as chamadas de mensagem REST para a API de credenciais. • A saída desta integração são as credenciais de verificação preenchidas na tabela [sn_vul_tenable_scan_credential],.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	• As credenciais importadas são usadas para acessar o scanner quando as solicitações de verificação são iniciadas a partir do Now Platform. • Esta integração está programada para ser executada semanalmente.
Tenable.io Integração de modelo	Um registro de modelo é enviado para Tenable.io durante a nova verificação. Esta integração recupera credenciais Tenable.io disponíveis para usar em novas verificações. As credenciais são específicas da instância e um único registro de modelo é importado e armazenado com segurança temporariamente na tabela [sn_vul_tenable_io_template].
Tenable.io Integração de plug-in	• Recupera os dados do plug-in do produto Tenable.io. Os dados recuperados são baseados na data em que os plug-ins foram atualizados pela última vez por uma Tenable.io execução de integração. • Esta importação garante que os identificadores Tenable.io (Dez IDs) sejam atuais. • Coordena as chamadas de mensagem REST para a API do plug-in. • A saída desta integração são as vulnerabilidades de terceiros.
Tenable.io Integração de vulnerabilidades corrigidas	• Recupera dados de vulnerabilidade com base em filtros de severidade do produto Tenable.io e os processa em sua instância. Itens vulneráveis são criados para registros de detecção que estão nos estados **Aberto** e **Reaberto**, porque esses registros exigem correção. Os itens vulneráveis existentes serão atualizados pelo Vulnerability Response se as detecções forem **Corrigidas**, mas os itens vulneráveis não serão criados para detecções **Corrigidas** por padrão, porque a Tenable considera as vulnerabilidades **CorrigidasMitigadas**. • Quando o sinalizador **Criar horários vulneráveis para detecções de vulnerabilidade fixa** é ativado no Assistente de configuração, novos IVs são criados no estado **Fixo** para que você tenha visibilidade das detecções que os criaram. Como os IVs são criados para detecções **fixas** que ainda não existem em sua instância, isso pode afetar negativamente o desempenho da importação. Você pode preferir deixar este recurso desativado para que as detecções **fixas** atualizem somente os estados dos itens vulneráveis existentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	• Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração é Itens vulneráveis (IVs) **encerrados/corrigidos**. Ele também cria ativos e entradas de terceiros se eles não existirem. • Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. Esta execução de integração está programada. É uma integração encadeada, o que significa que, após a conclusão bem-sucedida de uma execução, a integração de vulnerabilidades em aberto descrita abaixo é acionada. A partir do Tenable v3.3, você pode exibir as seguintes informações das execuções de integração de vulnerabilidade: • **Total de partes:** número total de partes geradas pela Tenable • **Blocos disponíveis:** número de blocos disponíveis para download para ServiceNow
Tenable.io Abrir integração de vulnerabilidades	• Esta integração é acionada após a conclusão bem-sucedida da Tenable.io Integração de vulnerabilidades fixas. • Recupera dados de vulnerabilidade com base nos filtros de severidade do produto Tenable.io e os processa em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração são itens vulneráveis (IVs) **novos/reabertos**. Ele também cria itens de configuração e entradas de terceiros se eles não existirem. A Tenable considera as vulnerabilidades ativas como **cumulativas** (atuais).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.io

Integração	Descrição
	• Os dados são importados em blocos e armazenados na tabela [sn_vul_tenable_chunk_status]. O limpador de tabela remove automaticamente os dados armazenados desta tabela após 30 dias. A partir do Tenable v3.3, você pode exibir as seguintes informações das execuções de integração de vulnerabilidade: • **Total de partes:** número total de partes geradas pela Tenable • **Blocos disponíveis:** número de blocos disponíveis para download para ServiceNow

Tenable.sc integrações com a aplicação Vulnerability Response

As integrações Integração do Vulnerability Response com TenableTenable.sc na aplicação [].

Começando com Vulnerability Response v20.0, se um ativo for verificado por um agente, a coluna Agente existente exibirá o valor, verdadeiro na lista de itens descobertos, o que indica que é uma verificação autentica.

Lista de Tenable.sc integrações

Várias origens são compatíveis com todas as integrações Tenable.io e Tenable.sc. Você pode adicionar e implantar várias instâncias das seguintes integrações em seu ambiente do Assistente de configuração em Vulnerability Response. Você também instala e configura a aplicação Integração do Vulnerability Response com Tenable no Assistente de configuração.

- Tenable.sc é uma integração no local que oferece a opção de usar um MID Server se o produto Tenable.sc e sua instância Now Platform estiverem no mesmo ambiente.
- Se o produto Tenable.sc e sua instância Now Platform não estiverem no mesmo ambiente, você precisará usar um MID Server.

Integrações do Tenable.sc

Integração	Descrição
Tenable.sc Integração de ativos	Para evitar a criação de itens descobertos duplicados com dados de ativo importados, a integração de ativo do produto Tenable.sc é composta por duas integrações. **A Tenable.sc Open Assets Integration** Esta integração importa dados de vulnerabilidade sobre seus ativos que a Tenable considera **Cumulativos** (atuais) ou **Abertos**. Os itens vulneráveis (IVs) criados em sua instância com esses dados de ativo importados são considerados abertos, ou seja, no estado **Aberto**. Esses itens vulneráveis requerem investigação e podem precisar de correção. **A Tenable.sc Integração de ativos fixos**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	Esta integração importa dados de vulnerabilidade sobre seus ativos que a Tenable considera **Atenuados** (não mais vulneráveis) ou **Corrigidos**. Os itens vulneráveis desses ativos passam do estado **Aberto** para o estado **Encerrado/Corrigido** em sua instância, pois os resultados das verificações mostram que eles não estão mais vulneráveis. • Recupera todos os dados de ativo do produto Tenable.sc e os processa em sua instância. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de ativos. • A saída desta integração são itens descobertos. • O filtro de consulta da Tenable selecionado no Assistente de configuração também se aplica à Integração de ativos Tenable.sc. Somente os ativos com as vulnerabilidades que correspondem às condições do filtro de consulta são importados.
Tenable.sc Integração de plug-in	• Recupera os dados do plug-in do produto Tenable.sc. Os dados recuperados são baseados na data em que os plug-ins foram atualizados pela última vez por uma Tenable.sc execução de integração. • Essa importação garante que os Tenable.sc Identificadores (Dez IDs) sejam atuais e que somente as vulnerabilidades ativas sejam importadas. • Coordena as chamadas de mensagem REST para a API de plug-ins. • A saída desta integração são as vulnerabilidades de terceiros.
Tenable.sc Integração de vulnerabilidades corrigidas	• Recupera dados de vulnerabilidade com base em filtros de severidade do produto Tenable.sc e os processa em sua instância. Itens vulneráveis são criados para registros de detecção que estão nos estados **Aberto** e **Reaberto**, porque esses registros exigem correção. Os itens vulneráveis existentes serão atualizados pelo Vulnerability Response se as detecções forem **Corrigidas**, mas os itens vulneráveis não serão criados para detecções **Corrigidas** por padrão, porque a Tenable considera as vulnerabilidades **CorrigidasMitigadas**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	• Quando o sinalizador **Criar horários vulneráveis para detecções de vulnerabilidade fixa** é ativado no Assistente de configuração, ele cria novos IVs no estado **Fixo** para que você tenha visibilidade das detecções que os criaram. Como os IVs são criados para detecções **fixas** que ainda não existem em sua instância, isso pode afetar negativamente o desempenho da importação. Você pode preferir deixar este recurso desativado para que as detecções **fixas** atualizem somente os estados dos itens vulneráveis existentes. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de vulnerabilidades. • A saída desta integração é Itens vulneráveis (IVs) **encerrados/corrigidos**. Ele também cria ativos e entradas de terceiros se eles não existirem. Esta execução de integração é uma execução programada. É uma integração encadeada, o que significa que, após a conclusão bem-sucedida de uma execução, a Tenable.sc Integração de vulnerabilidades em aberto descrita abaixo é acionada. **Nota:** Por padrão, os IDs de família 0 e 39 são excluídos desta integração.
Tenable.sc Abrir integração de vulnerabilidades	• Esta integração é acionada após a conclusão bem-sucedida da Tenable.sc Integração de vulnerabilidades fixas. • Recupera dados de vulnerabilidade com base nos filtros de consulta selecionados do produto Tenable.sc e os processa em sua instância. • Cria itens vulneráveis correspondentes para vulnerabilidades ativas. • Cria ICs exclusivos para ativos incompatíveis ou atualiza ICs existentes com o atributo do identificador de partição de rede para ativos em seu ambiente que compartilham o mesmo endereço IP. • Coordena as chamadas de mensagem REST para a API de vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	• A saída desta integração é **Atualizar/criar novos** itens vulneráveis (IVs) se eles ainda não existirem. Ele também cria itens de configuração e entradas de terceiros se eles não existirem. **Nota:** Por padrão, os IDs de família 0 e 39 são excluídos desta integração.
Tenable.sc Integração de credencial de verificação	• Esta integração recupera as credenciais de verificação configuradas em Tenable.sc. • Coordena as chamadas de mensagem REST para a API de credenciais. • A saída desta integração são as credenciais de verificação preenchidas na tabela [sn_vul_tenable_scan_credential]. • As credenciais importadas são usadas para acessar o scanner quando as solicitações de verificação são iniciadas a partir do Now Platform. • Esta integração está programada para ser executada semanalmente.
Tenable.sc Integração de vulnerabilidades de preenchimento	• Esta integração de preenchimento importa todas as vulnerabilidades abertas e corrigidas que podem ter sido perdidas durante uma importação. • Esta integração importa vulnerabilidades abertas e corrigidas dos últimos sete dias para atualizar suas detecções e itens vulneráveis. • Esta integração pode afetar seu desempenho. • Esta integração está desabilitada por padrão. • Para atualizar seus dados de vulnerabilidade e evitar possíveis problemas de desempenho, talvez você prefira programar as Vulnerabilidades corrigidas e as Integrações de vulnerabilidades abertas da Tenable.sc para serem executadas quando nenhuma outra verificação estiver em execução. • A saída desta integração é:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações do Tenable.sc

Integração	Descrição
	○ Itens vulneráveis (IVs)**encerrados/corrigidos**. Ele também cria ativos e entradas de terceiros se eles não existirem. ○ para **atualizar/criar novos** itens vulneráveis (IVs) se eles ainda não existirem. Ele também cria itens de configuração e entradas de terceiros se eles não existirem.

Autenticação de usuário e Tenable.sc

A autenticação do usuário é compatível com sua instância Now Platform® e a versão 5.13 do produto Tenable.sc. A autenticação do usuário será necessária se você estiver usando a versão 5.12 e anterior do produto Tenable.sc.

Quando você seleciona a autenticação de usuário para as Tenable.sc integrações, os tokens podem expirar e ser substituídos durante as execuções de integração. Na coluna Anotações no registro de execução de integração de vulnerabilidade (VIN), a seguinte mensagem é exibida para um processo quando um token expira, Erro: falha na validação de token. Nenhuma ação será necessária se esta mensagem for exibida. Os tokens expirados são atualizados automaticamente em segundo plano e a mensagem não indica uma pausa ou erro com o processo de integração.

Preparando para a integração de vulnerabilidade da Tenable

Prepare-se para a integração de vulnerabilidade da Tenable ServiceNow® executando as tarefas de configuração a seguir.

Antes de começar

Uma integração bem-sucedida requer planejamento e execução cuidadosa das tarefas de pré-integração. Para uma instalação e configuração sem problemas da aplicação Integração do Vulnerability Response com Tenable, convém imprimir a check-list a seguir e verificar se os itens listados foram concluídos antes de instalar a aplicação e importar dados de vulnerabilidade para sua instância Now Platform®.

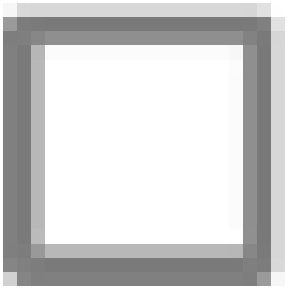
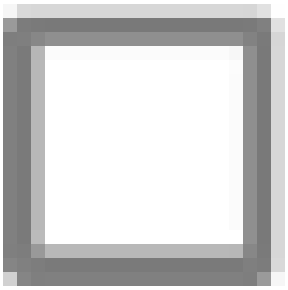
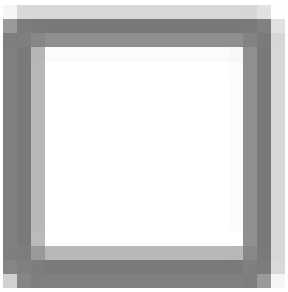
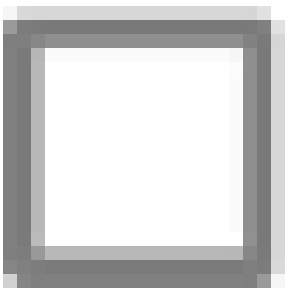
Nota:
Se você estiver importando dados com a integração criada pela Tenable e quiser começar a usar a ServiceNow® Integração do Vulnerability Response com a Tenable, consulte a

Para obter informações atuais de limpeza e migração de dados da integração criada pela Tenable para a integração criada por ServiceNow, consulte o artigo Diretrizes para migrar da integração do Vulnerability Response da Tenable para a integração do Vulnerability Response da ServiceNow com a Tenable [KB0960667] .

Função necessária: administrador para baixar e instalar a aplicação.

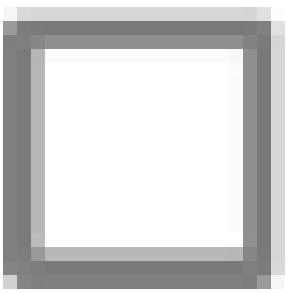
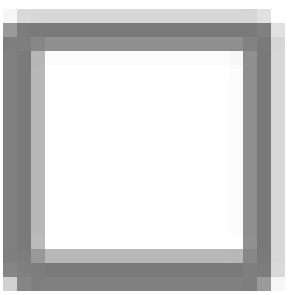
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	(Opcional) Se ainda não estiver instalado e ativado, talvez você prefira instalar a aplicação Vulnerability Response antes de instalar a aplicação de terceiros. Para obter mais informações sobre como instalar e ativar a aplicação Vulnerability Response, consulte Como instalar Vulnerability Response. Esta integração requer a versão 12.1 de Vulnerability Response ou posterior.
	Se você ainda não o tiver em sua instância, obtenha direitos e baixe a aplicação Integração do Vulnerability Response com Tenable para sua instância Now Platform®. A aplicação Integração do Vulnerability Response com Tenable oferece suporte ao produto Tenable.sc a partir da versão 5.13. Consulte .
	Estime o número de itens vulneráveis que você espera importar. Verifique se sua instância pode aceitar o número de itens vulneráveis que você espera importar. Uma instância subdimensionada pode levar a longos tempos de carregamento. Se você não souber o tamanho da sua instância ou se precisar de assistência, entre em contato com o ServiceNow® Suporte técnico.
	Verifique se você tem grupos ou usuários para gerenciar as integrações e corrigir itens vulneráveis. **admin** O administrador do sistema usa o Assistente de configuração para instalar a aplicação Integração do Vulnerability Response com Tenable. Se não for atribuído, o administrador atribuirá o administrador de vulnerabilidade (sn_vul.vulnerability_admin) e outras funções no Assistente de configuração. **sn_vul.vulnerability_admin** Depois de atribuído, o administrador de vulnerabilidade conclui a configuração das integrações da Tenable. Esta função tem acesso completo à aplicação Vulnerability Response (VR) e seus registros. Configura todas as aplicações e regras de VR e configura integrações de terceiros. **sn_vul_tenable.configure_integration** Pode configurar a integração de vulnerabilidade da Tenable. Esta função contém a função granular sn_vul_tenable.read_integration. **sn_vul_tenable.read_integration**

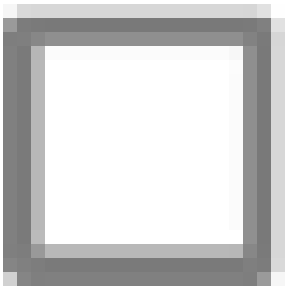
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	Pode exibir (ler) registros da integração de vulnerabilidade da Tenable. **Grupo do Vulnerability Response** Por padrão, o grupo do Vulnerability Response está disponível no Assistente de configuração. Os usuários atribuídos ao grupo Vulnerability Response herdam as funções sn_vul.read_all e sn_vul.remediation_owner automaticamente. O administrador do sistema executa a atribuição inicial de funções a usuários e grupos no Assistente de configuração para a integração. Por padrão, o grupo Vulnerability Response está disponível. Se ainda não tiver sido criado, talvez você prefira criar grupos adicionais e adicionar usuários com o módulo Administração de usuários em sua instância antes de usar o Assistente de configuração. Consulte Criação de um grupo de usuários . Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que os usuários podem fazer e ver na aplicação Vulnerability Response. Para obter a atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração.
	Para promover um desempenho aprimorado para sua primeira importação, convém desabilitar determinados recursos, regras ou trabalhos em sua instância. • Desabilite as calculadoras de vulnerabilidade se você não as usar. Essas calculadoras, além de qualquer outra que você tenha definido, são executadas sempre que um registro de item vulnerável é criado ou atualizado. Consulte Desabilitar calculadoras de vulnerabilidade. • Durante a importação inicial de registros, determinadas regras de negócios relacionadas à notificação podem fazer com que muitas notificações sejam geradas, afetando o desempenho. Antes da importação inicial, talvez você prefira Desabilitar as regras de negócios relacionadas à notificação, conforme descrito em Importar modificações para a integração de vulnerabilidade da Tenable.
	Verifique se você habilitou todos os recursos, regras, plug-ins de dependência ou trabalhos em sua instância necessários para a integração. • Tenable.sc é uma integração no local que oferece a opção de usar um MID Server se o produto Integração do Vulnerability Response com Tenable e sua instância Now Platform estiverem no mesmo ambiente. Se o produto Tenable.sc e sua instância Now Platform não estiverem no mesmo ambiente, você precisará usar um MID Server. Para obter mais informações sobre MID Servers em sua instância, consulte MID Server .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefa	Descrição
	• Verifique se o plug-in IntegrationHub está instalado e ativado. Este plug-in permite que os componentes do sistema de base chamem sistemas externos usando APIs de integração e ative etapas de protocolo como REST. Navegar até **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e localize o plug-in. Se não estiver instalado em sua instância, instale-o e ative-o.
	Obter credenciais da Tenable. Verifique se você tem nomes de conta, senhas e outras informações de serviço exigidas pelos seus produtos Tenable para que você tenha acesso a eles. Tenable.io requer acesso de Administrador com um atributo de permissão maior ou igual a 64. Tenable.sc requer acesso de Analista de Segurança ou Gerente. **Nota:** A partir da v3.8 de Integração do Vulnerability Response com Tenable, o acesso a Tenable.io não precisa mais de privilégios de administrador. Um usuário básico com um atributo de permissão igual a 16 também pode acessar o produto.

Você está pronto para Instalar a aplicação Integração do Vulnerability Response com Tenable usando o Assistente de configuração.

Instalar a aplicação Integração do Vulnerability Response com Tenable usando o Assistente de configuração

Antes de executar o ServiceNow® Tenable Vulnerability Integration, você precisa baixar a aplicação Integração do Vulnerability Response com Tenable do ServiceNow Store e instalá-lo e configurá-lo usando o Assistente de configuração no aplicativo Vulnerability Response.

Antes de Iniciar

Antes de instalar a aplicação Tenable, verifique se você concluiu todos os itens da check-list em Preparando para a integração de vulnerabilidade da Tenable.

Nota:
Este processo se aplica somente a aplicações que são baixadas para instâncias de produção. Se você estiver baixando aplicações para instâncias de subprodução ou desenvolvimento, não será necessário obter direitos. Prossiga para Ativar uma aplicação ServiceNow Store.

Funções necessárias: administrador para atribuição inicial da função sn_vul.vulnerability_admin e instalação da aplicação Tenable no Assistente de configuração. Administrador de vulnerabilidade (sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto) para configurar a aplicação no Assistente de configuração depois que ele for instalado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Administração** > **Assistente de configuração** > **Instalação da aplicação de integração**.

   Após alguns momentos, as aplicações disponíveis para instalação em sua instância serão exibidas.

2. Localize o bloco **Tenable (Plataforma Tenable)** e clique em **Instalar**.

   Esta ação instala a aplicação Integração do Vulnerability Response com Tenable que você baixou do ServiceNow Store.

3. Siga os prompts fornecidos no Assistente de configuração para continuar com a instalação.

4. Para obter mais informações sobre como instalar aplicações usando o Assistente de configuração, consulte Instalar Vulnerability Response aplicações de terceiros usando o Assistente de configuração.

O que Fazer Depois

Depois de concluir a instalação no Assistente de configuração, navegue até **Configuração de integração>Integrações do scanner** no Assistente de configuração para continuar com a configuração. Se você quiser mais informações para complementar os prompts fornecidos no Assistente de configuração, consulte Configurar a integração de vulnerabilidade da Tenable usando o assistente de configuração.

Configurações de recuperação de dados para a integração de vulnerabilidade da Tenable

As configurações de recuperação de dados a seguir ajudam a determinar especificamente o tipo e o escopo dos dados que você deseja importar da ServiceNow® Tenable Vulnerability Integration para sua instância Now Platform®.

As configurações descritas nas seções a seguir ajudam a controlar os dados que você deseja importar. Além disso, você pode definir os valores desses filtros em Instâncias de integração. Para exibir instâncias de integração, navegue até **Integração de vulnerabilidade Tenable** > **Instâncias de Integração** e clique na sua integração, Tenable.io ou Tenable.sc.

Na página Instância de integração exibida, clique nos Parâmetros de instância de integração para exibir uma lista de parâmetros ou nas guias Integrações de vulnerabilidade para uma programação, Detalhes de REST, Detalhes de integração, Fontes de dados e informações de execução de integração.

Configurações e filtros comuns de severidade e recuperação para Tenable.io e Tenable.sc na sua instância Now Platform

As configurações a seguir estão disponíveis para as integrações Tenable.io e Tenable.sc na sua instância Now Platform. Essas e outras definições de configuração são exibidas na página Instância de integração da sua instância Now Platform. Você pode preferir deixar essas configurações em seus padrões para as primeiras execuções de integração.

Tenable.io

inserir_fixo

Se você habilitar o sinalizador **insert_fixed** no Assistente de configuração para a integração de importação de vulnerabilidades, novos IVs serão criados para detecções no estado **Fixo** que ainda não existem na sua instância.

severidade_crítica

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de severidade crítica das Tenable.io Integrações de vulnerabilidades abertas e Tenable.io Vulnerabilidades fixas.

severidade_alta

Este filtro é habilitado por padrão (verdadeiro) para receber vulnerabilidades de severidade de alto nível das Tenable.io Integrações de vulnerabilidades abertas e Tenable.io Vulnerabilidades fixas.

severidade_média

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de severidade de nível médio das Tenable.io Integrações de vulnerabilidades abertas e Tenable.io Vulnerabilidades fixas.

severidade_info

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de severidade de nível de informação das Tenable.io Integrações de vulnerabilidades abertas e Tenable.io Vulnerabilidades fixas.

severidade_baixa

Este filtro está inativo por padrão (falso). Habilite este filtro para receber vulnerabilidades de severidade de baixo nível das Tenable.io Integrações de vulnerabilidades abertas e Tenable.io Vulnerabilidades fixas.

tamanho

Esta configuração define o número de registros de plug-in a serem incluídos no conjunto de resultados da Tenable.io Integração de plug-ins. Deve estar no formato int32. O valor padrão é 1.000. O tamanho máximo é 10.000.

num_assets

O número máximo de vulnerabilidades por bloco exportado das Tenable.io Integrações de vulnerabilidades fixas e Tenable.io Vulnerabilidades abertas. O valor padrão é 50.

chunk_size

Especifica o número de ativos por bloco exportado pela Tenable.io integração de ativos. O padrão é 1.000.

Tenable.sc

assíncrono_request

Este parâmetro está inativo por padrão (falso). Habilite ou desabilite este parâmetro para fazer chamadas de API assíncronas ou síncronas com Tenable.sc respectivamente. Para chamadas síncronas, se houver um tempo limite de 30 segundos, entre em contato com o suporte do produto Tenable para ajustar a caixa. Este parâmetro, uma vez habilitado, é aplicável a todas as integrações de Tenable.sc. Para clientes existentes que usam chamadas assíncronas, um script de correção está disponível, o que adiciona um novo parâmetro async_request às instâncias de integração Tenable.sc existentes. Para exibir os scripts de correção, navegue até **Definição do Sistema** > **Corrigir Scripts**.

inserir_fixo

Se você habilitar o sinalizador **insert_fixed** no Assistente de configuração para a integração de importação de vulnerabilidades, novos IVs serão criados para detecções no estado **Fixo** que ainda não existem na sua instância.

deslocamento

Especifica o número de ativos, plug-ins e vulnerabilidades importados em uma execução de integração.

Filtros de consulta

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os filtros de consulta são configurados no console da Tenable. Esses filtros de consulta têm IDs que podem ser selecionados no Assistente de configuração ou na página Instâncias de integração na sua instância Now Platform. Esses filtros são aplicados ao recuperar os dados das integrações Tenable.sc.

Mensagens REST para a integração de vulnerabilidade da Tenable

As ServiceNow® mensagens REST de integração de vulnerabilidade da Tenable são usadas para fazer chamadas para a API da Tenable.

Tenable.io Mensagem REST de ativos

A mensagem REST de Tenable.io ativos recupera informações de ativos para a Tenable.io integração de ativos. As mudanças no registro do método de mensagem REST afetam as solicitações feitas a Tenable.io para recuperar informações de ativos. O trabalho de exportação de ativos é enviado com os seguintes filtros:

- "is_deleted": falso
- "is_licensed": verdadeiro

Tenable.io Mensagem REST de plug-ins

A mensagem REST de plug-ins Tenable.io recupera informações de plug-in para a integração de plug-in Tenable.io. As mudanças no registro do método de mensagem REST afetam as solicitações feitas a Tenable.io para recuperar informações de plug-ins.

Tenable.io Mensagem REST de vulnerabilidades

A mensagem REST de vulnerabilidades Tenable.io recupera informações de vulnerabilidades abertas e encerradas da Tenable.io Integração de vulnerabilidade. As mudanças no registro do método de mensagem REST afetam as solicitações feitas a Tenable.io para recuperar informações de vulnerabilidades.

Mensagem REST de consultas Tenable.sc

A mensagem REST de consultas da Tenable.sc recupera as informações do filtro de consulta da integração de ativos da Tenable.sc e da integração de vulnerabilidades da Tenable.sc em que o filtro de consulta está configurado.

Tenable.sc Mensagem REST de plug-ins

A mensagem REST de plug-in Tenable.sc recupera informações de plug-in para a integração de plug-ins Tenable.sc. As mudanças no registro do método Obter plug-ins da mensagem REST afetam as solicitações feitas a Tenable.sc para recuperar informações de plug-ins.

Nome do parâmetro	Valor	Descrição
tipo	ativo	Indica a origem da qual a Tenable extrai dados. Usado por código. Mudanças não são recomendadas.
campos	id, descrição, cvssVector,cvssV3Vector, cvssV3TemporalVector, sinopse, cvssVector, baseScore, temporalScore,	Indica a lista de campos importados da Tenable.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do parâmetro	Valor	Descrição
	cvssV3Vector, cvssV3BaseScore, cvssV3TemporalVector, name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, família, cvssV3TemporalScore, explore tipo, direitos autorais, versão, sourceFile, dependências, necessáriosPorts, necessáriosUDPPorts, srcPort, dstPort,protocol, checkType, cvssVectorBF, sigSeverity, patchPubDate, patchModDate, vulnPubDate, modificadoTempo, md5	

Tenable.sc Mensagem REST de vulnerabilidades

A mensagem REST de vulnerabilidades Tenable.sc recupera informações de vulnerabilidade da integração Tenable.sc. As mudanças no método Buscar vulnerabilidades da mensagem REST ou Buscar vulnerabilidades corrigidas ou, a partir da v14.0 Vulnerability Response e v2.2 da Integração de vulnerabilidade da Tenable, Buscar registro de vulnerabilidades de preenchimento afetam as solicitações feitas a Tenable.sc para recuperar informações de vulnerabilidades.

Tenable.sc Mensagem REST de credenciais de verificação

Tenable.sc Mensagem REST de política

A mensagem POST REST de política Tenable.sc adiciona uma política para os plug-ins solicitados. A política gerada será usada em Tenable.sc solicitações de verificação.

Tenable.sc Verificar mensagem REST

A mensagem POST REST de verificação da Tenable.sc adiciona uma verificação que depende do acesso e da permissão definidos no corpo da solicitação da mensagem REST. Ele usa política, ID de plug-in e IP(s) no corpo da solicitação para a solicitação de verificação.

Tenable.sc Mensagem REST do resultado da verificação

A mensagem Tenable.sc Scan Result GET REST fornece detalhes da verificação gerada usando a mensagem Scan REST. Ele usa o scanResultId na resposta das mensagens REST de verificação e recupera os detalhes da verificação acionada.

Tenable.sc Credenciais de verificação

A mensagem REST de credenciais de verificação Tenable.sc recupera as informações de credenciais de Tenable.sc. As mudanças no registro do método "Importar" da mensagem REST afetam as solicitações feitas a Tenable.sc para recuperar as informações de credenciais.

Nome do parâmetro	Valor	Descrição
campos	id, nome, descrição, tipo	Indica a lista de campos importados de Tenable.sc
filtros	utilizável	Indica que a integração extrai somente credenciais utilizáveis de Tenable.sc

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome do parâmetro	Valor	Descrição
		Mudanças em qualquer um dos parâmetros não são recomendadas.

Transformação de dados para a integração de vulnerabilidade da Tenable

Depois de identificar os dados a serem importados, eles são recuperados do produto Tenable e processados por meio de um conjunto de fontes de dados e transformações em sua instância.

Durante a instalação, os mapas de severidade normalizados são instalados no módulo Mapeamento de severidade normalizado. Esses mapas transformam os níveis de severidade da Tenable importados em níveis de severidade padrão para processamento em sua instância. Para obter informações sobre como criar mapas de severidade, consulte Criar um mapa de severidade do Vulnerability Response na documentação do Vulnerability Response.

Importação de ativo da Tenable.io

Os dados do ativo importado são carregados primeiro na tabela Importação de ativo Tenable.io [sn_vul_tenable_io_asset_import].

O mapa de transformação de integração de ativos da Tenable.io é usado para transformar as informações de ativos importados. As mudanças nesta transformação alteram como os dados da importação do ativo da Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação**. Pesquise Transformação de ativo Tenable.io.

As tabelas a seguir listam os campos do mapa de transformação por integração.

Campos do mapa de transformação de ativo da Tenable.io

Campo de origem	Campo de destino	Descrição
u_id	source_id	A Tenable fornece um ID exclusivo para ativos e mapas para o registro do item descoberto e é usado para pesquisa de IC.
u_ipv4s	ip_address	Mapeia o primeiro valor de IP para o campo ip_address no registro do item descoberto.
u_mac_addresses	mac_address	Mapeia o primeiro valor de mac_address para o campo de endereço mac no registro do item descoberto.
u_fqdns	fqdn	Mapeia o primeiro valor fqdn para o campo fqdn no registro do item descoberto.
u_netbios_names	netbios	Mapeia o primeiro valor netbios para o campo netbios no registro do item descoberto.
u_operating_systems	os	Mapeia o primeiro valor de SO para o campo de SO no registro do item descoberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campos do mapa de transformação de ativo da Tenable.io

Campo de origem	Campo de destino	Descrição
(Antes da v 14.0 Vulnerability Response e v2.2 da integração de vulnerabilidade da Tenable)u_last_scan_time	data_última_verificação	Mapeia para o campo last_scan_date no registro do item descoberto.
u_last_authenticated_scan_date	last_auth_scan_date	Mapeia para o campo last_auth_scan_date no registro do item descoberto.
[script]	nome	Mapeia o nome do host usando a lógica do script.
u_tags		Os marcadores são salvos em sn_sec_cmn_host_tag. O mapeamento de marcadores para ativos é salvo em sn_sec_cmn_m2m_src_ci_tag.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Tempo e finalidade do script do mapa de transformação de ativo da Tenable.io

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Modificar ou excluir não é recomendado.
onBefore (antes de um conjunto de importação concluir a transformação).	Uma função usada para atualizar valores no host e verificar se o host já existe. Com base nos resultados, modifica os valores em um import_set. Para uso interno. Modificar ou excluir não é recomendado.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos ICs criados e ICs que foram atualizados e ignorados. Para uso interno. Modificar ou excluir não é recomendado.

Integração de plug-ins Tenable.io

O mapa de transformação de plug-ins Tenable.io é usado para transformar plug-ins importados do Tenable.io.

Nota:
As mudanças neste mapa de transformação alteram como os dados recebidos dos plug-ins da Tenable são processados.

Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação**. Pesquise a transformação do plug-in Tenable.io.

A carga dos plug-ins da Tenable.io contém todos os campos na coluna u_attributes da tabela sn_vul_tenable_io_plugin_import. O campo de atributos é analisado e mapeado para os registros da tabela de entrada de terceiros, conforme listado na tabela a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
id	id	Mapeia o ID da origem e adiciona o prefixo TEN- a ele. Por exemplo, se o ID recebido for 12345, o ID na tabela de destino será TEN-12345.
Descrição	resumo	Mapeia a descrição do plug-in para a coluna de resumo.
[script]	fonte	A origem do TPE importado é Tenable.io.
[script]	source_instance	Referência à implantação da Tenable que importa este registro.
família	categoria	Mapeia a família do plug-in para a coluna da categoria
plug-in_modification_date	last_modified	Mapeia o plugin_modification_date para o último campo modificado.
data_publicação_plug-in	date_published	Mapeia o plugin_publication_date para a data de publicação.
tem_patch	correção_tipo	Mapeia o tipo de correção do valor has_patch.
synopsis	ameaça	Mapeia as informações de ameaça sobre esta vulnerabilidade.
cvss_base__score	pontuação	Mapeia a pontuação base de cvss para a coluna de pontuação na tabela de entrada de terceiros.
solução	solução	Mapeia a solução fornecida pelo scanner para a coluna de solução na tabela de entrada de terceiros.
explore_available	exploração	Mapeia o explore_available fornecido pelo scanner para a coluna de exploração na tabela de entrada de terceiros
vpr.pontuação	source_risk_score	Mapeia a pontuação vpr fornecida pelo scanner para source_risk_score na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 - Crítico • 7 – 9 – Alto • 4 – 7 – Médio • 0-4 - Baixo
vpr.drivers.age_of_vuln	age_of_vuln	Mapeia a idade da vulnerabilidade do scanner para a coluna

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		age_of_vuln na tabela de entrada de terceiros.
vpr.drivers.exploit_code_maturity	explore_code_maturity	Mapeia a maturidade do código de exploração do scanner para explore_code_maturity na tabela de entrada de terceiros.
vpr.drivers.product_coverage	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
vpr.drivers.threat_sources_last28	ameaça_fontes	Mapeia as origens de ameaça nos últimos 28 dias do scanner para o Threat_sources na tabela de terceiros.
vpr.drivers.threat_intensity_last28	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para o Threat_intensity na tabela de entrada de terceiros.
vpr.drivers.threat_recency	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para Threat_recency na tabela de entrada de terceiros.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mapeia a pontuação de impacto do cvss3 para a coluna v3_impact_subscore na tabela de entrada de terceiros.
cvss_pontuação_temporais	cvss_pontuação_temporais	Mapeia a pontuação temporal para CVSS v2.
cvss_v3_tempo_pontuação	v3_tempo_pontuação	Mapeia a pontuação temporal para CVSS v3.
risk_factor	source_severity	Mapeia para a severidade de origem na tabela de entrada de terceiros.
nome	nome	Mapeia o nome do plug-in para o nome na tabela de entrada de terceiros.
stíg_severidade	stíg_severidade	Mapeia a pontuação vpr fornecida pelo scanner para source_risk_score na tabela de entrada de terceiros.
plug-in_type	check_type	Mapeia o tipo de plug-in para check_type na tabela de entrada de terceiros.
unsupported_by_vendor	unsupported_by_vendor	Mapeia o campo unsupported_by_vendor para a coluna unsupported_by_vendor.
[script]	explore_attack_vector	A coluna explore_attack_vector na tabela de entrada de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		terceiros é preenchida com base em explore_available e v3_attack_vector das colunas.

Além dos campos diretos, outras informações são adicionadas como listas relacionadas às entradas de terceiros.

Campo de origem	Descrição
cve	Insere dados relacionados a CVE na tabela de referência (sn_vul_nvd_entry). Se o mesmo CVE na tabela de entrada do NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada do NVD. O mapeamento pode ser encontrado em sn_vul_m2m_entry_cve.
bid	A lista de traqs de erros é adicionada como uma referência.
ver_também	A lista de URLs é adicionada como uma referência.
xrefs	A lista de X-REF é adicionada como referência.
[script]	A lista de explorações para esse plug-in e insere mapeamento para estrutura de exploração aplicável e plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Modificar ou excluir não é recomendado.
onBefore (antes de um conjunto de importação concluir a transformação).	Uma função usada para atualizar os valores na entrada do terceiro e verificar se a entrada do terceiro já existe. Com base nos resultados, modifica os valores em uma entrada de terceiros. Para uso interno. Modificar ou excluir não é recomendado.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos ICs criados e ICs que foram atualizados e ignorados. Para uso interno. Modificar ou excluir não é recomendado.

A inclusão de script TenableIOPluginsImportProcessor é chamada a partir do script de transformação onBefore. Ele obtém a saída da integração de plug-ins Tenable.io e a transforma em Now Platform entradas de vulnerabilidade de terceiros. Quaisquer mudanças nesta inclusão de script podem alterar a transformação dos dados dos plug-ins Tenable.io na tabela de entrada de terceiros.

Importação de vulnerabilidades da Tenable.io

O mapa de transformação de item vulnerável da Tenable.io é usado para transformar informações de vulnerabilidades abertas e fixas importadas da Tenable.io.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
As mudanças neste mapa de transformação alteram como os dados da importação de vulnerabilidades da Tenable são processados.

O mesmo mapa de transformação é usado para a integração de vulnerabilidades fixas da Tenable.io e a integração de vulnerabilidades abertas da Tenable.io. Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação**. Pesquise o mapa de transformação do item vulnerável Tenable.io.

Campo de origem	Campo de destino	Descrição
u_asset.uuid	id	O Uuid é mapeado para o campo id do registro cmdb_ci.
u_asset.ipv4	ip_address	O campo ipv4 é mapeado para o campo de endereço IP do registro cmdb_ci.
u_asset .last_authenticated_results	last_auth_scan_date	A data da última verificação autenticada é mapeada para a data da última verificação de autenticação do registro cmdb_ci.
u_asset.mac_address	mac_address	O endereço Mac é mapeado para o campo de endereço MAC do host do registro cmdb_ci.
u_asset.netbios_name	netbios	O NetBIOS é mapeado para o campo netBIOS do registro cmdb_ci.
u._plugin.cvss3_base_score	v3_base_score	A pontuação base do CVSS v3 é mapeada para a pontuação base v3 do registro de entrada do terceiro.
u._plugin.cvss3_tempo_score	v3_tempo_pontuação	A pontuação temporal do CVSS v3 é mapeada para a pontuação temporal do v3 no registro de entrada de terceiros.
u._plugin.cvss_base_score	pontuação	A pontuação base do CVSS é mapeada para o campo de pontuação do registro de entrada de terceiros.
u._plugin.cvss_tempo_score	temporal_score	A pontuação temporal é mapeada para a pontuação temporal no registro de entrada do terceiro.
u_plugin.description	resumo	A descrição é mapeada para o campo de resumo no registro de entrada do terceiro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_plugin.family	categoria	Mapeia a família de plug-ins para a coluna de categoria do registro de entrada de terceiros.
u_plugin.modification_date	last_modified	A data da última modificação é mapeada para a data da última modificação do plug-in no registro de entrada do terceiro.
u_plugin.publication_date	date_published	A data de publicação é mapeada para o campo de data de publicação do registro de entrada do terceiro.
u_plugin.risk_factor	source_severity	O fator de risco é mapeado para o campo source_severity do registro de entrada do terceiro.
u_plugin.solução	solução	A solução é mapeada para o campo de solução do registro de entrada do terceiro.
u_plugin.sinopse	ameaça	A sinopse é mapeada para o campo de ameaça do registro de entrada do terceiro.
u_id_severidade	prioridade	A prioridade é mapeada para o ID de severidade da carga útil. O valor padrão é 5.
u_plugin.exploit_available	exploração	Mapeia o explore_available fornecido pelo scanner para a coluna de exploração na tabela de entrada de terceiros.
vpr.pontuação	source_risk_score	Mapeia a pontuação vpr fornecida pelo scanner para source_risk_score na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 - Crítico • 7 – 9 – Alto • 4 – 7 – Médio • 0-4 - Baixo
u_plugin.vpr.drivers.age_of_vuln	age_of_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_plugin.vpr.drivers.exploit_code_maturity	explore_code_maturity	Mapeia a maturidade do código de exploração do scanner para explore_code_maturity na tabela de entrada de terceiros.
u_plugin.vpr.drivers.product_coverage	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_plugin.vpr.drivers.threat_sources_last28	ameaça_fontes	Mapeia as origens de ameaça nos últimos 28 dias do scanner para Threat_sources na tabela de entrada de terceiros.
u_plugin.vpr.drivers.threat_intensity_last28	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para o Threat_intensity na tabela de entrada de terceiros.
u_plugin.vpr.drivers.threat_recency	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para Threat_recency na tabela de entrada de terceiros.
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS3 v3 para a coluna v3_impact_subscore na tabela de entrada de terceiros.
u_plugin.type	check_type	Mapeia o tipo de plug-in para check_type na tabela de entrada de terceiros.
u_plugin.unsupported_by_vendor	unsupported_by_vendor	Mapeia o campo unsupported_by_vendor no plug-in para a coluna unsupported_by_vendor.
[script]	explore_attack_vector	A coluna explore_attack_vector na tabela de entrada de terceiros é preenchida com base em explore_available e v3_attack_vector das colunas.
u_plugin.family_id	Family_id	Mapeia o ID da família do plug-in para a coluna family_id na tabela de entrada de terceiros.
port	port	A porta é mapeada para o campo de porta do registro do item vulnerável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
protocolo	protocolo	O protocolo é mapeado para o campo de protocolo do registro do item vulnerável.
u_first_found	first_found	O primeiro encontrado é mapeado para o primeiro campo encontrado do registro do item vulnerável.
u_last_found	last_found	O último encontrado é mapeado para o último campo encontrado do registro do item vulnerável.
u_state	state	O estado é mapeado para o campo Estado no registro do item vulnerável
[script]	fonte	A origem da integração é preenchida. Os itens vulneráveis criados a partir desta integração têm o Tenable.io como origem.
[script]	integration_instance	integration_instance é o nome da instância da qual o item vulnerável é importado.
u_plugin.name	nome	Mapeia o nome do plug-in para o nome na tabela de entrada de terceiros.
u_plugin.sting_severity	stíg_severidade	Mapeia a severidade padrão do plug-in para a coluna de severidade padrão na tabela de entrada de terceiros

Além dos campos diretos, outras informações são adicionadas como listas relacionadas às entradas de terceiros.

Campo de origem	Descrição
cve	Insere dados relacionados a CVE na tabela de referência (sn_vul_nvd_entry). Se o mesmo CVE na tabela de entrada do NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada do NVD. O mapeamento pode ser encontrado em sn_vul_m2m_entry_cve.
bid	A lista de traqs de erros é adicionada como uma referência.
ver_também	A lista de URLs é adicionada como uma referência.
xrefs	A lista de X-REF é adicionada como referência.
[script]	A lista de explorações para esse plug-in e o mapeamento de inserções para a estrutura

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Descrição
	de exploração aplicável e o plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação aciona o TenableIOVulnerabilitiesProcessor, que importa dados do Tenable.io usando o conjunto de importação e carrega cada registro na tabela de IC do CMDB, na tabela de itens vulneráveis e na tabela de vulnerabilidade de terceiros.Para uso interno. Modificar ou excluir não é recomendado.
onBefore (antes de um conjunto de importação concluir a transformação).	Uma função para verificar se a entrada e as detecções de terceiros já existem. Caso contrário, esses registros serão criados em suas respectivas tabelas. Para uso interno. Modificar ou excluir não é recomendado.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para atualizar a contagem de ICs, IVs e Detecções conforme importados do Tenable.io. Para uso interno. Modificar ou excluir não é recomendado.

Importação de ativo da Tenable.sc

Os dados de ativo importados do Tenable.sc são carregados primeiro na tabela de importação de ativo do Tenable.sc (sn_vul_tenable_sc_asset_import). O mapa de transformação de integração de ativos da Tenable.sc é usado para transformar as informações de ativos importados. As mudanças nesta transformação alteram como os dados da importação de ativos da Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação**. Pesquise a Transformação do ativo Tenable.sc.

Campo de origem	Campo de destino	Descrição
u_uuid	id	O uuid não é preenchido a partir da API da Tenable, portanto, o atributo "u_uniqueness" é usado para criar um campo uuid exclusivo para ativos e mapeá-lo para o registro cmdb_ci.
u_ip	ip_address	Mapeia o campo ip da API para o campo ip_address em um registro cmdb_ci.
u_macaddress	mac_address	Mapeia o campo de endereço eletrônico da API para o campo de endereço no registro cmdb_ci.
u_dnsname	fqdn	Mapeia o campo dnsname da API para o campo fqdn no registro cmdb_ci.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_netbiosname	netbios	Mapeia o campo netbios da API para o campo netbios no registro cmdb_ci.
u_oscpe	os	As informações do SO são extraídas do atributo oscpe na carga útil e as mapeiam para o campo os no registro cmdb_ci.
u_lastauthrun	last_auth_scan_date	Mapeia o campo lastauthrun da API para o campo last_auth_scan_date no registro do item descoberto.
u_lastauthrun e u_lastunauthrun	data_última_verificação	O lastauthrun é extraído da API da Tenable ou lastunauthrun. Com base no valor que aparece na carga útil, o campo last_scan_date no registro do item descoberto é preenchido.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Modificar ou excluir não é recomendado.
onBefore (antes de um conjunto de importação concluir a transformação).	Função usada para atualizar os valores no host e verificar se o host já existe. Com base nos resultados, modifica os valores em um import_set. Para uso interno. Modificar ou excluir não é recomendado.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos ICs criados e ICs que foram atualizados e ignorados. Para uso interno. Modificar ou excluir não é recomendado.

Importação de plug-ins Tenable.sc

Os dados de plug-ins importados do Tenable.sc são carregados primeiro na tabela de importação de plug-ins do Tenable.sc (sn_vul_tenable_sc_plugin_import). O mapa de transformação de plug-in Tenable.sc é usado para transformar as informações de plug-in que foram importadas. As mudanças nesta transformação alteram como os dados da importação do plug-in da Tenable são processados. Para acessar este mapa de transformação, navegue até **Conjuntos de importação do sistema** > **Mapas de transformação**. Pesquise o mapa de transformação do plug-in Tenable.sc.

Campo de origem	Campo de destino	Descrição
u_id	id	Mapeia o ID da origem e adiciona o prefixo TEN-. Por exemplo, se o ID recebido for 12345, o ID na tabela de destino será TEN-12345.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_description	resumo	Mapeia a descrição do plug-in para a coluna de resumo.
[script]	fonte	O TPE importado desta integração tem Tenable.sc como origem.
[script]	source_instance	Referência à implantação da Tenable que importa este registro.
u_family	categoria	Mapeia o campo de nome no objeto de família do plug-in para a coluna de categoria.
u_plugin_modification_date	last_modified	Mapeia o plugin_modification_date para o último campo modificado.
u_plugin_publication_date	date_published	Mapeia o plugin_publication_date para a data de publicação.
u_has_patch	Remediation_type	Mapeia o tipo de correção do valor has_patch.
u_sinopse	ameaça	Mapeia as informações de ameaça sobre esta vulnerabilidade.
u_cvss_base_score	pontuação	Mapeia a pontuação base do CVSS para a coluna de pontuação na tabela de entrada de terceiros.
u_solution	solução	Mapeia a solução fornecida pelo scanner para a coluna de solução na tabela de entrada de terceiros.
u_cvss_tempo_pontuação	cvss_pontuação_temporais	Mapeia a pontuação temporal para CVSS v2.
u_cvss_v3_tempo_pontuação	v3_tempo_pontuação	Mapeia a pontuação temporal para CVSS v3.
u_risk_factor	severidade de origem	Mapeia para a severidade de origem na tabela de entrada de terceiros.
u_cvss_v3_base_score	v3_base_score	Mapeia a pontuação base do CVSS na tabela de entrada de terceiros.
u_exploit_available	exploração	Mapeia a exploraçãoDisponível fornecida pelo scanner para a coluna de exploração na tabela de entrada de terceiros.
u_vpr_score	source_risk_score	Mapeia a pontuação VPR do scanner para a pontuação de risco de origem na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 - Crítico • 7 – 9 – Alto

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		• 4 – 7 – Médio • 0-4 - Baixo
u_vpr_context[id=age_of_vuln]	age_of_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_vpr_context[id=exploit_code_maturity]	explore_code_maturity	Mapeia a maturidade do código de exploração do scanner para explore_code_maturity na tabela de entrada de terceiros.
u_vpr_context[id=product_coverage]	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_vpr_context[id="threat_sources_last_28"]	ameaça_fontes	Mapeia origens de ameaça nos últimos 28 dias do scanner para Threat_sources na tabela de terceiros.
u_vpr_context[id="threat_intensity_last_28"]	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para o Threat_intensity na tabela de entrada de terceiros.
u_vpr_context[id="threat_recency"]	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para Threat_recency na tabela de entrada de terceiros.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS v3 do scanner para v3_impact_subscore na tabela de entrada de terceiros.
u_name	nome	Mapeia o nome do plug-in para a coluna de nome na tabela de entrada de terceiros.
u_sting_severity	stíg_severidade	Mapeia o campo stíg_severity no plug-in para stíg_severidade na tabela de entrada de terceiros.
u_check_type	check_type	Mapeia o tipo de verificação para check_type na tabela de entrada de terceiros.
u_family.id	id_da_família	Mapeia o plug-in family_id para family_id na tabela de entrada de terceiros.
[script]	explore_attack_vector	A coluna explore_attack_vector na tabela de entrada de terceiros é preenchida com base em explore_available e v3_attack_vector das colunas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Além dos campos diretos, outras informações são adicionadas como listas relacionadas às entradas de terceiros.

Campo de origem	Descrição
u_cpe	A lista de CPEs é adicionada como referência.
u_see_also	A lista de URLs é adicionada como uma referência.
u_exploit_frameworks	A lista de explorações para esse plug-in e insere mapeamento para estrutura de exploração aplicável e plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Modificar ou excluir não é recomendado.
onBefore (antes de um conjunto de importação concluir a transformação).	Função usada para atualizar os valores na entrada do terceiro e verificar se a entrada do terceiro já existe. Com base nos resultados, modifica os valores em uma entrada de terceiros. Para uso interno. Modificar ou excluir não é recomendado.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de plug-ins criados e ignorados. Para uso interno. Modificar ou excluir não é recomendado.

A inclusão de script TenableSCPluginsImportProcessor é chamada a partir do script de transformação onBefore. Ele obtém a saída da integração de plug-ins Tenable.sc e a transforma em entradas de vulnerabilidade de terceiros da Servicenow. Quaisquer mudanças nesta inclusão de script podem alterar a transformação dos dados dos plug-ins Tenable.sc na tabela de entrada de terceiros.

Importação de vulnerabilidades da Tenable.sc

O mapa de transformação Tenable.sc Open Vulnerabilities é usado para transformar dados importados da integração de vulnerabilidades abertas Tenable.sc, e o mapa de transformação Tenable.sc e Vulnerabilidades fixas é usado para transformar dados importados da integração de vulnerabilidades fixas Tenable.sc.

Nota:
As mudanças nesses mapas de transformação alteram como os dados da importação de vulnerabilidades fixas/em aberto da Tenable são processados.

Para acessar os mapas de transformação de vulnerabilidades abertas e fixas da Tenable.sc, navegue até **Integração de vulnerabilidade Tenable** > **Administração** > **Instâncias de Integração** > **Integração de vulnerabilidades fixas/em aberto da Tenable.sc** > **Fontes de dados** > **Vulnerabilidades em aberto/corrigidas da Tenable.sc** > **Transformações**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_pluginID	Id	Usado como o identificador do plug-in. Este campo é mapeado para o ID do plug-in no registro de entrada do terceiro.
u_riskfactor	source_severity	Este campo é mapeado para source_severity no registro de entrada de terceiros.
u_severidade	prioridade	O campo de prioridade é mapeado com a severidade. O valor padrão é 5.
u_hasbeenmitigado	state	Hasbeenmitigado é mapeado para o campo de estado do registro de vulnerabilidade. Para a integração de vulnerabilidades corrigidas, todos os IVs estão no estado "Encerrado".
u_ip	ip_address	O endereço IP é mapeado para o campo de ip do host da tabela cmdb_ci.
u_port	port	A porta é mapeada para o campo de porta do registro do item vulnerável.
u_protocol	protocolo	O protocolo é mapeado para o campo de porta do registro do item vulnerável.
u_firstVen	first_found	O primeiro valor visto é mapeado para o primeiro campo encontrado do registro IV.
u_lastVen	last_found	O último valor visto é mapeado para o último campo encontrado do registro IV.
u_exploitDisponível	exploração	ExploitAvailable é mapeado para o campo de exploração no registro de entrada do terceiro.
u_sinopse	ameaça	A sinopse é mapeada para o campo de ameaça no registro de entrada do terceiro.
u_description	resumo	A descrição é mapeada para o campo de resumo no registro de entrada do terceiro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_solution	solução	A solução é mapeada para o campo de solução no registro de entrada do terceiro.
u_basescore	pontuação	BaseScore é mapeado para o campo de pontuação no registro de entrada do terceiro.
Pontuação_temporais	temporal_score	A pontuação temporal é mapeada para a pontuação temporal no registro de entrada do terceiro.
u_cvssv3basescore	v3_base_score	O cvssv3basescore é mapeado para a pontuação base v3 no registro de entrada do terceiro.
u_cvsspontuação temporal	v3_tempo_pontuação	A pontuação cvssv3 temporal é mapeada para a pontuação temporal v3 no registro de entrada do terceiro.
u_pluginpublicar data	date_published	A data de publicação do plug-in é mapeada para a data de publicação do plug-in no registro de entrada de terceiros.
u_pluginmoddate	last_modified	A data da última modificação é mapeada para a data da última modificação do plug-in no registro de entrada do terceiro.
u_dnsname	fqdn	DnsName é mapeado para o campo FQDN do registro cmdb_ci.
u_macaddress	mac_address	MacAddress é mapeado para o campo mac_address do registro cmdb_ci.
u_netbiosName	netbios	NetBIOSName é mapeado para o campo NETBIOS do registro cmdb_ci.
u_ip	ip	O IP é mapeado para o campo IP do registro cmdb_ci.
hostUniqueness	uuid	A exclusividade do host não é mapeada para nenhum campo, mas é usada para determinar o UUID do host.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
u_family	categoria	Mapeia o campo de nome no objeto de família do plug-in para a coluna de categoria do registro de entrada do terceiro.
u_plugintext	prova	O texto do plug-in é mapeado para a prova no registro.
[script]	fonte	A origem da integração é preenchida. Os itens vulneráveis criados a partir desta integração têm Tenable.sc como origem.
[script}	integration_instance	integration_instance é o nome da instância da qual o item vulnerável é importado.
u_vpr_score	source_risk_score	Mapeia a pontuação VPR do scanner para a pontuação de risco de origem na tabela de entrada de terceiros.
[script]	source_risk_rating	Mapeia a pontuação vpr para a classificação de risco padrão com base nos intervalos de pontuação: • 9 - 10 - Crítico • 7 – 9 – Alto • 4 – 7 – Médio • 0-4 - Baixo
u_vpr_context[id=age_of_vuln]	age_of_vuln	Mapeia a idade da vulnerabilidade do scanner para age_of_vuln na tabela de entrada de terceiros.
u_vpr_context[id=exploit_code_maturity]	explore_code_maturity	Mapeia a maturidade do código de exploração do scanner para explore_code_maturity na tabela de entrada de terceiros.
u_vpr_context[id=product_coverage]	product_coverage	Mapeia a cobertura do produto do scanner para product_coverage na tabela de entrada de terceiros.
u_vpr_context[id=”threat_sources_last_28]	ameaça_fontes	Mapeia as origens de ameaça nos últimos 28 dias do scanner para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Campo de destino	Descrição
		Threat_sources na tabela de terceiros.
u_vpr_context[id=”threat_intensity_last_28]	ameaça_intensidade	Mapeia a intensidade da ameaça nos últimos 28 dias do scanner para o Threat_intensity na tabela de entrada de terceiros.
u_vpr_context[id=”threat_recency”]	ameaça_recência	Mapeia as informações de recência da ameaça do scanner para Threat_recency na tabela de entrada de terceiros.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Mapeia a pontuação de impacto do CVSS v3 do scanner para v3_impact_subscore na tabela de entrada de terceiros.
u_pluginname	nome	Mapeia o nome do plug-in para a coluna de nome na tabela de entrada de terceiros.
u_stiqueseveridade	stíg_severidade	Mapeia o campo stíg_severity no plug-in para stíg_severidade na tabela de entrada de terceiros.
u_checktype	check_type	Mapeia o tipo de verificação para check_type na tabela de entrada de terceiros.
u_family.id	id_da_família	Mapeia o plug-in family.id para family_id na tabela de entrada de terceiros.
[script]	explore_attack_vector	A coluna explore_attack_vector na tabela third_party_entry é preenchida com base em explore_available e v3_attack_vector das colunas.

Campo de origem	Descrição
u_cve	Insere dados relacionados a CVE na tabela de referência (sn_vul_nvd_entry). Se o mesmo CVE na tabela de entrada do NVD (sn_vul_nvd_entry) for encontrado, ele associará a vulnerabilidade atual à entrada do NVD. O mapeamento é encontrado em sn_vul_m2m_entry_cve.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo de origem	Descrição
u_id	A lista de traqs de erros é adicionada como uma referência.
u_cpe	A lista de CPEs é adicionada como referência.
u_seealso	A lista de URLs é adicionada como uma referência.
u_xrefs	A lista de X-REFs é adicionada como referência.
u_exploitframeworks	A lista de explorações para esse plug-in e o mapeamento de inserções para a estrutura de exploração aplicável e o plug-in para sn_vul_m2m_framework_vul.

Há três scripts de transformação executados durante o processo de transformação. A tabela a seguir lista quando cada script é executado e sua finalidade.

Quando o script é executado	Finalidade
onStart (quando um conjunto de importação iniciou a transformação)	Esta transformação é usada para inicializar os valores em import_set para o processo de integração. Para uso interno. Modificar ou excluir não é recomendado.
onBefore (antes de um conjunto de importação concluir a transformação).	Função usada para atualizar os valores na vulnerabilidade e verificar se a vulnerabilidade já existe. Com base nos resultados, modifica os valores em uma tabela de itens vulneráveis. Para uso interno. Modificar ou excluir não é recomendado.
onComplete (quando um conjunto de importação concluiu a transformação).	Esta transformação é usada para definir os valores de novos IVs criados e IVs que foram atualizados e ignorados. Para uso interno. Modificar ou excluir não é recomendado.

Definir parâmetros de filtro adicionais para importações de Tenable.io

Personalize os parâmetros de filtragem das consultas programadas com Tenable Vulnerability Integration para ajudar a refinar ainda mais os dados de vulnerabilidade importados com o produto Tenable.io.

Antes de Iniciar

Casos de uso: como gerente ou analista de vulnerabilidade, convém filtrar os dados de suas consultas para que você possa revisar somente os detalhes específicos da vulnerabilidade. Por exemplo, digamos que você queira exibir vulnerabilidades importadas que são filtradas por `cidr_range`, `num_assets`, `indexed_at`e `plugin_family`. Ou digamos que você queira executar uma integração Tenable.io de modo que uma execução importe somente vulnerabilidades críticas a cada quatro horas e outra seja executada a cada 24 horas para buscar todas as outras vulnerabilidades não críticas.

Para ajudá-lo a coletar esses dados, você pode adicionar parâmetros compatíveis com a Tenable para ajudá-lo a importar os detalhes da vulnerabilidade específica de que precisa.

Sem adicionar chamadas de API ou codificação adicionais, este recurso permite que você personalize suas informações de solicitação HTTP com parâmetros da Tenable em seu Now Platform. As seguintes integrações Tenable.io oferecem suporte à filtragem, fornecendo conteúdo JSON no corpo da solicitação:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Integração de ativos
- Integração de vulnerabilidade fixa
- Abrir integração de vulnerabilidades

Você deve saber como usar cadeias de caracteres JSON para este recurso.

Função necessária: sn_vul.vulnerability_admin

Procedimento

1. Localize os parâmetros compatíveis com o produto Tenable.io no site do desenvolvedor que você deseja usar para sua filtragem.

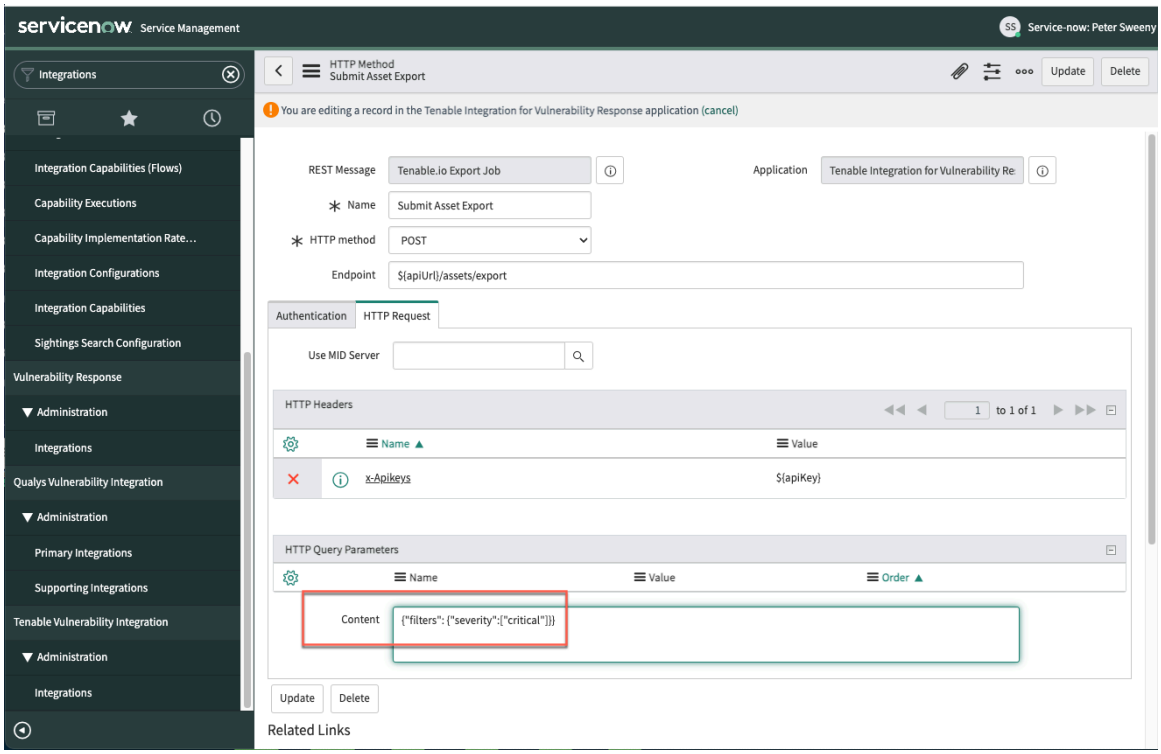
   Os parâmetros e valores inseridos no produto Tenable.io são compatíveis somente no nível da instância de integração.

2. Navegar até **Todos** > **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
3. Na página da lista de integrações da Tenable, clique no registro da integração Tenable.io que você deseja abrir.
4. Com a guia Métodos REST da Tenable selecionada, clique no ícone de informações (I) do método REST seguido por **Abrir registro**.
5. Selecione a guia **Solicitação HTTP**.
6. Para editar o registro, na parte superior da página, clique no link em. Para editar o registro, clique **aqui**.
7. No registro Método REST no campo Conteúdo, insira o conteúdo JSON que você deseja como parte do corpo da solicitação.

   Na imagem a seguir, como exemplo, o parâmetro de severidade das vulnerabilidades importadas, `{"filters": {"severity": ["critical"]}}` foi personalizado para a integração de ativos Tenable.io. Este valor importa somente vulnerabilidades críticas (pontuação de CVSS de 10,0).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se você quiser inserir mais de um parâmetro, consulte a documentação Tenable.io para obter mais informações sobre como separar cada valor.

8. Clique em **Atualizar**.

Relatório de integração de vulnerabilidade da Tenable

Exiba relatórios sobre vulnerabilidades e itens vulneráveis nos painéis Vulnerability Response.

Visualizações de dados nos espaços Vulnerability Response

Os espaços Vulnerability Response incluem visualizações de dados que podem ajudar a monitorar o andamento da correção. Você pode determinar o nível de ameaça para sua organização exibindo o número e a severidade das vulnerabilidades ativas que são importantes para sua organização em visualizações de dados dinâmicos que são atualizadas conforme os dados de vulnerabilidade mudam. Consulte Vulnerability Response Espaços, Explorando o Vulnerability Manager Workspace e Explorando o Espaço de correção de problemas de TI para obter mais informações sobre as visualizações de dados dinâmicos que estão disponíveis.

Versões anteriores de Vulnerability Response

O painel de visão geral do Vulnerability Response (Vulnerability Management) fornece uma visão executiva de vulnerabilidades e itens vulneráveis, ajudando o Administrador de Vulnerabilidades a identificar rapidamente as áreas de preocupação. O painel de correção do Vulnerability Response (Correção de vulnerabilidade) permite que um especialista em correção se concentre nas tarefas de correção e nos itens vulneráveis que possui.

Para obter mais informações, consulte Usando os painéis padrão Vulnerability Response.

Função necessária: responsável pela correção.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que os usuários podem fazer e ver na aplicação Vulnerability Response. Para obter a atribuição inicial das

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração.

Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

para exibir o painel, navegue até **Vulnerability Response** > **Visão Geral da Correção**.

Gráfico de status de execução da integração para a integração de vulnerabilidade da Tenable

O módulo Status de execução de integração da Tenable fornece uma exibição gráfica do status das execuções de integração da Tenable.

No gráfico, aponte para qualquer parte do gráfico para exibir um resumo dos dados específicos dessa parte. Se você clicar em qualquer parte do gráfico de barras, uma lista será aberta para fornecer informações mais detalhadas.

Função necessária: administrador de vulnerabilidade.

Persona e funções granulares estão disponíveis para ajudá-lo a gerenciar o que os usuários podem fazer e ver na aplicação Vulnerability Response. Para obter a atribuição inicial das funções de persona no Assistente de configuração, consulte Atribua as funções de persona Vulnerability Response usando o Assistente de configuração.

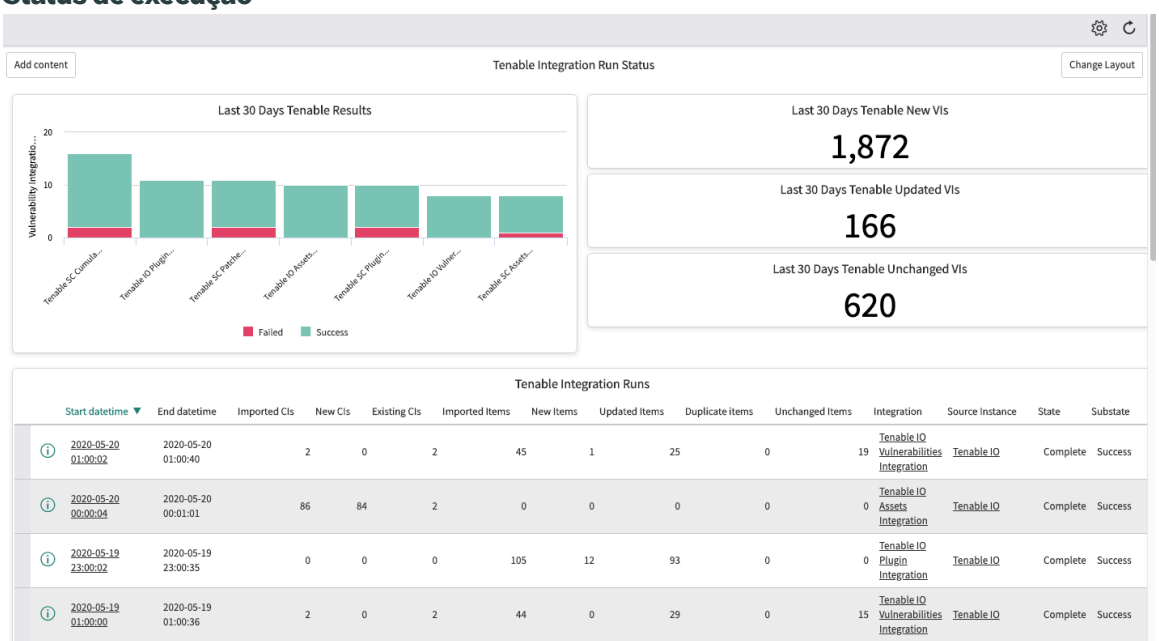
Para obter mais informações sobre como gerenciar funções granulares, consulte Gerenciar persona e funções granulares para Vulnerability Response.

Para exibir os dados, navegue até **Todos** > **Integração de vulnerabilidade Tenable** > **Status da Execução da Integração**.

A partir da versão 19.0 do Vulnerability Response, este painel está disponível na IU da nova experiência.

Nota:
Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Status de execução



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

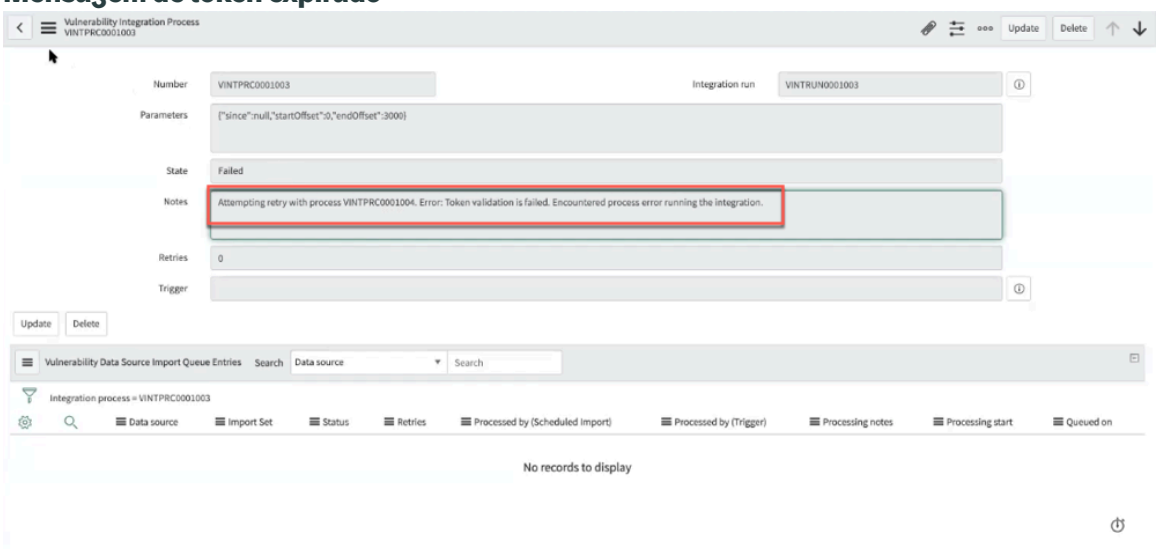
Relatórios do gráfico de status de execução da integração da Tenable

Nome	Descrição
Resultados do Tenable nos últimos 30 dias	O número de execuções de integração concluídas para cada integração. Mostra execuções bem-sucedidas e com falha. Cada execução exibida como uma barra no gráfico.
VIs novos do Tenable nos últimos 30 dias	O número de novos itens vulneráveis importados nos últimos 30 dias. Mostrado como um número inteiro.
VIs atualizados do Tenable nos últimos 30 dias	O número de itens vulneráveis atualizados importados nos últimos 30 dias. Mostrado como um número inteiro.
VIs inalterados do Tenable nos últimos 30 dias	O número de itens vulneráveis duplicados importados nos últimos 30 dias. Mostrado como um número inteiro.
Execuções de integrações do Tenable	Os registros de execução de integração em uma lista. **Nota:** **V16.1:** para verificar as detecções para esta integração, compare as detecções ou descobertas com os dados de detecção ServiceNow`sn_vul_detection`] na tabela . Enquanto a integração está em andamento, pode haver uma mudança na detecção ou na contagem de descobertas. Este relatório exibe a contagem de detecções na coluna "Contagem até a data" na instância, após a conclusão da execução da integração.

Expiração da validação do token

Se uma execução de integração do Tenable.sc falhar por qualquer motivo, o token de autenticação do Tenable.sc expirará automaticamente e uma mensagem será exibida no registro do Processo de integração de vulnerabilidade.

Mensagem de token expirado



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Um novo token é gerado automaticamente para o próximo processo de integração. Todos os processos de integração, com falha e bem-sucedidos, são exibidos na guia Processo de integração de vulnerabilidade no registro do Processo de integração de vulnerabilidade.

Iniciar nova verificação para a integração Tenable.sc

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados iniciando novas verificações na plataforma Tenable. Você pode iniciar uma nova verificação sob demanda de itens vulneráveis para o produto Tenable.sc da sua instância Now Platform®.

Antes de Iniciar

Funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Nota:
Tenable.sc não é compatível com a inicialização de uma nova verificação em máquinas baseadas em agente.

Verifique se o scanner está ativado antes de começar. Navegar até **Vulnerability Response** > **Verificação de Vulnerabilidades** > **Scanners**.

Por Que e Quando Desempenhar Esta Tarefa

Para iniciar a nova verificação nos espaços, consulte Verificar novamente Tenable.io e Tenable.sc itens vulneráveis dos espaços Vulnerability Response.

Siga as etapas listadas abaixo para iniciar uma nova verificação no ambiente clássico.

Para ajudar a reduzir a sobrecarga e o volume envolvidos nas verificações completas programadas, os proprietários de correção, especialistas em TI, analistas de vulnerabilidade ou gerentes de vulnerabilidade podem iniciar novas verificações direcionadas sob demanda para vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas verificações de item vulnerável (IV), tarefas de correção (RT), entrada de terceiros (TPE) ou registros de item descoberto da sua instância Now Platform.

As novas verificações permitem que os proprietários de correção e os analistas de vulnerabilidade verifiquem se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

Por exemplo, todo o ambiente é verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada de seus Now Platform para Tenable.sc itens vulneráveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Ao solicitar uma nova verificação da sua instância Now Platform®, a seleção das credenciais Integração do Vulnerability Response com Tenable é opcional. O ServiceNow® Tenable.sc Scan Credential Integration importa e atualiza as credenciais do scanner do produto Tenable.sc em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais da Tenable.

Observe que esses dados importados não incluem senhas da Tenable ou outras informações confidenciais da conta da Tenable. A ServiceNow® Tenable.sc Integração de credencial de verificação é habilitada (Ativo) automaticamente no Assistente de configuração em sua instância quando você configura as Tenable.sc Integrações de vulnerabilidades (Tenable.sc Integrações de vulnerabilidades abertas e corrigidas).

Observe as seguintes informações sobre as credenciais importadas para que os usuários possam vê-las conforme necessário na instância Now Platform :

- As credenciais criadas com a função de usuário administrador Tenable.sc estão disponíveis para usuários em todas as suas organizações.
- As credenciais criadas com a função de usuários organizacionais Tenable.sc estão disponíveis somente para usuários dessa organização. Essas credenciais não são importadas para o Now Platform para usuários fora da organização do criador, a menos que sejam compartilhadas com a conta do usuário que está sendo usada para se conectar à instância.

Consulte o site de documentação Tenable.sc para obter mais informações.

Consulte Configurar a integração de vulnerabilidade da Tenable usando o assistente de configuração para obter mais informações sobre como configurar a aplicação Tenable.sc. Para exibir mais informações sobre o Scan Credential Integration, navegue até **Todos** > **Integração de vulnerabilidade Tenable** > **Integrações** > **Integração de credencial de verificação da Tenable.sc**.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- `sn_sec_cmn.record_threshold_heartbeat`: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- `sn_sec_cmn.maximum_heartbeat_delay`: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Itens vulneráveis**.
2. Localize o registro do item vulnerável do qual você deseja acionar uma nova verificação e abra-o.

   Nota:
   Você só pode iniciar novas verificações de IVs com Tenable.sc como origem. Verifique se Tenable.sc é exibido na coluna **Origem** nas exibições de Lista de IV ou nos campos **Origem** em registros individuais. Você pode usar o construtor de condição para agrupar IVs por origem. Ou, se a coluna Origem não for exibida na exibição da lista de IVs, no canto superior esquerdo da lista, clique no ícone **Personalizar lista** (ícone de engrenagem) e use o Slushbucket para mover a **origem** de **Disponível** para **Selecionado**.

3. Como alternativa, navegue até **Todos** > **Vulnerability Response** > **Tarefas de correção** ou **Vulnerability Response** > **Bibliotecas** > **Terceiros** para a tarefa de correção ou registros de entrada de terceiros, respectivamente, que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o botão **Verificar novamente** está disponível nos seguintes registros:

   - Em um único registro de IV, o IV deve ser do produto Tenable.sc e em qualquer estado diferente de **Encerrado**. Para vários registros de IV, todos os IVs devem ser do produto Tenable.sc e em qualquer estado diferente de **Encerrado**.
   - Em um registro RT, a tarefa de correção pode estar em qualquer estado diferente de **Encerrado**e todos os IVs associados devem ser do produto Tenable.sc.
   - Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro IV associado do produto Tenable.sc em qualquer estado diferente de **Encerrado**.

4. No canto superior direito do registro, clique em **Verificar novamente**.
   Você será solicitado a escolher as credenciais do scanner para acessar o scanner. Essas são as credenciais importadas pela Tenable.sc Scan Credential Integration.
5. Na caixa de diálogo, selecione os filtros e os tipos de credencial desejados.
6. Clique **em Solicitar verificação**.

   Uma mensagem será exibida indicando que a verificação está sendo processada. O status de todas as novas verificações pode ser encontrado a qualquer momento nas listas relacionadas à verificação nos registros IV, RT e TPE usados para iniciar as novas verificações. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e todas as outras verificações iniciadas a partir de um determinado registro.

   O campo Estado no registro de verificação primário é marcado como concluído depois que todas as verificações secundárias são concluídas com sucesso. O secundário verifica os dados de importação. O registro de verificação primário é um contêiner para as verificações secundárias.

   Sua instância Now Platform® rastreia o status de nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando Now Platform® parou de acompanhar seu status de nova verificação, não quando a nova verificação real parou. Todos os IVs que fizeram a transição ou farão a transição para **Encerrado/Corrigido** são importados com a próxima importação programada da integração de vulnerabilidades corrigidas da Tenable.sc.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Iniciar nova verificação para a integração Tenable.io

Verifique se os itens vulneráveis foram corrigidos entre os ciclos de verificação programados iniciando novas verificações na plataforma Tenable. Você pode iniciar uma nova verificação sob demanda de itens vulneráveis para o produto Tenable.io da sua instância Now Platform®.

Antes de Iniciar

Funções necessárias: sn_vul.write_all ou sn_vul.write_assigned

Verifique se o scanner está ativado antes de começar. Navegar até **Vulnerability Response** > **Verificação de Vulnerabilidades** > **Scanners**.

Por Que e Quando Desempenhar Esta Tarefa

- Consulte e Verificar novamente registros e tarefas de correção no Vulnerability Manager Workspace e Verifique novamente itens vulneráveis e tarefas de correção no Espaço de correção de problemas de TI para iniciar uma nova verificação nos espaços do Vulnerability Response.
- Siga as etapas listadas abaixo para iniciar uma nova verificação no ambiente clássico.

Nota:
Tenable.io não é compatível com a inicialização de uma nova verificação em máquinas baseadas em agente.

Para ajudar a reduzir a sobrecarga e o volume envolvidos com verificações completas programadas, como proprietário de correção, especialista de TI, analista de vulnerabilidade ou gerente de vulnerabilidade, você pode iniciar novas verificações direcionadas sob demanda. você pode verificar vulnerabilidades específicas em ativos (itens de configuração) em seus ambientes. Você pode iniciar novas verificações a partir de item vulnerável (IV), tarefas de correção (VUL), entrada de terceiros (TPE) ou registros de item descoberto (SDI) da sua instância Now Platform. As novas verificações permitem que você verifique se suas atividades de correção, patches e outras ações corrigiram vulnerabilidades específicas em seus itens de configuração (ICs).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Ao solicitar uma nova verificação da sua instância Now Platform®, a seleção das credenciais Integração do Vulnerability Response com Tenable é opcional. O ServiceNow® Tenable.io Scan Credential Integration importa e atualiza as credenciais do scanner do produto Tenable.io em sua instância. Esta integração é executada semanalmente para importar e armazenar com segurança seus dados de credenciais da Tenable.

Observe que esses dados importados não incluem senhas da Tenable ou outras informações confidenciais da conta da Tenable.

As informações a seguir descrevem as credenciais que você importa para que os usuários possam vê-las conforme necessário na sua instância Now Platform :

- As credenciais criadas com a função de usuário administrador Tenable.io estão disponíveis para usuários em todas as suas organizações.
- As credenciais criadas com a função de usuários organizacionais Tenable.io estão disponíveis somente para usuários dessa organização. Essas credenciais não são importadas para o Now Platform para usuários fora da organização do criador, a menos que sejam compartilhadas com a conta do usuário que está sendo usada para se conectar à instância.

  Consulte o site de documentação Tenable.io para obter mais informações.

- A integração de modelo Tenable.io e a integração de credencial de verificação Tenable.io devem ser ativadas antes de iniciar novas verificações. Para exibir mais informações sobre o Scan Credential Integration, navegue até **Integração de vulnerabilidade Tenable** > **Integrações** > **Integração de credencial de verificação da Tenable.io**.

  Por padrão, as integrações de modelo e credencial de verificação são desativadas. Quando você insere suas credenciais para Tenable.io, todas as integrações Tenable.io são ativadas automaticamente. Para ativar ou desativar manualmente essas integrações:

  1. Navegar até **Todos** > **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
  2. Na lista exibida, localize os registros de integração Tenable.io desejados.
  3. Abra cada registro e marque a caixa de seleção **Ativo** para ativar a integração.
  4. Clique em **Atualizar** para salvar suas mudanças.
  5. Retorne ao Assistente de configuração para continuar com sua configuração para Tenable Vulnerability Integration com Vulnerability Response.

Consulte Configurar a integração de vulnerabilidade da Tenable usando o assistente de configuração para obter mais informações sobre como configurar os produtos Tenable.io e Tenable.sc.

Digamos que todo o seu ambiente seja verificado uma vez a cada três semanas. A verificação completa mais recente foi concluída há uma semana, mas você aplicou um patch ontem para corrigir uma vulnerabilidade crítica. Devido à natureza desta vulnerabilidade, você não pode esperar duas semanas pela próxima verificação programada para verificar se ela foi corrigida. Para verificar se o patch corrigiu com sucesso uma vulnerabilidade crítica descoberta durante uma verificação anterior, você pode iniciar uma nova verificação direcionada de seus Now Platform para Tenable.io itens vulneráveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode exibir resultados atualizados nos registros a partir dos quais iniciou as verificações após a próxima importação programada da integração de vulnerabilidades corrigidas.

Durante a execução da integração, vários processos são gerados e os dados são recebidos na forma de páginas. Cada processo pode conter uma ou mais entradas da fila de importação com dados anexados em páginas. Essas entradas devem processar os dados dentro do limite de uma hora. No entanto, se o tamanho da carga for grande, o tempo de processamento poderá exceder uma hora ou ficar travado, resultando em um erro de tempo limite de integração. A integração continua a processar os dados, apesar do erro de tempo limite. Para evitar essa falha de comunicação, a partir da versão 18.2.4 do Vulnerability Response, os carimbos de data/hora (pulsações) são enviados periodicamente para indicar se a fila está ativa e processando dados. O campo **Último registro processado** na página Entrada da fila de importação é atualizado com base na contagem de registros que a fila de importação cria ou atualiza. Caso uma entrada da fila de importação exceda o limite de uma hora, o sistema verificará o campo **Último registro processado** para ver se ele também tem mais de uma hora. Em caso afirmativo, isso indica que a entrada da fila de importação está travada e expirou para evitar mais atrasos no processamento.

Nota:
O campo **Último registro processado** é atualizado com base no que é definido nas seguintes propriedades do sistema:

- `sn_sec_cmn.record_threshold_heartbeat`: define o número de registros processados, após o qual a pulsação (carimbo de data/hora) é enviada para a entrada da fila de importação.
- `sn_sec_cmn.maximum_heartbeat_delay`: define o tempo após o qual a entrada da fila de importação deve atingir o tempo limite.

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Itens vulneráveis**.
2. Localize o registro do item vulnerável do qual você deseja acionar uma nova verificação e abra-o.

   Nota:
   Se você estiver usando o scanner Tenable.io, só poderá iniciar novas verificações de IVs com Tenable.io como origem. Verifique se Tenable.io é exibido na coluna **Origem** nas exibições de Lista de IV ou nos campos **Origem** em registros individuais. Você pode usar o construtor de condição para agrupar IVs por origem. Ou, se a coluna Origem não for exibida na exibição da lista de IVs, no canto superior esquerdo da lista, clique no ícone **Personalizar lista** (ícone de engrenagem) e use o Slushbucket para mover a **origem** de **Disponível** para **Selecionado**.

3. Como alternativa, navegue até **Todos** > **Vulnerability Response** > **Tarefas de correção** ou **Vulnerability Response** > **Bibliotecas** > **Terceiros** para os registros que você deseja usar para a nova verificação.

   Dependendo da sua escolha, o botão **Verificar novamente** está disponível nos seguintes registros:

   - Em um único registro de IV, o IV deve estar em qualquer estado diferente de **Encerrado**. Para vários registros de IV, todos os IVs devem ser do produto Tenable.io e em qualquer estado diferente de **Encerrado**.
   - Para registros de tarefa de correção, somente tarefas de correção em qualquer estado diferente de **Encerrado** são compatíveis. Todos os IVs associados devem estar em qualquer estado diferente de **Encerrado** e usar Tenable.io como origem.

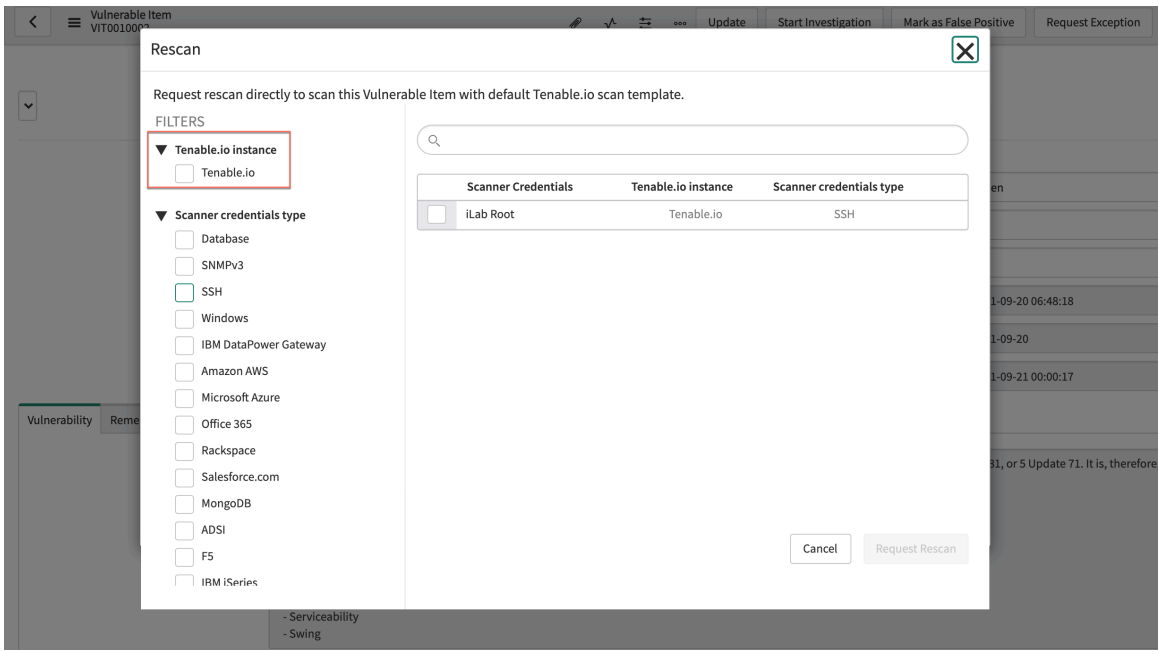
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Em um registro de entrada de terceiros (TPE), o registro deve ter pelo menos um registro IV associado do produto Tenable.io em qualquer estado diferente de **Encerrado**.
- Em registros de itens descobertos, o registro deve ter pelo menos um registro IV associado do produto Tenable.io em qualquer estado diferente de **Encerrado**.
- Na lista Itens vulneráveis, você pode selecionar itens vulneráveis individuais que deseja verificar novamente. Use o menu Ações nas linhas selecionadas no canto inferior esquerdo da tela para iniciar a nova verificação. Você será solicitado a inserir suas credenciais.

4. No canto superior direito de um registro, clique em **Verificar novamente**.
   Você será solicitado a escolher a instância ou as instâncias para a nova verificação e as credenciais do scanner que deseja usar para acessar o scanner. As credenciais exibidas são aquelas importadas pela Tenable.io Scan Credential Integration.
5. Na caixa de diálogo, selecione a instância e ou as instâncias e os tipos de credencial que você deseja usar.

   Na imagem a seguir, uma instância de integração, Tenable.io, é exibida. Se você tiver mais de uma instância Tenable.io, todas elas serão exibidas na seção Tenable.io no formulário.



6. Clique **em Solicitar nova verificação**.

   Uma mensagem é exibida indicando que a verificação está sendo processada e que um registro de verificação primário foi criado. O status de todas as verificações secundárias pode ser encontrado a qualquer momento nas listas relacionadas à verificação no IV, na tarefa de correção, no TPE e nos registros de SDI usados para iniciar as novas verificações. Na mensagem, clique em **Exibir detalhes** para exibir o status da nova verificação e todas as outras verificações iniciadas a partir de um determinado registro.

   O campo Estado no registro de verificação primário é marcado como concluído depois que todas as verificações secundárias são concluídas com sucesso. O secundário verifica os dados de importação. Cada verificação oferece suporte a uma combinação exclusiva de instância de integração, TPE, IP e ID de rede. Você pode ver várias verificações secundárias em um registro de verificação primário. Por exemplo, o número máximo de endereços IP que uma verificação secundária pode suportar é 1000. Se houver 1002 IPs para um item vulnerável, duas verificações secundárias serão criadas e listadas na lista

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

relacionada Verificações para oferecer suporte à solicitação. O registro de verificação primário é um contêiner para as verificações secundárias e seu estado de reflete o status das verificações secundárias.

Sua instância Now Platform® rastreia o status de nova verificação até que ela seja concluída com sucesso ou até que o período de acompanhamento definido expire, o que acontecer primeiro. O tempo limite não interrompe a verificação. O tempo limite se refere a quando Now Platform® parou de acompanhar seu status de nova verificação, não quando a nova verificação real parou. Todos os IVs que fizeram a transição, ou farão a transição, para **Encerrado/Corrigido** são importados com a próxima importação programada da Tenable.io Integração de vulnerabilidades fixas.

Para verificações com erro, você pode verificar as verificações secundárias no registro de verificação primário. Exiba o erro na carga de resposta da verificação secundária.

Você pode exibir resultados atualizados nos registros a partir dos quais iniciou as verificações após a próxima importação programada da integração de vulnerabilidades corrigidas.

Atualizar itens de configuração com o identificador de partição de rede para Tenable Vulnerability Integration

Crie itens de configuração (ICs) exclusivos para ativos em seu ambiente que compartilham endereços IP. Identifique os ativos distintos em seu ambiente e atualize automaticamente os ICs em seu item descoberto existente, item vulnerável e registros de detecção para fornecer mais detalhes sobre suas vulnerabilidades.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Por padrão na aplicação Vulnerability Response, uma maneira de identificar seus ativos é por endereço IP. Em determinados casos, os ativos podem compartilhar endereços IP, mas eles são armazenados como um IC no seu CMDB.

Por exemplo, conforme mostrado nas tabelas a seguir, vários ativos (IC) em seu ambiente podem compartilhar endereços IP, mas têm IDs de rede e repositório exclusivos. No entanto, por padrão, esses ativos são normalmente identificados e armazenados como um único IC (IC 1) durante a pesquisa de endereço IP.

Pesquisa de IP padrão e criação de IC

Origem	Endereço IP	Network_id	Item de configuração
Tenable.io: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1
	123.12.12.141	03713	IC 1

Origem	Endereço IP	Repository_id	Item de configuração
Tenable.sc: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1
	123.12.12.141	13	IC 1

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode criar ICs individuais para ativos que têm o mesmo endereço IP para que possa identificá-los como ativos distintos. Iniciando de uma importação de dados recente, você pode atualizar seus ICs existentes com mais granularidade que inclua o identificador de partição de rede [network_partition_identifier] executando o trabalho programado, *`Update existing discovered items with network partition identifier`*.

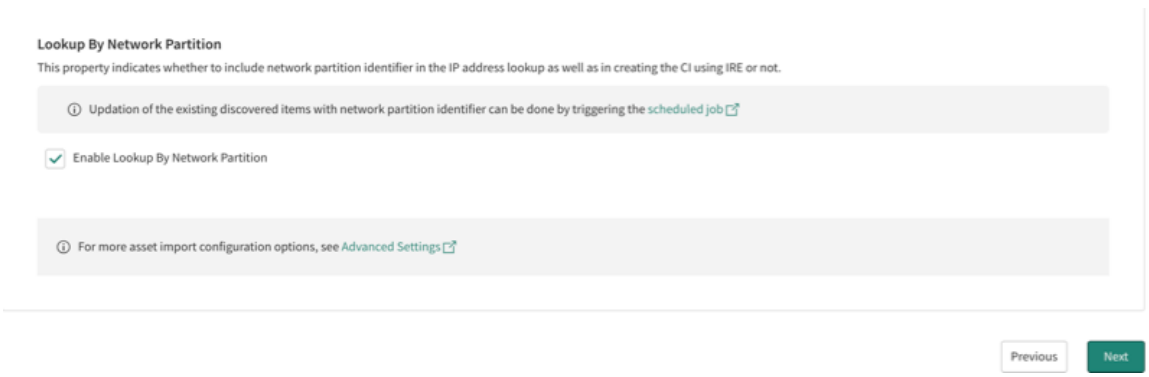
Este trabalho programado está desabilitado por padrão. Ative este recurso para os ativos e integrações de vulnerabilidades fixas e abertas para os produtos Tenable.io e Tenable.sc no Assistente de configuração para exibir este identificador em seus registros.

Quando ativado, este trabalho programado adiciona o identificador de partição de rede [network_partition_identifier] aos registros de IC existentes a partir de dados importados. Os ICs existentes criados pelo IRE também são atualizados. O trabalho programado também cria ICs que incluem o identificador da partição de rede que começa com a próxima importação. Como alternativa, você pode iniciar o trabalho sob demanda para atualizar os dados existentes.

Quando você atualiza a partir da v14.0 de Vulnerability Response e v2.2 do Tenable Vulnerability Integration, os CMDB CI Class Models (1.0.21.) são compatíveis. Os modelos de classe têm o identificador de partição de rede [network_partition_identifier] nas regras de identificação de Identificação e Reconciliação (IRE).

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Assistente de configuração** > **Configuração de Integração** > **Integrações do Scanner**.
2. Selecione Tenable.io integrações ou Tenable.sc integrações.
3. **Edite** a integração necessária.
4. Selecionar **Configuração de importação de ativo**.
5. Selecionar **Habilitar pesquisa por partição de rede** caixa de seleção do **Habilitar pesquisa por partição de rede** seção.



6. Clique em **Avançar**.

   Os identificadores de partição de rede NETWORK_ID e REPOSITORY _ID estão incluídos e atualizam os ICs existentes ou criam ICs com o próximo trabalho programado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atributo do identificador de partição de rede incluído na pesquisa de IP e na criação de IC

Origem	Endereço IP	NETWORK_Identifi	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Tenable.io: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	03712	IC 1	IC 1
	123.12.12.141	03713	IC 1	IC 2

Origem	Endereço IP	REPOSITÓRIO_ID	IC para ativos sem identificador de partição de rede	Ativos de ICs com identificador de partição de rede
Tenable.sc: integrações de ativos e vulnerabilidades fixas e abertas	123.12.12.141	12	IC 1	IC 1
	123.12.12.141	13	IC 1	IC 2

Com o próximo trabalho programado, as regras de pesquisa de identificação de IC de endereço IP e endereço IP incompleto incluem o atributo do identificador de partição de rede automaticamente para uma importação de dados das integrações de ativos e vulnerabilidades fixas e abertas para os produtos Tenable.io e Tenable.sc.

Depois de habilitar a propriedade do sistema e salvar os registros, você pode atualizar os itens descobertos existentes com ICs que incluem o identificador de partição de rede iniciando os trabalhos programados sob demanda.

Importar modificações para a integração de vulnerabilidade da Tenable

Configure modificações opcionais e simplifique alguns dos dados especificamente para a integração de importação de vulnerabilidades da Tenable na ServiceNow® Integração de vulnerabilidade da Tenable.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin

Por Que e Quando Desempenhar Esta Tarefa
Este conjunto de tarefas requer codificação e conhecimento avançado sobre o Now Platform.

Siga estas etapas para criar importações separadas por domínio para as integrações de vulnerabilidades da Tenable. O exemplo a seguir é para a integração Tenable.io Open Vulnerabilities, mas este conteúdo é aplicável às outras integrações da Tenable.

Procedimento

1. Crie um domínio.
2. Para cada domínio criado, crie um usuário e atribua o usuário a esse domínio.

   Pense neste usuário como um espaço reservado run_as para o domínio em Tenable.io.

Tradução automática

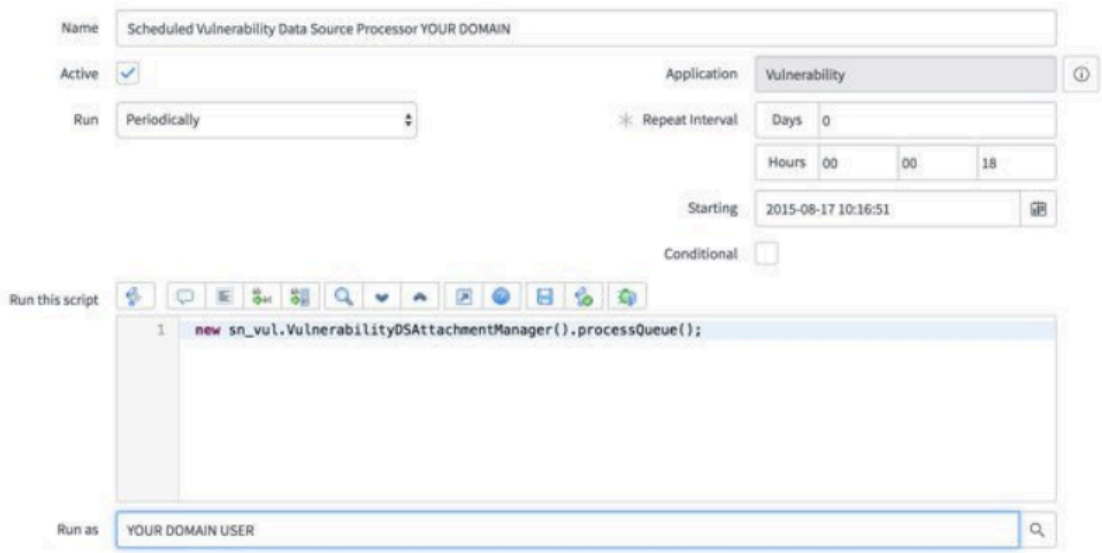
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Abra a integração de vulnerabilidades.
   O usuário é o equivalente ao usuário VR.System no domínio global e deve ter as seguintes funções: sn_vul.tenable_configure_integration, import_admin e sn_vul.vulnerability_write. Este usuário requer acesso a fontes de dados, mapas de transformação e dados de vulnerabilidade.

   Nota:
   Considere este usuário como específico para esta função. O usuário não deve ter nenhuma outra finalidade

4. Em cada domínio, crie um trabalho programado copiando o Processador de Fonte de Dados de Vulnerabilidade Programada encontrado em **Definição do Sistema** > **Trabalhos programados**.
5. Anexe o domínio ao nome para identificar o trabalho programado.
6. Altere o usuário run_as para o usuário que você criou na etapa anterior.

   Nota:
   Edite a seguinte ação de IU para que a integração seja executada no domínio do usuário run_as.



7. Edite a ação de IU Executar agora na integração de vulnerabilidades em aberto da Tenable.io para adicionar este bloco de código à parte superior do arquivo.
   ```
   //sys id below is of Tenable.io integration if(current.sys_id == "4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }
   ```

   Nota:
   Edite as inclusões de script a seguir para que a integração seja executada no domínio do usuário run_as.

8. Edite o método de inclusão de script VulnerabilityIntegrationUtils addIntegrationRun para adicionar o código realçado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. Edite o método de inclusão de script VulnerabilityIntegrationUtils addProcessRun para adicionar o código realçado.

```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Edite o método de inclusão de script DataSourceVulnReportRefreshProcessor _processFromDataSourceGroups para mudar este código original: Código _processFromDataSourcesGroups original para código _processFromDataSourcesGroups editado.
11. Edite o método de inclusão de script VulnerabilityDSAttachmentManager, queueItem, para adicionar os seguintes blocos de código realçados queueItem, _getNext, _processQueueEntry.

Você está pronto para importações de detecção de host separadas por domínio.

Desabilitar calculadoras antes da importação

Siga estas etapas para desabilitar a calculadora padrão se não for usada. Se você não usar calculadoras de vulnerabilidade, é melhor desabilitar as calculadoras padrão, além de quaisquer outras que você tenha definido. As calculadoras de vulnerabilidade são executadas sempre que um registro de item vulnerável é acessado e pode afetar o desempenho da instância.

Função necessária: sn_vul.vulnerability_admin.

12. Navegar até **Todos** > **Vulnerabilidade** > **Administração** > **Calculadoras de vulnerabilidade**.
13. Abra o grupo Impacto de vulnerabilidade.
14. Abra a calculadora de pontuação e impacto baseado em serviço.
15. Desmarque o campo Ativo para desativar a calculadora.
16. Clique em Atualizar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você desativou a calculadora padrão.

Desabilitar regras de negócios baseadas em notificação antes da importação inicial

Siga estas etapas para desabilitar Desabilitar regras de negócios relacionadas à notificação antes da importação de registro inicial. Durante a importação inicial de registros, determinadas regras de negócios relacionadas à notificação podem gerar muitas notificações, afetando o desempenho. Essas regras de negócios devem ser modificadas para desativá-las durante a importação.

A função necessária é sn_vul.vulnerability_admin.

17. Navegar até **Todos** > **Definição do Sistema** > **Regras de negócios**.
18. Pesquise notificações de IC afetado.
19. Abra a regra de negócios e insira a seguinte condição: `current.sys_class_name != “sn_vul_vulnerable_item"`.
20. Clique em **Atualizar**.
21. Repita este procedimento para as seguintes regras de negócios:
    - Notificações de centro de custos afetado
    - Notificações do grupo afetado
    - Notificações de local afetado

Nota:
Após a conclusão da importação do registro inicial, você terá a opção de reativar essas regras de negócio. No entanto, considere deixá-los desabilitados. Eles podem gerar um grande número de notificações e afetar o desempenho da sua instância.

Modificar uma data de início inicial

Siga estas etapas para modificar uma data de início inicial. Durante a instalação usando o Assistente de configuração, você define uma data de início inicial para as integrações da Tenable. Você pode redefinir essa data de início no Assistente de configuração ou na integração primária, conforme mostrado nas etapas a seguir.

22. Navegar até **Todos** > **Integração de vulnerabilidade Tenable** > **Administração** > **Integrações**.
23. Clique em qualquer integração.
24. Clique em Detalhes da integração.
25. Defina o campo Hora de início com um valor no passado, para que todas as vulnerabilidades verificadas e detectadas desde essa hora sejam detectadas.

    Se você configurou o Tenable usando o Assistente de configuração, o campo Hora de início será preenchido previamente, inicialmente para três meses antes da data de hoje e, subsequentemente, para a data de hoje. Observação: considere definir o valor como no máximo um mês no passado. Isso evita que uma grande quantidade de dados exceda as limitações de taxa da API da Tenable, bem como aciona os tempos limites de execução.

26. Clique em **Enviar** ou **Atualizar**.
27. **Opcional:** Clique **em Executar agora** para executar imediatamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

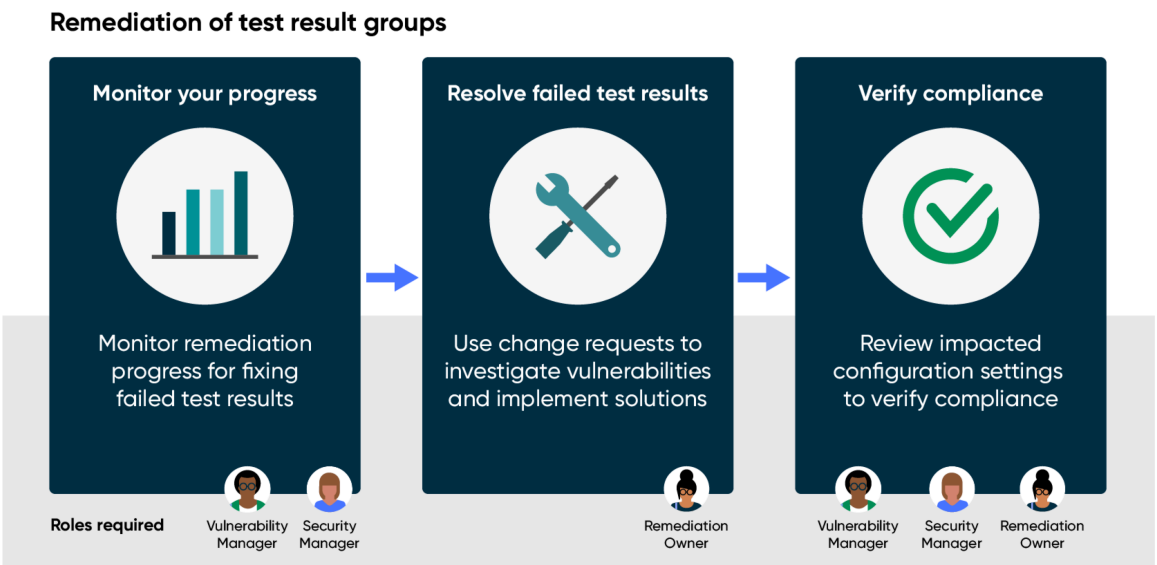
Configuration Compliance correção

Configuration Compliance A correção é principalmente um processo manual aumentado por trabalhos programados (integrações), tarefas de grupo de resultados de testes, fluxos de trabalho e solicitações de mudança.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste



Plug-ins SCA de terceiros separados adquirem e transformam dados em Configuration Compliance. Antes de usar Configuration Compliance para corrigir itens de configuração, você deve instalar uma integração de scanner de terceiros e executar pelo menos uma verificação de rede.

Use solicitações de mudança para corrigir falhas de teste individuais de grupos de resultados de teste.

Os estados dos grupos de resultados de testes fazem a transição automaticamente conforme as solicitações de mudança associadas se movem por seus ciclos de vida com Sincronização de estado entre solicitações de mudança e tarefas de correção. Usuários com a função itil podem criar e gerenciar solicitações de mudança diretamente de grupos de resultados de testes.

Criar manualmente uma tarefa de correção Configuration Compliance

Você pode criar manualmente uma tarefa de correção no módulo **Grupos de resultados de teste** e executar a correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa
O uso de regras de grupo de resultados de testes preenche automaticamente a guia **Resultados de testes**. A criação manual é útil para um grupo que não precisa de uma regra ou de ser repetido.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

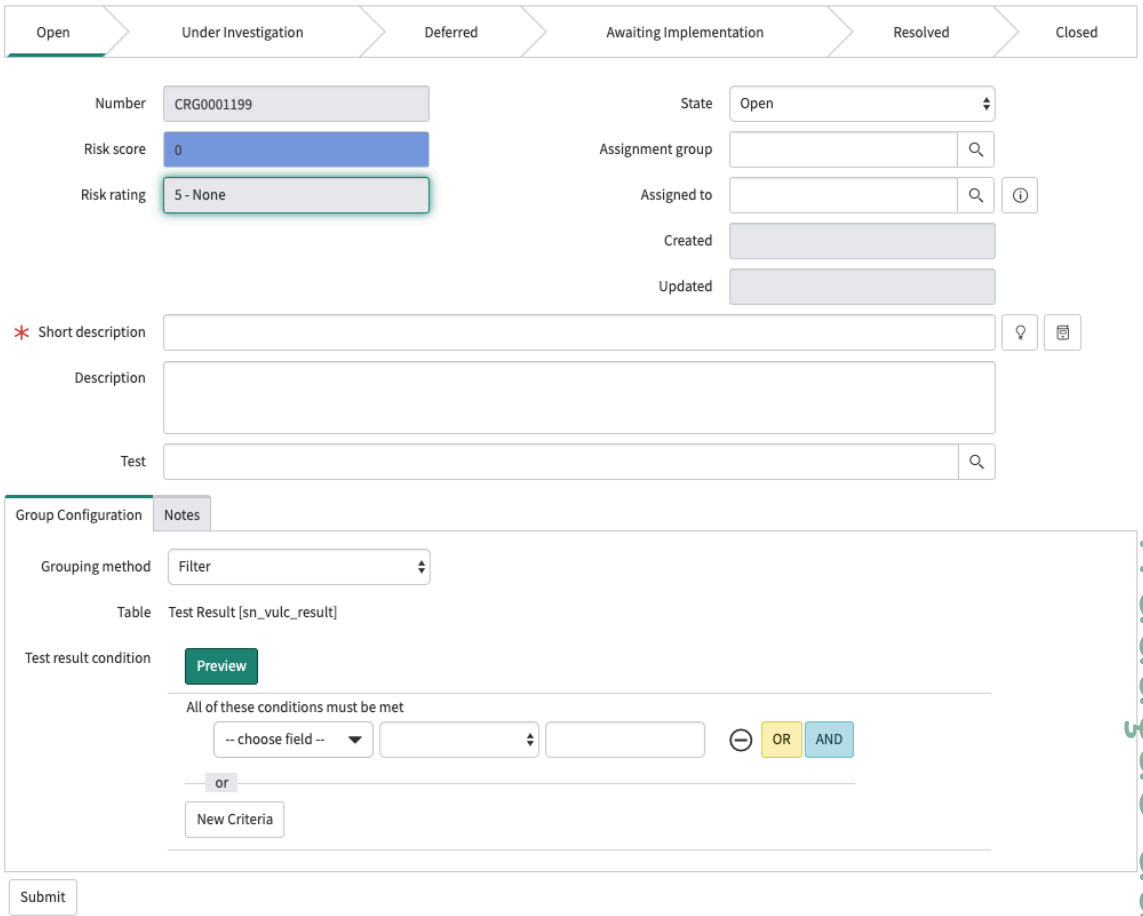
Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento
1. Navegar até **Todos** > **Configuration Compliance** > **Tarefas de correção**.
2. No painel de navegação, clique em **Minhas tarefas abertas** ou **Todas as tarefas abertas** para exibir a lista.
3. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Grupo de resultados de testes



4. Preencha os campos no formulário de Tarefa de correção, conforme apropriado.

Formulário de Tarefa de correção

Campo	Descrição
Número	ID atribuído automaticamente no sistema.
Pontuação de risco	Preenchido automaticamente pela calculadora de pontuação de risco. Esta é uma pontuação de risco de acúmulo. Esta pontuação de risco é ponderada, com 85% da pontuação da pontuação de risco máxima em todos os Resultados de testes não "Encerrados" (Aberto, Em investigação, Aguardando implementação, Adiado, Resolvido) e 15% da pontuação do número de testes resultados que não estão "Encerrados".
Pontuação de risco	Preenchido automaticamente pela calculadora de pontuação de risco. Com base em um intervalo de pontuações de risco em uma escala numérica de 1 a 5 que classifica o risco geral com base em um intervalo de pontuações de risco de 1 - Crítico a 5 - Nenhum. Este campo substitui o campo Prioridade nas versões anteriores.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

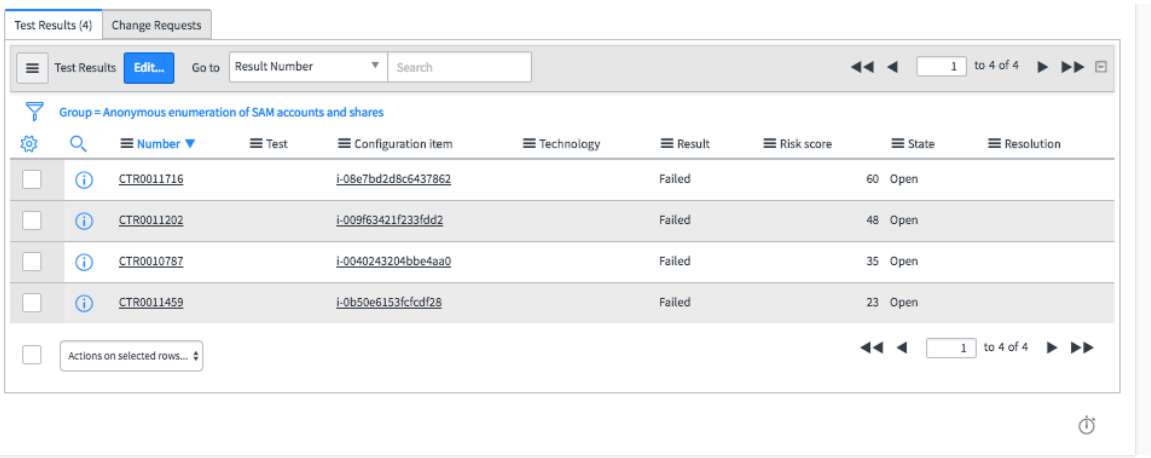
Campo	Descrição
Estado	**Aberto**inicialmente , é o estado de correção do grupo. Para obter mais informações, consulte Configuration Compliance estados.
Grupo de atribuição	Atribua o grupo de resultados de testes a um grupo de correção.
Atribuído a	Atribua uma equipe para corrigir o grupo de resultados de testes.
Criado em	Data em que você criou este grupo.
Atualizado em	Data em que você atualizou este grupo.
Descrição resumida	Nome do grupo de resultados de testes.
Descrição	Descrição deste grupo de resultados de testes.
Testar	Selecione um Teste de configuração para este Grupo de resultados de testes.
Guias relacionadas	
Configuração de Grupo	Métodos de agrupamento a serem usados: ◦ Manual (padrão): ◦ Regra de filtro ou grupo: Tabela: pré-selecionada como Resultado de testes [sn_vulc_result] Condição de resultado de testes: escolha os filtros a serem usados. **Nota:** O link de condição de correspondência de registros acima das condições de filtro exibe os registros de resultado de testes que você escolheu em uma nova janela. Clique em **Visualizar** para ver quantos resultados seus critérios de filtro retornam antes de salvar o novo grupo. A lista relacionada Resultados de testes deve ser criada manualmente, clicando no botão **Editar** na guia relacionada **Resultados de testes**.
Anotações	Anotações de trabalho relacionadas a este grupo de resultados de testes.

5. Clique com o botão direito do mouse no cabeçalho para **Salvar** ou clique em **Enviar** para salvar e retornar à lista de grupos de resultados de testes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibe as listas relacionadas **Resultados de testes** e **Solicitação de mudança**.



Criar manualmente um grupo de resultados de testes Configuration Compliance na lista Resultados de testes

Você pode criar manualmente um grupo de resultados de **testes da lista Resultado** de testes e executar a correção do grupo de resultados de testes resultante.

Antes de Iniciar

Função necessária: sn_vulc.admin

Por Que e Quando Desempenhar Esta Tarefa

Este método requer a seleção de resultados de testes a serem incluídos e a criação do grupo no menu **Ações em linhas selecionadas**. Este método é bom para resultados que não são filtrados facilmente ou situações em que você deseja especificar resultados de testes para correção.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

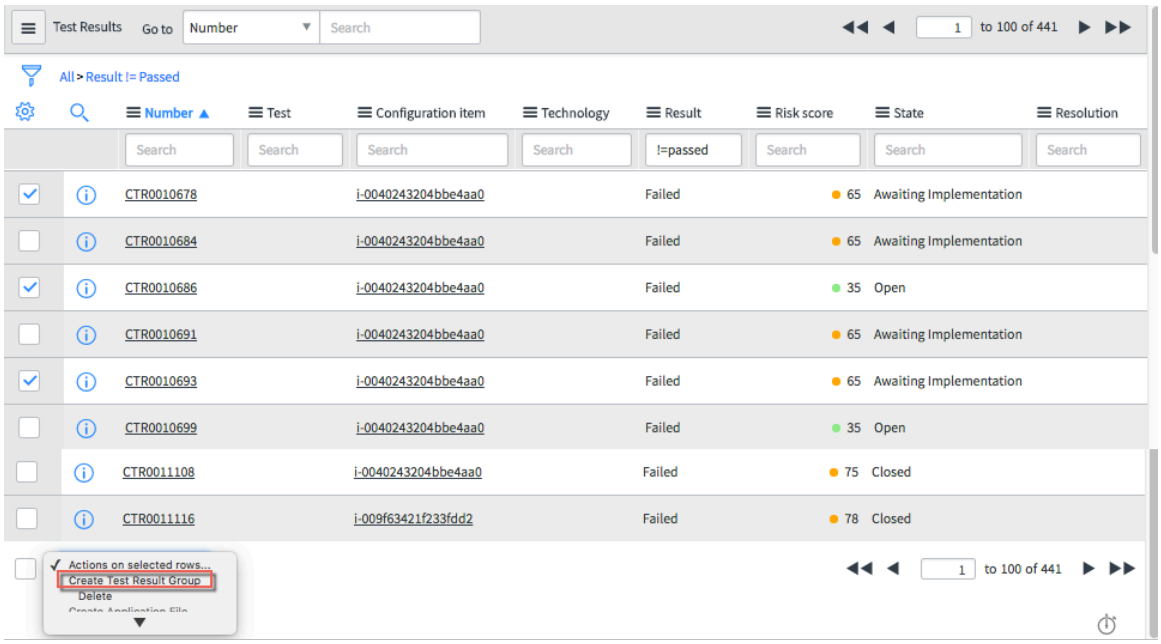
Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

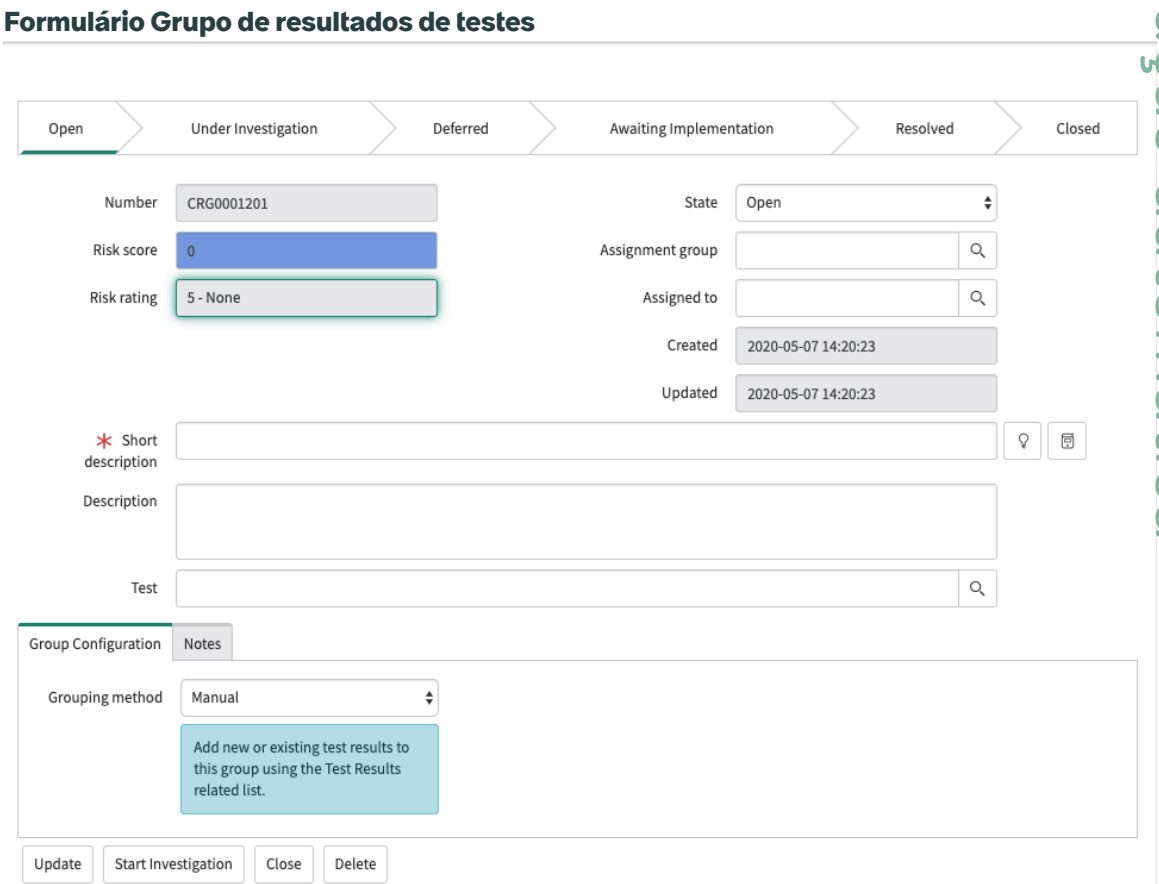
1. Navegar até **Todos** > **Configuration Compliance** > **Resultados de testes**.
2. No painel de navegação, selecione um módulo de Resultado de teste para abrir uma lista.
3. Selecione os resultados de testes a serem incluídos no grupo, marcando a caixa ao lado de cada um.
4. Abre o menu **Ações nas linhas selecionadas...** na parte inferior da lista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



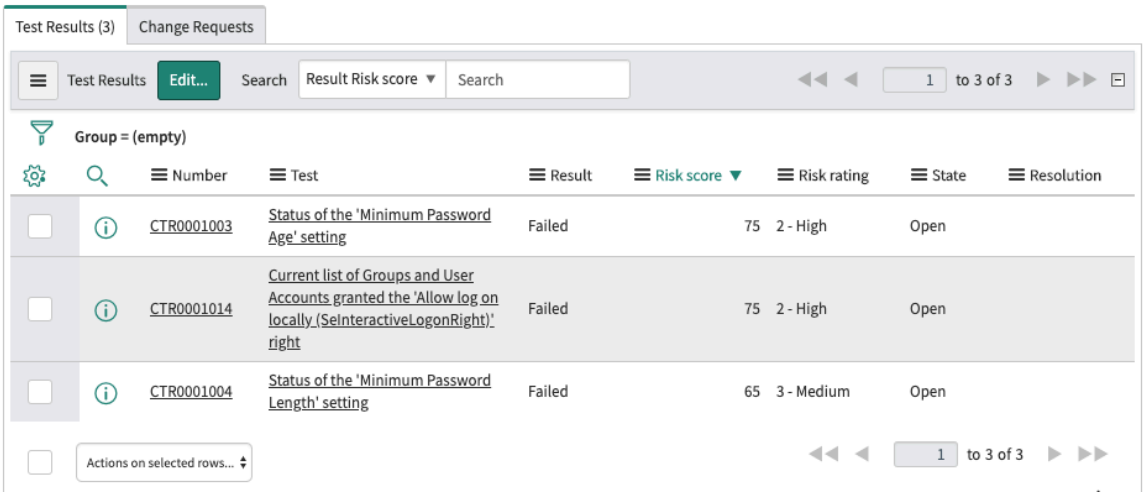
5. Escolha **Criar grupo de resultados de testes**.
O grupo de resultados de testes é criado e é aberto.



Os resultados de testes selecionados para o grupo são exibidos na lista relacionada Resultados de testes junto com todas as solicitações de mudança associadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Número	ID atribuído automaticamente no sistema.
Pontuação	Preenchido automaticamente pela calculadora de acúmulo de pontuação de risco. Esta é uma pontuação de risco de acúmulo. Esta pontuação de risco é ponderada, com 85% da pontuação da pontuação de risco máxima em todos os Resultados de testes não "Encerrados" (Aberto, Em investigação, Aguardando implementação, Adiado, Resolvido) e 15% da pontuação do número de testes resultados que não estão "Encerrados".
Classificação	Preenchido automaticamente pela calculadora de acúmulo de pontuação de risco. Com base em um intervalo de pontuações de risco em uma escala numérica de 1 a 5 que classifica o risco geral com base em um intervalo de pontuações de risco de 1 - Crítico a 5 - Nenhum. Este campo substitui o campo Prioridade nas versões anteriores.
Pontuação de risco histórico	Preenchido automaticamente pela calculadora de acúmulo de pontuação de risco. A pontuação de risco inerente em todos os resultados de testes aprovados em um grupo de resultados de testes. Este campo exibe a quantidade de risco que foi corrigida por um grupo de teste e só é exibido depois que um grupo de teste está no estado "Encerrado" e a pontuação de risco é zero.
Estado	**Aberto**inicialmente , é o estado de correção do grupo. Para obter mais informações, consulte Configuration Compliance estados.
Grupo de atribuição	Atribua o grupo de resultados de testes a um grupo de correção.
Atribuído a	Atribua uma equipe para corrigir o grupo.
Criado em	Data em que você criou este grupo.
Atualizado em	Data em que você atualizou este grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descrição resumida	Nome do grupo de resultados de testes.
Descrição	Descrição de texto deste grupo de resultados de testes.
	Selecione um Teste de configuração para este Grupo de resultados de testes.
Guias relacionadas	
Configuração de Grupo	Métodos de agrupamento a serem usados: ○ Manual (padrão) ○ Filtro Tabela: pré-selecionada como resultado de testes Condição de resultado de testes: escolha os filtros a serem usados. **Nota:** O link de condição de correspondência de registros acima das condições de filtro exibe os registros de resultado de testes que você escolheu em uma nova janela. Clique em **Visualizar** para ver quantos resultados seus critérios de filtro retornam antes de salvar o novo grupo.
Anotações	Anotações de trabalho relacionadas a este grupo de resultados de testes.
Listas relacionadas	
Resultados de testes	Resultados de testes incluídos neste grupo.
Solicitações de mudança	Solicitações de mudança associadas a este grupo.

7. Clique com o botão direito do mouse no cabeçalho para **Salvar** ou clique em **Enviar** para salvar e retornar à lista de grupos de resultados de testes.

Como criar uma solicitação de mudança no Configuration Compliance

Você pode criar uma solicitação de mudança a partir de um grupo de resultados de testes (TRG) na aplicação Configuration Compliance.

Antes de Iniciar

Função necessária: usuário com a função itil

Por Que e Quando Desempenhar Esta Tarefa

Como especialista em TI ou correção, crie uma solicitação de mudança (CHG) diretamente de um grupo de resultados de testes para todos os resultados de testes do grupo. Crie uma solicitação de mudança com informações preenchidas previamente para agilizar sua investigação de vulnerabilidades que exigem intervenção manual.

Você pode criar, aprovar, implementar, revisar e fechar solicitações de mudança diretamente dos grupos de resultados de testes atribuídos a você. Você pode criar três tipos de solicitações de mudança com informações preenchidas previamente de um grupo de resultados de testes:

Padrão

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma mudança pré-autorizada de baixo risco, relativamente comum e que segue um procedimento ou instrução de trabalho especificada.

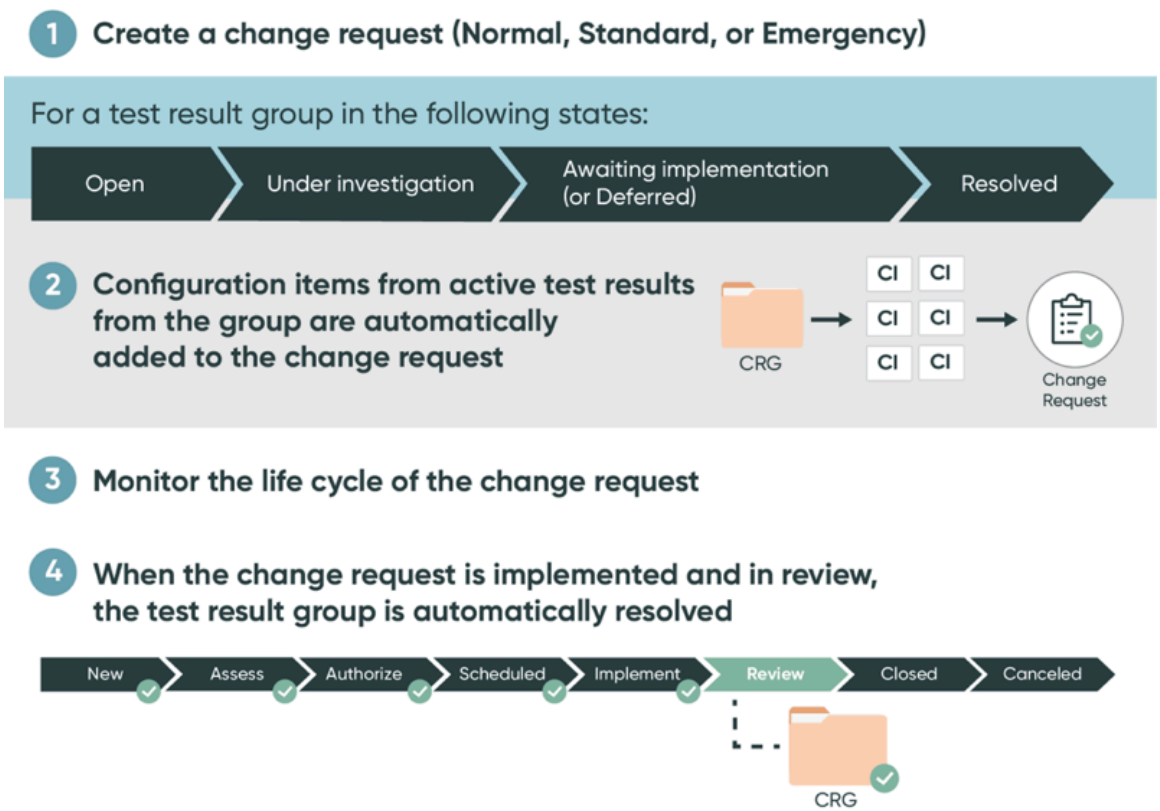
Normal

As solicitações de mudança normais seguem um processo prescritivo que requer dois níveis de aprovação antes de ser implementado, revisado e encerrado.

Emergência

Uma mudança para resolver um incidente grave.

A imagem a seguir ilustra o fluxo básico para criar uma solicitação de mudança a partir de um grupo de resultados de testes. As etapas detalhadas para este fluxo seguem a imagem.



A partir da versão 19.0 do Vulnerability Response, você pode criar solicitações de mudança para Grupos de resultados de testes (TRGs) no Espaço de correção de TI. Para obter mais informações, consulte Criar uma solicitação de mudança no Espaço de correção de problemas de TI.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Grupos de resultados de testes** > **Meus Grupos Abertos**.
   A lista de grupos de resultados de testes atribuídos aos seus grupos é exibida.
2. Na coluna Número, clique no grupo de resultados de testes para o qual você deseja criar uma solicitação de mudança.
   Você pode criar solicitações de mudança de grupos de resultados de testes em qualquer estado diferente de **Encerrado** ou **Em revisão**.

   O registro do grupo de resultados de testes é exibido.
3. No canto superior direito do registro, clique em **Criar mudança**.
   O formulário de solicitação de mudança é exibido.
4. Preencha os campos.
   a. Na lista do campo **Aplica-se a**, escolha um para continuar.
5. Na caixa de seleção **Adicionar ICs ao CR**, escolha um para continuar.
6. Na lista do campo **Tipo de mudança**, escolha uma para continuar.

   O recurso lê automaticamente os tipos de solicitações de mudança que você configura em seu catálogo no ITSM Change Management. Por exemplo, se você alterar o nome das solicitações de mudança padrão no ITSM de Padrão para Pré-aprovado, seu novo nome será exibido automaticamente na lista Tipo de mudança no formulário Criar solicitação de mudança.
7. Os campos na seção Visualização da solicitação de mudança do formulário são preenchidos previamente com informações do grupo de resultados de testes.
   Se necessário, edite esses campos.
8. Clique **em Criar mudança**.
   A solicitação de mudança é exibida. Na lista relacionada ICs afetados, os ICs dos resultados de testes que corresponderam aos seus critérios são exibidos. Se a solicitação de mudança exigir aprovação, o botão **Solicitar Aprovação** será exibido.

   Depois que a solicitação de mudança é criada, o grupo de resultados de testes passa para o estado **Aguardando implementação**. Depois que a solicitação de mudança para este grupo de resultados de testes for resolvida, se não houver outras solicitações de mudança em aberto associadas a este grupo de resultados de testes, o grupo de resultados de testes também será movido para o estado **Resolvido**.

   Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

   Nota:
   Você ainda pode mover manualmente solicitações de mudança e grupos de resultados de testes pelos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que uma solicitação de mudança mudou seu estado, ou você adiciona uma solicitação de mudança ou a remove de um grupo de resultados de testes, a sincronização de estado pode potencialmente substituir sua intervenção manual. No entanto, os estados de solicitações de mudança não movem automaticamente o grupo de resultados de testes dos estados Encerrado ou Adiado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Associar um grupo de resultados de testes a uma solicitação de mudança existente

Associe um grupo de resultados de testes na aplicação Configuration Compliance a uma solicitação de mudança existente.

Antes de Iniciar

Função necessária: um usuário com a função itil

Por Que e Quando Desempenhar Esta Tarefa

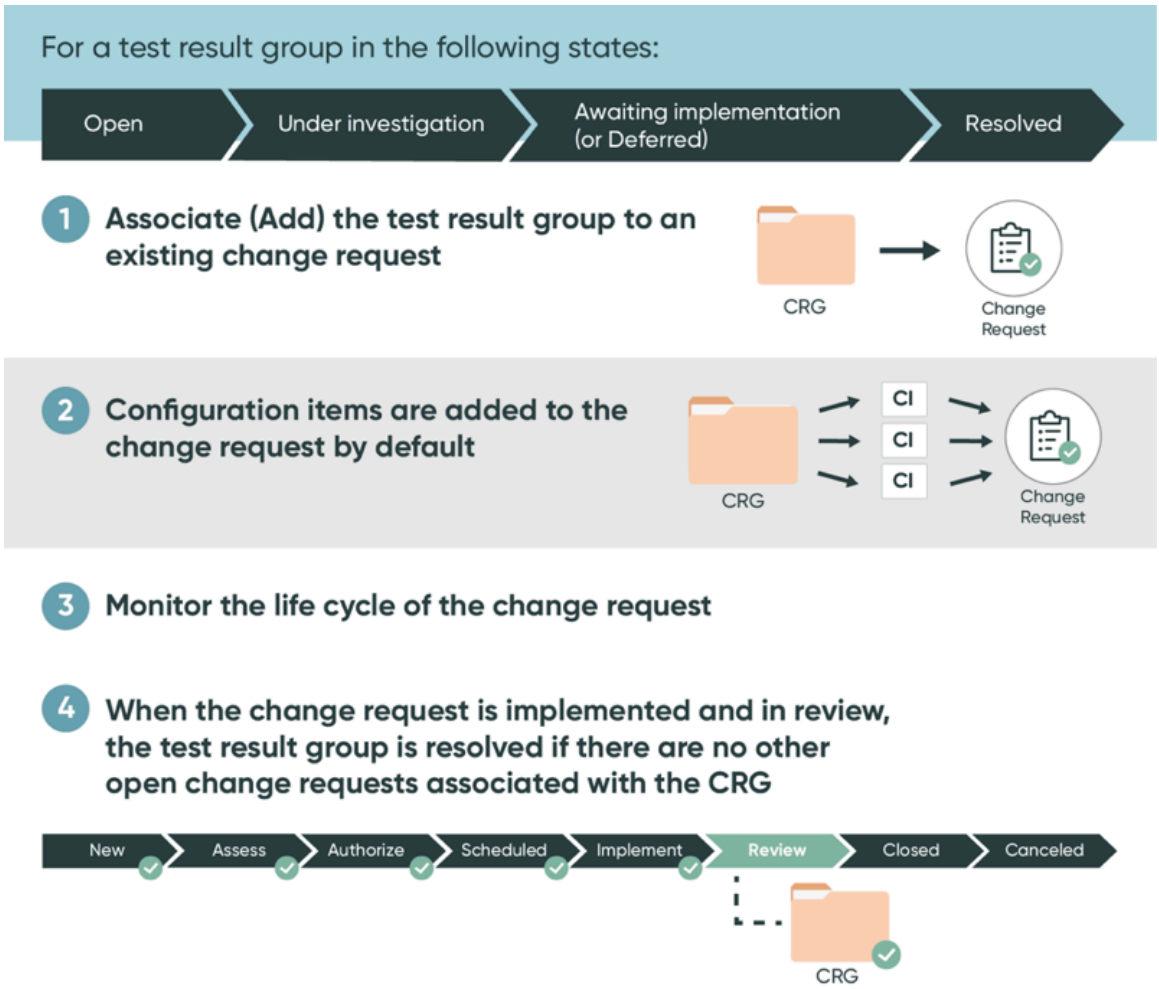
Como especialista em TI ou correção, evite criar solicitações de mudança duplicadas (CHG) enquanto trabalha para resolver seus grupos de resultados de testes, associando um grupo de resultados de teste (TRG) a uma solicitação de mudança que já está disponível em sua instância.

Você pode associar grupos de resultados de testes atribuídos a você ou ao seu grupo de atribuição a solicitações de mudança existentes diretamente dos registros do grupo de resultados de testes. A imagem a seguir ilustra o fluxo básico para associar uma solicitação de mudança existente a um TRG. As etapas detalhadas para este fluxo seguem a imagem.

Nota:
Você pode associar uma solicitação de mudança existente a um TRG em qualquer estado diferente de **Cancelado** (**Aberto**, **Em investigação**, **Aguardando implementação**, **Encerrado**e **Adiado**). As solicitações de mudança, incluindo as encerradas nos últimos 90 dias, estão disponíveis para associação no formulário. Quando você associa uma solicitação de mudança a um TRG existente, somente os resultados de testes ativos e seus itens de configuração são adicionados à solicitação de mudança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Grupos de resultados de testes** > **Meus Grupos Abertos**.
   A lista de grupos de resultados de testes atribuídos aos seus grupos é exibida.
2. Na coluna Número, clique no grupo de resultados de testes para o qual você deseja criar uma solicitação de mudança.

   O registro do grupo de resultados de testes é exibido.
3. No canto superior direito do registro, clique em **Criar mudança**.
   O formulário de solicitação de mudança é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Role até a lista relacionada Solicitações de mudança e selecione-a.
   Todas as solicitações de mudança associadas ao TRG são exibidas junto com o botão **Adicionar**.
5. Clique em **Adicionar**.
   A caixa de diálogo Adicionar solicitação de mudança existente ao grupo de resultados de testes é exibida.
6. Clique no ícone de pesquisa e selecione um item na lista.
   Você pode filtrar a lista exibida para restringir sua pesquisa.
7. Clique em **Enviar**.
   O TRG é exibido junto com uma mensagem que indica que a solicitação de mudança foi associada com sucesso ao grupo de resultados de testes. Na lista relacionada de solicitações de mudança, a nova solicitação de mudança é exibida. Os ICs do grupo de resultados de testes são adicionados por padrão à solicitação de mudança e são exibidos na lista relacionada ICs afetados. Você também pode adicionar ICs à solicitação de mudança a partir desta lista relacionada. Uma mensagem indica o número de resultados de testes que foram movidos para o novo grupo e o novo TRG é exibido.

Nota:
Para menos de 200 resultados de testes, a operação de divisão é feita de forma síncrona e os resultados do teste são exibidos no novo grupo.

Para mais de 200 resultados de testes, a operação de divisão é feita de forma assíncrona em segundo plano e pode levar alguns segundos para que os resultados do teste apareçam no novo grupo. A seguinte mensagem também é exibida: n resultados de testes serão movidos de TRGxxxxxxx para o novo grupo de resultados de testes GRCxxxxx em breve.

Você pode associar qualquer solicitação de mudança ao TRG, com as seguintes exceções:

- Solicitações de mudança no estado **Cancelado**.
- Solicitações de mudança no estado **Encerrado** há mais de 90 dias.
- Solicitações de mudança já associadas ao TRG. O sistema não permitirá que você associe uma solicitação de mudança que já esteja associada ao TRG.

Depois que a solicitação de mudança para este grupo de resultados de testes for resolvida, se não houver outras solicitações de mudança em aberto associadas a este grupo de resultados de testes, o grupo de resultados de testes também será movido para o estado**Resolvido**.

Nota:
Você ainda pode mover manualmente solicitações de mudança e grupos de resultados de testes pelos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que uma solicitação de mudança mudou seu estado, ou você adiciona uma solicitação de mudança ou a remove de um grupo de resultados de testes, a sincronização de estado pode potencialmente substituir sua intervenção manual. No entanto, os estados de solicitações de mudança não movem automaticamente o grupo de resultados de testes dos estados Encerrado ou Adiado.

Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

Dividir um grupo de resultados de testes

Em um grupo de resultados de testes (TRG) existente na aplicação Configuration Compliance, identifique um subconjunto de resultados de testes que você deseja mover para um novo grupo de resultados de testes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

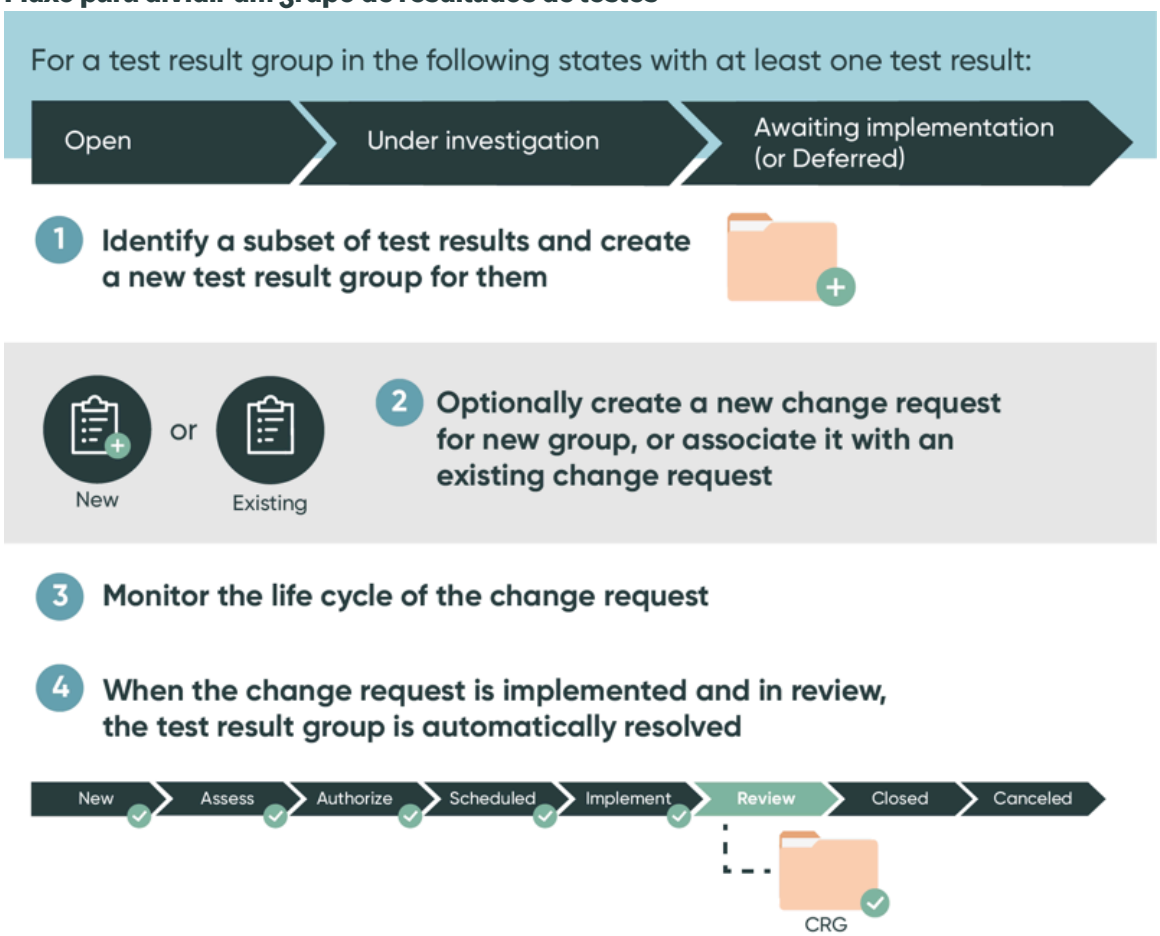
Antes de Iniciar
Função necessária: um usuário com a função itil

Por Que e Quando Desempenhar Esta Tarefa
Como especialista em TI ou correção, você pode dividir grupos de resultados de testes existentes nos estados **Aberto**, **Em investigação**ou **Aguardando implementação** com mais de um resultado de teste. Ao criar um novo TRG com resultados de testes que correspondam a critérios específicos, você pode trabalhar com um grupo específico de resultados de testes sem afetar o grupo original.

Quando você especifica as condições dos resultados de testes que deseja mover para um novo grupo de resultados de testes com o construtor de condição, somente os resultados de testes ativos que correspondem aos seus critérios são movidos para o novo grupo. Você não precisa criar solicitações de mudança (CHGs) ao dividir um TRG. Você tem a opção de dividir um TRG ao mesmo tempo em que cria uma solicitação de mudança ou pode dividir um TRG sem criar uma solicitação de mudança.

A imagem a seguir ilustra o fluxo básico para dividir um grupo de resultados de teste. As etapas detalhadas para este fluxo seguem a imagem.

Fluxo para dividir um grupo de resultados de testes



Os casos de uso para dividir resultados de testes de TRGs existentes em novos grupos podem incluir os seguintes exemplos:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Quando você deseja criar uma solicitação de mudança ou solicitações de mudança para um grupo de divisão.
- Quando você reatribui um grupo de divisão a outro usuário em seu grupo de atribuição.
- Quando você solicita um adiamento ou exceção para um grupo de divisão porque sabe que alguns resultados de testes em itens de configuração (IC) específicos não podem ser corrigidos em um determinado intervalo de tempo.

[store-future: BEGIN review]A partir da versão 19.0 do Vulnerability Response, você pode dividir tarefas para grupos de resultados de testes do Espaço de correção de TI.[End]

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Testes** > **Grupos de resultados de testes** > **Meus Grupos Abertos**.
   A lista de grupos de resultados de testes atribuídos aos seus grupos é exibida.
2. Na coluna Número, clique no grupo de resultados de testes que você deseja dividir.

   O registro do grupo de resultados de testes é exibido.
3. Para criar um subconjunto de resultados de testes para um novo grupo que corresponda a critérios específicos, siga estas etapas.

   No canto superior direito do registro, clique em **Dividir grupo**.

   Você pode preferir este método de criação de um novo grupo se estiver trabalhando em um grupo grande com vários resultados de testes.

   O formulário de grupo de resultados do teste de divisão é exibido.
4. Com o construtor de condição exibido, especifique as condições dos resultados de testes que você deseja mover para um novo grupo de resultados de testes.

   Por exemplo, talvez você prefira filtrar somente os resultados de testes que correspondam às seguintes condições:

   - No estado **Aberto**.
   - Pontuações de risco superiores a 75.
   - O resultado é **Falha**.

   Se os resultados do teste corresponderem ao seu filtro depois de inserir as condições, uma mensagem será exibida com o número de resultados de testes correspondentes.

   Se for exibida uma mensagem informando que nenhum resultado de teste corresponde ao seu filtro ou que todos os resultados de testes correspondem aos seus critérios, ajuste

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

as condições para que pelo menos um resultado de teste corresponda aos critérios do filtro.

5. Clique em **Visualizar itens** para exibir os resultados de testes correspondentes.
   Uma nova janela, Grupos de resultados de testes, exibe os itens.
6. Para visualizar detalhes sobre os resultados do teste que correspondem aos seus critérios de filtro, siga estas etapas antes de clicar em **Dividir grupo** para criar o novo grupo.
   Esses detalhes incluem o grupo de atribuição e a quem o resultado do teste foi atribuído. Exibir essas informações na visualização pode ajudar a garantir que o novo grupo seja atribuído corretamente.

   a. Com a lista Grupos de resultados de testes exibida na visualização, clique em um item na coluna Resultado.
      O registro de Resultado de testes é exibido.

   b. Verifique se os campos **Grupo de atribuição** e **Atribuído a** estão corretos.

   c. Clique em **Atualizar**.

7. Quando estiver pronto para criar o novo grupo, clique em **Dividir grupo**.
   Uma mensagem indica o número de resultados de testes movidos para o novo grupo e o novo TRG é exibido. Para ajudar a identificar o novo grupo, convém editar o texto no campo **Descrição resumida** e editar os campos Grupo de atribuição ou Atribuído a novamente, se necessário.

   Nota:
   Para menos de 200 resultados de testes, a operação de divisão é feita de forma síncrona e os resultados do teste são exibidos no novo grupo.

   Para mais de 200 resultados de testes, a operação de divisão é feita de forma assíncrona em segundo plano e pode levar alguns segundos para que os resultados do teste apareçam no novo grupo. A seguinte mensagem também é exibida: n resultados de testes serão movidos de TRGxxxxxxx para o novo grupo de resultados de testes GRCxxxxx em breve.

8. Como alternativa, você pode criar um novo grupo de resultados de testes selecionando resultados de testes diretamente na lista relacionada Resultados de testes em um grupo de resultados de testes.

   Você pode preferir este método se tiver apenas alguns resultados de testes em um grupo ou se souber exatamente quais testes deseja mover para um novo grupo.

   a. Com o registro do grupo de resultados de testes exibido, role até a lista relacionada Resultados de testes.

   b. Na coluna da extrema esquerda, marque as caixas de seleção dos resultados de testes para os quais você deseja criar um novo TRG.

   c. Na lista Ações nas linhas selecionadas no canto inferior esquerdo do registro, clique em **Dividir grupo**.

   d. No formulário Grupo de resultados do teste de divisão exibido, para ajudá-lo a identificar o novo grupo, talvez você prefira editar o texto no campo **Descrição resumida**.

   e. Clique **em Dividir grupo**.
      Uma mensagem indica o número de resultados de testes que foram movidos para o novo grupo e o novo TRG é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois que a solicitação de mudança para este grupo de resultados de testes for resolvida, se não houver outras solicitações de mudança em aberto associadas a este grupo de resultados de testes, o grupo de resultados de testes também será movido para o estado **Resolvido**.

Nota:
Você ainda pode mover manualmente solicitações de mudança e grupos de resultados de testes pelos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que uma solicitação de mudança mudou seu estado, ou você adiciona uma solicitação de mudança ou a remove de um grupo de resultados de testes, a sincronização de estado pode potencialmente substituir sua intervenção manual. No entanto, os estados de solicitações de mudança não movem automaticamente o grupo de resultados de testes dos estados Encerrado ou Adiado.

Para obter mais informações, consulte Sincronização de estado entre solicitações de mudança e tarefas de correção.

O que Fazer Depois
Você pode criar ou associar solicitações de mudança para seus novos grupos de resultados de testes. Para obter mais informações, consulte Associar um grupo de resultados de testes a uma solicitação de mudança existente e Como criar uma solicitação de mudança no Configuration Compliance.

Remover atribuições de grupos de resultados de testes para você ou seus grupos

Reatribua os registros de resultado de testes na aplicação Configuration Compliance se os registros tiverem sido atribuídos incorretamente a você ou ao seu grupo.

Antes de Iniciar
Função necessária: sn_vulc.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa
Iniciando com v14.3 da aplicação Configuration Compliance, se você determinar que os grupos de resultados de testes (TRG) e seus resultados de testes associados não estão dentro do seu escopo de correção, ou se você achar que os registros foram atribuídos incorretamente a você ou aos seus grupos, convém remover a si mesmo ou aos seus grupos dos campos Atribuído a e Grupo de atribuição nos registros TRG.

O botão **Cancelar atribuição** é exibido nos registros do TRG em qualquer estado que não seja Encerrado ou Resolvido.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegue até um registro de grupo de resultados de testes atribuído a você que esteja em qualquer estado diferente de Encerrado ou Resolvido.
2. Para limpar os campos **Atribuído a** e **Grupo de atribuição**, na parte superior do registro, selecione **Cancelar atribuição**.
3. Na caixa de diálogo **Cancelar atribuição**, forneça as anotações de trabalho e selecione **Enviar**.
   - As anotações de trabalho que você forneceu são exibidas na seção Anotações.
   - Na guia **Aprovação** de mudança de estado, o registro de aprovação de mudança de estado (CA#) exibe o estado Em revisão, o que ajuda a rastrear o fluxo de trabalho de aprovação.
   - Na guia **Aprovações solicitadas**, a solicitação para a remoção de você ou do seu grupo de atribuição é exibida como o estado Solicitado.

Resultado

A solicitação é aprovada usando um fluxo de trabalho de aprovação padrão de um nível. Para obter mais informações, consulte Aprovar uma solicitação de cancelamento de atribuição no Configuration Compliance.

- Se sua solicitação for aprovada, o registro de aprovação de mudança de estado e o registro de aprovação solicitado mudarão para **Aprovado**. Você e seus grupos serão removidos dos campos **Atribuído a** e **Grupo de atribuição**. Não atribuído é exibido no campo **Tipo de atribuição** e o grupo de resultados de testes é exibido na lista do módulo Não atribuído para a aplicação Configuration Compliance.

  Notificações de que os registros não estão atribuídos são enviadas automaticamente para gerentes de vulnerabilidade ou analistas no grupo de notificação de cancelamento de atribuição. Para obter mais informações sobre as notificações e as propriedades deste recurso, consulte Remoção de atribuições de grupos de resultados de teste do Configuration Compliance.

- Se sua solicitação for rejeitada, o registro de aprovação de mudança de estado e o registro de aprovação solicitado mudarão para Rejeitado.

Nota:
Como administrador de vulnerabilidade, você pode definir a propriedade do sistema `sn_vulc.unassign_test_result_group.approval_required` como **falsa** para desabilitar o processo de aprovação.

O que Fazer Depois

Navegue até o módulo Não atribuído para a aplicação [Configuration ComplianceVulnerability Response contêiner

Aprovar uma solicitação de cancelamento de atribuição no Configuration Compliance

Aprove solicitações para a remoção de grupos de resultados de testes de um grupo de atribuição ou de um usuário individual na aplicação Configuration Compliance.

Antes de Iniciar

Função necessária: sn_vulc.unassign_approver

Por Que e Quando Desempenhar Esta Tarefa

Por padrão, uma configuração de aprovação é fornecida. Para aprovações de cancelamento de atribuição, um aprovador é necessário no grupo de aprovação Aprovador - Nível 1.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por padrão, o grupo de aprovação de cancelamento de atribuição (Cc de cancelamento de atribuição do aprovador - nível 1) é criado e os usuários que fazem parte desse grupo podem aprovar a solicitação. Por padrão, este grupo contém a função de aprovador de desatribuição, sn_vulc.unassign_approver. Você pode modificar ou criar um grupo e atualizar a configuração de aprovação navegando até **Todos** > **Configuration Compliance** > **Minhas aprovações** > **Regras de aprovação** > **Solicitação de mudança de campo de grupo de resultados de testes** > **Desatribuir grupo de resultados de testes**.

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Minhas aprovações**.
2. Selecione uma solicitação da sua fila.
3. Aprove ou rejeite a solicitação adicionando os comentários apropriados.

Fechamento automático de resultados de testes

Você pode fechar automaticamente os resultados de testes (TRs) associados aos itens de configuração (ICs) desativados.

Para configurar a opção de fechamento automático, navegue até a propriedade do sistema **sn_vulc.auto_close_test_results_linked_to_retired_CIs** e defina-a como verdadeiro. Para fechar automaticamente TRs relacionados a ICs desativados, consulte Fechar automaticamente os resultados de testes relacionados a ICs desativados.

Para obter informações sobre como trabalhar com itens de configuração desativados, consulte Como trabalhar com itens de configuração desativados no Configuration Compliance.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Como trabalhar com itens de configuração desativados no Configuration Compliance

Os itens de configuração (ICs) desativados são movidos para o estado desativado, arquivado ou excluído no Configuration Management Database (CMDB). Configuration Compliance contém resultados de testes (TRs) que são compostos por ICs. Quando o estado de um IC é atualizado para desativado, os TRs associados são encerrados com o subestado "IC desativado".

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Se o CMDB mudar o status da fase do ciclo de vida de um IC para desativado, você poderá optar por fechar automaticamente os TRs associados. Para obter mais informações sobre como fechar automaticamente os TRs associados, consulte Fechar automaticamente os resultados de testes relacionados a ICs desativados.

O IC desativado é eventualmente arquivado ou excluído permanentemente do CMDB.

Impacto da desativação dos ICs:

- **Impacto nos itens descobertos:** quando o IC é desativado, o DI relacionado é marcado como "IC desativado".
- **Impacto nos resultados de testes:** quando o estado de uma DI é atualizado para "IC desativado", o TR associado é fechado e a seção de anotações é atualizada automaticamente.

Nota:
O estado de um DI é atualizado automaticamente para "IC desativado" sempre que o estado do ciclo de vida de um IC é atualizado. Por outro lado, o estado de um TR é atualizado para Encerrado somente quando a propriedade **sn_vulc.auto_close_test_results_linked_to_retired_CIs** está definida como verdadeira. Para obter mais informações sobre como fechar automaticamente os TRs associados, consulte Fechar automaticamente os resultados de testes relacionados a ICs desativados.

O trabalho programado *`Close Test Results for decommissioned CIs`* é executado diariamente para os DIs atualizados. Se a opção de configuração de fechamento automático estiver habilitada para ICs desativados, ela identificará a DI que contém um IC desativado e fechará o TR relacionado com o subestado "IC desativado". Se todos os TRs em um grupo de resultados de testes estiverem fechados e seu subestado for IC desativado, o grupo de resultados de testes também será fechado com o subestado "Cancelado".

Nota:
Se um IC voltar para o estado original do estado "Descontinuado", a entrada "Itens descobertos" também será atualizada. Os TRs são abertos automaticamente quando os dados são ingeridos novamente do scanner.

Fechar automaticamente os resultados de testes relacionados a ICs desativados

Se o Configuration Management Database (CMDB) mudar o status da fase do ciclo de vida de um item de configuração (IC) para desativado, você poderá optar por fechar automaticamente os resultados de testes (TRs) associados.

Antes de Iniciar
Função necessária: sn_vulc.admin

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Para fechar automaticamente os TRs associados, você deve habilitar a propriedade do sistema **sn_vulc.auto_close_test_results_linked_to_retired_CIs** para fechar automaticamente os TRs que estão associados a ICs desativados. Se esta opção estiver habilitada, os TRs novos e existentes relatados para o mesmo IC serão criados ou atualizados automaticamente no estado "Encerrado". Eles são baseados no ID do ativo na carga do scanner e no status de entrada dos itens descobertos. Para obter mais informações sobre o impacto de ICs desativados, consulte Como trabalhar com itens de configuração desativados no Configuration Compliance.

Nota:
O estado de um DI é atualizado para "IC desativado" sempre que o estado do ciclo de vida de um IC é atualizado. Por outro lado, o estado de um TR é atualizado para Encerrado somente quando a propriedade do sistema **sn_vulc.auto_close_test_results_linked_to_retired_CIs** está habilitada.

Procedimento

1. Navegar até **Propriedades do sistema** > **Todas as propriedades** e filtrar por `sn_vulc.auto_close_test_results_linked_to_retired_CIs` na coluna Nome.
2. Selecione a propriedade.
3. Para fechar automaticamente os resultados de testes associados aos ICs desativados, defina o valor da propriedade como verdadeiro.

Fechando automaticamente resultados de testes obsoletos em Configuration Compliance

Você pode ativar o recurso Fechar automaticamente resultados de testes obsoletos para fechar automaticamente os resultados de testes mais antigos que não foram encontrados recentemente por suas integrações de terceiros. Mover esses resultados de testes para **Encerrado-obsoleto** reduz o número de resultados de testes ativos e grupos de resultados de testes em sua instância e ajuda a reconciliar ativos em seu Configuration Management Database (CMDB).

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Visão geral

O módulo Fechar automaticamente resultados de testes obsoletos ajuda a fechar automaticamente resultados de testes mais antigos e obsoletos que não foram encontrados recentemente por suas integrações de terceiros. Os resultados de testes são movidos para **Encerrado-obsoleto** com base nas condições definidas no construtor de condição.

Termos-chave

Resultado do teste

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os resultados dos testes são resultados importados de bibliotecas de testes de configuração que são mapeados para estruturas, políticas e fontes autorizadas que definem como uma classe de ativos de tecnologia deve ser controlada. A aplicação Configuration Compliance não calcula os resultados do teste, mas os importa com integrações de terceiros.

Data da última verificação do ativo

Refere-se ao valor da coluna Data da última verificação de conformidade da configuração da tabela Item descoberto que está relacionada ao resultado do teste. Esta data se refere à data e hora mais atuais em que um ativo foi verificado pela última vez por um scanner de terceiros.

Data da última falha

Refere-se à data da última coluna vista da tabela Resultados de testes quando o valor do campo **Resultado** é [falha].

Resultados de testes obsoletos

Refere-se aos resultados de testes em sua instância que são antigos e não foram encontrados, atualizados ou detectados por verificações de integração de terceiros por um período significativo.

Resultados de testes encontrados pela última vez

Esta opção de pesquisa usa uma data e hora fornecidas pelo scanner de terceiros. Este termo se refere à data mais atual ou mais recente (dias atrás) em que os resultados de testes foram encontrados novamente pelo scanner. Este parâmetro pode ser configurado.

Caso de uso

Às vezes, os ativos (itens de configuração) podem ser desativados em seu ambiente ou limpos por scanners de terceiros. Quando isso acontece, os resultados do teste de configuração associado dos ativos não são atualizados na aplicação Configuration Compliance por detecções importadas e se tornam inativos (obsoletos).

Para reduzir o número de resultados de testes (TRs) ativos e grupos de resultados de testes (TRGs) em sua instância, ative o recurso Fechar automaticamente resultados de testes obsoletos. Este recurso fecha automaticamente os resultados de testes antigos que têm estados inalterados ou não foram importados recentemente por suas integrações.

Como exemplo, suponha que um item de configuração (IC) específico tenha vários IDs de ativo e um desses IDs não tenha sido importado nas detecções de um scanner de terceiros nos últimos 90 dias. Se você definir o construtor de condição no módulo Fechar automaticamente resultados de testes obsoletos para fechar resultados de testes que não foram encontrados ou atualizados nos últimos 90 dias ou mais, este recurso fechará automaticamente todos os resultados de testes que correspondam a esta filtragem.

Nota:
Este recurso fecha somente as detecções de resultado de testes com base nas condições de filtro que você definiu no construtor de condição e são detectadas por suas integrações de scanner de terceiros.

O campo Resolução

Para diferenciar entre as detecções que são encerradas por scanners de terceiros, como os produtos Qualys e Tenable.io e o recurso Encerrar automaticamente resultados de testes obsoletos em sua instância, um novo valor para o campo **Resolução**, [Closed-Stale], foi foi adicionado. **Encerrado-obsoleto** indica que um TR foi encerrado pelo recurso de fechamento automático. **Encerrado** ou **Corrigido-Encerrado** indica que um TR foi encerrado por um scanner.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acúmulo de estados de TR para TRGs com o recurso de fechamento automático

A progressão de estado e a precedência dos resultados de testes são: **Em aberto** > **Encerrado** > **Fixo-Encerrado** > **Encerrado obsoleto**.

1. Se algum TRG em um TRG estiver **Aberto**, o estado do TRG não será alterado.
2. Se pelo menos um TR for **Encerrado - Corrigido** e o restante for **Encerrado - Obsoleto**, o estado do TRG mudará para **Encerrado - Corrigido**.
3. Se todos os TRs em um TRG forem **Encerrado - Obsoleto**, o estado do TRG mudará para **Encerrado - Cancelado**.

Integrações compatíveis

Para obter mais informações sobre as integrações de terceiros que oferecem suporte a este recurso, consulte Noções básicas sobre o Qualys Vulnerability Integration e Tenable.io integrações com as aplicações Vulnerability Response e Configuration Compliance.

Usar encerramento automático de resultados de testes obsoletos no Configuration Compliance

Ative Fechar automaticamente resultados de testes obsoletos (TRs) para fechar automaticamente os resultados de testes mais antigos com base nas condições do filtro que você definiu.

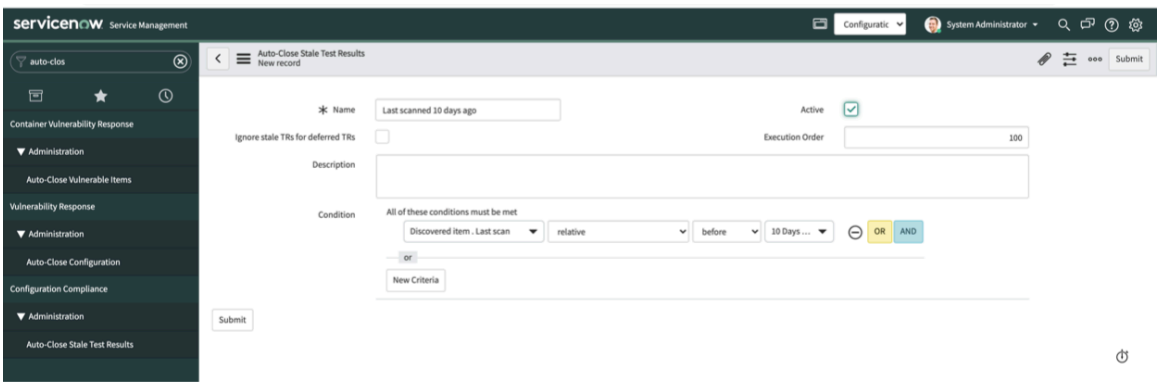
Antes de Iniciar

Para obter mais informações sobre este recurso, os principais termos e qualquer configuração que possa ser necessária para suas integrações de terceiros que importam dados de resultado de testes, consulte Fechando automaticamente resultados de testes obsoletos em Configuration Compliance.

Função necessária: sn_vulc.admin

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Administração** > **Fechar automaticamente os Resultados de testes obsoletos**.
2. No formulário, preencha os campos.



Campo	Valor
Nome	Nome para este registro de configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Valor
Ativo	Se selecionado, este registro ficará ativo e fechará automaticamente todos os resultados de testes que correspondam aos critérios de filtro.
Ignorar TRs obsoletos para TRs adiados	Se selecionado, todos os TRs mapeados para os estados **Em revisão** ou **Adiado** serão ignorados e não encerrados. Se você desmarcar esta opção, todos os TRs que corresponderem aos seus critérios serão encerrados.
Ordem de execução	100 é o valor padrão. Este valor determina a ordem de execução em ordem crescente para cada registro de configuração usado para localizar e marcar resultados de testes que estão obsoletos.
Descrição	Uma descrição para este registro. Este texto pode ajudá-lo a encontrá-lo facilmente se você criar um número maior de registros.
Condição	As condições de filtragem usadas para encontrar TRs que você deseja fechar. O filtro padrão é **Item descoberto** > **Últimas varreduras** > .

3. Clique em **Enviar**.

   O trabalho programado, *`Auto-Close Stale Test Results`*, é executado diariamente. Este trabalho identifica os TRs com base nas condições que você forneceu e faz a transição daqueles que correspondem a **Closed-Stale**.

   Depois que os TRs forem marcados como **Encerrado-obsoleto**, se o scanner encontrar esses TRs novamente, os resultados do teste serão reabertos e os estados mudarão para**Aberto**.

   Se um TR estiver marcado como **Encerrado-Obsoleto**e o scanner descobrir que ele foi corrigido, o TR mudará para**Encerrado-Corrigido**. Os estados também são acumulados para grupos de resultados de teste (TRGs), conforme descrito na lista a seguir:

   a. Se algum TRG em um TRG estiver **Aberto**, o estado do TRG não será alterado.
   b. Se pelo menos um TR for **Encerrado - Corrigido** e o restante for **Encerrado - Obsoleto**, o estado do TRG mudará para **Encerrado - Corrigido**.
   c. Se todos os TRs em um TRG forem **Encerrado - Obsoleto**, o estado do TRG mudará para **Encerrado - Cancelado**.

Fechar um grupo de resultados de testes

Se você determinar que o problema associado a um grupo de resultados de testes pode ser encerrado imediatamente sem análise adicional, poderá usar o recurso **Fechar**.

Antes de Iniciar

Função necessária:

- sn_vulc.admin
- sn_vulc.remediation_owner

Nota:
Com a função sn_vulc.remediation_owner, você pode reatribuir ou fechar grupos de resultados de testes atribuídos a você ou aos seus grupos de atribuição.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Abra o registro do grupo de resultados de testes.
2. Clique no botão **Fechar**.
3. Descreva por que o problema está sendo encerrado na janela pop-up.
4. Clique em **Fechar**.

Tópicos relacionados

Configuration Compliance estados

Solicitação e aprovação de uma exceção para um grupo de resultados de testes

Você pode solicitar o adiamento da correção de um grupo de resultados de testes por um período especificado. Usuários que fazem parte do grupo de aprovadores podem aprovar solicitações de exceção.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Para solicitar ou aprovar solicitações de exceção, consulte:

- Solicitar uma exceção para um grupo de resultados de testes no Configuration Compliance
- Aprovar uma solicitação de exceção no Configuration Compliance

Nota:

Notificações por e-mail são enviadas em todas as fases do gerenciamento de exceções, fornecendo o status e outros detalhes de uma solicitação. Por exemplo, quando uma exceção é solicitada, o solicitante recebe um e-mail confirmando que a solicitação foi gerada. O aprovador também recebe um e-mail informando que uma exceção foi solicitada.

A partir da v14.11 de Configuration Compliance, você pode configurar os intervalos de tempo para aprovar exceções, junto com notificações por e-mail para o aprovador e o solicitante após um determinado número de dias. Quando uma solicitação é gerada, o resultado do teste muda para o status Em revisão e um registro de mudança de estado é criado. Se o aprovador não responder dentro do intervalo de tempo configurado, o resultado do teste será revertido para o status Aberto. O estado anterior é armazenado no campo **backup_state**. Para obter mais informações, consulte Configurar regras de aprovação para Gestão de exceções.

Solicitar uma exceção para um grupo de resultados de testes no Configuration Compliance

Solicite uma exceção para adiar a correção de um grupo de resultados de testes por um período especificado se não puder ser corrigido imediatamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vulc.remediation_owner

Por Que e Quando Desempenhar Esta Tarefa
A partir da versão 19.0 do Vulnerability Response, você pode solicitar exceções para grupos de resultados de testes no Espaço de correção de TI. Para obter mais informações sobre como solicitar exceções para resultados de testes no Espaço de correção de TI, consulte Solicitar uma exceção no Espaço de correção de problemas de TI.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento
1. Navegar até **Todos** > **Configuration Compliance** > **Grupos de resultados de testes** > **Todos os Grupos**.
2. Selecione o grupo de resultados de testes para o qual você deseja solicitar uma exceção.
   O grupo selecionado deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
3. No formulário Grupo de resultados de testes, clique em **Solicitar exceção**.

   Nota:
   Dependendo se Vulnerability Response ou GRC: Policy and Compliance Management está selecionado no **Configuration Compliance** > **Gestão de exceção** tela, o formulário de Exceção de solicitação muda. Veja Configurar Gestão de exceções para Configuration Compliance

4. Se Vulnerability Response for selecionado na tela Gerenciamento de exceções, faça o seguinte:

   a. No formulário, preencha os campos.

Formulário de Exceção de solicitação

Campo	Descrição
Até	Data em que a solicitação de exceção expira. Esta data deve estar dentro da duração selecionada no **Todos** > **Configuration Compliance** > **Administração** > **Gestão de exceção** tela. Quando a solicitação de exceção expira, o grupo é revertido para o estado Aberto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: A partir da versão 14.7 de Configuration Compliance (CC), se um grupo de resultados de testes adiados for reaberto por um scanner antes que a janela de exceção expire, o estado do grupo de resultados de testes mudará de Aberto para Adiado. Esta funcionalidade está desabilitada por padrão. Para habilitar esta funcionalidade, defina o valor da propriedade do sistema `sn_vulc.auto_defer_test_result_in_active_exc` como verdadeiro. Além disso, a data adiada até persiste mesmo depois que o grupo de resultados de testes é reaberto após a data de vencimento.
Motivo	Motivo da exceção. Estas são as opções: ▪ Risco aceito ▪ Aguardando janela de manutenção ▪ Correção indisponível ▪ Redução do controle no local ▪ Outro Para ver como adicionar novas opções de motivo, consulte Definir mapeamentos de motivo da política.
Informações adicionais	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser atualizado pelo responsável pela correção.

b. Envie a solicitação de exceção clicando em **Solicitar aprovação**.

Resultado
O estado do grupo de resultados de testes muda para Em revisão. Use a guia **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

Solicitar uma extensão para um grupo de resultados de testes

Solicite uma extensão para um grupo de resultados de testes adiados antes que ele atinja o adiado até a data de vencimento. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Antes de Iniciar
Função necessária: sn_vul.vulnerability_admin ou sn_vul.admin (obsoleto)

Por Que e Quando Desempenhar Esta Tarefa
Você também pode solicitar uma extensão nos espaços Vulnerability Response. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no Espaço do gerenciador de vulnerabilidades.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Grupo de resultados de testes**.
2. Abre um grupo de resultados de testes adiados.
3. Selecione **Solicitar extensão**.
4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Prorrogar até	Selecione a data em que o estado Adiar expira e o grupo de resultados de testes é reativado.
Motivo	Insira o motivo para adiar o problema. As opções incluem: ○ Aguardando janela de manutenção ○ Correção indisponível ○ Risco aceito ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.

Nota:

- A solicitação passa por dois níveis de aprovação.
- O botão Solicitar extensão não está disponível para grupos de resultados de testes criados como parte de uma regra de exceção.
- Se um grupo de resultados de teste adiados for estendido novamente, a contagem de adiamento de extensão aumentará no back-end.

Solicitar uma extensão para uma regra de exceção no Configuration Compliance

Solicite uma extensão para uma regra de exceção adiada antes que ela atinja o adiado até a data de vencimento. Como proprietário de correção, você não precisa mais esperar até a data de vencimento adiada para fazer essa solicitação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_vul.exception_approver

Por Que e Quando Desempenhar Esta Tarefa
Você também pode solicitar uma extensão nos espaços Vulnerability Response. Para obter mais informações, consulte Solicitar uma extensão para um item vulnerável adiado no Espaço do gerenciador de vulnerabilidades.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento
1. Navegar até **Todos** > **Configuration Compliance** > **Regras de exceção**.
2. Selecione uma regra de exceção aprovada.
3. Selecione **Solicitar extensão**.
4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Prorrogar até	Selecione a data até quando a regra de exceção deve ser estendida.
Motivo	Insira o motivo para adiar a regra de exceção. As opções incluem: ○ Risco aceito ○ Aguardando janela de manutenção ○ Correção indisponível ○ Controle de mitigação em vigor ○ Outro
Informações adicionais	Insira outras informações relevantes.

5. Selecione **Solicitar aprovação**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na aprovação da solicitação, os campos Adiado até, Motivo e Informações adicionais são atualizados na regra de exceção e nos grupos de resultados de testes associados. Um e-mail também é acionado no envio da solicitação e na ação subsequente do aprovador.

Nota:

- A solicitação passa por dois níveis de aprovação.
- Se uma regra de exceção adiada for estendida novamente, a contagem de adiamento de extensão aumentará no back-end.

Solicitar uma exceção para grupos de resultados de testes usando GRC: Policy and Compliance Management

Solicite exceções de política usando o recurso de gestão de exceções de política GRCPolicy and Compliance Management na aplicação [] de dentro de Configuration Compliance.

Antes de Iniciar

Antes de usar a integração de exceção de política para solicitar exceções de política, você deve baixar a aplicação GRC: Policy and Compliance Management do ServiceNow Store.

Função necessária: sn_vulc.remediation_owner

Você também pode solicitar exceções na IU clássica.

Por Que e Quando Desempenhar Esta Tarefa

A partir da versão 19.0 do Vulnerability Response, você pode solicitar exceções de política para grupos de resultados de testes (TRGs) no Espaço de correção de TI. Para obter mais informações, consulte Solicitar uma exceção usando GRC: Policy and Compliance Management no Espaço de correção de problemas de TI.

Nota:

A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Application Vulnerability Response** > **Itens vulneráveis da aplicação** (ou **Tarefas**de correção)>**Todos**e abra o item ou grupo para o qual você deseja solicitar uma exceção.
   O item ou grupo selecionado deve estar no estado Aberto, Sob investigação ou Aguardando implementação.
2. No formulário selecionado, clique em **Solicitar exceção**.
3. Se GRC: Policy and Compliance Management for selecionado na tela Gerenciamento de exceções, faça o seguinte.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. No formulário, preencha os campos.

Formulário de Exceção de solicitação

Campo	Descrição
Política	Política de gestão de vulnerabilidades para a qual você está solicitando uma exceção.
Objetivo do controle	Objetivos de controle associados à política selecionada. Se uma política não for selecionada, todos os objetivos de controle serão listados.
Válido de	Data em que a exceção será iniciada. O valor padrão é a data atual. Esta data não pode estar no passado.
Válido até	Data em que a exceção de política expira e quando o estado do item ou grupo vulnerável muda de Adiado para Aberto. **Nota:** O número de dias em que a exceção de política é válida não pode exceder a **Duração máxima da exceção (dias)** que você definiu para a política em Política e conformidade. Para obter mais informações, consulte Criar uma política .
Motivo	Motivo para solicitar uma exceção.
Justificativa	Detalhes relacionados ao motivo pelo qual esta solicitação está sendo feita. Este campo deve ser preenchido pelo responsável pela correção.

b. Envie a solicitação de exceção clicando em **Solicitar aprovação**.
O estado do grupo de resultados de testes muda para Em revisão e uma exceção de política é criada. Use a guia **Aprovação de mudança de estado** para rastrear o status da solicitação de exceção.

c. Exiba a exceção de política clicando na lista relacionada Exceções de política.

d. Clique no número da exceção de política.

e. No campo **Aprovador**, selecione o nome do aprovador.

f. Clique na guia Origem e selecione um objetivo de **controle no campo Objetivo** de controle.

g. Clique na guia Avaliação de risco e selecione a classificação de **risco** no campo Classificação de risco.

h. Salve o formulário.

i. Clique na guia **Controles afetados**.

j. Adicione os controles clicando em **Adicionar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

k. Salve o formulário.

> **Nota:**
> Você pode gerar uma revisão de conformidade clicando em **Solicitar revisão de conformidade**.

O formulário de aprovação é enviado ao aprovador.

O aprovador pode aprovar a solicitação clicando em **Aprovar** ou solicitar aprovação adicional clicando em **Solicitar aprovação adicional**.

O estado do registro muda para Adiado. O motivo declarado é aquele que você selecionou ao gerar a solicitação de exceção. A guia **Adiamento** fornece anotações adicionais sobre o registro.

> **Nota:**
> Se a solicitação for rejeitada, o registro será movido para o estado anterior.

4. Clique em **Enviar**.
Para obter mais informações sobre a integração de exceção de política e a transferência entre o proprietário de correção e o gerente de conformidade, consulte Configuração opcional do Policy and Compliance Management .

Aprovar uma solicitação de exceção no Configuration Compliance

Aprovar solicitações de exceção para grupos de resultados de testes que não podem ser corrigidos imediatamente. Você deve avaliar essas solicitações quanto ao risco e aprová-las para adiamento até que possam ser corrigidas.

Antes de Iniciar
Função necessária: sn_vulc.exception_approver

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Minhas aprovações**.

2. Selecione uma solicitação da sua fila.

3. Aprove ou rejeite a solicitação com os comentários apropriados.

> **Nota:**
> No caso de um fluxo de trabalho de aprovação de dois níveis, após a aprovação de primeiro nível, a solicitação é enviada para o segundo nível para aprovação posterior. Se não houver usuários no segundo nível, a solicitação será aprovada automaticamente após a aprovação de primeiro nível.
>
> Depois que a solicitação é aprovada, o grupo de resultados de testes passa para um estado Adiado. Em caso de rejeição, o grupo de resultados de testes é revertido para o estado anterior.

Definir mapeamentos de motivo da política

Você pode definir as opções de motivo para que estejam disponíveis para qualquer usuário que solicite uma exceção.

Antes de Iniciar
Função necessária: sn_vul.compliance.manager e sn_vulc.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Policy and Compliance** > **Exceções da Política** > **Registro de Integração**.

   Nota:
   Você pode selecionar um motivo nas opções de motivo disponíveis na tabela Opções de motivo ou adicionar um novo motivo.

2. Clique no registro de integração do Vulnerability Response - CVIT do contêiner.
3. Para adicionar uma opção de motivo existente, execute as seguintes etapas:
   a. Na lista de Opções de motivo, clique em **Novo**.
   b. Clique no ícone de lupa para selecionar um motivo.
4. Para adicionar novas opções de motivo à tabela Opções de motivo, execute as seguintes etapas:
   a. Na lista de Opções de motivo, clique em **Novo**.
   b. Clique no ícone de lupa.
   c. Clique em **Nova**.
   d. No formulário, preencha os campos.

Formulário Lista de seleção de motivos

Campo	Descrição
Rótulo	Rótulo exclusivo para esta opção.
Valor	Valor exclusivo para esta opção. Este valor é mapeado na tabela Mapeamentos de motivo de exceção de política para as respectivas aplicações. Para navegar até esta tabela, insira sn_sec_cmn_policy_reason_mapping.LIST no navegador de filtros.
Ordem	Ordem para esta opção. Os motivos são solicitados com base neste número.
Padrão	Opção para indicar que esta opção de motivo estará disponível sempre que uma exceção de política sob demanda for solicitada. Se o registro de integração não contiver opções específicas da aplicação, todas as opções de motivo que tenham o campo **Padrão** selecionado estarão disponíveis.
Ativo	Opção para exibir a opção na lista de opções de motivo.

5. Clique em **Enviar**.

Análise e relatório para Configuration Compliance

Os relatórios a seguir são fornecidos para monitoramento.

Exiba políticas, ICs, testes e resultados de testes nos Configuration Compliance relatórios de visão geral.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Configuration Compliance relatório

A página inicial Configuration Compliance fornece uma exibição executiva de políticas, ICs, testes e resultados de testes, ajudando a equipe de segurança a identificar áreas de preocupação rapidamente. Configuration Compliance gráficos de significância podem ser adicionados, conforme necessário. Você também pode retornar informações relacionadas a Configuration Compliance usando o recurso de pesquisa global.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

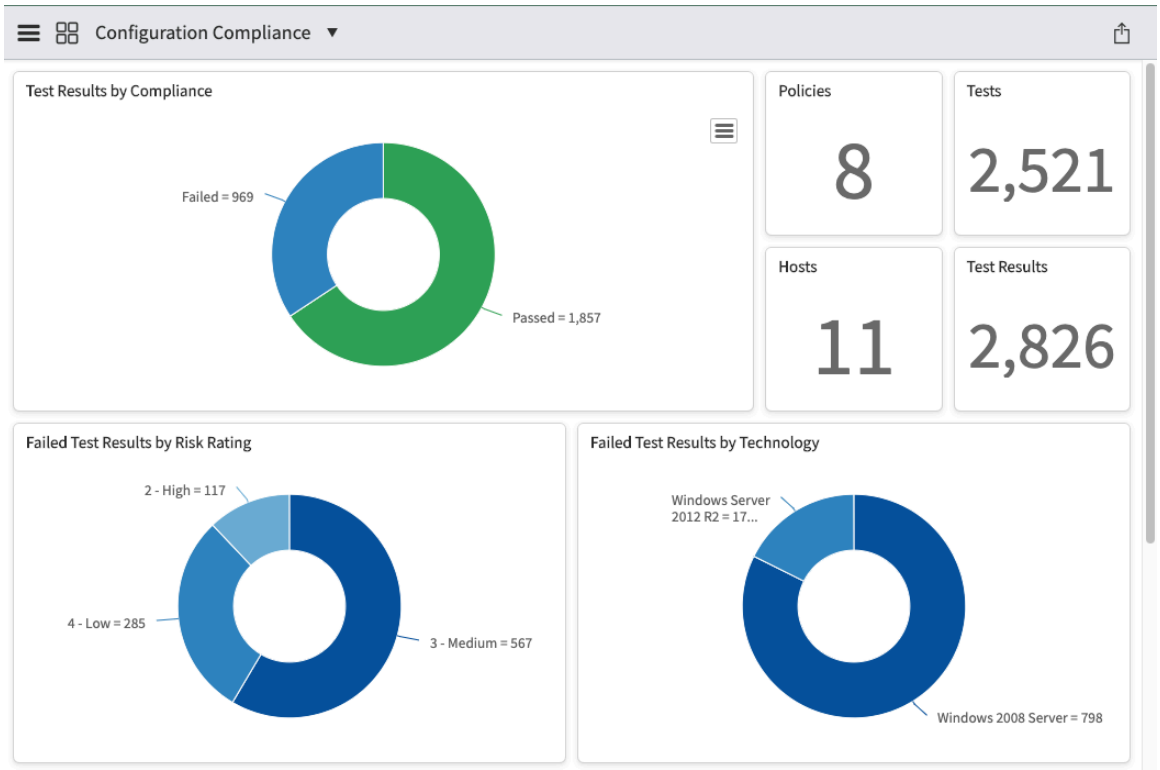
Em cada gráfico, você pode apontar para qualquer parte de um gráfico (barra, pizza, ponto de dados) para exibir dados gerais específicos dessa parte do gráfico. Se você clicar em qualquer parte de um relatório, uma lista será aberta para fornecer informações detalhadas.

Nota:
Qualquer pessoa com a função sn_vulc.read pode exibir o painel. Qualquer pessoa na função sn_vulc.write ou sn_vulc.admin pode criar e editar um painel. Somente sn_vulc.admin pode excluir um painel.

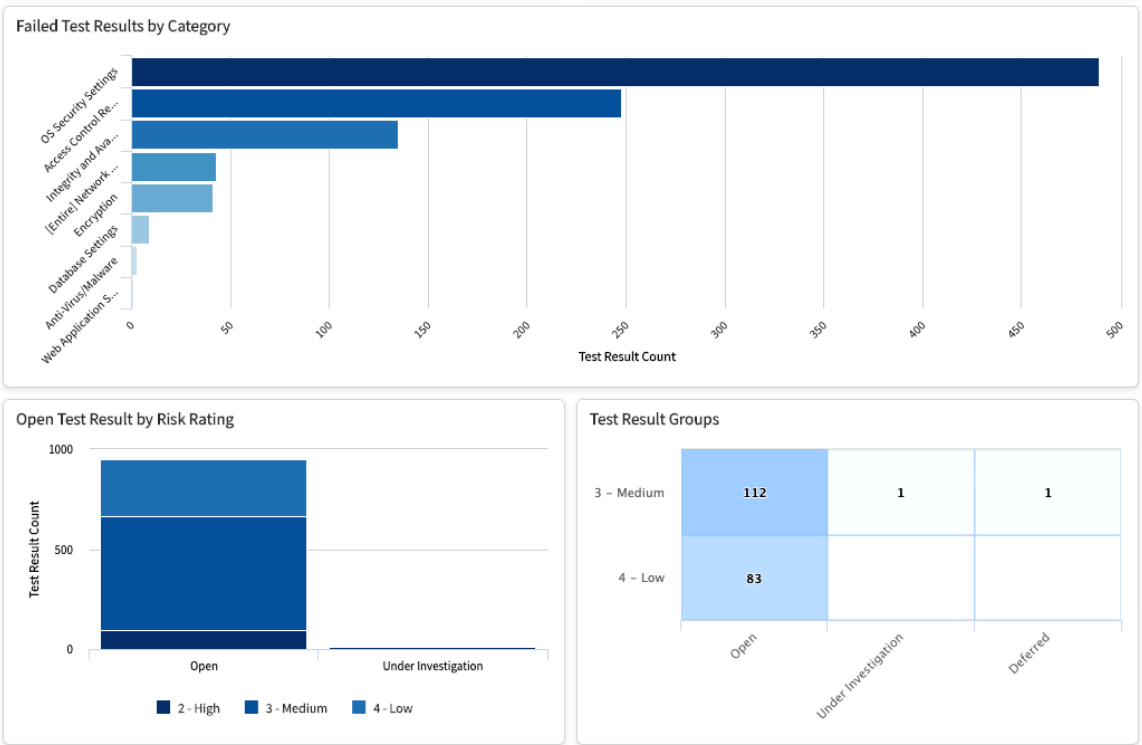
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de visão geral de vulnerabilidade



Relatório do Configuration Compliance



Relatórios de visão geral de vulnerabilidade

Nome	Visual	Descrição
Resultados de testes por conformidade	Donut	Exibe o número de testes abertos que foram aprovados ou reprovados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relatórios de visão geral de vulnerabilidade

Nome	Visual	Descrição
Políticas	Número	Número de políticas com resultados de testes com falha.
Testes	Número	Número de testes com resultados de testes com falha.
Hosts	Número	Número de hosts com resultados de testes com falha.
Resultados de testes	Número	Exibe o número de resultados de testes.
Resultados de testes com falha por classificação de risco	Donut	Exibe o número de testes com falha por classificação de risco.
Resultados de testes com falha por tecnologia	Donut	Exibe modelos com testes com falha.
Resultados de testes com falha por categoria	Barra	Exibe as categorias com o maior número de resultados de testes com falha.
Abrir resultado de testes por classificação de risco	Barra	Exibe o número de resultados de testes em aberto por classificação de risco.
Grupos de resultados de testes	Gráfico	Exibe grupos de resultados de testes por estado e classificação de risco.

Configuration Compliance painel

Este Solução Análise da plataforma contém conteúdo Performance Analytics e Relatórios pré-empacotado para uso com outros produtos Now Platform. Este Solução Análise da plataforma fornece visibilidade em nível de host fora de conformidade e configurações do plano de controle de nuvem.

Esta Solução Platform Analytics contém conteúdo pré-empacotado de Performance Analytics e Reporting para uso com outros produtos da Now Platform. Esta solução de análise de plataforma fornece visibilidade sobre configurações de plano de controle de nuvem e de nível de host fora de conformidade.

O painel do Performance Analytics para Configuration Compliance contém vários widgets que apresentam dados para diferentes dimensões. Ele fornece uma exibição abrangente das tendências de conformidade, problemas de configuração, tendências de correção e gestão de exceções.

Nota:
O plug-in Performance Analytics para Configuration Compliance deve ser instalado para exibir o painel Configuration Compliance [PA] na estrutura Next Experience. Se não estiver instalado, você poderá exibir o painel existente, que foi criado usando a estrutura de relatório.

Ativar Performance Analytics para Configuration Compliance

Ative a aplicação do pacote de conteúdo ServiceNow Store para o Solução Análise da plataforma.

Antes de Iniciar
Ative a versão de assinatura completa de Performance Analytics na instância em que você está ativando esta Solução Now Intelligence. Você pode ativar Performance Analytics em uma instância de não produção sem comprar uma assinatura. Para obter mais informações, consulte Ativar assinatura do Performance Analytics .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você precisa de uma conta Now Support e permissão para solicitar aplicações para as instâncias em consideração. A conta Now Support e a instância devem fazer parte da mesma empresa. Para obter mais informações, consulte Instalar um produto ServiceNow no ServiceNow Store.

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Use Performance Analytics para o painel Configuration Compliance para gerar relatórios sobre os grupos de resultados de testes, o status de conformidade, as ações de correção e as solicitações de exceção.

Procedimento

1. Navegar até **Todos** > **Aplicações do sistema** > **Todas as aplicações** > **ServiceNow Store**.
2. Procure Performance Analytics por Configuration Compliance e verifique se você tem os direitos válidos.
3. Pesquise Performance Analytics para Configuration Compliance.
4. Instale a aplicação.

   Ao instalar esta aplicação, você também ativa a aplicação Configuration Compliance.

Exibindo o painel Performance Analytics para Configuration Compliance

Você pode gerenciar seus problemas de configuração mais importantes e corrigi-los rapidamente exibindo os relatórios no painel Configuration Compliance Performance Analytics (PA).

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Funções necessárias de Now Platform

As funções a seguir são necessárias para o painel Configuration Compliance Performance Analytics :

- administrador: um administrador pode instalar e ativar o Performance Analytics para Configuration Compliance e fazer mudanças nas propriedades do sistema.
- pa_admin: um administrador do Performance Analytics pode criar e revisar os trabalhos em segundo plano, indicadores, detalhamentos, widgets e painéis. Este administrador também pode configurar e iniciar a coleta de dados.
- sn_vulc.read: um usuário com a função de leitura pode revisar os dados do painel.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesse o painel Configuration Compliance

Para abrir o painel, navegue até **Todos** > **Configuration Compliance** > **Visão geral**.

A partir da versão 14.9 do Configuration Compliance, este painel também pode ser exibido na IU da nova experiência. Para exibir o painel na nova IU, navegue até **Espaços** > **Espaço para gerentes de vulnerabilidades** e clique no ícone**Painéis**. Dependendo da sua função, o painel padrão será exibido. Para exibir outros painéis, clique no menu suspenso ao lado do nome do painel. Para obter mais informações, consulte Visão geral dos painéis e Visão geral dos painéis.

Nota:
Se você estiver em Tokyo, poderá exibir os painéis na IU do Next Experience, mas com alguma perda funcional.

Configuration Compliance [PA] guias do painel

Guia Visão geral

A guia **Visão geral** fornece cinco filtros. Esses filtros são a categoria de ativo, o tipo de recurso de nuvem, o provedor de serviços de nuvem, a conta de nuvem e a região de nuvem, que você pode aplicar para visualizar os relatórios dos filtros aplicados. Se você selecionar uma categoria e aplicar as mudanças, todos os widgets compatíveis com a categoria serão atualizados. Cada widget exibe o filtro aplicado na parte inferior e o número de filtros aplicados no ícone de filtro do widget. Clique no relatório em um widget para exibir as informações adicionais na guia **Detalhes de KPI**. Na guia **Detalhes de KPI**, você pode:

- Mostrar os registros.
- Compare os registros.
- Altere o tipo de gráfico.
- Selecione o intervalo de datas.
- Exiba as tendências baseadas na duração.
- Aplique os filtros adicionais, incluindo os filtros que estão indisponíveis na guia **Visão geral**. Um exemplo é o marcador de Host.

O exemplo a seguir mostra como você pode aplicar os filtros na guia **Visão geral** e executar as ações na guia **Detalhes de KPI**.

Guia Visão geral no painel do Configuration Compliance

Guia Conformidade

A guia **Conformidade** exibe a porcentagem de conformidade das várias fontes autorizadas, como a Lei de Responsabilidade e Portabilidade de Seguro Saúde (HIPAA) e a DISA (Data Interchange Standards Association). Você pode refinar esta lista usando os filtros de cabeçalho da coluna e selecionando uma categoria.

O exemplo a seguir mostra como você pode filtrar os dados na guia **Conformidade**.

Guia Conformidade no painel do Configuration Compliance

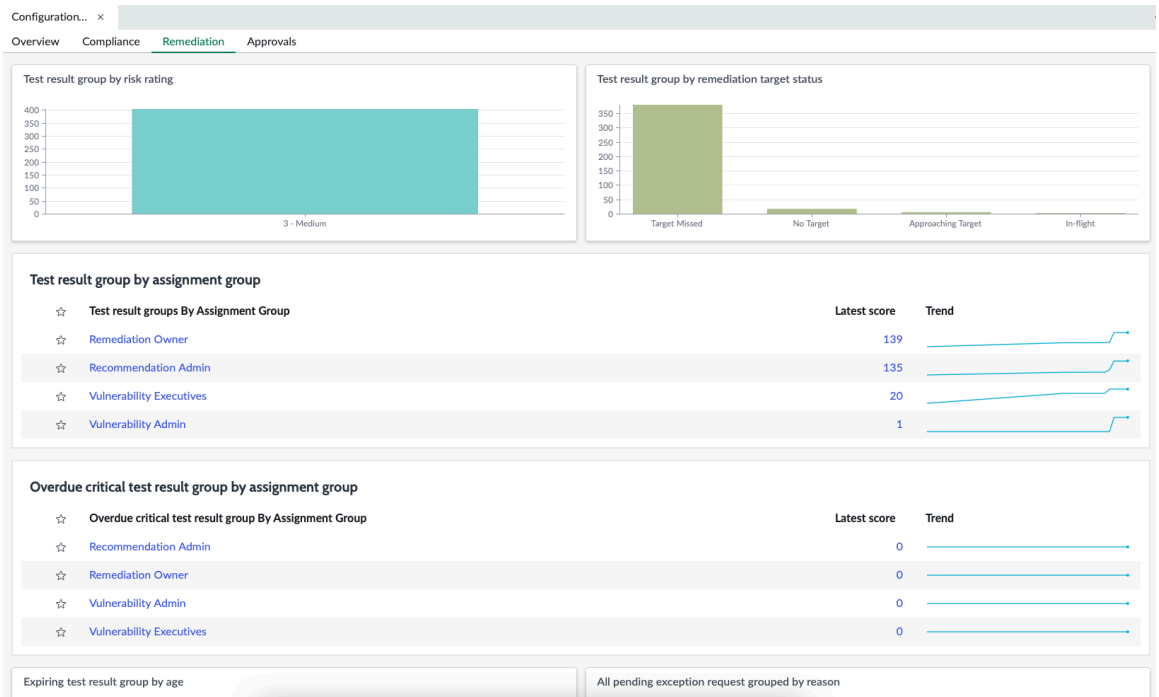
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Guia Correção

A guia **Correção** exibe as informações sobre o andamento da correção. Você pode usar esta guia para ver a higiene de correção de erro de configuração.

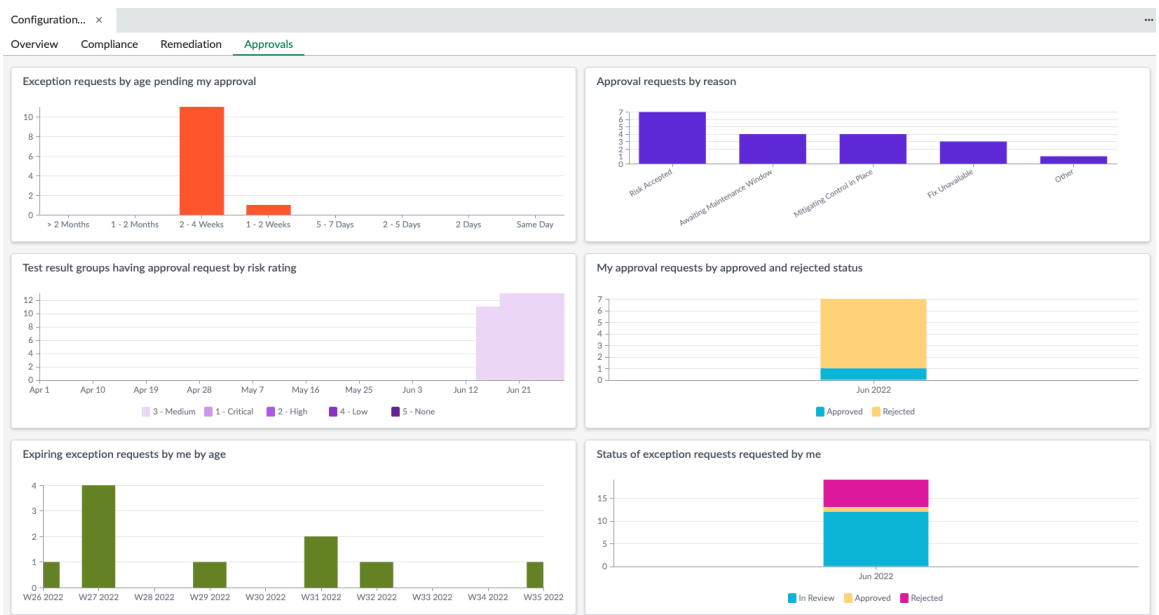
O exemplo a seguir mostra a guia **Correção**.



Guia Aprovações

Os relatórios na guia **Aprovações** exibem as informações sobre as solicitações de exceção e seu status de aprovação.

O exemplo a seguir mostra a guia **Aprovações**.



Detalhamentos

Os detalhamentos usados pelos indicadores são os seguintes:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Motivo adiado
- Idade
- Grupo de atribuição
- Status da Correção
- Resultado
- Pontuação de risco
- Categoria do ativo
- Marcador de host
- Teste de configuração
- Provedor de serviços em nuvem
- Região da nuvem
- Conta de nuvem
- Tipo de recurso de nuvem

Filtros

Na guia **Visão geral**, você pode aplicar os filtros a seguir aos widgets para visualizar os dados filtrados.

Nome	Tipo	Descrição
Categoria do ativo	Escolha	Tipo de ativo. As quatro opções são: • Nuvem • Contêiner • Infraestrutura • OT
Tipo de recurso de nuvem	Escolha	Tipo de recurso. Um exemplo é uma máquina virtual. Os dados no filtro são preenchidos quando você executa a integração.
Provedor de serviços em nuvem	Escolha	Provedor de serviço para a nuvem. As três opções são: • Amazon Web Services (AWS • Microsoft Azure • Google Cloud Platform (GCP)

Tradução automática

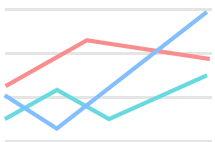
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome	Tipo	Descrição
Conta de nuvem	Escolha	ID da conta que é criado quando uma conta é criada em um serviço em nuvem. Por exemplo, AWS. Os dados de ID da conta são preenchidos no filtro quando você executa a integração.
Região da nuvem	Escolha	Local onde o recurso está hospedado.

Nota:
Você pode selecionar várias opções nos filtros e selecionar **Aplicar**. Cada widget mostra os filtros aplicados e os filtros que não foram aplicados. Dependendo dos dados disponíveis, o relatório é gerado. O widget também mostra a contagem do filtro compatível.

Visualizações de dados

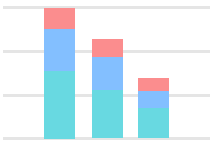
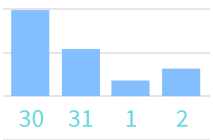
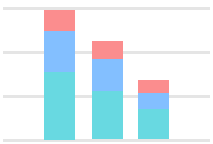
Visualizações da guia Visão geral

Nome do relatório	Tipo	Tabela de origem	Descrição
Tendência de conformidade	Gráfico de linhas 	Resultados de testes	Informações sobre a tendência de conformidade: • Recursos: número total de recursos disponíveis no sistema. • Falha: número de recursos com pelo menos um resultado de teste com falha. • Aprovado: número de recursos com todos os resultados de testes no estado aprovado.
Grupo de resultado do teste	Pontuação única	Resultados de testes	Número de grupos de resultados de testes, que estão presentes no sistema e estão em um estado ativo.
Grupos de resultados de teste críticos próximos do vencimento	Pontuação única	Resultados de testes	Número de grupos de resultados de testes em que a classificação de risco é "crítica" e o status

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

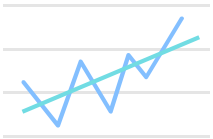
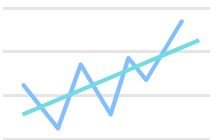
Visualizações da guia Visão geral

Nome do relatório	Tipo	Tabela de origem	Descrição
			de correção é "atingindo a meta".
Resultados de testes por classificação de risco	Barra 	Resultados de testes	Resultados de testes no estado com falha, que são agrupados de acordo com a classificação de risco.
Resultados de testes por idade	Barra 	Resultados de testes	Resultados de testes no estado com falha, que são agrupados de acordo com quando os resultados de testes foram criados.
Resultados de testes encerrados por adesão à meta de correção	Barra 	Resultados de testes	Resultados de testes no estado aprovado, o que indica que este teste está encerrado.
Resultados de testes críticos atrasado por grupo de atribuição	Lista e Pontuação	Resultados de testes	Número de resultados de testes em que a classificação de risco é "crítica" e o status da correção é "meta não atingida". O relatório indica que os resultados do teste estão em um estado Aberto. Se os resultados do teste ultrapassarem a data de destino da correção, eles serão considerados atrasados.
Resultados de testes atrasados - serviços	Lista, Pontuação e Tendência	Exibição do banco de dados de painéis de PA para serviços	Número de resultados de testes para serviços em que o status de correção é

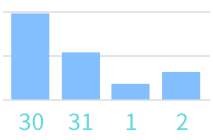
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações da guia Visão geral

Nome do relatório	Tipo	Tabela de origem	Descrição
			"meta não atingida". Este relatório também exibe o nome dos serviços ou departamentos com os resultados de teste mais altos.
Resultados de testes atrasados - responsáveis pelo serviço	Lista, Pontuação e Tendência 	Exibição do banco de dados de painéis de PA para serviços	Número de resultados de testes para responsáveis pelo serviço cujo status de correção é "meta não atingida". Este relatório também exibe o nome dos serviços ou departamentos com os resultados de teste mais altos.

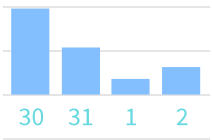
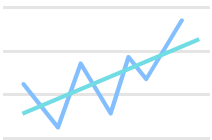
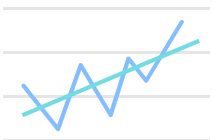
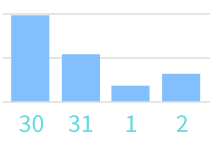
Visualizações da guia de correção

Título	Tipo	Tabela de origem	Descrição
Grupo de resultados de teste por classificação de risco	Barra 	Grupo de resultado do teste	Detalhamento das classificações de risco de todos os grupos de resultados de testes que estão no estado ativo.
Grupo de resultados de teste por status do destino de correção	Barra	Grupo de resultado do teste	Detalhamento das metas de correção de todos os grupos de resultados de testes que não atingiram a meta, não têm meta e estão se aproximando da meta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

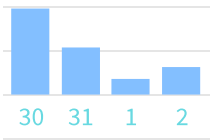
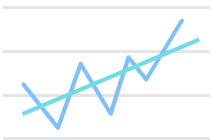
Visualizações da guia de correção

Título	Tipo	Tabela de origem	Descrição
			
Grupo de resultados de teste por grupo de atribuição	Lista, Pontuação e Tendência 	Grupo de resultado do teste	Detalhamento dos grupos de resultados de testes que são baseados em um grupo de atribuição.
Grupo de resultados de teste crítico atrasado por grupo de atribuição	Lista, Pontuação e Tendência 	Grupo de resultado do teste	Detalhamento dos grupos de resultados de testes que são baseados em um grupo de atribuição. Esses grupos de resultados de testes têm uma classificação de risco "crítica" e sua meta de correção não foi atendida.
Expiração do grupo de resultados do teste por idade	Barra 	Grupo de resultado do teste	Grupos de resultados de testes que vão expirar em uma determinada duração. Um máximo de 10 buckets de duração podem ser criados.
Todas as solicitações de exceção pendentes agrupadas por motivo	Barra	Aprovação de mudança de estado	Solicitações de aprovação de mudança de estado

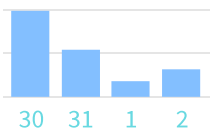
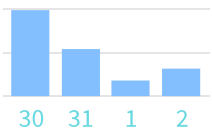
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações da guia de correção

Título	Tipo	Tabela de origem	Descrição
			que são agrupadas pelo motivo da exceção.
Exceções críticas nos resultados de testes por grupo de atribuição	Lista, Pontuação e Tendência 	Resultados de testes	Resultados de testes que estão em um estado adiado e crítico e são agrupados com base no grupo de atribuição.

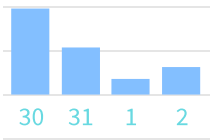
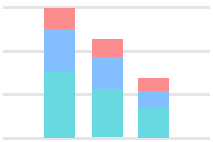
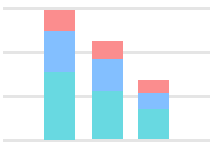
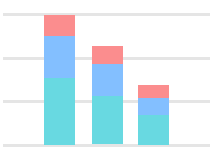
Visualizações da guia Aprovações

Relatórios	Tipo	Tabela de origem	Descrição
Solicitações de exceção por idade com minha aprovação pendente	Barra 	Aprovação	Solicitações de exceção criadas por você e que estão com aprovação pendente. As solicitações são agrupadas de acordo com a duração da solicitação.
Solicitações de aprovação por motivo	Barra 	Aprovação de mudança de estado	Declare solicitações de aprovação de mudança para criar uma exceção e inclua o motivo da exceção.
Grupos de resultados de teste com solicitação de aprovação por classificação de risco	Barra	Grupo de resultado do teste	Grupos de resultados de teste que têm uma solicitação de aprovação baseada na criticidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visualizações da guia Aprovações

Relatórios	Tipo	Tabela de origem	Descrição
			
Minhas solicitações de aprovação por status aprovado e rejeitado	Barra 	Aprovação de mudança de estado	Solicitações de exceção que são agrupadas pelos status aprovado e rejeitado.
Expiração das solicitações de exceção por mim por idade	Barra 	Aprovação de mudança de estado	Solicitações de exceção que vão expirar nas próximas semanas. As solicitações de exceção são agrupadas com base em semanas. Sempre que uma solicitação de exceção é criada, uma data é selecionada para a validade da solicitação de exceção. O cálculo da idade da solicitação é baseado nesta data.
Status das solicitações de exceção solicitadas por mim	Barra 	Aprovação de mudança de estado	Solicitações de exceção que são criadas por você e que são agrupadas de acordo com os seguintes status: • Em revisão • Aprovada • Rejeitada

Configuration Compliance informações de referência

Vários tipos de componentes são instalados com a ativação da aplicação Configuration Compliance, incluindo tabelas, trabalhos programados e funções de usuário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os tópicos a seguir fornecem informações de referência, solução de problemas, além de dados de campo nos formulários e registros encontrados em Configuration Compliance.

- Componentes instalados com Configuration Compliance
- Campos de resultados de testes
- Resolvendo Configuration Compliance problemas de importação
- Modificar data de início dos resultados de PC da Qualys

Exibir Configuration Compliance políticas

Depois de importar os resultados de uma verificação de terceiros para sua instância, você poderá ver sua conformidade de teste no nível de política. Use esta exibição antes de uma auditoria dessa política e de quaisquer registros de teste associados.

Antes de Iniciar

Função necessária: sn_vulc.read e sn_vulc.remediation_owner para exibir

Por Que e Quando Desempenhar Esta Tarefa

As políticas são registros importados e não editáveis dentro de Configuration Compliance.

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Políticas**.
2. Clique na **Descrição resumida** da política que você deseja exibir.

Configuration Compliance campos de formulário de política

Campo	Descrição
Fonte	Nome do sistema do scanner de terceiros ou o nome inserido no plug-in ServiceNow para a API usada para se comunicar com Configuration Compliance.
Tecnologias	Lista de tecnologias associadas à política na aplicação scanner de terceiros.
Identificador da origem	Identificador atribuído a esta política pelo scanner de terceiros.
Origem criada	Data e hora em que a política foi definida na aplicação scanner de terceiros.
Origem atualizada	Data e hora em que a política foi modificada pela última vez na aplicação scanner de terceira política.
Descrição resumida	Descrição resumida ou título atribuído à política na aplicação scanner de terceiros.
Descrição	Descrição detalhada da política conforme definida na aplicação do scanner de terceiros.
Testes	Lista de testes que fazem referência a esta política. Importado do scanner de terceiros. Você pode navegar na lista para obter informações detalhadas sobre um teste específico, se necessário.
Status da correção (versão 12.0)	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Exclui os adiados	Esses valores não incluem ICs de resultados de testes adiados. ○ **ICs restantes**: o número (contagem) de itens de configuração (ICs) com resultados de testes ativos (qualquer estado diferente de **Encerrado**) para esta política. ○ Percentual de**ICs corrigidos**: percentual de ICs em conformidade para esta política. Este número exclui ICs com resultados de testes adiados. ○ **Total de ICs**: o número total de ICs afetados por esta política. Esta contagem exclui resultados de testes adiados.
Inclui os adiados	Os valores representam ICs de todos os resultados de testes ativos (qualquer estado diferente de **Encerrado**). ○ **ICs restantes**: o número de ICs exclusivos associados a um ou mais resultados de testes não encerrados aos quais esta política foi aplicada. ○ Percentual de**ICs corrigidos**: o percentual de ICs em conformidade para esta política. ○ **Total de ICs**: número total de ICs afetados por esta política.

A partir da versão 12.0, para atualizar esses valores sob demanda, abaixo da guia Status de correção, clique no link **Atualizar status** relacionado. Uma mensagem é exibida indicando que os dados estão sendo atualizados. Clique no link **Exibir status** para exibir o andamento da atualização. Após alguns momentos, todos os dados que foram alterados ou atualizados desde o último trabalho programado são atualizados no registro. Os valores de campo atualizados são atualizados.

Exibir Configuration Compliance fontes autorizadas

Use este módulo para exibir informações de resumo sobre cada fonte autorizada e para pesquisar as publicações de origem que foram usadas para criar o registro.

Antes de Iniciar

Função necessária:

- sn_vulc.admin para atualizar
- sn_vulc.remediation_owner para exibir

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Dados de suporte** > **Fontes Autorizadas**.
2. Clique na **Descrição resumida** da fonte autorizada que você deseja exibir.

Configuration Compliance campos de formulário de fontes autorizadas

Campo	Descrição
Número	Número de ID atribuído à fonte autorizada pela sua instância durante o processo de importação.
Fonte	Nome do sistema da aplicação do scanner de terceiros ou o nome inserido no plug-in do scanner para a API que se comunica com Configuration Compliance.
Identificador da origem	Identificador atribuído à fonte autorizada pelo scanner de terceiros.
Descrição resumida	Nome fornecido a esta fonte autorizada no scanner de terceiros.
Fornecedor	Nome da organização ou publicação que foi a fonte original de informações para esta fonte autorizada.
Citações	Lista de informações citadas sobre os resultados de testes. Importado do scanner de terceiros. Você pode navegar nesta lista para obter informações detalhadas sobre um teste específico, se necessário.

3. **Opcional:** Adicione um **fornecedor**.
4. Clique em **Atualizar**.
5. Você pode excluir este registro clicando em **Excluir**.
   Remove o registro da sua instância. Se ainda estiver em uso na integração de terceiros, ele retornará na próxima importação

Exibir Configuration Compliance tecnologias

Use este módulo para exibir informações de resumo sobre cada fonte autorizada e citação (também conhecida, na Qualys, como uma estrutura). Você pode pesquisar as publicações de origem que foram usadas para criar o registro.

Antes de Iniciar

Função necessária:

- sn_vulc.admin para atualizar
- sn_vulc.remediation_owner para exibir

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Dados de suporte** > **Tecnologias**.
2. Clique na **Descrição resumida** da fonte autorizada que você deseja exibir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuration Compliance campos de formulário de fontes autorizadas

Campo	Descrição
Número	Número de ID atribuído à fonte autorizada pela sua instância durante o processo de importação.
Fonte	Nome do sistema do scanner de terceiros ou o nome inserido no plug-in do scanner de terceiros para a API que se comunica com Configuration Compliance.
Identificador da origem	Identificador atribuído à fonte autorizada pelo scanner de terceiros.

3. Você pode excluir este registro clicando em **Excluir**.
   Remove o registro da sua instância. Se ainda estiver em uso na integração de terceiros, ele retornará na próxima importação

Exibir Configuration Compliance testes

Use este módulo para pesquisar informações detalhadas sobre esses testes. Estão incluídas as citações de origem de especialistas que foram usadas ao criá-las, as políticas de configuração de terceiros nas quais elas são usadas e os resultados obtidos na verificação.

Antes de Iniciar

Função necessária:

- sn_vulc.admin para atualizar
- sn_vulc.remediation_owner para exibir

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Controles**.
2. Navegar até **Todos** > **Configuration Compliance** > **Testes**
3. Na lista, abra o controle (teste de conformidade) que você deseja exibir.

A partir da versão 12.0, para atualizar esses valores sob demanda, abaixo da guia Status de correção, clique no link **Atualizar status** relacionado. Uma mensagem é exibida indicando que os dados estão sendo atualizados. Clique no link **Exibir status** para exibir o andamento da atualização. Após alguns momentos, todos os dados que foram alterados ou atualizados desde o último trabalho programado são atualizados no registro. Valores

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de campo como**Pontuação**de **risco , Classificação**de risco , **Data de destino**da correção , **Estado**e os campos na guia **Status** da correção são atualizados.

Configuration Compliance campos de formulário de teste

Campo	Descrição
Número	Número atribuído ao controle durante o processo de importação.
Resultado	Status da verificação. Aprovado ou Reprovado. Se este teste pertencer a várias tarefas de correção, seu estado será determinado seguindo uma ordem de precedência.
Fonte	Nome do sistema da aplicação de integração de terceiros ou o nome inserido no plug-in para a API usada para se comunicar com Configuration Compliance.
Criticidade	Gravidade do problema de configuração ou problemas associados ao controle, conforme definido na integração de terceiros. O nível de criticidade é ajustado para corresponder à granularidade de indicadores de vulnerabilidade semelhantes disponíveis em Vulnerability Response. Os níveis possíveis são: **Crítico** O problema de configuração associado ao controle está causando uma interrupção em um ou mais ICs críticos para os negócios. **Alto(a)** O problema de configuração associado ao controle é uma ameaça, mas não está causando o desligamento de recursos críticos de rede. **Moderado(a)** O problema de configuração associado ao controle é um risco, mas não é uma ameaça imediata. **Baixa** O problema de configuração associado ao controle é uma ameaça de baixo nível e pode ser ignorado em favor de ICs que correm maior risco. **Secundário(a)** O problema de configuração associado ao controle é um risco menor e pode ser ignorado, se necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Identificador da origem	Identificador atribuído ao controle pela integração de terceiros.
Categoria	Categoria de classificação principal fornecida a este tipo de controle pelo fornecedor terceirizado.
Pontuação de risco	Esta é uma pontuação de risco de acúmulo. Esta pontuação de risco é ponderada, com 85% da pontuação da pontuação de risco máxima em todos os Resultados de testes não "Encerrados" (Aberto, Em investigação, Aguardando implementação, Adiado, Resolvido) e 15% da pontuação do número de testes resultados que não estão "Encerrados".Valor calculado por calculadoras de pontuação de risco que se baseia na criticidade dos negócios e nos valores de criticalidade de teste dos resultados de testes.
Subcategoria	Subcategoria atribuída a esta classe de teste pelo fornecedor terceirizado.
Pontuação de risco	Com base em um intervalo de pontuações de risco em uma escala numérica de 1 a 5 que classifica o risco geral com base em um intervalo de pontuações de risco de 1 - Crítico a 5 - Nenhum. Este campo substitui o campo Prioridade nas versões anteriores.
Tecnologias	Lista de tecnologias cobertas por este teste.
Origem criada	Data em que o teste foi definido pela primeira vez na integração de terceiros.
Origem atualizada	Data em que o teste foi atualizado pela última vez na integração de terceiros.
Descrição resumida	Descrição resumida ou título inserido ou atribuído ao teste na integração de terceiros.
Status da correção (v 12.0)	
Exclui os adiados	Esses valores não incluem resultados de testes adiados. ○ **Resultados de testes em aberto**: o número (contagem) de resultados de testes ativos (qualquer estado diferente de **Encerrado**) para este teste de configuração. ○ **Percentual de resultados de testes corrigidos**: o percentual de resultados de testes corrigidos para esta tarefa de correção. ○ **Total de resultados de testes**: o número total de resultados de testes para esta tarefa de correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Inclui os adiados	Esses valores incluem resultados de testes adiados. ○ **Resultados de testes em aberto**: o número (contagem) de todos os resultados de testes ativos (qualquer estado diferente de **Encerrado**) para esta tarefa de correção. ○ **Percentual de resultados de testes corrigidos**: o percentual de resultados de testes corrigidos para esta tarefa de correção. ○ **Total de resultados de testes**: o número total de resultados de testes para esta tarefa de correção.
Descrição	Descrição longa do teste. Para a integração de vulnerabilidade da Qualys, este campo é padronizado para o conteúdo da Qualys Cloud Platform página de capa.
Correção	Instruções de etapas que descrevem como corrigir a não conformidade.
Guias relacionadas	
Citações	Lista de citações inseridas para cada fonte autorizada associada ao teste.
Políticas	Lista de Configuration Compliance políticas que usam este teste.
Resultados de testes	Lista de ICs afetados pelo problema de configuração ou problemas associados a este teste. Você pode acessar testes individuais, ServiceNow itens de configuração ou a lista de tecnologias afetadas, se necessário.
Declarações de Política de GRC	Se o plug-in GRC Policy and Compliance Management estiver instalado, esta guia conterá a política GRC relacionada. Você pode editar esta lista para adicionar ou remover declarações de política.

Tradução automática

Exibir Configuration Compliance resultados de testes

Exibir resultados de testes Configuration Compliance para auditoria e correção.

Antes de Iniciar

Função necessária:

- sn_vulc.read para exibir
- sn_vulc.remediation_owner para exibir e atualizar
- sn_vulc.admin para excluir

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Resultados de testes**.
2. Abra o controle que você deseja exibir.

Configuration Compliance campos de formulário de resultados de testes

Campo	Descrição
Número	O número atribuído ao teste durante o processo de importação.
Fonte	O nome do sistema da aplicação SCA de terceiros ou o nome inserido no plug-in da aplicação para a API que é usada para se comunicar com Configuration Compliance.
Identificador da origem	O identificador atribuído ao controle pela aplicação SCA.
Resultado	Aprovado, Falha, Erro ou Desconhecido. Importado da Qualys.
Pontuação de risco	Resultado da calculadora para este teste.
Pontuação de risco	Com base em um intervalo de pontuações de risco em uma escala numérica de 1 a 5 que classifica o risco geral com base em um intervalo de pontuações de risco de 1 - Crítico a 5 - Nenhum. Este campo substitui o campo Prioridade nas versões anteriores.
Estado	Calculado a partir dos grupos de resultados de testes aos quais o resultado do teste pertence. Se o resultado do teste pertencer a vários grupos, uma ordem de precedência será aplicada para determinar o estado.
Resolução	Calculado a partir dos grupos de resultados de testes aos quais o resultado do teste pertence. Se o resultado do teste pertencer a vários grupos, uma ordem de precedência será aplicada para determinar a resolução.
Visto pela primeira vez	Data importada pela primeira vez em Configuration Compliance. A partir da v13.1.1, o campo **Visto pela primeira vez** exibe a data fornecida pelo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	scanner. Caso contrário, ele exibirá a data importada pela primeira vez em Configuration Compliance.
Visto pela última vez	Data da última importação para Configuration Compliance. A partir da v13.1.1, o campo **Visto pela última vez** exibe a data fornecida pelo scanner. Caso contrário, exibirá a data da última importação para Configuration Compliance.
Última aprovação	Data mais recente em que o resultado do teste foi aprovado.
Testar	Nome do teste.
Item de configuração	Nome do IC anexado ao teste.
Tecnologia	Versão do software em execução no IC.
Descrição	Descrição do teste
Valores Esperados	Valores esperados configurados no Qualys e importados por Configuration Compliance. Este valor é uma expressão booliana que, quando avaliada como verdadeira, torna o resultado do teste **Aprovado**. A expressão pode ser uma combinação de operadores lógicos, de conjunto ou de expressão regular.
Valores reais	Valores retornados pelo teste. Esses valores são conectados à expressão booliana de valores esperados para determinar se o resultado deve ser aprovado ou reprovado. Eles são importados da Qualys. A partir da versão 14.9 do Configuration Compliance, os valores de Evidência estendida e Causa de falha são adicionados à coluna Valores reais.
Correção	Instruções de correção.
Guias relacionadas	
Grupos de resultados de testes	Grupos de resultados de testes associados a este resultado de testes.
Histórico de Resultado de testes	Lista relacionada de resultados de testes que mostram o histórico de resultados de aprovação/reprovação para o mesmo IC/tecnologia/teste.

Exibir um grupo de resultados de testes

Você pode exibir ou, alternativamente, criar um grupo de resultados de testes e executar a correção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária:

- sn_vulc.admin para atualizar ou criar
- sn_vulc.remediation_owner para exibir

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Procedimento

1. Navegar até **Todos** > **Configuration Compliance** > **Grupos de resultados de testes**.
2. Na lista, clique no registro que você deseja exibir.
3. Como alternativa, clique em **Novo** para criar um novo grupo de resultados de testes e preencha os campos.

Campos de formulário Grupo de resultados de testes do Configuration Compliance

Campo	Descrição
Número	O número gerado automaticamente para este registro.
Estado	Status de andamento do grupo. ○ Em aberto ○ Sob investigação ○ Aguardando Implementação ○ Adiado ○ Resolvido ○ Encerrado
Pontuação de risco	Essa pontuação é o valor acumulado das pontuações de risco para todos os resultados de testes ativos em um grupo de resultados de testes. Essa pontuação muda conforme os resultados de testes são corrigidos no grupo de resultados de testes.
Grupo de atribuição	Grupo selecionado para trabalhar neste grupo de resultados de testes.
Pontuação de risco	A quantidade de risco que um resultado de teste com falha representa para o seu sistema. Ele se baseia em um intervalo de pontuações de risco em uma escala numérica de 1 a 5 que classifica os riscos como Críticos (1) a Nenhum (5).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Atribuído a	Indivíduo do grupo de atribuição selecionado que trabalha neste conjunto de tarefas.
Destino de correção	Data em que os resultados de testes devem ser corrigidos, desde a primeira identificação.
Criado em	A data e a hora em que este grupo de resultados de testes foi criado.
Status da Correção	Status da correção do grupo. É determinado pelo resultado do teste com a data de vencimento mais próxima. Para grupos em aberto, os estados incluem Em andamento, Aproximando-se da meta e Meta não atingida. Para grupos fechados, os estados incluem Sem meta, Meta atingida e Meta não atingida. Para datas de destino de correção calculadas, se o grupo de resultados de testes estiver fechado, o status de correção geral de todos os resultados de testes encerrados será mostrado no grupo de resultados de testes. Eles determinam se o grupo atendeu à data ou não. Um status de correção de grupo de resultado de teste encerrado será **Sem destino** se nenhum de seus resultados encerrados tiver uma data de meta de correção. Será **Meta** não atingida se algum dos resultados encerrados não tiver atingido a data de destino. Será **Meta** atingida se pelo menos um resultado encerrado atender à meta e nenhum dos outros a perder.
Atualizado em	A data e a hora em que este registro foi modificado pela última vez.
Descrição resumida	Breve descrição deste grupo de resultados de testes.
Descrição	Descrição longa do grupo de resultados de testes que inclui a lista de softwares associados a este grupo de resultados de testes.
Testar	O teste de configuração associado a este grupo de resultados de testes.
Status da correção (versão 12.0)	
Exclui os adiados	Esses valores não incluem resultados de testes adiados. ○ **Resultados de testes em aberto**: o número (contagem) de resultados de testes ativos (qualquer estado diferente

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	de **Encerrado**) para este grupo de resultados de testes. ○ **Percentual de resultados de testes corrigidos**: o percentual de resultados de testes corrigidos (encerrados) para este grupo de resultados de testes. ○ **Total de resultados de testes**: o número total de resultados de testes para este grupo de resultados de testes.
Inclui os adiados	Os valores representam todos os resultados de testes ativos (qualquer estado diferente de **Encerrado**). ○ **Resultados de testes em aberto**: o número (contagem) de resultados de testes ativos (qualquer estado diferente de **Encerrado**) para este grupo de resultados de testes. ○ **Percentual de resultados de testes corrigidos**: o percentual de resultados de testes corrigidos (encerrados) para este grupo de resultados de testes. ○ **Total de resultados de testes**: o número total de resultados de testes para este grupo de resultados de testes.
Configuração de Grupo	O tipo de filtragem usado para selecionar os resultados de testes para o grupo de resultados de testes.
Método de agrupamento	Nome do método usado.
Regra de grupo	Nome da regra de grupo usada.
Anotações	Anotações do sistema associadas ao registro.
Links relacionados	**Versão 12.0: atualizar link de status**. Atualize os valores no registro de resultado de testes sob demanda. Exibir todos os dados que foram alterados ou atualizados desde o último trabalho programado.
Resultados de testes	Os resultados de testes neste grupo de resultados de testes.
Solicitações de mudança (v 12.0)	A lista de solicitações de mudança associadas a este grupo de resultados de testes.
Aprovações de mudança de estado (v 12.0)	Status e estados das aprovações de solicitação de mudança associadas a este grupo de resultados de testes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Sincronização de estado entre solicitações de mudança e tarefas de correção

Há um relacionamento sincronizado entre os campos de estado das tarefas de correção e os campos de estado das solicitações de mudança (CHGs) na aplicação Configuration Compliance.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Conforme uma solicitação de mudança passa por seu ciclo de vida, ela também muda o estado de todas as tarefas de correção relacionadas automaticamente. A sincronização de estado é habilitada por uma propriedade do sistema por padrão em sua instância quando você baixa a aplicação [Configuration Compliance de ServiceNow Store começando com v12.0.

Quando a sincronização de estado está habilitada, o campo Estado CHG muda o campo Estado da tarefa de correção automaticamente nos seguintes casos:

- Quando uma nova solicitação de mudança é criada para uma tarefa de correção, se não estiver em **Aguardando implementação**, o estado da tarefa de correção avança para **Aguardando implementação**.
- Quando uma solicitação de mudança existente é associada a uma tarefa de correção, se não estiver em **Aguardando implementação**, o estado da tarefa de correção avança para **Aguardando implementação**.
- Depois que as tarefas em uma solicitação de mudança são concluídas (Implementado) e o CHG é movido para o estado **Revisar**, a tarefa de correção avança para **Resolvido**.

Para obter mais informações e exemplos de sincronização de estado, consulte as seções a seguir.

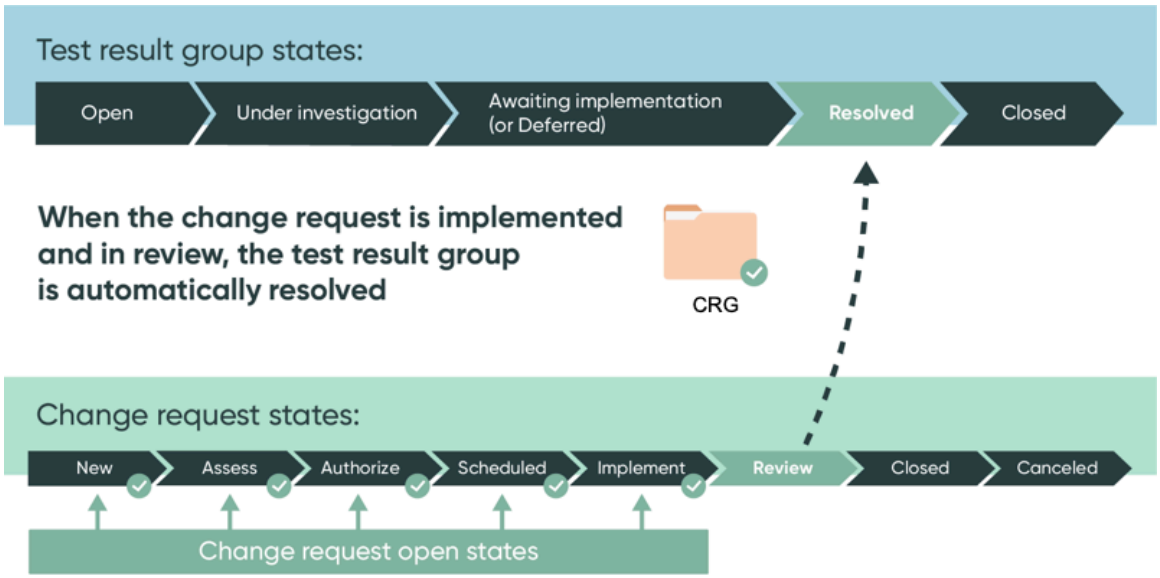
Nota:
Você ainda pode mover manualmente solicitações de mudança e tarefas de correção pelos estados de seus ciclos de vida em seus respectivos registros com a sincronização de estado habilitada, mas quando o sistema registra que uma solicitação de mudança mudou seu estado, ou você adiciona uma solicitação de mudança ou remove de uma tarefa de correção, a sincronização de estado pode substituir sua intervenção manual. No entanto, os estados da solicitação de mudança não movem automaticamente a tarefa de correção de **Encerrado**.

Sincronização de estado de encaminhamento

A imagem a seguir ilustra como os estados CHG movem automaticamente os estados da tarefa de correção em um ciclo de vida de avanço, ou seja, de **Aberto** para **Resolvido**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você pode criar novas solicitações de mudança para qualquer tarefa de correção em um estado diferente de **Resolvido** ou **Encerrado**. A sincronização de estado move automaticamente o TRG bidirecionalmente pelos estados **Aberto**, **Sob investigação**, **Aguardando implementação**e **Resolvido**. Este movimento é baseado em determinados valores do campo de estado na solicitação de mudança. A sincronização de estado entre a solicitação de mudança e a tarefa de correção é invocada automaticamente, a menos que a caixa de seleção (**Adicionar ICs ao CR**) seja exibida em um formulário e você opte por desmarcar a caixa de seleção.

A tarefa de correção não avança para **Resolvido** quando um CHG está em seus estados abertos. Qualquer CHG em estados anteriores a **Revisão** em seu ciclo de vida, como **Novo**, **Avaliar**, **Autorizar**, **Programado** ou **Implementar**, conforme mostrado na figura anterior, são considerados estados abertos para o CHG. Os estados em aberto não movem o campo de estado na tarefa de correção, pois as investigações ou tarefas no CHG não foram concluídas. A sincronização de estado é invocada quando um CHG é criado ou associado à tarefa de correção ou quando o estado de um relacionamento existente muda no CHG. Os estados CHG concluídos são **Revisão** e **Encerrado**com sucesso. Quando um CHG é encerrado com sucesso, seus códigos encerrados são: Bem- **sucedido**ou **Bem-sucedido com problemas**. Nesse caso, a tarefa de correção avança para **Resolvido**.

Sincronização de estado para trás

Como um CHG é processado durante seu ciclo de vida, ele pode ser cancelado em algum momento. Nesse caso, se o CHG for **Cancelado**ou **Encerrado** (com um código de encerramento **Malsucedido**), a tarefa de correção voltará automaticamente para **Sob investigação**. A tarefa de correção retorna para **Sob investigação**porque não há nenhum plano ativo para corrigir a vulnerabilidade.

Se uma tarefa de correção estiver em um estado **Resolvido** e você criar um novo CHG ou associá-lo a um CHG existente em um dos estados abertos iniciais, a tarefa de correção voltará automaticamente para **Aguardando Implementação**. A tarefa de correção retorna para este estado, pois agora há mais trabalho atribuído ao CHG.

Tarefas de correção com mais de um CHG

Se uma tarefa de correção em **Aguardando implementação** tiver mais de um CHG associado a ela, a sincronização de estado será baseada no status do CHG no estado mais

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

antigo de seu ciclo de vida. Por exemplo, digamos que uma tarefa de correção tenha quatro CHGs associados a ela, CHG1, CHG2, CHG3 e CHG4, conforme mostrado na tabela a seguir.

Número CHG	Estado CHG
1	**Implementar**
2	**Cancelado**
3	Encerrado (código de encerramento **malsucedido**)
4	Encerrado (código de encerramento **malsucedido**)

A sincronização de estado entre o CHG e a tarefa de correção, neste caso, é baseada no CHG1, que está no estado mais antigo dos quatro CHGs, (**Implementar**). Nesse caso, a tarefa de correção permanece em **Aguardando implementação**.

Em outro exemplo, se uma tarefa de correção estiver no estado **Resolvido** e tiver um CHG existente que foi implementado e está no estado **Revisão**, e um novo CHG for criado, a tarefa de correção voltará de **Resolvido** para **Aguardando Implementação**. A sincronização de estado é baseada no CHG no estado **Novo**, que é o CHG no estado mais antigo.

Número CHG	Estado CHG
1	Revisar
2	Novo

Além disso, quando as tarefas de correção têm mais de um CHG, o estado da tarefa de correção muda automaticamente nos seguintes casos:

- Quando um CHG avança para **Revisão**, se todos os outros CHGs associados à tarefa de correção estiverem nos estados **Revisão** ou **Encerrado** (com um código de encerramento bem-sucedido), a tarefa de correção muda automaticamente para **Resolvido**. Quaisquer outros CHGs relacionados que sejam cancelados ou encerrados sem sucesso serão ignorados.
- Quando um CHG é movido para **Cancelado** ou**Encerrado** (código de fechamento de **Malsucedido**), se todos os outros CHGs associados à tarefa de correção estiverem no mesmo estado, a tarefa de correção fará a transição automaticamente de volta para **Sob investigação .**

Para obter mais informações sobre os estados da tarefa de correção e o que você pode fazer em cada estado, consulte Configuration Compliance estados.

Separação de domínios e Configuration Compliance

Separação de domínios é compatível com Configuration Compliance. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Nível de suporte: Padrão

- Inclui nível de suporte **Básico**.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como o Domain Separation funciona no Configuration Compliance

Com o Domain Separation, você pode padronizar procedimentos (Configuration Compliance) em toda a base de clientes que atende, com custos operacionais reduzidos e uma qualidade de serviço superior.

Espaços separados de trabalho do cliente para fluxos de trabalho, painéis, relatórios e assim por diante garantem que os dados do cliente sejam separados e nunca expostos a outros clientes.

Suporte à separação de domínio em Configuration Compliance por versões de versão

Liberação	Nível de suporte	Anotações
Orlando	Padrão	
Paris	Padrão	
Quebec	Padrão	
Rome	Padrão	
San Diego	Padrão	
Tóquio	Padrão	
Utah	Padrão	
Vancouver	Padrão	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A separação de domínio para a aplicação Configuration Compliance abrange a seguinte funcionalidade do produto:

- Ingere os resultados de testes de scanners de terceiros (Qualys) no domínio correto.

  Os dados ingerem no mesmo domínio do usuário de integração, cujas credenciais são usadas para integração.

- Verifica novamente hosts específicos de Configuration Compliance no domínio do qual foi solicitado.
- Usa o processo de pesquisa de IC do CMDB para garantir que as informações de IC dos scanners correspondam aos ICs no CMDB do domínio do usuário de integração.
- Calcula as pontuações de risco no nível de resultado do teste de acordo com a calculadora de pontuação de risco definida no mesmo domínio do usuário de integração.
- Regras de grupo de resultados de testes podem ser definidas, atribuídas e permanecem no mesmo domínio que o domínio do usuário de integração.
- As tarefas de correção criadas usando as regras de grupo de resultado de teste de documento permanecem no mesmo domínio em que as regras de grupo são criadas.
- O fluxo de trabalho de adiamento passa pelo processo de aprovação no mesmo domínio para o qual o adiamento é solicitado.
- Relatórios e painéis exibem os estados do resultado do teste, como idade dos resultados do teste, resultados de teste em aberto por IC, resultados de teste por impacto no domínio ao qual pertence.
- O conhecimento de scanners de terceiros (Qualys) pode ser ingerido no domínio global e os dados podem ser compartilhados entre vários clientes.

Nota:
Em todos os casos acima, os princípios abrangentes de visibilidade na separação de domínios separados na NOW Platform se aplicam.

Casos de uso

A aplicação Configuration Compliance gerencia o ciclo de vida de um resultado de teste de ponta a ponta. Os casos de uso a seguir reconhecem a separação de domínio:

- **Ingerir** resultados de testes de Qualys
  - Ingerir dados de várias instâncias
  - Desduplicar os resultados de testes
  - Corresponda ao IC do CMDB
- **Aprimoramento** de resultados de testes com pontuações de risco
  - Aprimoramento de ativos (CMDB)
  - Pontuação de risco
- **Agrupar** resultados de testes e atribuir a tarefa de correção
  - Agrupar automaticamente os resultados de testes
  - Atribuir automaticamente a tarefa de correção
- **Corrigir**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

  - Tarefa de correção atribuída como uma tarefa de correção
  - Ciclo de vida de correção abrangente
  - Fluxo de trabalho de adiamento
- **Medir** a postura de segurança da organização e do programa de gestão de conformidade
  - Tendência de resultados, por conformidade, categoria, criticidade e tecnologia
  - Status e distribuição de políticas, testes, hosts, resultados de testes e pontuação de risco

Configuração

Configurar o Domain Separation para Configuration Compliance não requer etapas adicionais. Todas as tabelas Configuration Compliance adquirem a coluna Domínio depois que a instância é separada por domínio. Você pode direcionar os dados de importação da integração de resultados de testes para domínios específicos. Para obter mais informações, consulte Criar importações separadas por domínio para uma integração. Para obter mais informações sobre precauções e configurações adicionais, consulte Configurações adicionais para Domain Separation.

Dados separados por domínio

Os dados podem ser separados por domínio, o que significa:

- Os resultados de testes ingeridos de scanners de terceiros permanecem no mesmo domínio que o domínio do usuário de integração e não podem ser acessados de nenhum outro domínio.
- Os resultados de testes ou hosts em um domínio não podem ser exibidos em outros domínios.
- O algoritmo de pontuação de risco e as regras de grupo de resultados de testes não podem ser exibidos por qualquer pessoa fora do domínio.
- Fluxos de trabalho de adiamento criados em um domínio não são visíveis em outro domínio.
- Todas as notificações por e-mail estão contidas no domínio ao qual pertencem.

Como os analistas de conformidade gerenciam seus próprios dados de aplicações

- Os analistas criam suas próprias regras de instalação de aplicações, gerenciamento de aplicações de várias origens e pesquisa de IC.
- Os analistas podem configurar integrações específicas exclusivamente para uso no domínio.
- Os analistas podem criar seus próprios fluxos de trabalho de adiamento e gerenciamento de mudanças.
- Os analistas podem criar suas próprias regras de grupo de resultados de testes, lógica de pontuação de risco para priorizar resultados com precisão, atribuir automaticamente tarefas de correção e atribuir ao grupo de atribuição correto.
- Os usuários do domínio criam uma tarefa de correção manual e a fecham.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Lógica de negócios e processos que podem ser separados por domínio pelo proprietário da instância

- Configuration Compliance usuários e grupos
- Configuration Compliance integrações (começando com a versão Madrid)
- Configuração de configuração completa (gestão de usuários e grupos, instalação de aplicações, gestão de aplicações de várias origens, regras de pesquisa de IC, regras de grupo de resultados de testes, calculadoras de risco etc.)
- Concluir o ciclo de vida da correção, incluindo o adiamento

Tópicos relacionados

Domain Separation para provedores de serviço

Campos de resultados de testes

Os resultados de testes são criados automaticamente durante as importações de integração de vulnerabilidade de terceiros.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Configuration Compliance não cria ou atualiza os resultados do teste, mas os importa como parte de uma integração de terceiros. Quando estiverem visíveis em Configuration Compliance, eles serão corrigidos usando **Grupos de resultados de testes**.

Campos de resultados de testes

Campo	Descrição
Número	Número atribuído ao resultado do teste durante o processo de importação.
Fonte	Nome do sistema da aplicação de integração de terceiros ou o nome inserido na aplicação para a API usada para se comunicar com Configuration Compliance.
Identificador da origem	Identificador atribuído ao resultado do teste pela integração de terceiros.
Pontuação de risco	Pontuação baseada no valor `Criticality` do teste. Se você não tiver instalado e configurado, um valor médio de 50 será usado.
Resolução	Resolução do resultado do teste, calculado a partir de grupos associados.
Resultado	Status da verificação. Aprovado ou Reprovado. Se este teste pertencer a várias tarefas de correção, seu estado será determinado seguindo uma ordem de precedência.
Estado	Estado do resultado do teste, calculado a partir de grupos associados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Grupo de atribuição	Grupo selecionado para trabalhar neste resultado de teste.
Atribuído a	Indivíduo do grupo de atribuição selecionado para trabalhar neste resultado de teste.
Tipo de designação	Tipo de atribuição. As opções são: • Regra • Manual • Nenhum(a)
Regra de atribuição	Qual regra de atribuição foi usada com este resultado de teste, quando aplicável.
Visto pela primeira vez	Hora e data em que o resultado do teste foi visto pela primeira vez.
Visto pela última vez	Hora e data em que o resultado do teste foi visto pela última vez.
Testar	O controle ao qual este resultado pertence.
Item de configuração	Item de configuração associado a este resultado de teste.
Tecnologia	Tecnologia associada a este resultado de teste.
Descrição	
Descrição	Descrição detalhada do resultado do teste conforme definido na aplicação do scanner de terceiros.
Valores Esperados	
Valores esperados	Descrição e valores esperados conforme definidos na aplicação do scanner de terceiros.
Valores reais	
Valores reais	Descrição e valores reais conforme definidos na aplicação do scanner de terceiros.
Correção	
Correção	Ação de correção conforme definido na aplicação scanner de terceiros.

A seguir estão os itens vulneráveis listas relacionadas.

Lista relacionada	Descrição
Grupos de resultados de testes	Grupos de resultados de testes associados a este resultado de testes.
Histórico de Resultado de testes	Lista de registros anteriores que contêm resultados diferentes.

Configuration Compliance mapas de criticalidade

Configuration Compliance mapeamento de criticalidade transforma campos de criticalidade da origem para campos em Configuration Compliance.

O sistema de base Configuration Compliance é fornecido com um mapeamento padrão Qualys Cloud Platform para padrão ServiceNow. Criar ou editar um mapa de criticalidade destina-se somente a mapeamentos de terceiros personalizados ou não padrão em seu ambiente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configuration Compliance estados

Com Configuration Compliance, você pode ver um modelo de estado para saber qual é o status do grupo de resultados de testes a qualquer momento. Os estados do grupo de resultados de testes controlam os estados de resultado de testes por precedência.

Nota:
A partir da v14.9 de Configuration Compliance, os seguintes termos foram renomeados:

Mudanças na terminologia

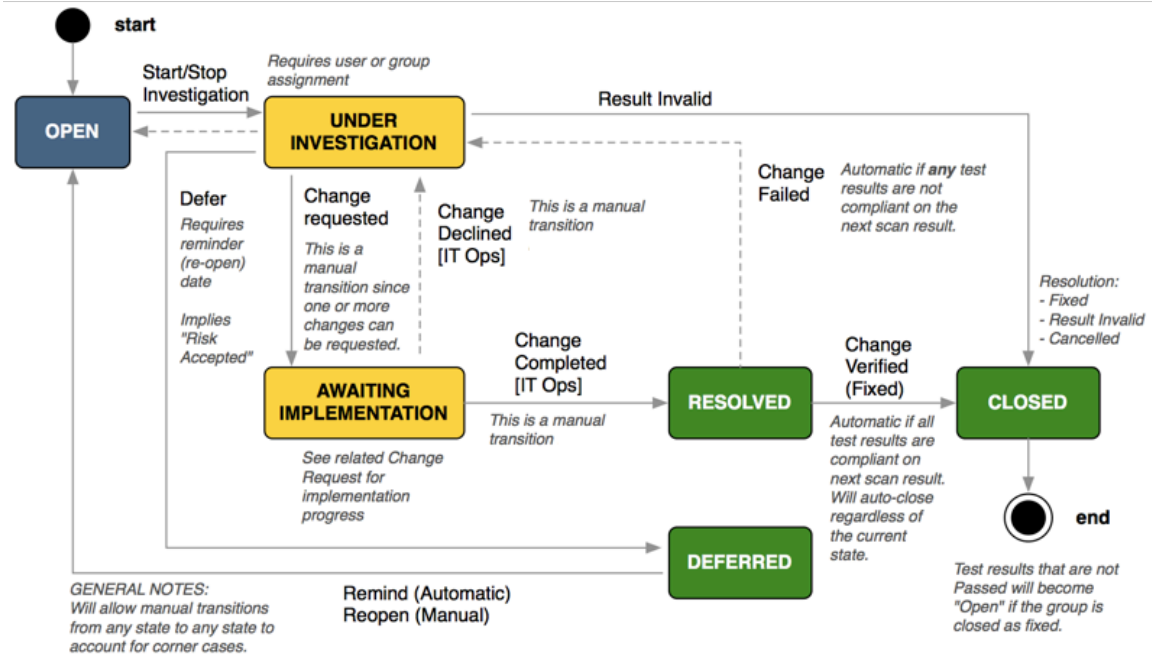
Terminologia anterior à v14.9	Terminologia v14.9 em diante
Grupo de resultados de testes	Tarefa de Correção
Regras de Grupo	Regras de tarefa de correção
Política	Grupo de teste

Estados da Tarefa de correção

As tarefas de correção têm muitos estados possíveis. A transição automática está disponível no estado Resolvido com base nos próximos resultados da verificação. Se todos os resultados de testes forem aprovados na próxima verificação, o grupo será encerrado. Caso contrário, ele fará a transição para o estado Sob investigação. O sistema verifica este estado fechado, mas reavalia o estado do grupo se um resultado de teste for adicionado ou excluído do grupo. As anotações de trabalho são atualizadas para refletir a transição.

A figura a seguir mostra como o estado de uma tarefa de correção faz a transição do estado Aberto para o estado Encerrado.

Fluxo de estado do Configuration Compliance



Nota:
Cada formulário de grupo contém os botões **Seguir** e **Atualizar**, que são padrão para tarefas ServiceNow.

A tabela a seguir lista os estados Configuration Compliance.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados do Configuration Compliance

Estado	Descrição
Em aberto	Estado após a criação.
Sob Investigação	Acionado pelo botão **Iniciar investigação**. A partir deste estado, você pode: **Criar uma solicitação de mudança** Para obter mais informações, consulte Como criar uma solicitação de mudança no Configuration Compliance. **Adiar** Forneça um motivo e selecione uma data de reabertura. **Fechar** Forneça uma resolução e anotações. Fecha o grupo. **Excluir** Confirmar a exclusão. Remove o grupo.
Adiado	Acionado pelo botão **Adiar**. A partir deste estado, você pode: **Reabrir** Faça a transição de volta para um estado Aberto. **Fechar** Forneça uma resolução e anotações. Fecha o grupo. **Excluir** Confirmar a exclusão. Remove o grupo. As informações de adiamento aparecem na guia relacionada **Adiar/ Fechar**. Na data de adiamento, o grupo é reaberto para correção.
Aguardando Implementação	Acionado pelo botão **Aguardando implementação**. A partir deste estado, você pode: **Criar um incidente de segurança** Para obter mais informações, consulte Criar um incidente de segurança. **Criar uma solicitação de mudança** Para obter mais informações, consulte Como criar uma solicitação de mudança no Configuration Compliance. **Resolver** Selecione uma **Resolução** e adicione anotações. As opções são: • Resultado Inválido • Cancelado • Corrigidos O estado se torna Resolvido. As anotações aparecem na guia relacionada **Resolução**. **Fechar** Selecione uma **Resolução** e adicione anotações. As opções são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estados do Configuration Compliance

Estado	Descrição
	• Resultado Inválido • Cancelado • Corrigidos O estado se torna Encerrado. As anotações aparecem na guia relacionada **Resolução**. **Excluir** Confirmar a exclusão. Remove o grupo.
Resolvido	Acionado a partir do botão **Resolver**. A partir deste estado, você pode: **Criar um incidente de segurança** Para obter mais informações, consulte Criar um incidente de segurança. **Reabrir** Faça a transição de volta para um estado Aberto. **Fechar** Selecione uma **Resolução** e adicione anotações. As opções são: • Resultado Inválido • Cancelado • Corrigidos O estado se torna **Encerrado**. As anotações aparecem na guia relacionada **Resolução**. **Excluir** Confirmar a exclusão. Remove o grupo. As anotações aparecem na guia relacionada **Anotações**. As informações de resolução aparecem na guia relacionada **Resolução**.
Encerrado	Acionado a partir do botão **Fechar**. A partir deste estado, você pode: **Reabrir** Faça a transição de volta para um estado Aberto. **Excluir** Confirmar a exclusão. Remove o grupo. As informações de fechamento aparecem na guia relacionada **Adiar/ Fechar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se a Tarefa de correção estiver marcada como Encerrada, com um subestado não fixo (como Risco aceito ou Irrelevante), os resultados de testes adicionados ao grupo terão seu estado atualizado para corresponder à Tarefa de correção.
- Se a Tarefa de correção estiver marcada como Encerrada ou Corrigida e o resultado de testes adicionado não for Encerrado ou Corrigido, o estado do resultado do teste não será alterado e o estado da tarefa de correção será alterado para Aberto.
- Se você determinar que os resultados têm prioridade baixa, poderá mudar o grupo deles para o estado Adiado por um período definido ou Fechá-los imediatamente.

Nota:
Quando as tarefas de correção são adiadas ou encerradas, você pode especificar subestados para definir melhor os motivos para isso. As anotações de trabalho são atualizadas para refletir a transição.

- Quando você cria uma nova tarefa de correção ou divide uma tarefa de correção, os campos **Motivo**e **Até** são reavaliados para os grupos de resultados de testes novos e antigos. Quando o estado de todos os resultados de testes é Adiado, o valor nos campos **Motivo** e **Até** é acumulado para o grupo de resultados de testes.
  - Se todos os resultados de testes em um grupo de resultados de testes forem adiados e tiverem o mesmo **Motivo**, o grupo de resultados de testes será atribuído ao mesmo **Motivo**. Caso contrário, o campo **Motivo** será alterado para **Nenhum**.
  - A data no campo **Até** é atualizada com a data até a mais próxima de todos os grupos de resultados de testes aos quais os resultados de testes pertencem.

Nota:
Esta avaliação é feita pelo trabalho programado *`Rollup test result values to test result group and configuration test`*, que é executado a cada uma hora.

Estados do resultado de testes

O estado de uma tarefa de correção também muda o estado dos resultados de testes associados. Este mecanismo tem dois casos.

Resultados de testes que pertencem a apenas um grupo

Os resultados correspondem ao estado da tarefa de correção com três exceções:

- Se a tarefa de correção mudar seu estado para Encerrado e sua resolução (subestado) para Fixo, o item ignorará essa mudança e voltará para o estado Aberto.
- Se a tarefa de correção mudar seu estado para Encerrado e sua resolução (subestado) para Cancelado, o item ignorará essa mudança e voltará para o estado Aberto.
- Se o status da origem do resultado de testes for Fixo (atualizado por uma verificação ou importação), quando a tarefa de correção mudar seu estado, o resultado do teste mudará seu estado para Encerrado (Corrigido), independentemente do estado da tarefa de correção.

Resultados de testes que pertencem a vários grupos

Os resultados de testes não correspondem ao estado da tarefa de correção automaticamente. Em vez disso, ele pesquisa entre todos os grupos associados para encontrar o estado com a precedência mais alta a ser aplicada. Este é o estado de precedência:

Encerrado (subestado: resultado inválido) > **Adiado** > **Resolvido** > **Aguardando implementação** > **Sob investigação** > **Aberto**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Encerrado (subestado: Fixo) e **Encerrado (subestado: Cancelado)** são dois casos especiais.

Exemplos de estado da Tarefa de correção

Por exemplo:

Estado das Tarefas de correção	Estado do resultado do teste
Grupo A: **Em aberto** > **Sob Investigação** Grupo B: **Aberto**	**Sob Investigação** Quando o Grupo A está Sob investigação e o Grupo B está Aberto, o resultado do teste muda para Sob investigação, pois após a pesquisa, entre o Grupo A e o Grupo B, o Grupo A tem o estado com a precedência mais alta.
Grupo A: **sob investigação** Grupo B: **Em aberto** > **Sob Investigação**	**Sob Investigação** Quando o Grupo B está Sob investigação e o Grupo A está Sob investigação, o resultado do teste permanece como Sob investigação, pois após a pesquisa, entre o Grupo A e o Grupo B eles têm o estado com a mesma precedência.
Grupo A: **sob investigação** Grupo B: **Sob Investigação** > **Aguardando Implementação**	**Aguardando Implementação** Quando o Grupo B está Aguardando Implementação e o Grupo A está Sob Investigação, o resultado do teste muda para Aguardando Implementação, pois após a pesquisa, entre o Grupo A e o Grupo B, o Grupo B tem o estado com a precedência mais alta
Grupo A: **Sob Investigação** > **Adiado** Grupo B: **Aguardando Implementação**	**Adiado** Quando o Grupo A é Adiado e o Grupo B é Aguardando Implementação, o resultado do teste muda para Adiado, pois após a pesquisa, o item 1 descobriu que entre o Grupo A e o Grupo B, o Grupo A tem o estado com a precedência mais alta
Grupo A: **Adiado** Grupo B: **Aguardando Implementação** > **Encerrado (resultado inválido)**	**Encerrado (resultado inválido)** > **Adiado** Quando o Grupo B é Encerrado e a resolução (subestado) é Resultado inválido e o Grupo A é Adiado, o resultado do teste muda para Encerrado (resultado inválido), pois após a pesquisa, entre o Grupo A e o Grupo B, o Grupo B tem o estado com a precedência mais alta.
Grupo A: **Adiado** Grupo B: **Encerrado (resultado inválido)** > **Abrir (via Reabrir)**	**Adiado** Quando o Grupo B é reaberto e seu estado muda para Aberto e o Grupo A é Adiado, o

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estado das Tarefas de correção	Estado do resultado do teste
	resultado do teste muda para Adiado, pois após a pesquisa, entre o Grupo A e o Grupo B, o Grupo A tem o estado com a precedência mais alta.

Casos especiais do estado do resultado de testes

Estado da tarefa de correção	Estado do resultado do teste
Grupo A: **Sob Investigação** Grupo B: **Aguardando Implementação** > **Encerrado (corrigido ou cancelado)**	**Sob Investigação** Quando o Grupo B é Encerrado (subestado Fixo ou subestado Cancelado) e o Grupo A é Sob investigação, o resultado do teste muda de Aguardando implementação (anteriormente, a precedência mais alta) para Sob investigação (atualmente, a precedência mais alta).
Grupo A: qualquer estado Grupo B: qualquer estado	Se o status da origem do resultado de testes for Fixo (atualizado por uma verificação ou importação), quando a tarefa de correção mudar seu estado, o resultado do teste mudará seu estado para Encerrado (Corrigido), independentemente do estado das outras tarefas de correção associadas estão em. A pesquisa de resultado de testes para o estado da tarefa de correção não ocorre.

Resolvendo Configuration Compliance problemas de importação

Resolva problemas com a importação de integração de terceiros.

Importar resolução de problemas

Problema	Resolução
Os resultados de testes estão ausentes	Verifique o `Start Time` na integração do **Qualys PC Results**. Pode não estar atrasado o suficiente. Consulte Modificar data de início dos resultados de PC da Qualys.
A integração está falhando	Verifique o status da **execução da integração de vulnerabilidade**. As entradas do processo de integração individual contêm o XML importado, que pode ser examinado em busca de informações inesperadas. Navegar até **Integração de Vulnerabilidade da Qualys** > **Integrações Primárias** > **Resultados do QualysPC** > **Execuções de integração de vulnerabilidade** guia relacionada. Escolha a execução mais recente. Examine o status e as anotações das entradas na lista relacionada **Processo de integração de vulnerabilidades** em busca de anomalias. .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modificar data de início dos resultados de PC da Qualys

Se os dados estiverem ausentes para a data de início na importação de Resultados de PC da Qualys, eles poderão ser modificados.

Antes de Iniciar

Função necessária: sn_vul_qualys.admin

Procedimento

1. Navegar até **Todos** > **Integração de Vulnerabilidade da Qualys** > **Administração** > **Integrações Primárias**.
2. Clique **em Qualys PC Results** integration.
3. Clique **em Detalhes da integração**.
4. Defina o campo **Hora** de início com um valor no passado, para que todos os resultados de testes verificados e detectados, desde essa hora, sejam detectados.

   Nota:
   Se a data for deixada em branco, nenhum dado será retornado na primeira execução. Defina o valor como no máximo um mês no passado. Esta configuração evita que uma grande quantidade de dados exceda as limitações de taxa da API da Qualys, bem como aciona os tempos limites de execução.

5. Clique em **Enviar** ou **Atualizar**.
6. **Opcional:** Clique **em Executar agora** para executar imediatamente.

Regras de pesquisa de IC para Microsoft Defender for Cloud Integration para Security Operations e Palo Alto Prisma Cloud

Você pode usar as regras de pesquisa de item de configuração (IC) para as integrações Microsoft Defender for Cloud Integration e Palo Alto Prisma Cloud para encontrar uma correspondência correta para os tipos de recurso usados com frequência no Configuration Management Database (CMDB).

Visão geral

O módulo Regras de pesquisa de IC contém as regras que ajudam a definir os campos que têm os dados correspondentes no Configuration Management Database (CMDB). Você pode usar essas regras para identificar as aplicações e as versões da aplicação. Todos os ativos Microsoft Defender for Cloud Integration e Palo Alto Prisma Cloud são identificados exclusivamente pela combinação de seu ID de objeto, conta de nuvem e datacenter lógico na ServiceNow plataforma. A descoberta ServiceNow preenche o ID do recurso na coluna `Object_id` do CMDB em diferentes formatos para os diferentes tipos de recurso. A tabela a seguir mostra os formatos de ID de objeto dos tipos de recursos usados com frequência que o serviço de descoberta usa para preencher a coluna `Object_id` do IC. Qualquer scanner que queira pesquisar um ativo de um tipo de recurso específico deve pesquisar usando o formato de ID de objeto correto. Você pode obter o formato de ID de objeto correto analisando a coluna de ID de objeto da classe de IC CMDB correspondente e, em seguida, tentando construir o ID de objeto usando os valores recebidos do scanner.

Formato de ID de objeto para vários tipos de recurso

Tipo de recurso	Formato
AWS::EC2::Instance	ID do objeto

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formato de ID de objeto para vários tipos de recurso

Tipo de recurso	Formato
AWS::ElasticLoadBalancing::LoadBalancer	Nome do balanceador de carga
AWS::S3::Bucket	arn:aws:s3:::<Bucket Name>

A correspondência de IC para um resultado de teste pode não ser encontrada com precisão no Configuration Management Database (CMDB), a menos que o mesmo formato do `object_id` seja usado na regra de pesquisa. Na maioria das vezes, as regras de pesquisa de IC OOB encontram uma correspondência para os tipos de recursos usados com mais frequência para Microsoft Defender for Cloud Integration e Palo Alto Prisma Cloud. Se as regras de pesquisa de IC a seguir não encontrarem os ICs no CMDB para os resultados de testes, você poderá criar uma regra de pesquisa de IC para um tipo de recurso. Para obter mais informações sobre como criar uma regra de pesquisa de IC, consulte Criar uma regra de pesquisa de IC.

Regras de pesquisa de IC

As regras de pesquisa de IC a seguir são específicas para Microsoft Defender for Cloud Integration e Palo Alto Prisma Cloud.

Bucket S3

Esta regra de pesquisa tenta encontrar o IC no CMDB pelo valor que foi obtido ao concatenar o `arn:aws:s3:::` e o nome do recurso. O valor obtido é pesquisado na coluna `object_id` da tabela `cmdb_ci_cloud_object_storage`. Esta regra de pesquisa se aplica somente quando o tipo de recurso é `AWS::S3::Bucket`.

Nome

Esta regra de pesquisa tenta encontrar o IC no CMDB pelo nome. O nome, que é pesquisado na coluna `Object_id` da classe de IC, corresponde a um tipo de recurso na tabela `sn_capi_resource_type`.

Nota:
Para a aplicação Palo Alto Prisma Cloud, esta regra de pesquisa de IC é executada somente para os tipos de recurso `AWS::RDS::DBInstance`, `AWS::ElasticLoadBalancing::LoadBalancer` e `AWS::CloudTrail::Trail` . Você pode adicionar os tipos de recursos para os quais deseja executar esta regra de pesquisa de IC.

ID do recurso

Esta regra de pesquisa tenta encontrar o IC no CMDB pelo ID do recurso. O ID do recurso, que é pesquisado na coluna `Object_id` da classe de IC, corresponde a um tipo de recurso na tabela `sn_capi_resource_type`.

Nota:
Você pode definir a prioridade de uma regra de pesquisa de IC no campo **Pedido**. A regra de pesquisa de IC com o menor valor de ordem é executada primeiro.

Comum do Vulnerability Response

O plug-in Vulnerability Response Common é instalado ao instalar a aplicação Vulnerability Response.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A partir da v20.0 do Vulnerability Response, você pode usar a estrutura de relatórios agregados no Vulnerability Response Common para criar relatórios de vulnerabilidades de host, vulnerabilidades de aplicação, vulnerabilidades de contêiner e configurações incorretas.

Estrutura de relatórios agregados

Usando a estrutura de relatórios agregados, você pode criar relatórios para os dados que envolvem consultas dinâmicas complexas e de longa execução para melhor desempenho.

A estrutura de relatórios agregados melhora o desempenho ao:

- usando menos recursos e renderizando relatórios com mais rapidez,
- agregar os dados e reutilizar agregações e detalhamentos (Agrupar por) e
- reduzindo as consultas ao banco de dados

Quando você tiver mais de um milhão de itens vulneráveis, use a estrutura fornecida no Vulnerability Response Common junto com os relatórios padrão.

Funções necessárias

As seguintes funções e tarefas estão associadas a esta solução:

- Now Platform administrador (admin): instale e ative este Solução Análise da plataforma e faça as mudanças necessárias nas propriedades do sistema.
- Performance Analytics Administrador (pa_admin): revise as agregações, os widgets e os painéis. Configure e inicie a coleta de dados. Compartilhe os painéis com as partes interessadas apropriadas.
- Administrador (sn_vul_cmn.admin): cria agregações.
- Gravação de VR (sn_vul_cmn.write): edite os dados nas agregações e nos resultados agregados.
- Leitura de VR (sn_vul_cmn.read): revise os dados nas agregações e nos resultados agregados.
- Analista de vulnerabilidade (sn_vul.vulnerability_analyst): revisa os resultados agregados.

Tópicos relacionados

Configurar uma agregação para dados de origem

Executar várias agregações simultaneamente

Configure o número de agregações que podem ser executadas simultaneamente

Criar um relatório usando uma agregação

Configurar uma agregação para dados de origem

Para analisar o desempenho de um aspecto específico em um processo de negócios que está registrado em uma tabela ServiceNow, crie uma agregação específica para o aspecto e crie um relatório para essa agregação.

Antes de Iniciar
Função necessária: sn_vul_cmn.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Relatórios de agregados** > **Definições de agregação** > **Todos** e clique em **Novo**.
2. No campo **Nome**, dê à agregação um nome descritivo.
3. No campo **Descrição**, forneça uma breve descrição sobre a agregação.
4. Na guia **Origem**, preencha os campos.

Campos da guia Origem

Campo	Descrição
Tabela	Tabela da qual você deseja buscar os dados para o relatório. Este menu suspenso contém tabelas app sec common, app-vul, app-vulc, app-vul-container e de vulnerabilidade da aplicação.
Agregar função	Função a ser aplicada à coluna selecionada em **Campo**. ○ **Contagem**: número de registros. ○ **Soma**: soma total dos valores na coluna selecionada em **Campo**. ○ **Média**: média de todos os valores em uma coluna selecionada em **Campo**. ○ **Máximo**: valor máximo na coluna selecionada em **Campo**. ○ **Mínimo**: valor mínimo da coluna selecionada em **Campo**. ○ **Contagem separada**: valores exclusivos na coluna selecionada em **Campo**.
Campo	Coluna na qual você deseja aplicar a função. **Nota:** Este campo não aparece quando você seleciona **Contagem** no campo **Função agregada**.

5. Na guia **Condições adicionais**, forneça a condição no campo **Condições** para selecionar um conjunto específico de registros para o qual você deseja obter os resultados agregados.
6. Na guia **Agrupar por**, selecione as colunas da tabela pelas quais você deseja agrupar ou empilhar os dados. Você pode selecionar até dois detalhamentos.

   Se você selecionar a coluna de **data** em qualquer grupo por campo, o campo **Tendência por** será exibido. Você pode obter os resultados de agregação que são categorizados por semana, dia, minutos etc. selecionando as opções no campo **Tendência por**.

7. Na guia **Programação**, selecione ou crie uma programação de agregação, que define a frequência com que você pode executar a agregação para buscar os dados.
   Para criar uma programação de agregação, consulte Executar várias agregações simultaneamente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Você não pode programar a execução de agregação para uma definição de agregação inativa.

8. Clique em **Enviar** para criar a agregação.
   A agregação aparece na lista Agregação. Na frequência predefinida, a agregação é executada e um registro é criado junto com uma data e hora de execução na lista relacionada Execuções programadas para cada execução.
9. Navegar até **Todos** > **Resultados agregados** e abra sua agregação para ver os Resultados agregados e as Execuções programadas.
   Os resultados agregados são listados na lista relacionada **Resultados agregados**. Se a execução de agregação falhar, consulte a coluna **Anotações** na lista relacionada de **Execuções programadas** para obter mais informações.
10. **Opcional:** Selecione **Executar agora** para coletar os resultados da agregação, independentemente da programação de agregação.
    Se você encerrar a execução programada quando ela estiver em andamento, nenhuma mudança será feita nos resultados agregados. Você também pode excluir ou desativar uma agregação.

O que Fazer Depois

Crie um relatório usando sua agregação. Para obter mais informações sobre como criar um relatório usando uma agregação, consulte Criar um relatório usando uma agregação.

Tópicos relacionados

- Estrutura de relatórios agregados
- Executar várias agregações simultaneamente
- Configure o número de agregações que podem ser executadas simultaneamente
- Criar um relatório usando uma agregação

Executar várias agregações simultaneamente

Você pode programar a execução de várias agregações usando uma única programação de agregação.

Antes de Iniciar

Função necessária: sn_vul_cmn.admin

Por Que e Quando Desempenhar Esta Tarefa

Suponha que você queira executar seis agregações ao mesmo tempo. Crie uma programação de agregação e adicione todas as agregações a ela. Essas agregações são executadas na frequência e hora definidas.

Procedimento

1. Navegar até **Todos** > **Relatórios de agregados** > **Programação**.
2. Selecione **Novo**.
3. No formulário de programação de agregação, preencha os campos.

Campo	Descrição
Nome da programação	Nome da programação de agregação.
Programar trabalho	Execução programada de script que define a frequência com que as agregações devem

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	ser executadas. Você pode criar um trabalho programado selecionando o botão **Novo**.

4. Selecione **Enviar**.
   A programação de agregação aparece na lista de programação de agregações.
5. Abra sua programação de agregação.
6. Selecione **Editar**, adicione as agregações à **Lista** de agregação e selecione **Salvar**.
   As agregações selecionadas aparecem na lista relacionada Agregações.

> **Nota:**
> Se você adicionar uma agregação inativa a uma programação, a execução programada não será iniciada.

7. Selecione **Atualizar**.
   Essas agregações são executadas na frequência definida na programação de agregação.

Tópicos relacionados

Estrutura de relatórios agregados

Configurar uma agregação para dados de origem

Configure o número de agregações que podem ser executadas simultaneamente

Criar um relatório usando uma agregação

Configure o número de agregações que podem ser executadas simultaneamente

Um novo processador ou um trabalho em segundo plano, o Aggregated Reporting Framework Processor, é enviado com o sistema de base, que executa os trabalhos programados relacionados à tabela do Aggregated Reports Framework. Isso permite que todo o subsistema seja executado em segundo plano e permite uma melhor utilização dos recursos do sistema quando eles estiverem disponíveis.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Configuração de trabalho em segundo plano – Calculadora de resultado de agregação comum do Vulnerability Response**.
2. Defina o número de agregações que você deseja executar simultaneamente no campo **Máximo de threads simultâneos** e selecione **Salvar**.
   Por padrão, quatro agregações são executadas simultaneamente.
3. Navegue até a lista Pools de processadores de trabalho em segundo plano, **sn_sec_cmn_background_job_processor_pool.list** e selecione **Novo** para criar um processador de trabalho em segundo plano para a Estrutura de relatórios agregados.
   Para obter mais informações sobre como criar um pool de processadores de trabalho em segundo plano, consulte Processamento paralelo avançado para trabalhos em segundo plano no Vulnerability Response .

> **Nota:**
> O número de processadores de trabalho em segundo plano deve ser igual ao número máximo de threads simultâneos fornecido no formulário **Configuração do trabalho em segundo plano - Vulnerability Response Common-Aggregation Result Calculator**. Consulte a Etapa 2.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

- Estrutura de relatórios agregados
- Configurar uma agregação para dados de origem
- Executar várias agregações simultaneamente
- Criar um relatório usando uma agregação

Criar um relatório usando uma agregação

Para visualizar e analisar os dados específicos de uma agregação que você criou, gere um relatório fornecendo uma condição para a agregação no construtor de condição.

Antes de Iniciar

Função necessária: pa_admin

Procedimento

1. Navegar até **Todos** > **Relatórios** > **Criar novo**.
2. Na guia **Dados**, preencha os campos.

Campos da guia Dados

Campo	Descrição
Nome do relatório	Nome do relatório.
Tipo de origem	Tipo da origem da qual os dados são obtidos. Selecione **Tabela**.
Tabela	Nome da tabela para a qual a agregação é criada. Selecione a tabela de resultados **agregados, Resultado agregado [sn_vul_cmn_aggregate_result]**.

3. No construtor de condição, defina a condição da agregação para a qual você deseja gerar um relatório.

Condição no construtor de condição

Parte	Descrição
Campo	Selecione **Agregação**.
Operador	Selecione **é**.
Valor	Nome da agregação.

4. Na guia **Dados**, clique em **Avançar**.
5. Na guia **Tipos**, selecione como você deseja visualizar os dados e clique em **Avançar**.
   Para saber mais sobre tipos de relatório, consulte Criação de relatórios .

   As visualizações compatíveis são gráfico de barras, gráfico de pizza e mapa térmico. Você pode modificar os gráficos de linhas e outras visualizações de tendências para usar as visualizações compatíveis com resultado agregado para representar os mesmos dados. A exibição de lista não é compatível.

6. Na guia **Configurar**, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Agrupar por	Selecione **Agrupado por 1** que você selecionou na guia **Agrupar por** para a agregação.
Empilhar por	Selecione **Agrupado por 2** que você selecionou na guia **Agrupar por** para a agregação.
Agregação	Aplique a função **Mínimo** ou **Máximo** no **Valor**.

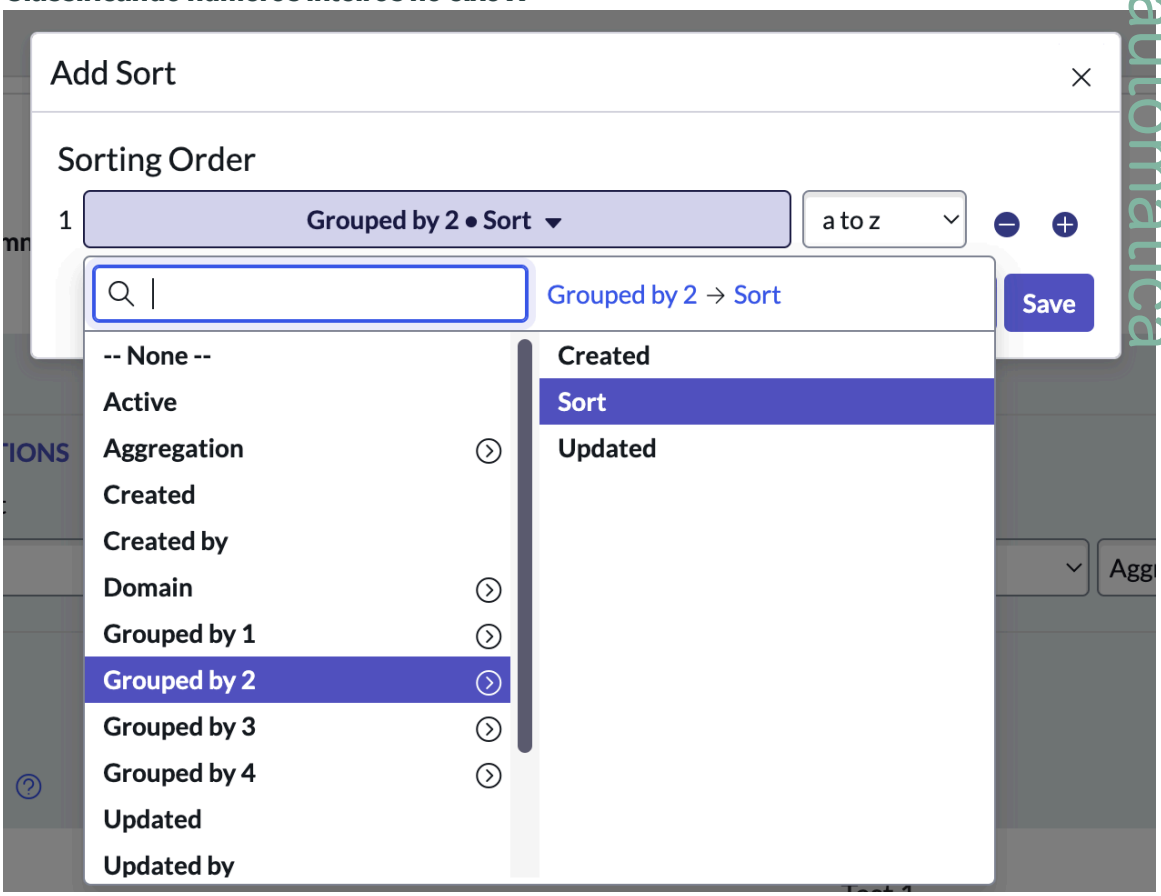
7. Na guia **Estilo**, preencha os campos conforme apropriado e clique em **Executar**.
   Para obter mais informações sobre os campos nas guias **Configurar** e **Estilo**, consulte o vídeo Como criar um relatório .
8. No construtor de condição, defina a condição da agregação para a qual você deseja gerar um relatório e clique em **Executar**.

   O relatório é exibido.
9. Para classificar os valores no eixo x, selecione **Adicionar classificação**.

   a. Para cadeias de caracteres, forneça a condição como **Agrupado por > az ou za** para classificar as cadeias de caracteres em ordem alfabética.

   b. Para valores de tipo de dados inteiros e de data, forneça a condição como **Agrupado por.classificação > az ou za** para classificar os valores em ordem crescente e decrescente, respectivamente.

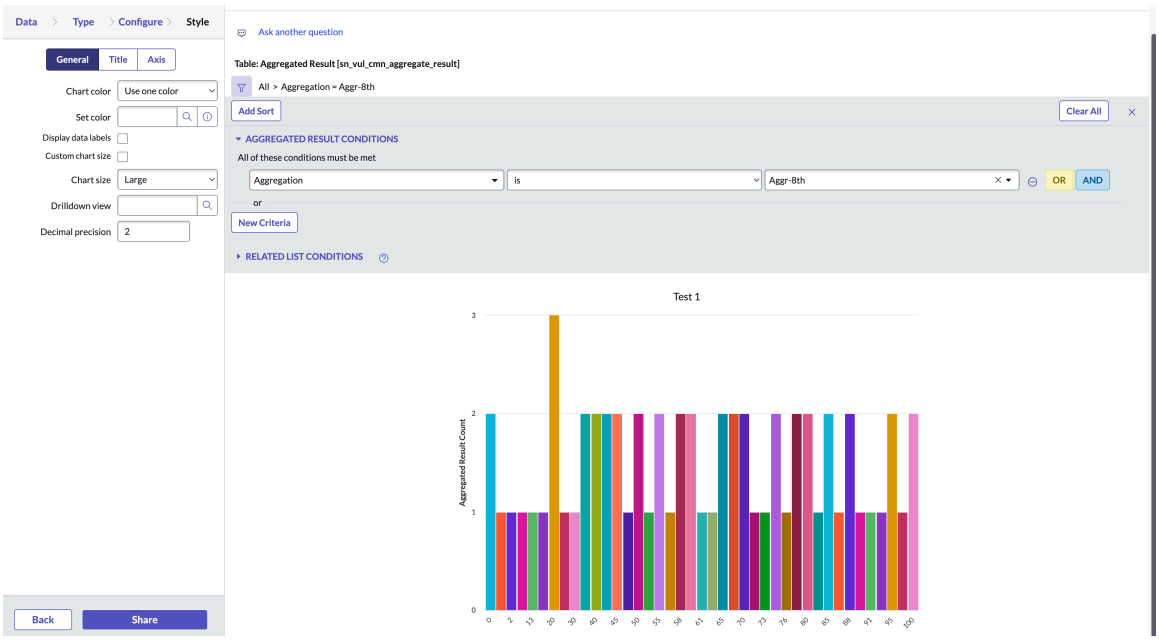
Classificando números inteiros no eixo X



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Selecione **Executar**.
Os valores inteiros e de data são classificados no eixo X.



10. Clique em **Salvar** para salvar seu relatório.
O relatório gerado para uma agregação é exibido na guia **Resultados** do respectivo formulário de **agregação**.

11. **Opcional:** Adicione seu relatório a um painel.
Para obter mais informações sobre como adicionar um relatório a um painel, consulte Como adicionar um relatório a um painel dinâmico .

O painel **Vulnerability Management [Aggregated]** que consiste em relatórios criados usando a estrutura de relatório em cache é enviado com o sistema de base. Para exibir este painel, navegue até **Todos** > **Performance Analytics** > **Painéis** > **Todos** > **Gestão de vulnerabilidades [Agregado]**. As agregações ativas correspondentes aos relatórios neste painel são enviadas com o sistema de base.

12. Compartilhe seu relatório com outros usuários.
Para obter mais informações sobre como compartilhar relatórios, consulte Distribuir relatórios .

Tópicos relacionados

Configurar uma agregação para dados de origem

Estrutura de relatórios agregados

Executar várias agregações simultaneamente

Configure o número de agregações que podem ser executadas simultaneamente

Inteligência contra ameaças

A aplicação ServiceNow® Inteligência contra ameaças permite encontrar indicadores de comprometimento (IoC) e aprimorar os incidentes de segurança com dados de inteligência contra ameaças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Explorar • Noções básicas do Inteligência contra ameaças • Domain Separation e Inteligência contra ameaças • Washington DC • Orquestração de inteligência contra ameaças • Vídeos do Security Operations	Configurar • Como instalar Inteligência contra ameaças • Definir uma origem de ameaça	Administrar Definir propriedades Inteligência contra ameaças
Usar • Modos e métodos de ataque • Indicadores de comprometimento • Observáveis • Security Case Management	Desenvolver • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação	Integrar • Integrações do Inteligência contra ameaças • ServiceNow Security Operations diretrizes de desenvolvimento de integração • Dicas para escrever integrações
Solucionar problemas e obter ajuda • Faça ou responda perguntas na comunidade do Security Operations • Pesquise artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente		

Tradução automática

Noções básicas do Inteligência contra ameaças

A aplicação Inteligência contra ameaças permite que você acesse e forneça um ponto de referência para os dados de Expressão de informações de ameaça estruturada (STIX™) da

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

sua empresa. Incluída em Inteligência contra ameaças está a aplicação Security Case Management, que fornece um meio para analisar ameaças à sua organização representadas por campanhas direcionadas ou agentes de estado.

O STIX é uma linguagem para descrever informações de ameaças cibernéticas de maneira padronizada e estruturada. Usando dados do STIX e perfis de Troca automatizada confiável de informações de indicador (TAXII™), os profissionais de ameaça podem usar informações compartilhadas de ameaças cibernéticas para isolar ameaças que foram identificadas anteriormente pela sua empresa e de outras fontes. O TAXII possibilita a troca automatizada generalizada de informações de ameaças cibernéticas.

Inteligência contra ameaças O oferece suporte ao STIX versões 1.1, 2.0 e 2.1.

STIX™ e TAXII™ são marcas comerciais da The MITRE Corporation.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Domain Separation e Inteligência contra ameaças

A separação de domínio é compatível com o módulo Inteligência contra ameaças que está disponível como parte do Security Incident Response. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Básico

- Inclui nível de suporte **Básico**.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Visão geral

No módulo Inteligência contra ameaças (como parte da aplicação Security Incident Response), a separação de domínio permite que os provedores de serviço (SPs) criem e gerenciem o repositório de inteligência contra ameaças das seguintes maneiras:

- Origens de ameaça e perfis de TAXII (Trusted Automated Exchange of Indicator Information, troca automatizada confiável de informações de indicador)
- Observáveis

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Indicadores de comprometimento
- Modos/métodos de ataque de ameaça e gestão de casos em toda a base de clientes que atendem com custos operacionais reduzidos e uma qualidade de serviço superior

Ter espaços de trabalho do cliente separados para fluxos de trabalho, painéis, relatórios e assim por diante garante que os dados do cliente sejam separados e nunca sejam expostos a outros clientes.

Suporte à separação de domínio em Inteligência contra ameaças por versão

A separação de domínio para o módulo Inteligência contra ameaças (como parte da aplicação Security Incident Response) abrange a seguinte funcionalidade do produto:

- Os observáveis de incidente de segurança são direcionados para o domínio apropriado do usuário cujo ID/credencial/escopo gera o incidente. Os observáveis extraídos do incidente são armazenados no domínio do incidente de segurança.
- Configuração de perfis de serviço TAXII para baixar uma ou mais coleções TAXII que oferecem feeds de informações de ameaças cibernéticas. A configuração é armazenada no domínio no qual o perfil está sendo configurado.
- Configurar o download de feeds de ameaças para o repositório IOC no domínio em que a configuração está sendo realizada.
- Criação de modo/métodos de ataque no domínio da origem de inteligência contra ameaças que fornece as informações automaticamente ou o domínio no qual um novo modo/método de ataque está sendo adicionado manualmente pelo usuário
- Criação de casos para investigação de longo prazo de incidentes, observáveis, ICs, usuários e indicadores de comprometimento (IOC) associados ao caso. O caso é armazenado no domínio criado pelo usuário.

Nota:
Em todos os casos acima, os princípios abrangentes de visibilidade em domínios separados na NOW Platform se aplicam. Como sempre, um incidente no domínio primário pode fazer referência a artefatos no domínio secundário, mas não o contrário.

Como a separação de domínio funciona em Inteligência contra ameaças (como parte de Security Incident Response)

A Inteligência contra ameaças faz parte do Security Incident Response nos níveis Professional e Enterprise, mas não com o nível Standard. Portanto, um plug-in separado é necessário. O módulo Inteligência contra ameaças (como parte da aplicação Security Incident Response) cria e gerencia as informações de inteligência contra ameaças associadas a incidentes de segurança em uma organização. Os casos de uso a seguir reconhecem a separação de domínio:

- Criação de observáveis de incidente de segurança no momento da criação do incidente
  - De analisadores de e-mail (baseado em plataforma, phishing relatado pelo usuário, personalizado)
  - De aplicações em armazenamentos de gestão de eventos e informações de segurança (SIEM) de terceiros
  - Digitado manualmente pelo analista do SOC
- Coleção de observáveis de fontes de feed de ameaças – Fontes de inteligência contra ameaças de coletas de TAXII

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Gerenciar observáveis de incidentes de segurança
  - Associar observáveis a indicadores relacionados
  - Associar observáveis a incidentes de segurança
  - Associar observáveis a observáveis secundários
  - Associar observável à origem do feed de ameaças
  - Adicionar anotações de segurança a observáveis
- Gerenciar indicadores de comprometimento
  - Associar indicadores a observáveis relacionados
  - Associar indicadores ao modo/método de ataque
  - Associar indicadores a tipos de indicador
  - Associar indicadores à origem do feed de ameaças
  - Adicionar anotações de segurança a indicadores
- Gerenciar casos
  - Criar caso (manualmente ou a partir de um incidente)
  - Editar um novo caso para adicionar detalhes (escolha o tipo de caso e a severidade, adicione incidentes, observáveis, itens de configuração, usuários, indicadores)
  - Excluir um caso

Configuração do Domain Separation

Configurar o Domain Separation para Inteligência contra ameaças não requer etapas adicionais. Todas as tabelas de Inteligência contra ameaças adquirem a coluna Domínio depois que a instância é separada por domínio.

Dados separados por domínio

Os dados podem ser separados por domínio, o que significa:

- Os observáveis de incidente de segurança em um domínio não podem ser exibidos no escopo de outros domínios.
- Os indicadores de comprometimento em um domínio não podem ser exibidos no escopo de outros domínios.
- Os modos/métodos de ataque associados a um domínio não podem ser exibidos no escopo de outros domínios.
- Os perfis de serviço TAXII associados a um domínio não podem ser exibidos no escopo de outros domínios.
- As origens de inteligência contra ameaças associadas a um domínio não podem ser exibidas no escopo de outros domínios.
- Os casos associados a um domínio não podem ser exibidos no escopo de outros domínios.

As propriedades da Inteligência contra ameaças são definidas no nível global e, portanto, não são separadas por domínio. As configurações incluem:

- O nome de domínio para recuperar informações adicionais para endereços IP/URLs
- A chave de API a ser usada para recuperação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Pesquisa de tabelas IoC locais antes de enviar para o scanner remoto
- Número de dias em que os observáveis locais são considerados
- Marcar um modo/método de ataque como inativo quando não for recebido de fontes de informações de ameaça
- Marcar um indicador como inativo quando não for recebido de qualquer origem por um número especificado de dias

Configuração

Todos os aspectos da configuração da funcionalidade de inteligência contra ameaças são autônomos em um ambiente separado por domínio.

As tarefas a seguir podem ser configuradas por domínio:

1. Criação de perfis de serviço TAXII
   - Escolha uma configuração de serviço do Discovery
   - Escolher uma configuração de serviço de coleta - Atribuir funções a usuários e grupos de usuários
2. Criação de origens de inteligência contra ameaças
   - Configure o serviço REST que fornece as informações de inteligência de ameaça
   - Programar o download de informações de inteligência contra ameaças
   - Escolha as informações de detalhes da ameaça para atribuir à origem
3. Criação de modo/métodos de ataque (manual)
   - Origem, tipo de malware, mecanismo de ataque, tipo de agente da ameaça, descrição, manipulação, efeito pretendido, visto pela primeira vez, visto pela última vez
   - Indicadores relacionados, modo/método de ataque secundário, incidentes de segurança associados

   Nota:
   Os modos/métodos de ataque também são criados automaticamente a partir das origens do feed de ameaças.

4. Configuração de listas padrão para as seguintes categorias de informações de ameaça:
   - Mecanismos de ataque
   - Métodos de descoberta
   - Feeds
   - Tipos de indicador
   - Efeitos pretendidos
   - Notificações
   - Tipos de observável
   - Definições de limite de taxa
   - Tipos de agente da ameaça
   - Motivações de ataque
   - Tipos de infraestrutura

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Capacidades de malware
- Tipos de malware
- Tipos de relatório
- Funções de agente da ameaça
- Tipos de ferramentas

Como os domínios de locatário gerenciam seus dados de aplicação próprios

- Os proprietários de domínio de locatário podem criar seus próprios perfis de serviço TAXII.
- Os proprietários de domínio de locatário podem criar suas próprias fontes de inteligência contra ameaças.
- Os proprietários de domínio de locatário podem criar seus próprios modos/métodos de ataque.
- Os proprietários de domínio de locatário podem criar suas próprias listas padrão para categorias de informações de ameaça.

Nota:
A lógica de negócios e os processos permitem que as programações de download da origem da inteligência contra ameaças sejam separadas por domínio pelo proprietário da instância.

Tópicos relacionados

Domain Separation para provedores de serviço

Configurar Inteligência contra ameaças.

Antes de executar Inteligência contra ameaças em sua instância, você deve baixá-lo do ServiceNow Store. Você também pode configurar propriedades e definir uma origem de ameaça.

Como instalar Inteligência contra ameaças

Antes de executar Inteligência contra ameaças em sua instância, você deve baixá-lo do ServiceNow Store.

Antes de Iniciar
Conclua a check-list de configuração a seguir antes da instalação. Essas tarefas de configuração são necessárias para uma instalação e configuração sem problemas.

Tarefas de configuração	Descrição
Verifique se você tem as funções ServiceNow necessárias para sua instância.	As funções a seguir são necessárias para instalação, configuração e verificação dos resultados esperados: • Se ainda não estiver atribuído, o administrador do sistema [admin] instalará a aplicação e atribuirá a

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tarefas de configuração	Descrição
	função de administrador de ameaças [sn_ti.admin]. • O administrador de ameaças [sn_ti.admin] supervisiona a configuração e verifica os resultados esperados.

Função necessária: administrador

Procedimento

Siga as instruções para download de uma aplicação do ServiceNow Store.

O que Fazer Depois

Definir propriedades Inteligência contra ameaças.

Componentes instalados com Inteligência contra ameaças

Vários tipos de componentes são instalados com a ativação do plug-in Inteligência contra ameaças, incluindo tabelas e funções do usuário.

Nota:
A tabela Arquivos da Aplicação lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Dados de demonstração estão disponíveis para este recurso.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
Administrador de ameaças [sn_ti.admin]	Tem controle total sobre todas as propriedades de ameaça, SLAs e notificações.	sn_ti.write
Leitor de ameaças [sn_ti.read]	Tem acesso de leitura às informações da ameaça.	sn.sec_cmn.int_read
Gravador de ameaças [sn_ti.write]	Tem acesso de gravação às informações da ameaça. Não é possível excluir modos de ataque, indicadores ou observáveis. Somente um administrador de ameaças pode excluí-los.	• sn_sec_cmn.int_write • sn_ti.read
Analista de MITRE [sn_ti.mitre_analyst]	Esta função permite o acesso de leitura aos módulos [MITRE-ATT&CK em Inteligência contra ameaças e ao módulo SIR.	• sn_ti.read • sn_si.read

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabelas instaladas

Tabela	Descrição
Mecanismo de ataque [sn_ti_ataque_mecanismo]	Organiza padrões de ataque hierarquicamente com base em mecanismos que são empregados com frequência ao explorar uma vulnerabilidade. As categorias que são membros desta exibição representam as diferentes técnicas usadas para atacar um sistema.
Modo/método de ataque [sn_ti_attack_mode]	Os modos e métodos de ataque são representações do comportamento dos adversários cibernéticos. Eles caracterizam o que um adversário faz e como ele faz isso em níveis crescentes de detalhes.
Método de descoberta [sn_ti_discovery_method]	Uma expressão de como um incidente foi descoberto.
Feed [sn_ti_feed]	Usado para configurar o Feed de ameaças (RSS) na Visão geral de ameaças.
Modo/método de ataque do indicador [sn_ti_m2m_indicator_attack_mode]	Usado para mapear modos/métodos de ataque para indicadores.
Indicador de compromisso [sn_ti_indicator]	Usado para transmitir padrões observáveis específicos combinados com informações contextuais destinadas a representar artefatos e/ou comportamentos de interesse em um contexto de segurança cibernética.
Indicador de Metadados de Comprometimento [sn_ti_indicator_metadata]	Usado para preencher registros TAXII.
Origem do Indicador [sn_ti_m2m_indicator_source]	Usado para coletar todas as fontes que relatam o indicador específico.
Tipo de Indicador [sn_ti_indicator_type]	Caracteriza um indicador de ameaça cibernética composto por um padrão que identifica determinadas condições observáveis, bem como informações contextuais sobre o significado dos padrões, como e quando ele atua e assim por diante.
Tipo de indicador associado [sn_ti_m2m_indicator_indicator_type]	Indicadores de links com seus tipos aplicáveis
Contagem de incidentes [sn_ti_observable]	Número de incidentes de segurança associados a um observável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Efeito pretendido [sn_ti_intended_efeito]	Usado para expressar o efeito pretendido de um agente de ameaça.
Resultado da verificação de IP [sn_ti_ip_result]	Usado para mostrar os resultados de uma pesquisa de IP.
Limite de taxa de malware [sn_ti_rate_limit]	Define um limite de taxa a ser usado em uma origem de pesquisa.
Verificação de malware [sn_ti_scan]	Uma pesquisa. Contém o que pesquisar, com a origem da pesquisa e um resumo dos resultados da pesquisa.
Entrada da fila de verificação de malware [sn_ti_scan_q_entry]	Um registro de pesquisa enfileirado para pesquisa ou processamento. Facilita as solicitações dentro dos limites de taxa declarados.
Resultado da verificação de malware [sn_ti_scan_result]	Exibe o resultado de uma pesquisa.
Scanner de Malware [sn_ti_scanner]	Define as origens de pesquisa de terceiros a serem usadas na execução de pesquisas.
Limite de taxa do scanner de malware [sn_ti_scanner_rate_limit]	Associa uma origem de pesquisa a um limite de taxa.
Tipo de malware [sn_ti_malware_type]	Usado para expressar os tipos de instâncias de malware.
Observável [sn_ti_observable]	Os observáveis no STIX representam propriedades com estado ou eventos mensuráveis pertinentes à operação de computadores e redes.
Tipo de contexto de observável [sn_ti_observable_context_type]	Armazena o contexto (origem, destino de um endereço IP e assim por diante) para um observável.
Indicador observável [sn_ti_m2m_observable_indicator]	Usado para relacionar observáveis a indicadores.
Origem de Observável [sn_ti_observable_source]	Usado para relacionar observáveis a origens de ameaça.
Tipo de Observável [sn_ti_observable_type]	Lista os vários tipos de observáveis, como endereços IP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Categoria de Tipo de Observável [sn_ti_observable_type_category]	Armazena a primeira categorização de observáveis (por exemplo, endereços IP e URLs). Ele é usado para determinar com mais precisão os tipos de observáveis.
Modo/método de ataque relacionado [sn_ti_m2m_attack_mode_attack_mode]	Usado para relacionar os modos de ataque entre si.
Observáveis Relacionados [sn_ti_m2m_observables]	Usado para relacionar observáveis entre si.
Tipo de verificação [sn_ti_scan_type]	A definição de um tipo de pesquisa, com registros iniciais de arquivo, URL e IP.
Caso de segurança [sn_ti_case]	Armazena registros de caso de segurança criados usando o Case Management.
IoC do caso de segurança [sn_ti_case_ioc]	Usado para gerenciar o relacionamento entre observáveis e casos.
Tarefa relacionada ao caso de segurança [sn_ti_m2m_case_task]	Usado para gerenciar o relacionamento entre tarefas (incidentes de segurança, solicitações de mudança e assim por diante) com casos de segurança.
Exclusão de Relacionamento de Caso de Segurança [sn_ti_case_relationship_exclusion]	Fornece a definição de inclusão e exclusão de registros relacionados em casos de segurança.
Vista [sn_ti_sighting]	O link m2m entre o observável e o resultado detalhado da Pesquisa de detecções usado na execução de uma solicitação de pesquisa de detecções.
Itens de Configuração de Vista [sn_ti_m2m_sighting_ci]	Mapeia itens de configuração para uma pesquisa de vistas.
Detalhe da pesquisa de detecções [sn_ti_sighting_search_detail]	Detalhes de uma pesquisa de vista, por exemplo, o número de itens externos internos encontrados.
Resultado da pesquisa de detecções [sn_ti_sighting_search]	O cabeçalho de uma execução de pesquisa de detecções.
Tipos de observável compatíveis [sn_ti_m2m_ind_type_obs_type]	Relaciona os tipos de indicador a tipos de observável válidos.
Tipo de verificação compatível [sn_ti_supported_scan_type]	Mapeia o tipo de pesquisa para uma origem de pesquisa/implementação específica do

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
	fornecedor. Indica que uma origem de pesquisa específica é compatível com o tipo.
Modo/método de ataque de tarefa [sn_ti_m2m_task_attack_mode]	Relaciona os modos de ataque às tarefas.
Indicador de tarefa [sn_ti_m2m_task_indicator]	Relaciona indicadores a tarefas.
Observável de tarefa [sn_ti_m2m_task_observable]	Relaciona observáveis a tarefas.
Vista da tarefa [sn_ti_m2m_task_sighting]	Armazena registros de tarefa (casos e incidentes de segurança) relacionados a um registro de vista.
Coleta TAXII [sn_ti_taxii_collection]	Define um feed de inteligência de risco cibernético que pode ser importado por um servidor TAXII.
Perfil TAXII [sn_ti_taxii_profile]	Define um repositório para compartilhar inteligência de risco cibernético. Contém coleções TAXII.
Tipo de agente da ameaça [sn_ti_threat_actor_type]	Fornece caracterizações de agentes mal-intencionados (ou adversários) que representam uma ameaça de ataque cibernético, incluindo a intenção presumida e o comportamento observado ao longo do tempo.
Origem da Inteligência contra ameaças [sn_ti_source]	Define uma origem para importar dados de ameaça.
Motivação de ataque associada [sn_ti_stix2_m2m_object_attack_motivation]	Coleta todas as motivações de ataque associadas a um objeto STIX.
Tipo de infraestrutura associada [sn_ti_stix2_m2m_infra_type]	Vincula a infraestrutura aos respectivos tipos.
Fase da cadeia de eliminação associada [sn_ti_stix2_m2m_indicator_kill_chain_phase]	Vincula as fases da cadeia de eliminação aos indicadores.
Fase da cadeia de eliminação associada [sn_ti_stix2_m2m_object_kill_chain_phase]	Vincula as fases da cadeia de eliminação a objetos STIX.
Capacidade de malware associado [sn_ti_stix2_m2m_malware_capability]	Vincula o malware aos respectivos recursos.
Tipo de malware associado	Vincula o malware aos seus tipos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_ti_stix2_m2m_malware_malware_type]	
Observável associado [sn_ti_stix2_m2m_malware_observable]	Coleta todos os observáveis associados a um malware.
Observável associado [sn_ti_stix2_m2m_observed_data_observable]	Coleta todos os observáveis associados a dados observados.
Tipo de relatório associado [sn_ti_stix2_m2m_report_report_type]	Vincula os relatórios de ameaças aos respectivos tipos.
Função de agente da ameaça associada [sn_ti_stix2_m2m_threat_actor_threat_actor_role]	Vincula os agentes de ameaça às suas funções.
Tipo de agente da ameaça associado [sn_ti_stix2_m2m_threat_actor_threat_actor_type]	Vincula os agentes de ameaça aos seus tipos.
Tipo de ferramenta associada [sn_ti_stix2_m2m_tool_tool_type]	Vincula ferramentas com seus tipos.
Motivação de ataque [sn_ti_stix2_attack_motoration]	A Motivação de ataque molda a intensidade e a persistência de um ataque. Os agentes de ameaça e os conjuntos de intrusão geralmente agem de uma maneira que reflete sua situação ou sentimento subjacente, e isso informa os defesas sobre a forma de ataque.
Padrão de ataque [sn_ti_stix2_attack_pattern]	Um tipo de TTP que descreve os métodos que os adversários usam para tentar comprometer os destinos.
Campanha [sn_ti_stix2_campaign]	Um agrupamento de comportamentos adversários que descreve um conjunto de atividades mal-intencionadas ou ataques (às vezes chamados de vagas) que ocorrem ao longo de um período em um conjunto específico de metas.
Linha de ação [sn_ti_stix2_course_of_action]	Uma recomendação de um produtor de inteligência para um consumidor sobre as ações que ele pode realizar em resposta à inteligência.
Referência externa [sn_ti_stix2_external_reference]	Ponteiros para informações representadas fora do STIX.
Avistamento de identidade [sn_ti_stix2_m2m_sighting_identity]	Coleta todas as identidades associadas a uma vista.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
Identidade [sn_ti_stix2_identity]	Indivíduos, organizações ou grupos reais (por exemplo, ACME, Inc.), bem como classes de indivíduos, organizações, sistemas ou grupos (por exemplo, o setor financeiro).
Referência externa do indicador [sn_ti_stix2_indicator_external_reference]	Representa referências externas associadas a indicadores.
Vista do indicador [sn_ti_stix2_indicator_sighting]	Representa vistas de indicadores.
Tipo de infraestrutura [sn_ti_stix2_infrastructure_type]	Representa os vários tipos de infraestrutura.
Infraestrutura [sn_ti_stix2_infrastructure]	Um tipo de TTP que descreve quaisquer sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados, destinados a oferecer suporte a alguma finalidade (por exemplo, servidores C2 usados como parte de um ataque, dispositivo ou servidor que fazem parte da defesa, servidores de banco de dados direcionados por um ataque e assim por diante).
Software instalado [sn_ti_stix2_m2m_malware_analysis_sw]	Coleta todos os softwares (tipos de software SCO) associados a uma análise de malware.
Conjunto de intrusão [sn_ti_stix2_intrusion_set]	Um conjunto agrupado de comportamentos adversários e recursos com propriedades comuns que se acredita ser orquestrado por uma única organização.
Fase da cadeia de eliminação [sn_ti_stix2_kill_chain_phase]	Representa as fases da cadeia de eliminação associadas a uma cadeia de eliminação.
Cadeia de eliminação [sn_ti_stix2_kill_chain]	Representa várias cadeias de eliminação.
Localização [sn_ti_stix2_location]	Representa uma localização geográfica fornecida pelo STIX.
Análise de malware [sn_ti_stix2_malware_analysis]	Os metadados e os resultados de uma análise estática ou dinâmica específica realizada em uma instância ou família de malware.
Capacidade do malware [sn_ti_stix2_malware_capability]	Representa recursos comuns que uma família de malware ou instância exibe.
Sistema operacional do malware	Coleta todos os sistemas operacionais (tipos de software SCO) associados ao malware.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_ti_stix2_m2m_malware_operating_system]	
Malware [sn_ti_stix2_malware]	Um tipo de TTP que representa código malicioso.
Definição de marcação [sn_ti_stix2_marking_definition]	Representa requisitos de manipulação ou compartilhamento para objetos STIX.
Avistamento de objeto [sn_ti_stix2_object_sighting]	Representa vistas de objetos STIX.
Relacionamento objeto-indicador [sn_ti_stix2_m2m_object_indicator]	Coleta todos os relacionamentos entre objetos STIX e indicadores STIX.
Relacionamento objeto-objeto [sn_ti_stix2_m2m_object]	Coleta todos os relacionamentos entre objetos STIX e outros objetos STIX, excluindo os indicadores.
Relacionamento objeto-observável [sn_ti_stix2_m2m_object_observable]	Coleta todos os relacionamentos entre observáveis do STIX e objetos do STIX.
Vista de dados observada [sn_ti_stix2_m2m_sighting_observed_data]	Coleta todos os objetos de dados observados associados a uma vista.
Dados observados [sn_ti_stix2_observed_data]	Transmite informações sobre entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes, usando os Objetos cibernéticos (SCOs) do STIX.
Tipo de relatório [sn_ti_stix2_report_type]	Representa a finalidade ou o assunto primário dos relatórios de ameaças.
Observável relatado [sn_ti_stix2_m2m_malware_analysis_observable]	Coleta todos os observáveis associados à análise de malware.
Objeto do STIX V2 [sn_ti_stix2_object]	Tabela primária comum para o objeto STIX.
STIX V2 Sighting [sn_ti_stix2_sighting]	Tabela primária comum para tabelas de vista STIX.
Função de agente da ameaça [sn_ti_stix2_threat_actor_role]	Representa funções que podem ser desempenhadas por agentes de ameaça.
Agente da ameaça	Os agentes da ameaça são indivíduos, grupos ou organizações reais que operam com intenção mal-intencionada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tabela	Descrição
[sn_ti_stix2_threat_actor]	
Grupo de ameaça [sn_ti_stix2_threat_grouping]	Agrupa todos os objetos STIX que compartilham algum contexto comum.
Anotação de ameaça [sn_ti_stix2_threat_note]	Fornece contexto e análise adicional não contida no objeto STIX correspondente.
Opinião sobre ameaças [sn_ti_stix2_threat_opinion]	Fornece avaliação da precisão das informações em um objeto STIX produzido por uma entidade diferente.
Relatório de ameaças [sn_ti_stix2_threat_report]	Relatórios são coleções de inteligência contra ameaças focadas em um ou mais tópicos, como uma descrição de um agente de ameaça, malware ou técnica de ataque, incluindo contexto e detalhes relacionados. Eles são usados para agrupar informações de ameaças relacionadas para publicar como uma história de ameaça cibernética abrangente.
Tipo de Ferramenta [sn_ti_stix2_tool_type]	As categorias de ferramentas que podem ser usadas para executar ataques.
Ferramenta [sn_ti_stix2_tool]	As ferramentas são um software legítimo usado por agentes de ameaça para executar ataques.
Vulnerabilidade [sn_ti_stix2_vulnerability]	Representa um ponto fraco ou defeito nos requisitos, projetos ou implementações da lógica computacional (exemplo de código) encontrado no software e em alguns componentes de hardware (exemplo de firmware). Eles podem ser explorados diretamente para afetar negativamente a confidencialidade, a integridade ou a disponibilidade desse sistema.

Tradução automática

Definir propriedades Inteligência contra ameaças

Inteligência contra ameaças As propriedades permitem que você controle como diferentes aspectos do sistema funcionam, incluindo a configuração de chaves de API.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração** > **Propriedades**.
2. Defina as seguintes propriedades, conforme necessário.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedades da Inteligência contra ameaças

Propriedade	Descrição
O nome de domínio para recuperar informações adicionais para endereços IP/URLs sn_ti.ip_lookup.web_site	O nome de domínio a ser usado para recuperar informações adicionais em seu banco de dados IoC. Esta propriedade é usada pela inclusão de script ThreatAdditionalInfo para preencher informações adicionais no formulário Observáveis. Valor padrão: http://api.ipinfodb.com/v3/ip-country/ **Nota:** A API de terceiros do pinfodb.com está disponível sem custo extra e é usada em muitos programas de software comerciais. Se você substituí-lo por um nome de domínio diferente, também deve fornecer a chave de API no próximo campo.
A chave de API a ser usada para o domínio, se houver sn_ti.ip_lookup.api_key	A chave de API a ser usada para recuperar informações adicionais em seu banco de dados IoC. Esta propriedade é usada (junto com a propriedade sn_ti.ip_lookup.web_site) pela inclusão de script ThreatAdditionalInfo para preencher informações adicionais no formulário Observáveis.
Não execute a pesquisa de ameaças automatizada em um observável quando o observável estiver associado a um IoC ou for considerado mal-intencionado. sn_ti.scan_ioc_before_sending **Nota:** Você precisa definir a duração na próxima propriedade (sn_ti.scan_ioc_num_days).	Opção para parar de executar a pesquisa automatizada de ameaças em um observável quando o observável for considerado mal-intencionado ou associado a um IoC pela duração configurada (em dias). Se você ainda precisar executar a pesquisa de ameaças para o observável, poderá fazê-lo manualmente. Valor padrão: sim
Duração (em dias) sn_ti.scan_ioc_num_days	Opção para definir a duração até a qual a pesquisa automatizada de ameaças do observável será ignorada. Valor padrão (em dias): 30

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
Não execute a pesquisa de ameaças automatizada em um observável se já estiver em execução. sn_ti.enable_threat_lookup_bypass **Nota:** Você precisa definir a duração na próxima propriedade (sn_ti.threat_lookup_bypass_times).	Se já houver um resultado de pesquisa de ameaças para um observável disponível, você terá a opção de ignorar a reexecução da pesquisa de ameaças automatizada para o mesmo observável até que a duração configurada tenha passado. Valor padrão: Não **Nota:** Se você estiver habilitando esta propriedade, certifique-se de adicionar um valor apropriado.
Duração (em minutos) sn_ti.threat_lookup_bypass_time	Opção para definir a duração após a qual a pesquisa automatizada de ameaças do observável pode ser executada novamente. Valor padrão (em minutos): 0
Defina uma duração de validade para substituições do usuário na descoberta observável. sn_ti.enable_observable_finding_system_override **Nota:** Você precisa definir a validade na próxima propriedade (sn_ti.observable_finding_override_expiry).	Opção para definir uma duração de validade para substituições do usuário nas descobertas observáveis. A descoberta de pesquisa de ameaças do observável não será alterada pelo sistema de base durante esta duração de validade. Valor padrão: Não. **Nota:** Se você estiver habilitando esta propriedade, certifique-se de adicionar um valor apropriado.
Validade (em minutos) sn_ti.observable_finding_override_expiry	Opção para definir o período de validade da descoberta observável. Valor padrão (em minutos): nenhum
Quando um modo/método de ataque não tiver sido recebido de nenhuma origem para o número especificado de dias, marque-o como inativo sn_ti.attack_mode_inactivate_days	Número de dias desde o último recebimento de um modo/método de ataque para que o registro seja marcado como inativo. Valor padrão: 360

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
	Nota: A caixa de seleção **Ativo** não está visível no formulário do **modo/ método de ataque** por padrão. No entanto, você pode adicioná-lo. Quando os modos/métodos de ataque estão inativos, eles não podem ser selecionados em outros formulários.
Quando um indicador não tiver sido recebido de qualquer origem para o número especificado de dias, marque-o como inativo sn_ti.indicator_inactivate_days	Número de dias desde o último recebimento de um indicador para que o registro seja marcado como inativo. Valor padrão: 180 **Nota:** A caixa de seleção **Ativo** não está visível no formulário do **Indicador** por padrão. No entanto, você pode adicioná-lo. Quando os indicadores estão inativos, eles não podem ser selecionados em outros formulários.
O tamanho máximo da carga (em MB) para um anexo do STIX que pode ser analisado. sn_ti.stix.max_payload_size	Especifica o tamanho máximo da carga útil para o anexo do STIX que você pode analisar. Valor-padrão: nenhum Valor máximo permitido: sem limite.
Tempo máximo em segundos que uma conexão HTTP de saída aguarda para obter dados de coleta de TAXII sn_ti.taxii.http.max_timeout	Especifica o tempo máximo que uma conexão HTTP de saída espera antes de buscar o próximo pacote de dados de coleta TAXII. Valor padrão: 300
Número máximo de objetos recuperados em uma chamada REST de um servidor TAXII (aplicável somente para TAXII versões 2.0 e 2.1) sn_ti.taxii.max_page_size	Especifica o número máximo de objetos recuperados em uma chamada REST do servidor TAXII para uma página. Valor padrão: 5000 Valor máximo permitido: 50000
Número máximo de novas tentativas para uma chamada REST TAXII 2.X com falha	Especifica o número máximo de novas tentativas para uma chamada REST TAXII com falha.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Propriedade	Descrição
sn_ti.taxii2.retry_count	Valor padrão: 3

3. Clique em **Salvar**.

Definir uma origem de ameaça

Você pode manter uma lista de Inteligência contra ameaças origens de ameaça. Cada origem inclui a capacidade de definir com que frequência uma origem é consultada. Você também pode executar uma origem de ameaça sob demanda para importar os dados necessários do Structured Threat Information eXpression (STIX).

Antes de Iniciar

Função necessária: sn_ti.admin

Por Que e Quando Desempenhar Esta Tarefa

Inteligência contra ameaças O emprega duas tecnologias para importar informações relacionadas a ameaças: STIX e TAXII (Trusted Automated Exchange of Indicator Information, troca automatizada confiável de informações do indicador).

O STIX fornece uma linguagem padronizada e estruturada para representar um amplo conjunto de informações de ameaças cibernéticas que inclui indicadores de atividade de comprometimento (IoC) (por exemplo, endereços IP e hashes de arquivo), bem como informações contextuais sobre ameaças, como modos/métodos de ataque, que juntos caracterizam de forma mais completa as motivações, capacidades e atividades de um adversário cibernético. Dessa forma, os dados do STIX fornecem informações valiosas sobre como sua organização pode se defender melhor contra ameaças cibernéticas.

A troca automatizada confiável de informações do indicador (TAXII) é usada para facilitar a troca automatizada de informações sobre ameaças cibernéticas. O TAXII define um conjunto de serviços e trocas de mensagens que permitem o compartilhamento de informações acionáveis de ameaças cibernéticas entre a organização e os limites de produto/serviço para a detecção, prevenção e mitigação de ameaças cibernéticas. Os perfis TAXII podem ser configurados como repositórios para compartilhar informações no formato STIX. Cada perfil contém uma ou mais coleções ou feeds TAXII.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Origens** > **Origens de Ameaças**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Nome	O nome da origem da ameaça.
Aplicação	A aplicação que contém este registro.
Ativo	Marque esta caixa de seleção para ativar a origem da ameaça.
Avançado	Marque esta caixa de seleção para exibir os scripts nos campos **Script de fábrica de integração** e **Processador de relatório**.
Descrição	Uma descrição desta origem de ameaça.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Preencha os campos na seção **Programação**, conforme apropriado.

Campo	Descrição
Executar	A frequência com que você deseja que a integração seja executada: Diariamente, Semanalmente, Periodicamente e assim por diante. Conforme observado, os campos subsequentes são exibidos com base na configuração deste campo.
Dia	O dia em que você deseja que a integração seja executada. ◦ Se você selecionou **Semanalmente** no campo **Executar**, este campo exibirá os dias da semana. ◦ Se você selecionou **Mensalmente** no campo **Executar**, este campo exibirá os dias do mês.
Hora	A hora em que você deseja que a integração seja iniciada.
Intervalo de repetição	Se você selecionou **Periodicamente** no campo **Executar**, este campo exibirá o número de dias e horas antes que a integração seja executada novamente.
Iniciando	Se você selecionou **Periodicamente** no campo **Executar**, este campo exibirá as datas e a hora a serem usadas como ponto de partida para atualizações periódicas.
Condicional	Selecione este campo se quiser adicionar parâmetros condicionais.
Condição	Se você marcou a caixa de seleção **Condicional**, insira as condições aqui.

5. Preencha os campos na seção **Detalhes da ameaça**, conforme apropriado.

Campo	Descrição
Indicador	O indicador a ser usado quando os dados não fornecem um explicitamente. Para listas de bloqueio, se vazias, um novo indicador será criado para cada observável.
Tipo de indicador	O tipo de indicador a ser usado para indicadores que são criados e os dados não fornecem explicitamente um tipo de indicador.
Modo/método de ataque	O modo/método de ataque a ser usado quando os dados não fornecem um explicitamente.
Tipo de Observável	O tipo de observável a ser usado para observáveis que são criados e os dados não fornecem explicitamente um tipo de observável.[IS1]
Ponderação	Insira um valor de peso para esta origem a ser usado no cálculo de confiança.

Nota:
O uso dos campos **Indicador**, **Tipo**de indicador , **Modo/método de ataque**e **Tipo de observável** é específico da implementação. O processador padrão, SimpleBlocklistProcessor, se comporta conforme as dicas das ferramentas descrevem. No entanto, uma origem de ameaça TAXII é totalmente orientada por dados. Qualquer processador de origem de ameaça personalizado seria capaz de usar sua própria estratégia. Esses campos são basicamente itens a serem expostos à integração/processador e a implementação decide como usá-los.

6. Preencha os campos na seção **Detalhes da origem**, conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Endpoint	Insira o URL do endpoint do serviço Web em que a origem da ameaça é acessada por Inteligência contra ameaças. Clique no ícone de cadeado para bloquear o URL.
Usar mensagem REST	Se você precisar de uma mensagem REST para acessar a origem da ameaça, marque esta caixa de seleção. Os campos de **mensagemREST e método REST** se tornam obrigatórios.
Mensagem REST	Clique no ícone de pesquisa e selecione a mensagem REST na lista ou clique em **Novo** para definir uma nova mensagem REST.
Método REST	Clique no ícone de pesquisa e selecione o método REST na lista ou clique em **Novo** para definir um novo método REST.
Script de integração	O script de integração padrão é **SimpleRESTSecurityDataIntegration**. Ele executa uma chamada REST simples, salva a resposta como um anexo e retorna o anexo para o processador. Este script atende às necessidades da maioria das organizações. Mas, se você quiser, pode clicar no ícone de pesquisa e selecionar um script de integração diferente ou definir um novo.
Script de fábrica de integração	Se a caixa de seleção **Avançado** estiver marcada, este campo exibirá o script real para criar o script de integração. Você pode editar o script conforme necessário. Essa habilidade é útil para implementações personalizadas. As integrações no sistema de base geralmente não precisam de nenhuma lógica de construtor personalizada.
Processador de relatórios	O script de integração padrão é **SimpleBlocklistProcessor**. Este script é um processador simples que aceita uma lista de bloqueios simples (simples, o que significa um documento de coluna única com observáveis, como URLs ou endereços IP) e cria observáveis. Ele usa os vários campos de **Detalhes da ameaça** para determinar quais campos definir quando os observáveis forem criados.
Script de fábrica do processador	Se a caixa de seleção **Avançado** estiver marcada, este campo exibirá o script real para construir o processador. Você pode editar o script conforme necessário. Este script geralmente é útil para implementações personalizadas. As integrações no sistema de base geralmente não precisam de lógica de construtor personalizada.

7. Clique em **Enviar**.

Nota:
Para obter mais informações sobre como configurar a paginação da origem da ameaça, consulte o artigo KB1213825.

Criar um perfil TAXII

Você pode manter perfis TAXII para compartilhar informações no formato STIX. Cada perfil contém uma ou mais coleções ou feeds TAXII.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Origens** > **Perfis TAXII**.
2. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os seguintes campos conforme apropriado.

4. Preencha os campos na seção **Configuração do serviço de descoberta**, conforme apropriado.

5. Preencha os campos na seção **Configuração do serviço de coleta**, conforme apropriado.

6. Clique em **Enviar**.

Repositório LOC

O repositório IoC contém objetos STIX, cada um desses objetos contém uma informação específica.

Ao combinar objetos STIX por meio de relacionamentos, você permite representações fáceis ou complexas de Cyber Threat Intelligence (CTI).

Inteligência contra ameaças O oferece suporte ao STIX versões 1.1, 2.0 e 2.1.

Modos e métodos de ataque

Modos e métodos de ataque, às vezes chamados de Táticas, técnicas e procedimentos (TTPs), são representações de como os adversários cibernéticos se comportam. Eles caracterizam o que esses adversários fazem e como eles fazem isso, em níveis crescentes de detalhe. Os modos e métodos de ataque se aplicam a STIX 1.1.

Por exemplo, um modo/método de ataque pode ser usar malware para roubar credenciais de cartão de crédito. Ou outra tática relacionada (em um nível inferior de detalhe) pode ser enviar e-mails direcionados com anexos que contenham código malicioso, que é executado após a abertura, captura informações de cartão de crédito ao pressionar as teclas e usa http para se comunicar com um servidor de comando e controle para informações de transferência.

Os modos e métodos de ataque se aplicam a STIX 1.1.

Definir um modo/método de ataque

Os modos e métodos de ataque são importados com os dados do STIX, mas você pode adicionar novos modos/métodos, conforme necessário.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Modo/método de ataque**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Selecionar marcador de classificação	Se você configurou e ativou marcadores de classificação para adicionar metadados ao registro, poderá selecionar um ou mais marcadores para especificar o grau de confidencialidade do modo/método de ataque. Se você não configurou ou ativou marcadores de classificação, esta lista suspensa não será exibida.
Título	Insira um nome descritivo para este modo/método de ataque.
Tipo de malware	Selecione o tipo de malware para este modo/método de ataque. Os tipos de malware disponíveis são recuperados do servidor do fornecedor como dados STIX.
Fonte	Selecione a fonte de dados da ameaça para este modo/método de ataque. Algumas fontes de dados estão incluídas no sistema de base. Você pode criar novas fontes de dados conforme necessário.
Mecanismo de ataque	Selecione o mecanismo de ataque para este modo/método de ataque. Os mecanismos de ataque representam as diferentes técnicas usadas para atacar um sistema. Os mecanismos de ataque disponíveis são recuperados do servidor do fornecedor como dados STIX.
Visto pela primeira vez	Esta data é recuperada do servidor do fornecedor como dados STIX.
Visto pela última vez	Esta data é recuperada do servidor do fornecedor como dados STIX.
Tipo de Ator da Ameaça	Selecione o tipo de agente da ameaça para este modo/método de ataque. Os tipos de agente de ameaça caracterizam agentes mal-intencionados (ou adversários) que representam uma ameaça de ataque cibernético, incluindo a intenção presumida e o comportamento observado ao longo do tempo. Os tipos de agente de ameaça disponíveis são recuperados do servidor do fornecedor como dados STIX.
Descrição	Insira uma descrição do modo/método de ataque.
Manipulação	Insira instruções sobre como lidar com este modo/método de ataque.
Efeito pretendido	Insira o efeito pretendido deste tipo de ataque.

4. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**.
Você pode exibir qualquer uma das listas relacionadas a seguir para exibir informações adicionais.

Lista relacionada	Descrição
Indicadores relacionados	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça.
Modo/método de ataque secundário	Lista os modos/métodos de ataque que são secundários do modo/método de ataque primário.
Tarefas Associadas	Lista as mudanças associadas ao modo/método de ataque primário.

Adicionar um IoC a um modo/método de ataque

Além de importar indicadores como dados STIX, você pode adicionar IoCs a um modo/método de ataque manualmente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Modo/método de ataque**.
2. Clique no modo de ataque ao qual você deseja adicionar um IoC.
3. Clique na lista relacionada **Indicadores** relacionados.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o IoC que você deseja adicionar.
6. Usando a interface de caixa de listagem dupla, adicione o IoC à lista de **indicadores relacionados**.
7. Clique em **Salvar**.

Adicionar um método de modo de ataque relacionado

Além de importar modos/métodos de ataque como dados do STIX, você pode adicionar modos/métodos de ataque relacionados manualmente.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Modo/método de ataque**.
2. Clique no modo de ataque ao qual você deseja adicionar um modo/método de ataque relacionado.
3. Clique na lista relacionada **de modo/método de ataque secundário**.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o modo/método de ataque que você deseja relacionar ao atual.
6. Usando a interface de caixa de listagem dupla, adicione o modo/método de **ataque** à lista de modo/método de ataque secundário.
7. Clique em **Salvar**.

Adicionar tarefa associada a um modo/método de ataque

Além de importar tarefas associadas (como mudanças e incidentes) como dados STIX, você pode adicioná-las a um modo/método de ataque manualmente.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Modo/método de ataque**.
2. Clique no modo de ataque ao qual você deseja adicionar uma tarefa associada.
3. Clique na lista relacionada **Tarefas associadas**.
4. Clique em **Editar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Conforme necessário, use os filtros para localizar as tarefas que você deseja associar ao modo/método de ataque.
6. Usando a interface de caixa de listagem dupla, adicione a tarefa à lista **Tarefas associadas**.
7. Clique em **Salvar**.

Indicadores de comprometimento

Indicadores de comprometimento (IoC) são artefatos observados em uma rede ou sistema operacional que provavelmente indicam uma invasão. IoCs típicos são assinaturas de vírus e endereços IP, hashes MD5 de arquivos de malware ou URLs ou nomes de domínio. O IoC se aplica a STIX 1.1 e 2.x.

Um IoC pode ser um único observável ou uma coleção de observáveis (por exemplo, um único URL incorreto conhecido ou a presença de um arquivo específico e alguns valores de chave de registro específicos).

Depois que os IoCs forem identificados em um processo de resposta a incidentes e perícia de computador, eles podem ser usados para detecção antecipada de futuras tentativas de ataque usando sistemas de detecção de intrusão e software antivírus.

O IoC se aplica a STIX 1.1 e 2.x.

Exibir um IoC

IoCs, às vezes chamados de indicadores, são normalmente recuperados de uma fonte de dados de ameaça como dados STIX. Se necessário, você também pode criar IoCs.

Antes de Iniciar

Função necessária: sn_ti.write

Procedimento

1. Depois que o trabalho programado tiver recuperado os dados de IoC da fonte de dados definida, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
   Os IoCs recuperados são listados.
2. Clique no IoC que você deseja exibir.
3. As informações a seguir são exibidas.

Campo	Descrição
Selecionar marcador de classificação	Se você configurou e ativou marcadores de segurança para adicionar metadados ao registro, poderá selecionar um ou mais marcadores para especificar o grau de confidencialidade do IoC. Se você não configurou ou ativou marcadores de segurança, esta lista suspensa não será exibida.
Título	Um nome descritivo para este indicador.
Visto pela primeira vez	A primeira data em que este indicador foi observado no sistema.
Visto pela última vez	A data mais recente em que este indicador foi observado no sistema.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Contagem encontrada	O número de vezes que o indicador foi encontrado.
Contagem fornecida	O número de vezes que o indicador foi importado das origens de ameaça definidas.
Anotações	Quaisquer anotações adicionais sobre o indicador. Este campo também pode conter pares de chave/valor JSON.

4. Você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Observáveis Relacionados	Lista os observáveis que estão vinculados ao indicador atual.
Modo/método de ataque relacionado	Lista os modos/métodos de ataque relacionados que foram identificados como relacionados a este indicador.
Tipo associado	Lista outros tipos de indicador associados a este IoC.
Fontes do Indicador	Lista as origens deste indicador, junto com o nível de confiança da origem.
Tarefas Associadas	Lista todas as tarefas, mudanças e incidentes associados ao IoC.
Metadados do Indicador	Se o campo **Anotações** contiver pares de chave/valor JSON válidos, eles serão analisados e exibidos. Se nenhum par de chave/valor JSON estiver presente, ou se o JSON for inválido, esta lista relacionada não será exibida.
Anotações de segurança	
Referências externas do indicador	
Fases da cadeia de eliminação associada	Lista as fases da cadeia de eliminação associadas a este objeto.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.

Adicionar um observável relacionado a um IoC

Além de importar observáveis como dados do STIX, você pode adicionar observáveis relacionados a um IoC manualmente.

Antes de Iniciar

Função necessária: sn_ti.write

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no indicador ao qual você deseja adicionar um observável relacionado.
3. Clique na lista relacionada **Observáveis** relacionados.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o observável que você deseja relacionar ao IoC.
6. Usando a interface de caixa de listagem dupla, adicione o observável à lista **Observáveis relacionados**.
7. Clique em **Salvar**.

Adicionar um modo/método de ataque relacionado a um IoC

Além de importar modos/métodos de ataque relacionados como dados STIX, você pode adicionar modos/métodos de ataque relacionados a um IoC manualmente.

Antes de Iniciar

Função necessária: sn_ti.write

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no indicador ao qual você deseja adicionar um modo/método de ataque relacionado.
3. Clique na lista **relacionada de modo/método de ataque** relacionado.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o modo/método de ataque que você deseja relacionar ao IoC.
6. Usando a interface de caixa de listagem dupla, adicione o modo/método de ataque à lista de modo/método de **ataque relacionado**.
7. Clique em **Salvar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Identificar tipos de indicador associados

Se um IoC não tiver tipos de indicador associados definidos, ele rastreará todos os tipos de observáveis. No entanto, se você associar um ou mais tipos de indicadores a um IoC, isso limitará os tipos de observáveis que podem ser associados ao IoC.

Antes de Iniciar
Função necessária: sn_ti.write

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no indicador ao qual você deseja associar um tipo de indicador.
3. Clique na lista relacionada **Tipo associado**.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o tipo de indicador que você deseja associar ao IoC.
6. Usando a interface de caixa de listagem dupla, adicione o tipo de indicador à lista **Tipo associado**.
7. Clique em **Salvar**.

Identificar origens de indicador

As origens de indicador normalmente são rastreadas automaticamente como parte do processo de importação de ameaça, mas outras origens podem ser adicionadas manualmente.

Antes de Iniciar
Função necessária: sn_ti.write

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no indicador ao qual você deseja adicionar fontes de indicador.
3. Clique na lista relacionada **Origens do indicador**.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar a origem do indicador que você deseja associar ao IoC.
6. Usando a interface de caixa de listagem dupla, adicione a origem do **indicador à lista Origens** do indicador.
7. Clique em **Salvar**.

Adicionar tarefas associadas a um IoC

Além de importar tarefas associadas (como mudanças e incidentes) como dados STIX, você pode adicioná-las a um IoC manualmente.

Antes de Iniciar
Função necessária: sn_ti.write

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
2. Clique no IoC ao qual você deseja adicionar uma tarefa associada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique na lista relacionada **Tarefas associadas**.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar as tarefas que você deseja associar ao IoC.
6. Usando a interface de caixa de listagem dupla, adicione a tarefa à lista **Tarefas associadas**.
7. Clique em **Salvar**.

Observáveis

Os observáveis representam propriedades com estado (como o hash MD5 de um arquivo ou o valor de uma chave de registro) ou eventos mensuráveis (como a criação de uma chave de registro ou a exclusão de um arquivo) que são pertinentes à operação de computadores e redes . Os observáveis se aplicam a STIX 1.1 e 2.x.

Conjuntos de observáveis cibernéticos são úteis para identificar indicadores de comprometimento quando são combinados com informações contextuais que representam os comportamentos de ameaças cibernéticas.

Os observáveis se aplicam a STIX 1.1 e 2.x.

Definir um observável

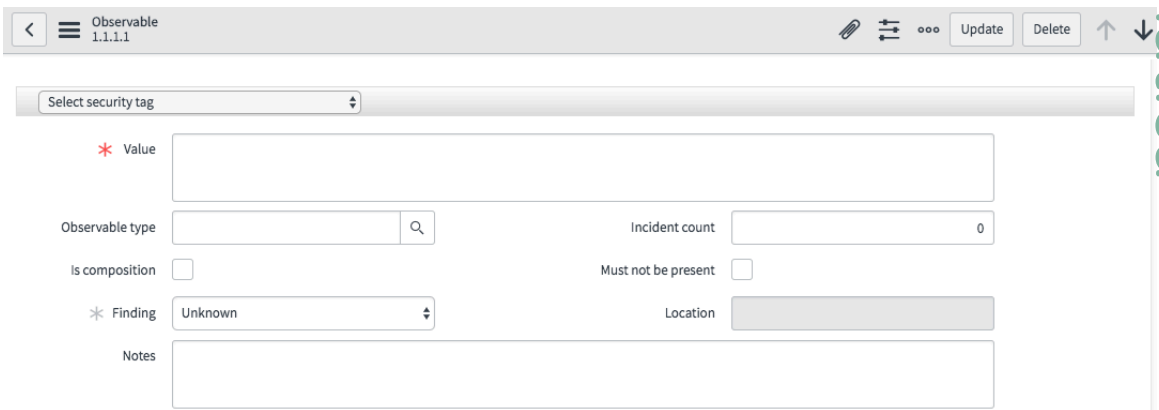
Os observáveis são recuperados do servidor do fornecedor como dados STIX. No entanto, você pode criar observáveis, conforme necessário.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique em **Nova**.



3. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Selecionar marcador de classificação	Se você configurou e ativou marcadores de segurança para adicionar metadados ao registro, poderá selecionar um ou mais marcadores para especificar o grau de confidencialidade do observável.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Se você não configurou ou ativou marcadores de segurança, esta lista suspensa não será exibida.
Valor	O valor (por exemplo, endereço IP ou hash) associado ao observável. **Nota:** Se uma verificação de ameaça em um endereço IP ou hash retornar malware ou alguma outra falha, o endereço IP ou o valor de hash será adicionado automaticamente à tabela Observável [sn_ti_observable]. Como tal, ele pode ser pesquisado no formulário Observáveis.
Tipo de observável	Selecione a classificação observável, como um endereço IP ou hash de arquivo. Esses tipos de observável são definidos no módulo **Tipos de observável**.
Contagem de incidentes	O número de vezes que o valor observável foi encontrado.
É composição	Este campo é exibido somente depois que o registro observável foi salvo. Se o **Tipo de observável** estiver definido como qualquer outra coisa que a **Composição de observável**e este novo observável for uma composição, marque esta caixa de seleção. Se o **tipo de observável** já estiver definido como **Composição de observável**, a caixa de seleção será marcada e somente leitura. Uma composição de observável é um observável que contém observáveis secundários.
Descoberta	Selecione uma das seguintes propriedades: ○ **Mal**-intencionado : indica que o observável é prejudicial à organização. ○ **Suspeito**: indica que o observável pode ser prejudicial para a organização. ○ **Limpar**: indica que o observável não é prejudicial à organização. ○ **Desconhecido**: indica que ainda não determinamos a descoberta do observável. ○ Valor padrão: desconhecido. Para obter mais informações, consulte Calculadoras descobertas de pesquisa de ameaças. **Nota:** Após um upgrade, os observáveis existentes são marcados como Mal-intencionados.
Operador	Este campo é exibido somente quando a caixa de seleção **É composição** está marcada. Dependendo da sua configuração neste campo, os observáveis e seus secundários são considerados ao decidir se um indicador associado está presente. Defina este campo como **E** se todos os observáveis secundários devem estar presentes para que um indicador associado seja considerado presente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Defina-o como **OU** se algum dos observáveis secundários estiver presente para que um indicador associado seja considerado presente.
Não deve estar presente	Este campo é exibido somente depois que o registro observável foi salvo. Se selecionado, este campo significa que a ausência do observável é o possível problema (por exemplo, uma chave de registro ausente).
Localização	Usando as configurações em duas propriedades e uma definição de inclusão de script, você pode carregar Carregar mais dados de IoC neste campo.
Anotações	Insira anotações adicionais sobre o observável.

4. Clique com o botão direito do mouse no cabeçalho do formulário e clique em **Salvar**.
   Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais.

Lista relacionada	Descrição
Indicadores relacionados	Lista os indicadores que foram identificados pela origem da ameaça.
Tarefas Associadas	Lista as mudanças associadas ao observável.
Observáveis secundários	Lista os observáveis relacionados que foram identificados pela origem da ameaça.
Recursos correspondentes para IP	Se o observável for um endereço IP, esta lista mostrará todos os recursos (itens de configuração) que tenham um endereço IP correspondente.
Origens observáveis	Lista as origens deste observável, junto com o nível de confiança da origem.
Anotações de segurança	Lista as anotações de segurança adicionadas a este observável.

Tradução automática

Adicionar um IoC relacionado a um observável

Além de importar observáveis como dados do STIX, você pode adicionar observáveis relacionados a um IoC manualmente.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no observável ao qual você deseja adicionar um IoC relacionado.
3. Clique na lista relacionada **Indicadores** relacionados.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o indicador que você deseja relacionar ao observável.
6. Usando a interface de caixa de listagem dupla, adicione o indicador à lista **Indicadores relacionados**.
7. Clique em **Salvar**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionar tarefas associadas a um observável

Além de importar tarefas associadas (como mudanças e incidentes) como dados do STIX, você pode adicioná-las a um observável manualmente.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no observável ao qual você deseja adicionar uma tarefa associada.
3. Clique na lista relacionada **Tarefas associadas**.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar as tarefas que você deseja associar ao observável.
6. Usando a interface de caixa de listagem dupla, adicione a tarefa à lista **Tarefas associadas**.
7. Clique em **Salvar**.

Adicionar um observável relacionado

Além de importar observáveis como dados do STIX, você pode adicionar observáveis relacionados manualmente.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no observável ao qual você deseja adicionar um observável relacionado.
3. Clique na lista relacionada **Observáveis secundários**.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar o observável que você deseja relacionar ao atual.
6. Usando a interface de caixa de listagem dupla, adicione o observável à lista **Observáveis** secundários.
7. Clique em **Salvar**.

Carregar mais dados de IoC

Dependendo das configurações em duas propriedades e de uma definição de inclusão de script, você pode carregar informações de geolocalização para endereços IP e sites no formulário Observáveis. Com personalização adicional, você também pode adicionar outras informações, como códigos de país e nomes de cidade.

Antes de Iniciar
As duas propriedades a seguir devem ser definidas:

- **O nome do domínio para recuperar informações adicionais para endereços IP/URLs** [sn_ti.ip_lookup.web_site]
- **A chave de API a ser usada para o domínio acima, se houver** [sn_ti.ip_lookup.api_key]

Função necessária: sn_ti.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no endereço IP ou URL do observável para o qual você deseja exibir mais dados de IoC.
   O campo **Local** mostra a geolocalização do IoC.
3. Clique no botão **Aprimorar dados** para carregar os dados IoC adicionais.
4. Você também pode configurar o formulário Observável para adicionar outros campos relacionados ao local, como o código do país e o código da cidade.

Nota:
Para carregar mais informações relacionadas ao local, edite a inclusão de script **ThreatAdditionalInfo** e forneça a chave de API apropriada do site que fornece as informações adicionais.

Identificar origens de observáveis

Se um observável não tiver origens definidas, ele usará todos os tipos de origens. No entanto, se você adicionar uma ou mais origens de ameaça a um observável, isso limitará as origens usadas.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Clique no observável ao qual você deseja adicionar origens de observável.
3. Clique na lista relacionada **Origens do observável**.
4. Clique em **Editar**.
5. Conforme necessário, use os filtros para localizar a origem que você deseja associar ao observável.
6. Usando a interface de caixa de listagem dupla, adicione a origem do **observável à lista Origens** do observável.
7. Clique em **Salvar**.

Realizar pesquisas em observáveis

Você pode executar pesquisas de inteligência contra ameaças em um ou mais observáveis para determinar se eles estão associados a ameaças de segurança conhecidas. As implementações de verificação executadas dependem daquelas que você ativou.

Antes de Iniciar

Antes de executar pesquisas, você deve ativar o plug-in Inteligência contra ameaças. Você também deve instalar o plug-in para uma ou mais das implementações de verificação:

- Integração do CrowdStrike Falcon Intelligence
- OPSWAT Metadefender
- Security Operations Recebi uma senha?
- VirusTotal

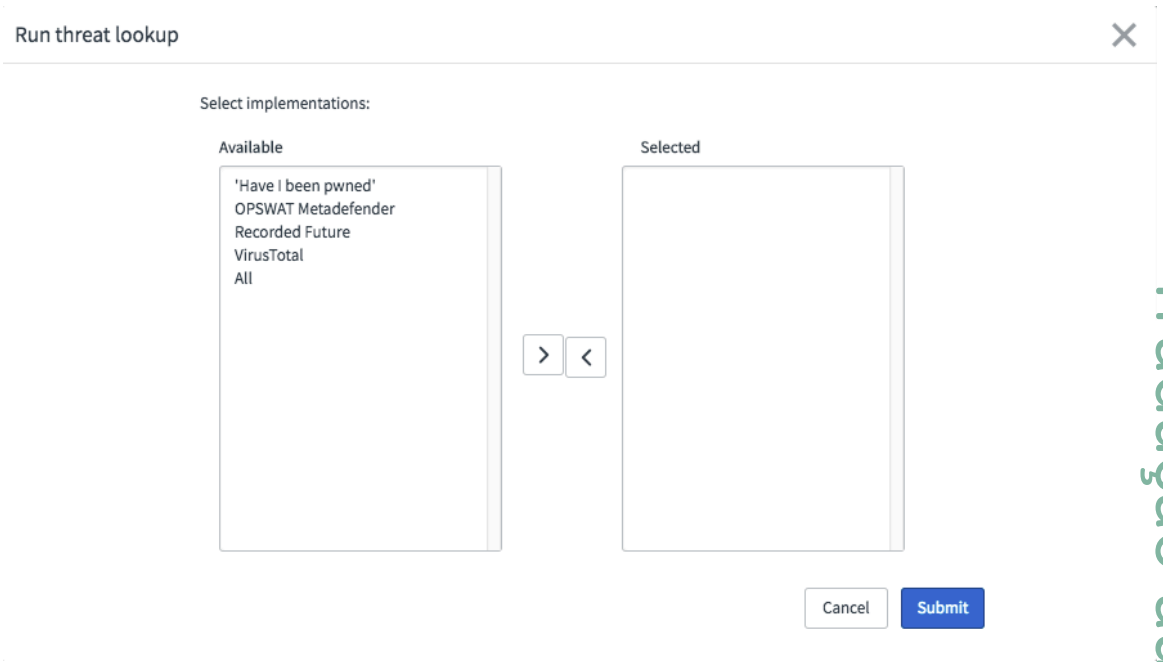
Função necessária: sn_ti.write

Tradução automática

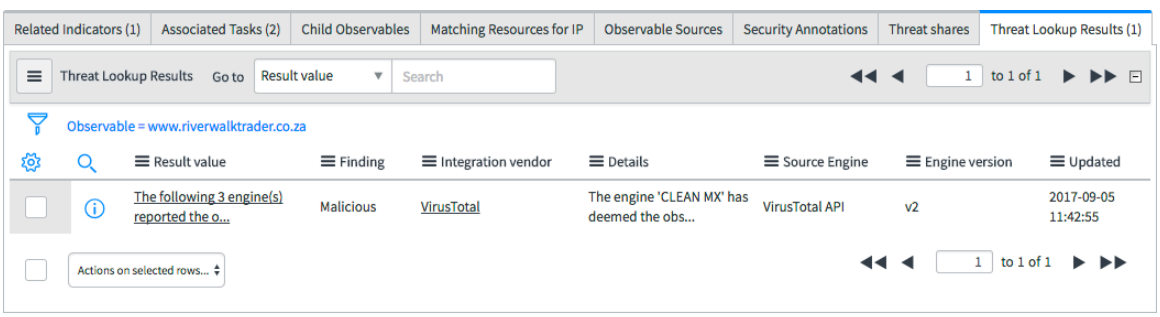
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Siga um destes procedimentos:
   - Para executar uma pesquisa em mais de um observável, selecione os observáveis, clique **em Ações nas linhas selecionadas**e selecione **Executar pesquisa de ameaça**.
   - Para executar uma pesquisa em um único observável, abra o registro do observável e clique no link relacionado **Executar pesquisa de ameaça**.



3. Selecione as implementações de pesquisa de ameaças que você deseja usar ou selecione **Todas** para executar pesquisas usando todas as implementações ativas e clique em **Enviar**.
   Uma mensagem indica que as pesquisas de ameaças foram iniciadas. O Integração do Security Operations - Fluxo de trabalho de pesquisa de ameaças executa e também executa os fluxos de trabalho de implementação das implementações de pesquisa de ameaças selecionadas. As pesquisas são realizadas e os resultados são gerados.
4. Quando as pesquisas forem concluídas, você poderá clicar na guia **Resultados da pesquisa de ameaças** para exibir os resultados.



Resultado de pesquisa de ameaças recentes: você também pode ver os resultados de pesquisa de ameaças mais recentes de cada fornecedor de integração ao clicar na guia **Resultado de pesquisa de ameaças recentes**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A guia **Resultado da pesquisa de ameaças recentes** não faz parte do sistema de base.

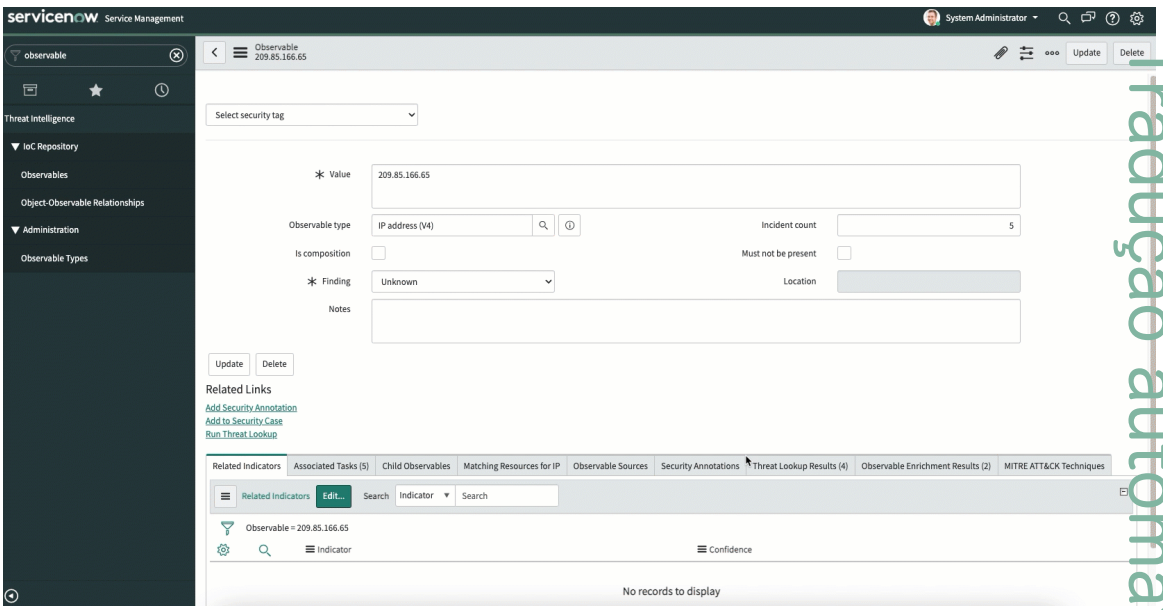
Para habilitar esta guia, execute o seguinte:

a. Clique com o botão direito do mouse no cabeçalho do formulário.

b. Navegar até **Configurar** > **Listas relacionadas**.

c. Localize **Resultados recentes da pesquisa de ameaças** na lista Disponível e mova-os para a lista Selecionado.

d. Clique em **Salvar**.
Agora você pode exibir os resultados recentes da pesquisa de ameaças de cada fornecedor de integração na guia **Resultado recente da pesquisa de ameaças**.

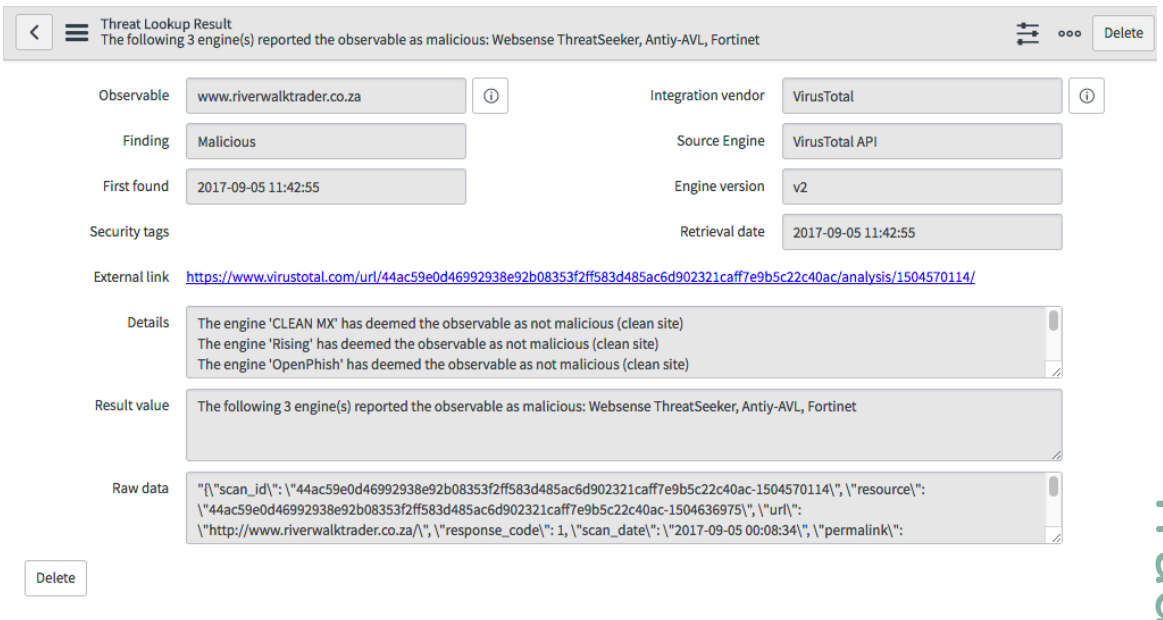


5. Para ver detalhes adicionais, incluindo resultados brutos de uma pesquisa específica, clique no **Valor do resultado**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Quando as implementações VirusTotal ou OPSWAT Metadefender são usadas, os detalhes são consolidados, conforme mostrado abaixo.



Executar aprimoramento de ameaça em observáveis

Você pode executar o aprimoramento de inteligência contra ameaças em um ou mais observáveis para determinar se eles estão associados a ameaças de segurança conhecidas. As implementações executadas dependem daquelas que você ativou.

Antes de Iniciar

Antes de executar o aprimoramento, você deve ativar o plug-in Inteligência contra ameaças. Você também deve instalar o plug-in para uma ou mais das implementações de aprimoramento:

- Integração do CrowdStrike Falcon Intelligence
- OPSWAT Metadefender
- Security Operations Recebi uma senha?
- VirusTotal
- Quemé?

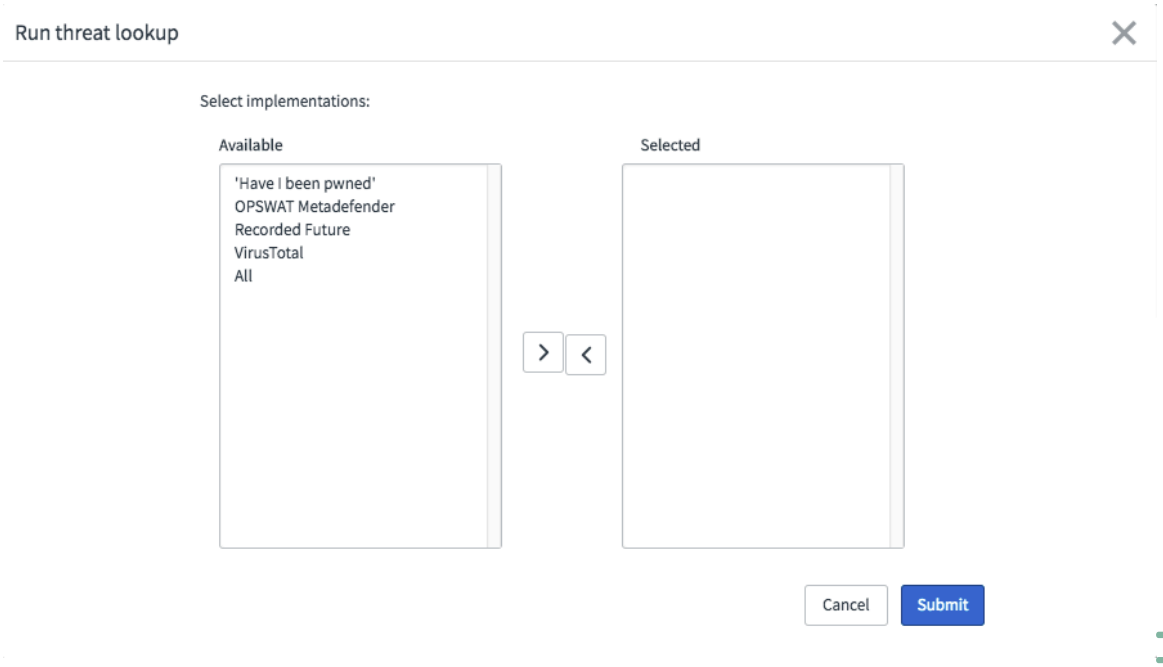
Função necessária: sn_ti.admin

Procedimento

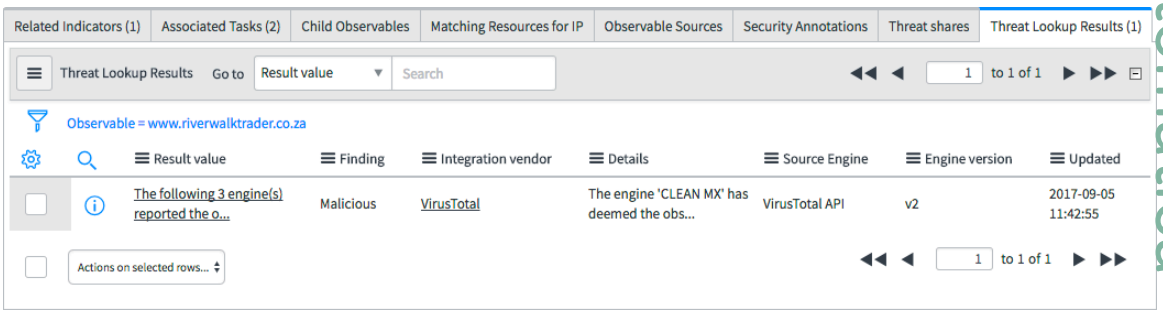
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Siga um destes procedimentos:
   - Para executar uma pesquisa em mais de um observável, selecione os observáveis, clique **em Ações nas linhas selecionadas**e selecione **Executar pesquisa de ameaça**.
   - Para executar uma pesquisa em um único observável, abra o registro do observável e clique no link relacionado **Executar pesquisa de ameaça**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Selecione as implementações de pesquisa de ameaças que você deseja usar ou selecione **Todas** para executar pesquisas usando todas as implementações ativas e clique em **Enviar**.
   Uma mensagem indica que as pesquisas de ameaças foram iniciadas. O Integração do Security Operations - Fluxo de trabalho de pesquisa de ameaças executa e também executa os fluxos de trabalho de implementação das implementações de pesquisa de ameaças selecionadas. As pesquisas são realizadas e os resultados são gerados.
4. Quando as pesquisas forem concluídas, você poderá clicar na guia **Resultados da pesquisa de ameaças** para exibir os resultados.

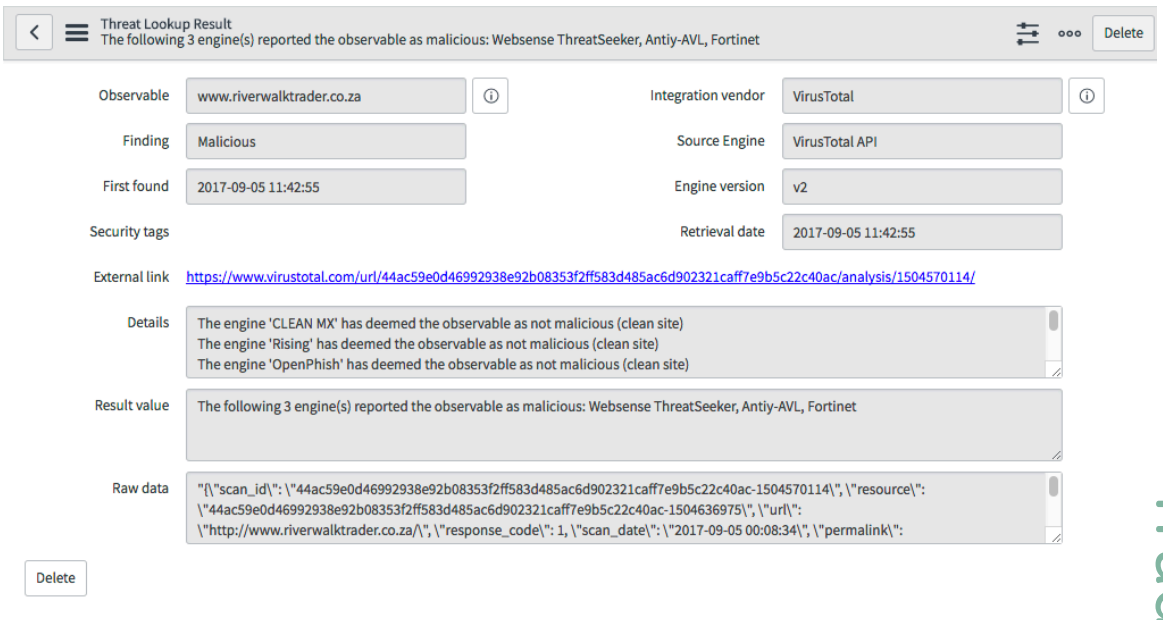


5. Para ver detalhes adicionais, incluindo resultados brutos de uma pesquisa específica, clique no **Valor do resultado**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Quando as implementações VirusTotal ou OPSWAT Metadefender são usadas, os detalhes são consolidados, conforme mostrado abaixo.



Padrões de ataque

Padrões de ataque são um tipo de Táticas, técnicas e procedimentos (TTPs) que descrevem os métodos pelos quais os adversários tentam comprometer os destinos. Os padrões de ataque se aplicam ao STIX 2.x.

Padrões de ataque são usados para ajudar a categorizar os ataques. Eles generalizam ataques específicos para os padrões que seguem e fornecem informações detalhadas sobre como os ataques são realizados.

Por exemplo, o Spear Phishing é um tipo comum de ataque em que um invasor envia uma mensagem de e-mail cuidadosamente criada para uma parte com a intenção de fazê-la clicar em um link ou abrir um anexo para entregar malware. Os padrões de ataque são mais específicos, como o Spear Phishing realizado por um agente de ameaça específico (por exemplo, o destino venceu uma contestação) que também pode ser um padrão de ataque.

Definir um padrão de ataque

Defina um padrão de ataque para ajudar a categorizar os ataques.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Padrões de ataque**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao padrão de ataque.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Fases da cadeia de eliminação associada	Lista as fases da cadeia de eliminação associadas a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Linha de ação	Lista o curso de ações associado a este objeto que são respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls) para impedir um ataque.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Campanhas

Uma campanha é um agrupamento de comportamentos adversários. Esses comportamentos descrevem um conjunto de atividades mal-intencionadas ou ataques que ocorrem ao longo do tempo em um conjunto específico de destinos. As campanhas se aplicam ao STIX 2.x.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As campanhas geralmente têm objetivos bem definidos e podem fazer parte de um conjunto de invasão.

As campanhas geralmente são atribuídas a um conjunto de intrusão e agentes de ameaça. Os agentes da ameaça podem reutilizar a infraestrutura conhecida do conjunto de invasão ou podem configurar uma nova infraestrutura específica para conduzir essa campanha.

As campanhas têm um objetivo comum nos incidentes que causam, nas pessoas ou nos recursos que direcionam e nos recursos que usam.

Por exemplo, um sindicato do crime ataque os executivos do ACME Bank. Eles usam uma variante específica de malware e novos servidores para obter informações secretas sobre uma futura fusão com outro banco.

Definir uma campanha

Defina uma campanha para agrupar comportamentos adversários.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Campanhas**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois

Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à campanha.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Linha de ação

Um curso de ação é uma ação realizada para impedir um ataque ou para responder a um ataque que está em andamento. O curso de ação se aplica ao STIX 2.x.

O curso de ação descreve respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls). Também pode descrever ações de nível superior, como treinamento de funcionários ou mudanças de política.

Por exemplo, um curso de ação para atenuar uma vulnerabilidade pode descrever a aplicação do patch que a corrige.

Definir um curso de ação

Defina um curso de ação para impedir um ataque ou para responder a um ataque que está em andamento.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Linha de ação**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao curso de ação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Malware	Lista o código malicioso associado a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Identidades

As identidades representam indivíduos, organizações ou grupos reais (ACME, Inc.) e classes de indivíduos, sistemas ou grupos (o setor financeiro). As identidades se aplicam ao STIX 2.x.

O SDO de identidade pode capturar informações básicas de identificação, informações de contato e os setores aos quais a identidade pertence. A identidade representa destinos de ataques, fontes de informações, criadores de objetos e identidades de agente de ameaça.

Definir identidades

Defina identidades que representam indivíduos, organizações ou grupos reais.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Identidades**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à identidade.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.

Infraestrutura

O SDO de infraestrutura representa um tipo de Táticas, técnicas e procedimentos (TTPs). Eles descrevem quaisquer sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados destinados a oferecer suporte a alguma finalidade de um ataque. A infraestrutura se aplica ao STIX 2.x.

Os elementos de um ataque são representados por outros SDOs ou SCOs. No entanto, o SDO de infraestrutura representa um grupo nomeado de dados que constitui a infraestrutura.

Exemplos de infraestrutura incluem servidores C2 usados em um ataque, um dispositivo ou um servidor que faz parte de uma defesa ou servidores de banco de dados direcionados por um ataque.

Definir infraestrutura

Defina uma infraestrutura que seja qualquer sistema, serviço de software e quaisquer recursos físicos ou virtuais associados destinados a oferecer suporte a alguma finalidade de um ataque.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Infraestrutura**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois
Agora você pode clicar em qualquer uma das listas relacionadas a seguir para exibir informações adicionais. Você também pode associar outros objetos à infraestrutura.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Tipos associados	Lista os tipos de indicador associados a este objeto.
Fases da cadeia de eliminação associada	Lista as fases da cadeia de eliminação associadas a este objeto.
Observáveis Associados	Lista os observáveis associados a este objeto.
Infraestrutura associada	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Dados observados	Lista os dados observados associados a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Conjunto de intrusão

Um conjunto de intrusão é um conjunto agrupado de comportamentos adversários e recursos com propriedades comuns. Um conjunto de intrusão geralmente envolve uma única organização. O conjunto de intrusão se aplica ao STIX 2.x.

Um conjunto de intrusão pode capturar várias campanhas ou outras atividades. Essas atividades compartilham atributos que indicam um agente de ameaça conhecido ou desconhecido.

A nova atividade pode ser atribuída a um conjunto de intrusão, mesmo que os agentes de ameaça por trás do ataque não sejam conhecidos. Os agentes de ameaça podem passar do suporte a um conjunto de intrusão para o suporte a outro ou podem oferecer suporte a vários conjuntos de intrusão.

Um conjunto de invasão é o pacote de ataque completo e pode ser usado por um longo período em várias campanhas para atingir várias finalidades.

Definir um conjunto de intrusão

Defina um conjunto de intrusão que é um conjunto agrupado de comportamentos adversários e recursos com propriedades comuns.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Conjunto de intrusão**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao conjunto de intrusão.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Motivações de ataque associadas	Lista todas as motivações secundárias que este conjunto de intrusão deseja alcançar.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Locais

Um local representa uma localização geográfica. Os locais são usados principalmente para fornecer contexto a outros SDOs. Os locais se aplicam ao STIX 2.x.

O local pode conter alguns ou todos os seguintes: região (América do Norte), endereço cívico (Nova York, EUA), latitude e longitude.

O SDO do local pode estar relacionado a uma identidade ou conjunto de intrusão para indicar que a identidade ou o conjunto de intrusão está nesse local. Também pode estar relacionado a um malware ou padrão de ataque para indicar que a vítima de destino está em um local específico.

Por exemplo, um Local pode ser usado em um relacionamento para descrever que o conjunto de intrusão Bourgeois Swallow se origina da Europa Oriental.

Pelo menos uma das seguintes propriedades ou conjuntos de propriedades deve ser fornecido:

- region
- país
- latitude e longitude

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir local

Defina um local geográfico para fornecer mais contexto a outros SDOs.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Locais**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao local.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Malware

Malware é um tipo de TTP que representa um código malicioso. Refere-se a um programa que é inserido secretamente em um sistema. O malware se aplica ao STIX 2.x.

A intenção de um malware é comprometer a confidencialidade, a integridade ou a disponibilidade dos dados, das aplicações ou do sistema operacional (SO) da vítima.

O Malware SDO caracteriza, identifica e categoriza instâncias e famílias de malware a partir de dados derivados da análise. Este SDO captura informações detalhadas sobre como o malware funciona e o que ele faz.

Definir um malware

Defina um malware que represente um código malicioso.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Malware**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao malware.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Tipos associados	Lista os tipos de indicador associados a este objeto.
Capacidades associadas	Lista os recursos identificados e associados a este objeto.
Fases da cadeia de eliminação associada	Lista as fases da cadeia de eliminação associadas a este objeto.
Observáveis Associados	Lista os observáveis associados a este objeto.
Malware associado	Lista o malware associado identificado com este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Sistemas operacionais associados	Os sistemas operacionais em que o objeto é executável. Isso se aplica a sistemas operacionais virtualizados, bem como aos que são executados em hardware.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Linha de ação	Lista o curso de ações associado a este objeto que são respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls) para impedir um ataque.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Análise de malware	Lista os registros de análise de malware associados a este objeto.
Observáveis relatados	Lista os observáveis relatados como parte deste objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

Análise de malware

A análise de malware captura os metadados e os resultados de um malware. A análise de malware se aplica ao STIX 2.x.

A análise de malware inclui análises estáticas ou dinâmicas realizadas em uma instância ou família de malware.

Definir análise de malware

Defina a análise de malware que captura os metadados e os resultados de uma análise estática ou dinâmica específica realizada em uma instância ou família de malware.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Análise de malware**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois
Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre os objetos associados à análise de malware.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Malware associado	Lista o malware associado identificado com este objeto.
Observáveis relatados	Lista os observáveis relatados como parte deste objeto.
Software instalado	Lista qualquer software não padrão instalado no sistema operacional usado para a análise dinâmica da instância ou família de malware.

Tradução automática

Dados observados

Os Dados observados transmitem informações sobre entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes, usando os Objetos cibernéticos (SCOs) do STIX. Os dados observados se aplicam ao STIX 2.x.

Os dados observados capturam uma única observação de uma única entidade (arquivo, conexão de rede), bem como a agregação de várias observações de uma entidade.

Você pode usar os Dados observados sozinhos (sem relacionamentos) para transmitir dados brutos coletados de qualquer origem. As origens incluem relatórios de analistas, áreas restritas e ferramentas de detecção baseadas em rede e host.

Por exemplo, Dados observados podem capturar informações sobre um endereço IP, uma conexão de rede, um arquivo ou uma chave de registro. Os dados observados não são uma declaração de inteligência, são simplesmente as informações brutas sem qualquer contexto para o que isso significa.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir dados observados

Defina os dados observados que transmitem informações sobre entidades relacionadas à segurança cibernética, como arquivos, sistemas e redes, usando os Objetos cibernéticos (SCOs) do STIX.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Dados observados**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados aos dados observados.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Observáveis Associados	Lista os observáveis associados a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.

Agentes da ameaça

Agentes de ameaça são indivíduos, grupos ou organizações que agem com intenção mal-intencionada. Os agentes da ameaça se aplicam ao STIX 2.x.

Um agente de ameaça não é um conjunto de invasão, mas pode oferecer suporte ou ser afiliado a vários conjuntos de invasão, grupos ou organizações ao longo do tempo.

Os agentes de ameaça usam seus recursos e os recursos de um conjunto de invasão para conduzir ataques e executar campanhas nos destinos.

Você pode identificar os agentes de ameaça por seus motivos, capacidades, objetivos, nível de sofisticação, atividades anteriores, recursos aos quais eles têm acesso e sua função na organização.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir agentes da ameaça

Defina os agentes de ameaça que são indivíduos, grupos ou organizações que agem com intenção mal-intencionada.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Agentes da ameaça**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao agente da ameaça.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Tipos associados	Lista os tipos de indicador associados a este objeto.
Funções associadas	Lista as funções associadas ao agente da ameaça.
Motivações de ataque associadas	Lista as motivações de ataque associadas ao agente da ameaça.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Grupos de ameaças

Um objeto de agrupamentos de ameaças afirma explicitamente que os objetos STIX referenciados têm um contexto compartilhado. Os agrupamentos de ameaças se aplicam ao STIX 2.x.

Um objeto de agrupamentos de ameaças representa um conjunto de dados que, após análise suficiente, amadurece para transmitir um incidente ou relatório de ameaça como um objeto de relatório do STIX. Por exemplo, um agrupamento pode ser usado para caracterizar uma investigação em andamento sobre um evento ou incidente de segurança.

Um objeto de agrupamentos de ameaças também pode ser usado para declarar que os objetos STIX referenciados estão relacionados a um processo de análise em andamento. Por exemplo, um analista de ameaças pode colaborar com outras pessoas em sua comunidade de confiança para examinar uma série de campanhas e indicadores.

O SDO de agrupamento de ameaças contém uma lista de referências a SDOs, SCOs e SROs, junto com uma declaração explícita do contexto compartilhado pelo conteúdo, uma descrição textual e o nome do agrupamento.

Definir grupos de ameaças

Defina agrupamentos de ameaças como objetos que têm um contexto compartilhado.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Grupos de ameaças**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao agrupamento de ameaças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Objetos agrupados	Lista os objetos agrupados como parte do agrupamento de ameaças.
Indicadores Agrupados	Lista os indicadores agrupados como parte do agrupamento de ameaças.
Observáveis agrupados	Lista os observáveis agrupados como parte do agrupamento de ameaças.

Definições de marcação

O objeto de definições de marcação representa uma marcação específica.

As marcações de dados representam restrições, permissões e outras orientações sobre como os dados podem ser usados e compartilhados.

Por exemplo, os dados podem ser compartilhados com a restrição de que não devem ser compartilhados novamente ou que devem ser criptografados em repouso.

No STIX, as marcações de dados são especificadas usando o objeto de definição de marcação. Essas definições são aplicadas a objetos STIX usando marcações de objeto e a propriedades individuais de objetos STIX por meio de marcações granulares.

Definir definições de marcação

Defina as definições de marcação que representam uma marcação de dados específica.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Definições de marcação**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois
Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à definição de marcação.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
	Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Objetos marcados	Listas de objetos marcados com a definição de marcação.
Indicadores marcados	Listas de indicadores marcados com a definição de marcação.

Anotações de ameaça

Uma anotação de ameaça transmite um texto informativo para fornecer análise adicional não contida nos objetos STIX, nos objetos de definição de marcação ou nos objetos de conteúdo de idioma aos quais a anotação está relacionada. As anotações de ameaça se aplicam ao STIX 2.x.

Por exemplo, um analista pode adicionar uma Anotação a um objeto Campanha criado por outra organização. A anotação pode indicar que ele viu publicações relacionadas a essa campanha em um fórum de hackers.

As anotações geralmente são criadas por analistas humanos e são compostas por texto orientado por humanos. Elas contêm uma propriedade extra para capturar o autor que criou a anotação.

Definir anotações de ameaça

Defina anotações de ameaça que transmitem informações para fornecer contexto ou análise adicional que não estão disponíveis em objetos existentes.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Anotações de ameaça**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois
Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados às anotações de ameaça.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Objetos associados	Listas de objetos aos quais as anotações de ameaça se aplicam.
Indicadores associados	Listas de indicadores aos quais as anotações de ameaça se aplicam.
Observáveis Associados	Lista os observáveis associados a este objeto.

Opiniões sobre ameaças

Uma opinião é uma avaliação da precisão das informações em um objeto STIX produzida por uma entidade diferente. As opiniões de ameaça se aplicam ao STIX 2.x.

A propriedade de opinião captura o nível de acordo ou desacordo usando uma escala fixa. A escala fixa também oferece suporte a um mapeamento numérico para permitir operações estatísticas consistentes em opiniões.

Por exemplo, um analista de uma organização consumidora pode dizer que "discorda plenamente" de um objeto Campanha e fornecer uma explicação sobre o motivo.

As opiniões são subjetivas e a especificação não aborda a melhor forma de interpretá-las.

Os analistas humanos criam opiniões e são compostos por texto orientado por humanos. Eles contêm uma propriedade extra para capturar o autor que criou a opinião.

Definir opiniões de ameaça

Defina as opiniões de ameaça como uma avaliação da precisão das informações em um objeto STIX.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Opiniões sobre ameaças**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à opinião de ameaça.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Objetos associados	Lista de objetos aos quais a opinião de ameaça se aplica.
Indicadores associados	Lista de indicadores aos quais a opinião de ameaça se aplica.
Observáveis Associados	Lista os observáveis associados a este objeto.

Relatórios de ameaças

Relatórios de ameaças são coleções de inteligência contra ameaças focadas em um ou mais tópicos. Os relatórios de ameaças se aplicam ao STIX 2.x.

Os relatórios de ameaças incluem a descrição de um agente da ameaça, malware, técnica de ataque, incluindo contexto e detalhes relacionados. Eles são usados para agrupar informações de ameaças relacionadas para que elas possam ser publicadas como uma história abrangente de ameaças cibernéticas.

O SDO do relatório de ameaças contém uma lista de referências a objetos STIX junto com uma descrição textual e o nome do relatório.

Definir relatórios de ameaças

Defina relatórios de ameaças que descrevam um agente de ameaça, malware, técnica de ataque, incluindo contexto e detalhes relacionados.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Relatórios de ameaças**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados aos relatórios de ameaça.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Tipos associados	Lista os tipos de indicador associados a este objeto.
Objetos relatados	Lista de objetos relatados no relatório de ameaça.
Indicadores relatados	Listas de indicadores relatados no relatório de ameaça.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Observáveis relatados	Listas de observáveis relatados no relatório de ameaça.

Vistas

As vistas indicam que um indicador ou objeto foi visto. Os objetos podem ser um malware, uma ferramenta, um agente de ameaça e assim por diante.

As vistas rastreiam quem e qual é o destino, como os ataques são realizados e para rastrear tendências no comportamento do ataque.

O objeto de relacionamento de vista contém propriedades extras não presentes nos objetos de relacionamento genéricos. Essas propriedades extras representam dados específicos para relacionamentos de vista.

Por exemplo, uma contagem ou que representa quantas vezes algo foi visto.

A vista é capturada como um relacionamento porque você não pode ter uma visão a menos que tenha algo que tenha sido avistado.

- O que foi detectado, como malware, campanha ou outro SDO
- Quem o avistou e/ou onde foi avistado, representado como uma identidade
- O que foi visto em sistemas e redes, representado como dados observados

Definir vistas do indicador

Defina vistas que indicam que um indicador foi visto.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Avistamentos do indicador**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à vista do indicador.

Listas relacionadas	Descrição
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Identidades	Lista de identidades associadas a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Listas relacionadas	Descrição
Dados observados	Lista os dados observados associados a este objeto.

Definir vistas de objeto

Defina a detecção de objeto que descreve que um objeto (malware, ferramenta, agente de ameaça e assim por diante) foi visto.

Antes de Iniciar
Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Avistamentos de objeto**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois
Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados à vista do objeto.

Listas relacionadas	Descrição
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Identidades	Lista de identidades associadas a este objeto.
Dados observados	Lista os dados observados associados a este objeto.

Ferramentas

As ferramentas são softwares legítimos usados por agentes de ameaça para executar ataques. As ferramentas se aplicam ao STIX 2.x.

As ferramentas permitem que você saiba como e quando os agentes de ameaça as usam para executar campanhas. Ao contrário do malware, essas ferramentas ou pacotes de software geralmente são encontrados em um sistema e têm finalidades legítimas para usuários avançados, administradores, administradores de rede ou até mesmo usuários normais.

Por exemplo, ferramentas de acesso remoto (RDP) e ferramentas de verificação de rede (Nmap) são ferramentas que um agente de ameaça usa durante um ataque.

Definir ferramentas

Defina ferramentas como software legítimo usado para executar ataques.

Antes de Iniciar
Função necessária: sn_ti.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Ferramentas**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao objeto da ferramenta.

Links relacionados e listas relacionadas	Descrição
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Fases da cadeia de eliminação associada	Lista as fases da cadeia de eliminação associadas a este objeto.
Tipos associados	Lista os tipos de indicador associados a este objeto.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Linha de ação	Lista o curso de ações associado a este objeto que são respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls) para impedir um ataque.
Identidades	Lista de identidades associadas a este objeto.
Indicadores	Lista os indicadores de comprometimento (IoC) relacionados que foram identificados pela origem da ameaça associada a este objeto.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Locais	Lista os locais que fornecem contexto geográfico para este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Vulnerabilidades	Lista um ponto fraco ou um defeito em um software ou hardware que os invasores exploram e que está associado a este objeto.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.

Vulnerabilidades

Uma vulnerabilidade é uma fraqueza ou um defeito em um componente de software ou hardware que os invasores exploram. As vulnerabilidades se aplicam ao STIX 2.x.

O ponto fraco ou defeito está nos requisitos, designs ou implementações do código encontrado em um componente de software ou hardware. Esse ponto fraco é explorado diretamente para afetar negativamente a confidencialidade, a integridade ou a disponibilidade desse sistema.

CVE é uma lista de vulnerabilidades e exposições de segurança da informação que fornece nomes comuns para problemas conhecidos publicamente [CVE].

Por exemplo, se um malware explorar CVE-2015-12345, um objeto Malware poderá ser vinculado a um objeto Vulnerability que faça referência a CVE-2015-12345.

Definir vulnerabilidades

Defina vulnerabilidade como um ponto fraco ou defeito em um componente de software ou hardware que os invasores exploram.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Vulnerabilidades**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

O que Fazer Depois

Clique em qualquer uma das listas relacionadas a seguir para exibir informações adicionais sobre objetos associados ao objeto de vulnerabilidade.

Links relacionados e listas relacionadas	Descrição
Mostrar Relacionamentos	Abre o Visualizador do STIX, onde você pode exibir o relacionamento do objeto STIX. Mostrar relacionamentos aparece somente quando o objeto tem um objeto associado.
Referências externas	Lista referências externas que se referem a informações que não sejam do STIX. Esta

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Links relacionados e listas relacionadas	Descrição
	propriedade é usada para fornecer um ou mais identificadores de objeto externo.
Padrões de ataque	Lista os padrões de ataque que ajudam a categorizar os ataques associados a este objeto.
Campanhas	Lista as campanhas associadas a este objeto.
Linha de ação	Lista o curso de ações associado a este objeto que são respostas técnicas ou automatizadas (aplicação de patches, reconfiguração de firewalls) para impedir um ataque.
Infraestrutura	Lista sistemas, serviços de software e quaisquer recursos físicos ou virtuais associados a este objeto.
Conjunto de intrusão	Lista um conjunto de comportamentos adversários e recursos com propriedades comuns associadas a este objeto.
Malware	Lista o código malicioso associado a este objeto.
Agentes da ameaça	Lista indivíduos, grupos ou organizações que agem com intenção mal-intencionada associada a este objeto.
Ferramentas	Lista o software legítimo usado por agentes de ameaça para executar ataques associados a este objeto.

Relacionamentos

Use os objetos de relacionamento para vincular dois SDOs ou objetos observáveis cibernéticos (SCOs) STIX para descrever como eles se relacionam entre si.

Os objetos de relacionamento do STIX (SROs) representam tipos de relacionamentos entre vários objetos do STIX. Os seguintes objetos de relacionamento estão disponíveis:

- **Relacionamento objeto-objeto**: este objeto define os relacionamentos entre SDOs, exceto o objeto do indicador. Um exemplo de relacionamento definido por objeto é que um padrão de ataque entrega um malware.
- **Relacionamento objeto-indicador**: este objeto define os relacionamentos entre o objeto do indicador e outros SDOs. Um exemplo de um relacionamento definido por objeto-indicador é que um indicador detecta evidências de uma campanha.
- **Relacionamento objeto-observável**: este objeto define relacionamentos entre SDOs e o objeto observável (SCO). Um exemplo de um relacionamento definido de objeto-observável é que uma infraestrutura consiste em objetos observáveis cibernéticos que fornecem informações de um possível ataque.

Relacionamentos de objeto do STIX

Objeto de Relacionamento	Origem de Exemplo	Meta de Exemplo	Descrição de exemplo
Relacionamentos objeto-objeto	Padrão de ataque	Malware	Este relacionamento descreve que este padrão de ataque é usado para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Relacionamentos de objeto do STIX

Objeto de Relacionamento	Origem de Exemplo	Meta de Exemplo	Descrição de exemplo
			entregar esta instância (ou família) de malware.
Relacionamentos objeto-indicador	Indicador	Padrão de ataque, Campanha, Infraestrutura, Conjunto de invasão, Malware, Agente da ameaça, Ferramenta	Este relacionamento descreve que o indicador pode detectar evidências do padrão de ataque relacionado, campanha, infraestrutura, conjunto de intrusão, malware, agente de ameaça ou ferramenta. A evidência pode não ser direta. Por exemplo, o indicador pode detectar evidências secundárias da campanha, como malware que é comumente usado por essa campanha específica.
Relacionamentos objeto-observável	Infraestrutura	Dados observados	Esse relacionamento descreve que o indicador é criado com base nas informações de um objeto de dados observado. Um exemplo de um relacionamento definido de objeto-observável é que uma infraestrutura consiste em objetos observáveis cibernéticos que fornecem informações de um possível ataque.

Definir relacionamentos objeto-objeto

Defina relacionamentos entre SDOs, exceto o objeto do indicador.

Antes de Iniciar

Função necessária: sn_ti.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Relacionamentos objeto-objeto**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

Definir relacionamentos objeto-indicador

Defina relacionamentos entre o objeto de indicador e outros SDOs.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Relacionamentos objeto-indicador**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

Definir relacionamentos objeto-observável

Defina relacionamentos entre SDOs e o objeto observável (SCO).

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório LOC** > **Relacionamentos observáveis de objeto**.
2. Clique em **Nova**.
3. Preencha os campos no formulário conforme apropriado.
4. Clique em **Enviar**.

Visualizador do STIX

O visualizador do STIX representa visualmente a estrutura do objeto STIX e seu relacionamento.

Você pode obter mais informações sobre o objeto ou relacionamento selecionado no painel de detalhes.

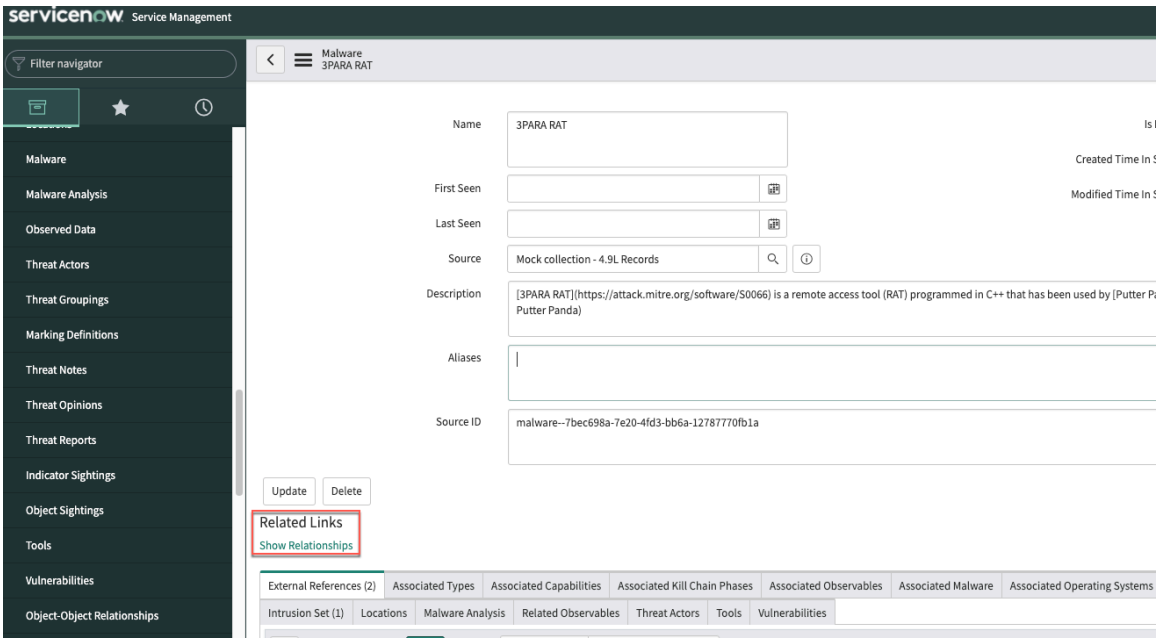
O gráfico de relacionamento mostra os relacionamentos de um objeto e fornece contexto para você investigar. Você pode clicar em qualquer nó do gráfico para ver mais detalhes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

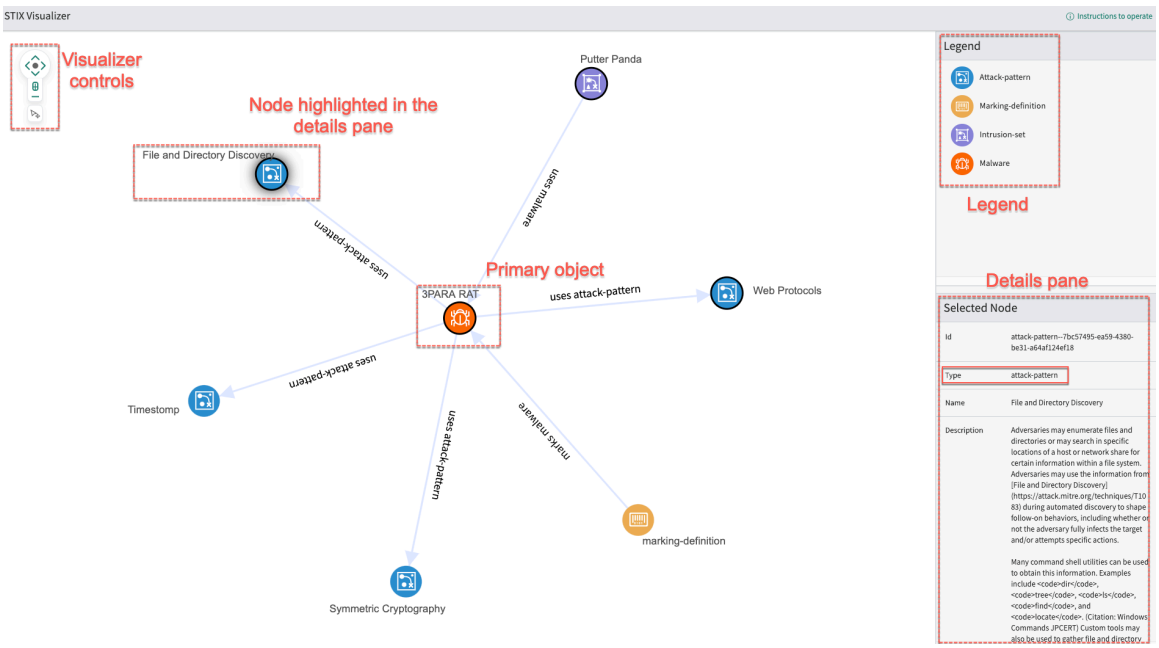
Nota:
O visualizador do STIX está disponível para todos os SDOs, exceto para os objetos de relatório e dados observados.

Acessar Visualizador do STIX



Clique em Mostrar relacionamentos na seção Links relacionados de qualquer um dos SDOs para exibir o visualizador do STIX.

Exibir detalhes no visualizador do STIX



No Visualizador, você pode exibir o objeto e seu relacionamento, o que fornece contexto para você investigar melhor. O Visualizador usa cores e ícones para ilustrar várias informações sobre os objetos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode ampliar um objeto, arrastar os nós ou fixá-los para enfocar um relacionamento específico.

Clique em qualquer objeto para abrir o painel de detalhes. No painel de detalhes, você pode obter mais informações associadas ao objeto.

MITRE-ATT&CK™ visão geral da estrutura do

A estrutura MITRE-ATT&CK é uma base de conhecimento de táticas, técnicas e procedimentos comuns (TTP) que sua organização pode acessar para desenvolver modelos de ameaça e metodologias específicas contra ataques cibernéticos.

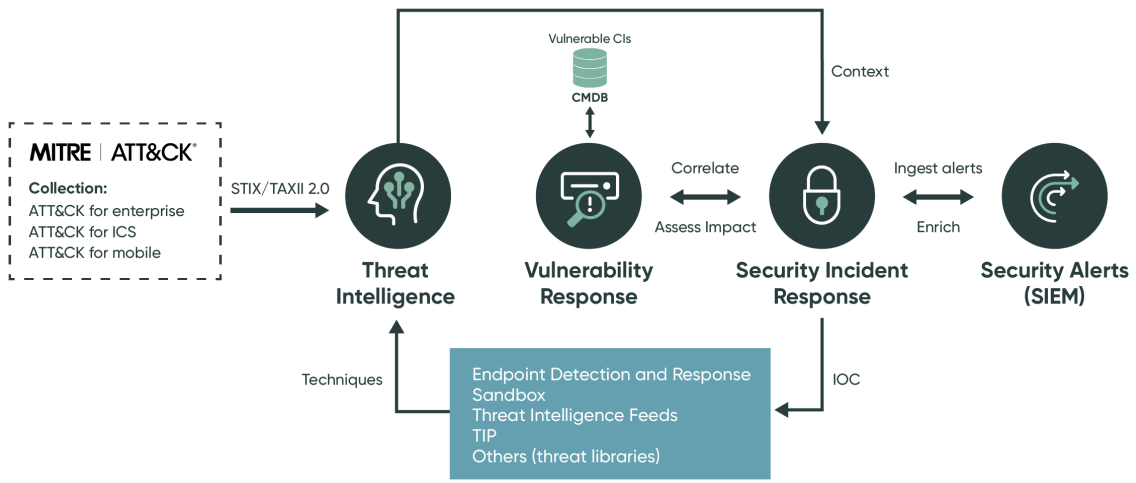
Visão geral

A estrutura MITRE de táticas, técnicas e conhecimento comum do adversário (ATT&CK) documenta e rastreia várias técnicas do adversário que são usadas durante diferentes fases de um ataque cibernético.

Usando a base de conhecimento da estrutura MITRE-ATT&CK, a comunidade de inteligência contra ameaças cibernéticas pode identificar rapidamente as ameaças e coordenar as respostas aos ataques cibernéticos.

MITRE-ATT&CK e Security Operations

Consulte o diagrama a seguir para saber como as informações de MITRE-ATT&CK fluem com aplicações Security Operations.



- O pré-carregado TAXII cliente se conecta ao servidor TAXII para ingerir as coletas de dados para Inteligência contra ameaças.
- As integrações existentes do Gerenciador de informações e eventos de segurança (SIEM) ingerem seus dados de ameaça (alertas e eventos) com TTPs relevantes e estão associadas a incidentes de segurança.
- Quando um IoC está associado a um incidente de segurança, Inteligência contra ameaças pesquisa automaticamente os feeds de ameaças para obter informações relevantes e envia IoCs para fontes de terceiros, como EDR, Sandbox ou TIP para análise adicional.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se alguma origem de terceiros contiver as informações de MITRE-ATT&CK, então Inteligência contra ameaças extrai as informações da técnica e aprimora os dados no repositório Inteligência contra ameaças para correlação e análise.
- MITRE-ATT&CK também compartilha informações de contexto de CVE para cada técnica. Sua equipe de segurança pode revisar as técnicas exploradas em Vulnerability Response para determinar se seus ativos essenciais para os negócios estão ameaçadas.

MITRE-ATT&CK matrizes, táticas e técnicas

O núcleo da estrutura MITRE-ATT&CK é uma matriz de táticas e técnicas do adversário. A sequência das táticas representa o que um adversário está tentando realizar na fase de um incidente. Quando sua equipe de segurança entende essa sequência, você tem a oportunidade de antecipar o próximo passo de um adversário e interromper a cadeia de eliminação. O ATT&CK consiste nas seguintes matrizes:

- Enterprise ATT&CK: descreve os comportamentos e as ações que um adversário realiza para comprometer e operar em uma rede e nuvem corporativas.

  Nota:
  A matriz Pre ATT&CK foi descontinuada em MITRE e foi mesclada com a matriz Enterprise.

- ICS ATT&CK: descreve as ações que um adversário realiza enquanto opera em uma rede de Sistemas de controle industrial (ICS).
- Mobile ATT&CK: descreve os comportamentos e as ações do adversário que se concentram em dispositivos móveis.

As táticas representam o motivo de uma técnica de ATT e CK. É o objetivo tático do adversário para executar uma ação.

As técnicas representam como um adversário atinge um objetivo tático executando uma ação.

As técnicas podem ser associadas a mais de uma tática. Por exemplo, a manipulação de token de acesso é usada por um adversário para obter a tática de escalação de privilégio ou evasão de defesa.

Uso de uma abordagem baseada em intenção para respostas a incidentes

Uma resposta baseada em intenção usa uma estrutura de cadeia de eliminação dinâmica e contextual que pode ajudar sua organização a correlacionar incidentes de segurança e identificar um grande escopo de ataques. Sua equipe de segurança pode usar uma resposta baseada em intenção para entender como a organização está sendo afetada e o que o invasor pode fazer em seguida. Esse tipo de resposta permite prever o comportamento de um invasor para que você possa concentrar seus recursos com eficácia.

Usando Security Incident Response, sua equipe de segurança pode gerenciar o ciclo de vida de cada incidente de segurança, desde a análise até a contenção, concentrando-se em indicadores de comprometimento (IOCs), como endereços IP, hashes de arquivo e domínios.

Ao integrar Security Incident Response com a estrutura MITRE-ATT&CK, os incidentes de segurança são tratados como links em um ataque maior em toda a empresa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como sua organização pode se beneficiar de MITRE-ATT&CK no Security Operations

Usar a estrutura MITRE-ATT&CK pode ajudar sua organização a fazer o seguinte:

- Equipe os analistas de segurança com MITRE-ATT&CK táticas, técnicas e procedimentos (TTPs) para analisar e responder melhor aos incidentes de segurança.
- Automatize os fluxos de trabalho de incidentes usando o playbook para detectar e conter ameaças no contexto da estrutura MITRE-ATT&CK.
- Priorize indicadores de comprometimento e busca de ameaças com MITRE-ATT&CK informações.
- Entenda a postura de segurança de alto nível da sua organização no contexto da estrutura MITRE-ATT&CK.

Administração do MITRE-ATT&CK

Você pode configurar, mapear fontes de dados, mapear a cobertura geral de detecção de técnica e manter o repositório MITRE-ATT&CK no Now Platform.

Introdução à estrutura MITRE-ATT&CK

Revise as informações a seguir antes de iniciar a configuração da estrutura MITRE-ATT&CK.

Check-list

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform, Inteligência contra ameaçase Security Incident Response.	Estas funções são usadas nos recursos do MITRE-ATT&CK: • O administrador (admin) instala as aplicações do ServiceNow Store e atribui as funções de administrador de incidentes de segurança (sn_si.admin) e administrador de inteligência contra ameaças (sn_ti.admin). • sn_ti.admin • sn_si.admin • sn_si.analyst • sn_ti.read • sn_ti.write • sn_ti.mitre_analyst — A função de analista do MITRE foi introduzida para permitir a navegação cruzada para os recursos MITRE entre Security Incident Response e o Threat Intelligence Support Common. Com esta função, você pode exibir o

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	módulo Inteligência contra ameaças MITRE e o módulo Security Incident Response no modo somente leitura. • sn_si.read Para obter mais informações, consulte Configurar Inteligência contra ameaças.
Verifique se as aplicações principais ServiceNow que são necessárias para oferecer suporte ao módulo MITRE-ATT&CK estão instaladas e ativadas.	Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas. • Componentes de IU comuns do suporte de inteligência contra ameaças (sn_ti_seismic) - Versão 1.0 ou superior • Suporte de inteligência contra ameaças comum - Versão 12.0 ou superior • Inteligência contra ameaças - Versão 12.0 ou superior • Security Incident Response - Versão 12.0 ou superior Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte obter direito de um produto ou aplicação do Security Operations e ativar uma aplicação da ServiceNow Store.
Separação de Domínio	Verifique a seção de separação de domínio se você pretende separar dados, processos e tarefas administrativas.

Entenda o modelo de dados de MITRE a STIX

Revise a terminologia usada por MITRE e STIX para usar e entender com eficiência a estrutura MITRE-ATT&CK™ no Now Platform.

MITRE objetos para mapeamento STIX

STIX é uma linguagem para descrever informações de ameaças cibernéticas de maneira padronizada e estruturada. O modelo de dados primário no módulo Inteligência contra ameaças são os objetos STIX. Enquanto os objetos MITRE são um subconjunto do modelo de dados primário STIX. Na estrutura MITRE-ATT&CK, MITRE fornece informações STIX] semelhantes com determinados rótulos e objetos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de objetoMITRE para STIX

Terminologia MITRE	Terminologia STIX
Técnica	Padrão de ataque
Mitigação	Linha de ação
Grupos	Conjuntos de intrusão
Malware	Malware
Ferramenta	Ferramenta

Estendendo dados no módulo Inteligência contra ameaças

Você pode manter uma lista de Inteligência contra ameaças origens de ameaça e importar os dados STIX necessários que incluem um conjunto abrangente de informações sobre ameaças cibernéticas. Você também pode usar os perfis TAXII para facilitar a troca automatizada de informações de ameaças cibernéticas.

Nota:
Para obter mais informações, consulte definir uma origem de ameaça e criar um perfil TAXII.

Estendendo dados no módulo MITRE-ATT&CK

Você pode estender os objetos Malware, Grupo, Mitigação e Ferramenta para uma técnica no repositório MITRE-ATT&CK.

Você pode criar um objeto e estabelecer um relacionamento entre uma técnica e o novo objeto no módulo Repositório do MITRE ATT&CK, mas não pode definir o tipo de relacionamento neste módulo. Para definir um tipo de relacionamento, navegue até o **Inteligência contra ameaças** > **Repositório LOC** > **Relacionamentos objeto-objeto** módulo.

Se você mapear o tipo de relacionamento entre uma técnica existente e um objeto existente, deverá definir a técnica como o objeto de destino e o objeto como o objeto de origem. Para fazer isso, navegue até o **Repositório LOC** > **Relacionamentos objeto-objeto** módulo.

Você pode criar um grupo e associá-lo a um padrão de ataque, mas no Repositório MITRE ATT&CK, você só pode estabelecer o relacionamento entre o grupo e o padrão de ataque. Para definir o tipo de relacionamento objeto a objeto, você deve fazê-lo no Repositório IoC.

Nota:
Para obter mais informações, consulte estender MITRE-ATT&CK dados e repositório IoC.

Domain Separation e MITRE-ATT&CK

Esta visão geral do Domain Separation pertence a MITRE-ATT&CK. A separação de domínio permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: Básico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como o Domain Separation funciona com MITRE-ATT&CK

Siga estas etapas para obter a separação de domínio:

- Crie um usuário com as funções sn_ti.admin necessárias no respectivo domínio.
- Replique o seguinte para cada domínio:
  - TAXII Coleções

    Nota:
    - Não ative as coleções no domínio global. Ative somente as coleções que estão replicadas e disponíveis em seu domínio.
    - Altere o campo **Executar como** nas coleções para o usuário com a função sn_ti.admin no respectivo domínio.

  - Definição de cobertura da técnica
  - Regra de extração da técnica
  - Regras de detecção – Mapeamentos MITRE ATT&CK
  - Cobertura de mitigação
    - Copie todos os registros de definição de cobertura de mitigação.
    - Copie a calculadora de redução de cobertura ou crie uma nova calculadora para o respectivo domínio.
  - Grupo de ameaças - Definições de mapa térmico de técnica

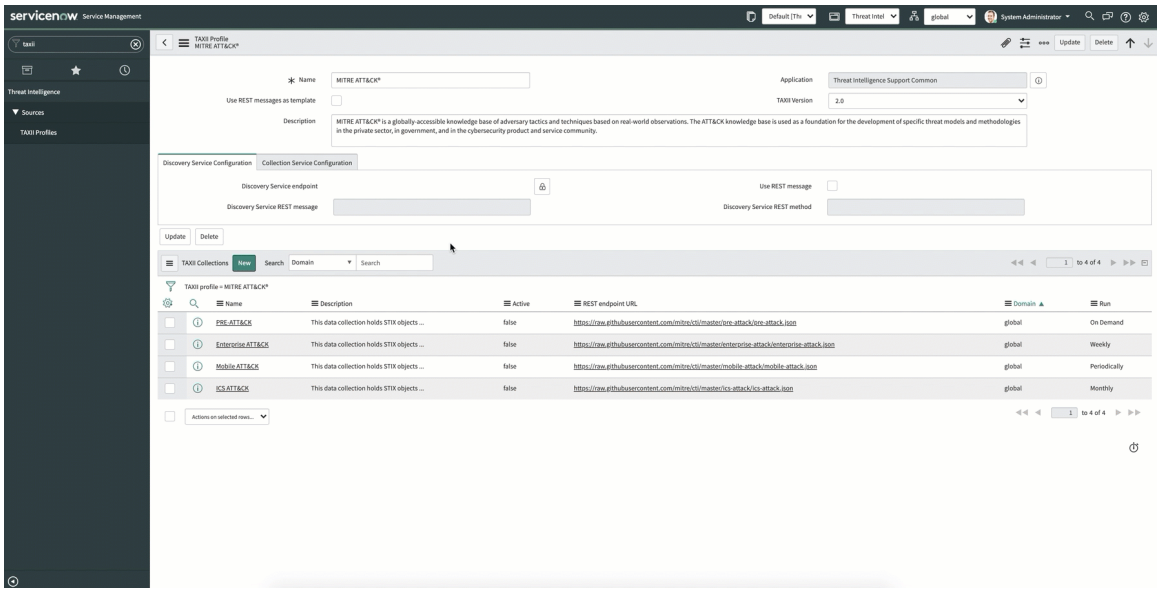
Replicar coleta de TAXII

1. Navegar até **Inteligência contra ameaças** > **Origens** > **Perfis TAXII**.
2. Na barra de cabeçalho, use o seletor de domínio para selecionar seu domínio.
3. Selecione a coleta TAXII relevante para sua organização (Enterprise ATT&CK, Mobile ATT&CK ou ICS ATT&CK).
4. Clique com o botão direito do mouse na barra de cabeçalho e selecione **Inserir e permanecer**. A coleta TAXII duplicada é criada no domínio selecionado
5. Navegue de volta para o perfil MITRE ATT&CK TAXII para exibir a coleção TAXII duplicada.

A ilustração a seguir mostra como selecionar o domínio TOP/Initech, replicar a coleta TAXII no domínio e verificar a coleta TAXII replicada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Configurar a estrutura MITRE-ATT&CK™

Ative o perfil MITRE-ATT&CK e configure um trabalho programado para que você possa configurar coleções MITRE-ATT&CK para detecção de ameaças em sua organização.

Antes de Iniciar

Função necessária: sn_ti.admin

Por Que e Quando Desempenhar Esta Tarefa

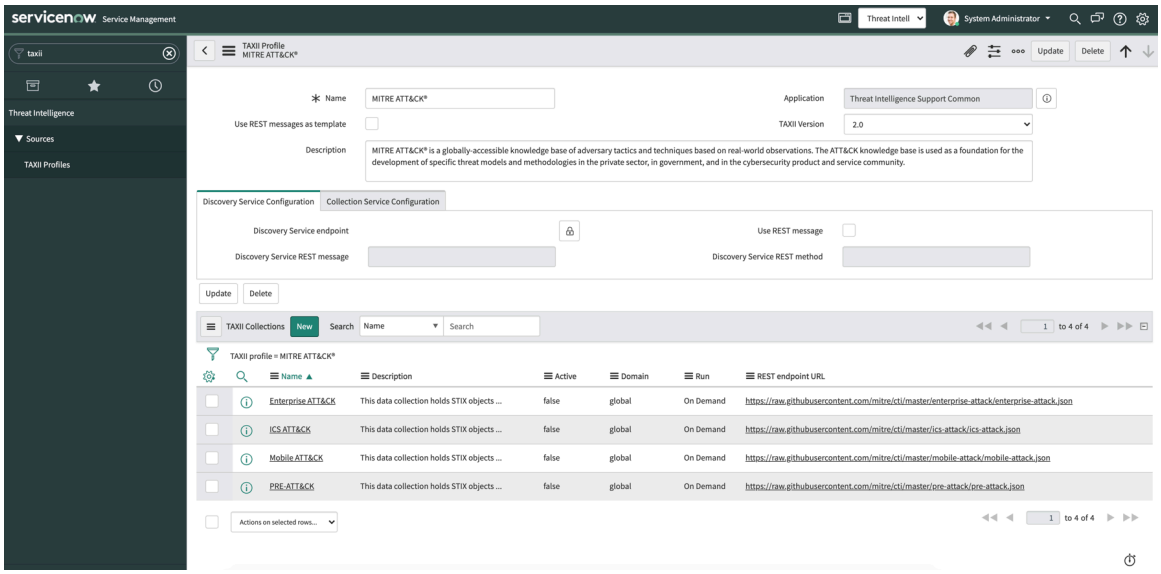
Expressão de informações de ameaça estruturada (STIX™) é uma linguagem para descrever informações de ameaça cibernética de maneira padronizada e estruturada. Usando dados do STIX e perfis de Troca automatizada confiável de informações de indicador (TAXII™), as equipes de segurança podem usar informações compartilhadas de ameaças cibernéticas para isolar ameaças que foram identificadas anteriormente pela sua empresa e de outras fontes.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Origens** > **Perfis TAXII**.
   Você verá os perfis TAXII disponíveis.
2. Clique no perfil **MITRE ATT&CK** fornecido com o sistema de base.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para ativar a coleção TAXII, defina a opção **Ativo** como verdadeiro para a coleção TAXII que seja relevante para sua organização (Enterprise ATT&CK, Mobile ATT&CK ou ICS ATT&CK).

Coleta de TAXII	Descrição
Enterprise ATT&CK	Descreve os comportamentos e as ações que um adversário realiza para comprometer e operar em uma rede e nuvem corporativas. **Nota:** A matriz Pre ATT&CK foi descontinuada em MITRE e foi mesclada com a matriz Enterprise.
Móvel ATT&CK	Descreve os comportamentos e as ações do adversário que se concentram em dispositivos móveis.
ICS ATT&CK	Descreve as ações que um adversário realiza ao operar em uma rede de Sistemas de controle industrial (ICS).

4. Para atualizar periodicamente a coleção, defina a opção **Executar** conforme apropriado para sua organização.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por padrão, esta opção é definida como Sob demanda.

Nota:

a. As coleções são empacotadas como parte do plug-in Inteligência contra ameaças Core. Instalar ou atualizar o Threat Intelligence Support Common - Versão 12.0 ou superior e o Threat Intelligence - Versão 12.0 ou superior garante que os dados das coleções sejam preenchidos automaticamente.

b. Ative a coleção TAXII somente para a coleção que você pretende usar em sua organização e desabilite as outras coleções. Por exemplo, se você pretende usar a matriz Enterprise ATT&CK, ative o Enterprise ATT&CK no nível de coleção TAXII e no nível Matrizes. Desabilite as outras matrizes Mobile ATT&CK e ICS ATT&CK na coleção TAXII e no nível Matrizes.

c. Nas listas relacionadas TAXII Coleções, se você selecionar a opção Executar como Diariamente, ocorrerá um erro e o padrão da opção será Sob demanda. Este erro ocorre porque a programação da atualização de dados MITRE-ATT&CK diária é restrita para otimizar a carga nos servidores MITRE. Além disso, MITRE atualiza os dados do ATT&CK apenas duas vezes por ano.

d. As coleções TAXII não são atualizadas a menos que você ative a coleção TAXII.

e. As atualizações das coleções existentes podem ser recuperadas do servidor MITRE programando a frequência de "execução" em cada coleção.

f. As personalizações feitas nos dados do repositório MITRE-ATT&CK (malware, grupo, mitigação e objetos de ferramenta para uma técnica) são salvas durante as atualizações programadas.

g. MITRE atualiza a base de conhecimento MITRE-ATT&CK em que alguns objetos são identificados como revogados ou obsoletos, novos objetos são adicionados ou objetos existentes são modificados. Se MITRE revogar qualquer tática ou técnica, esses objetos serão marcados como revogados no Now Platform. Os objetos revogados são mantidos no repositório, mas não estão disponíveis para uso no Now Platform.

O que Fazer Depois

Depois que a configuração do perfil TAXII é concluída, os dados do repositório MITRE-ATT&CK são importados em intervalos regulares para o Now Platform®. Você pode ver esses dados navegando até **Repositório do MITRE ATT&CK** > **Matrizes** e **Repositório do MITRE ATT&CK** > **Técnicas**.

Gerenciar matrizes

Gerencie as matrizes que foram importadas das coleções MITRE TAXII. Matrizes são uma coleção de táticas e técnicas. Você pode exibir as matrizes para revisar se suas coleções estão disponíveis no repositório MITRE-ATT&CK.

Antes de Iniciar

Nota:

Revise e verifique se somente a matriz que você pretende usar em sua organização está definida como ativa e desabilite as outras matrizes. Por exemplo, se você pretende usar a matriz Enterprise ATT&CK, a matriz Enterprise ATT&CK será ativada no nível de coleta TAXII e no nível de matrizes. Desabilite as outras matrizes Mobile ATT&CK e ICS ATT&CK na coleção TAXII e no nível Matrizes.

Função necessária:

Tradução automática

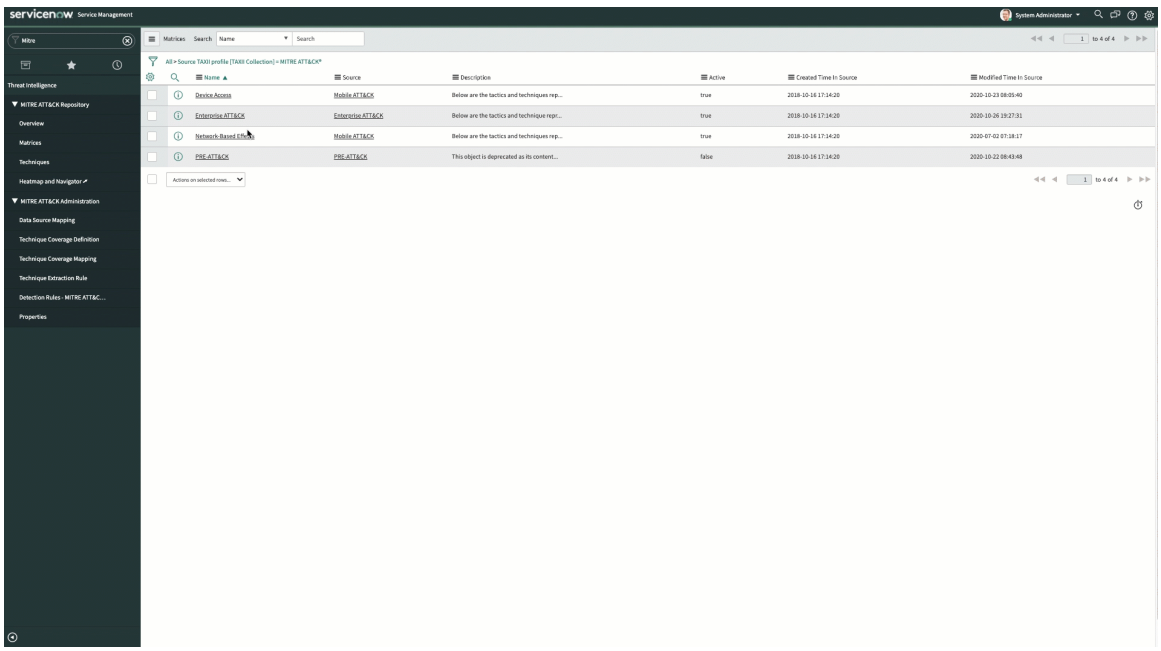
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Matrizes**.
   Todas as matrizes estão desabilitadas por padrão.
2. Para ativar uma matriz, aponte para **Ativo**, clique duas vezes e selecione **verdadeiro**.
3. Para exibir todas as informações associadas, clique em uma matriz.
4. Para exibir todas as táticas associadas a esta coleção, clique na guia **Táticas do MITRE**.
5. Para exibir detalhes adicionais e as técnicas associadas a uma tática selecionada, clique em uma tática.
6. Na guia **Técnicas do MITRE ATT&CK**, selecione uma técnica.
7. Nas listas relacionadas, exiba as associações que estão disponíveis para a técnica que você selecionou.

Na ilustração a seguir, você pode ver o caminho de navegação da matriz Enterprise ATT&CK até a tática Acesso inicial (TA0001) e, em seguida, até a técnica Phishing (T1566). Na página Padrão de ataque – Técnica de phishing, você pode exibir a lista relacionada: Tática, Subtécnica, Grupo, Mitigação, Referências externas, Malware e Ferramentas.



O que Fazer Depois

Você pode estender as informações em alguns desses objetos de lista relacionados com base na técnica selecionada. Por exemplo, você pode adicionar novas informações para Grupo, Mitigação, Referências externas, Malware e Ferramentas.

Gerenciar técnicas

Gerencie as técnicas que foram importadas das coleções MITRE TAXII. As técnicas contêm várias maneiras pelas quais os invasores desenvolveram para empregar uma determinada

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

tática. Você pode revisar e desativar técnicas que não são relevantes para sua organização. Em STIX, as técnicas são conhecidas como padrões de ataque.

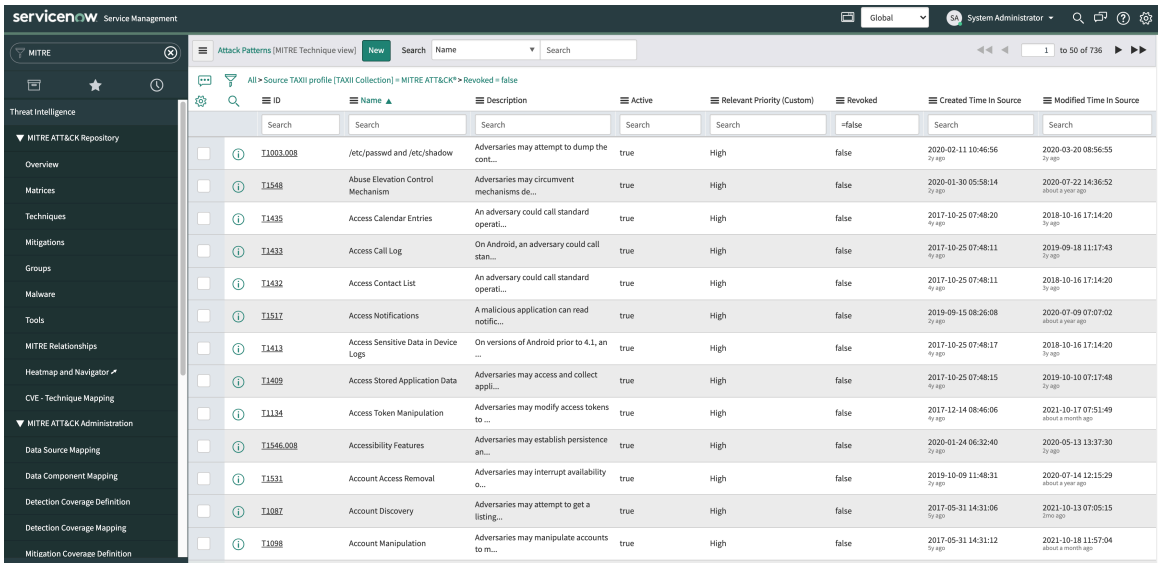
Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Técnicas**.



   A lista de técnicas e subtécnicas agora está listada.

2. Para revisar e desativar técnicas que não são relevantes para sua organização, vá para a exibição de lista da técnica selecionada e, na coluna Ativa, atualize a configuração para **falso**e salve a configuração. Desative as técnicas que não são usadas por outros objetos no repositório MITRE-ATT&CK.

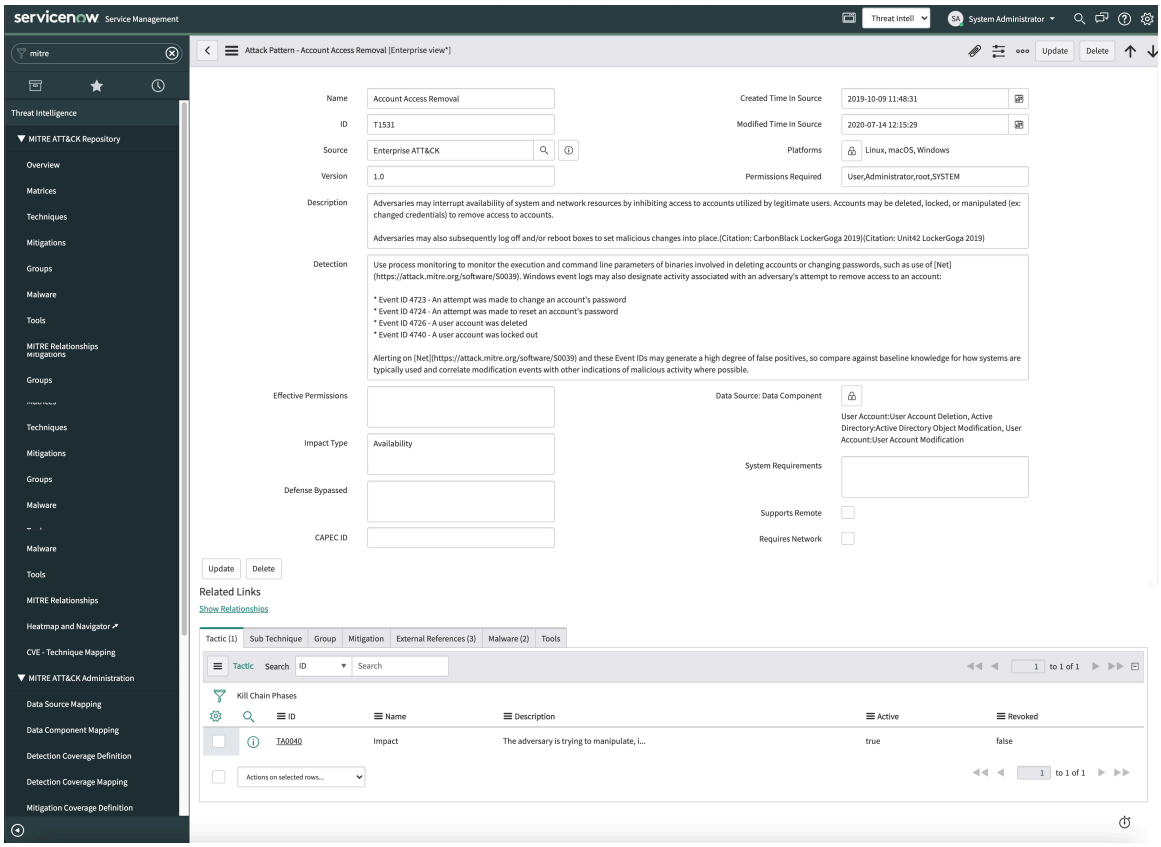
3. Para priorizar uma técnica, atribua uma prioridade no campo **Prioridade relevante (personalizada)**. A prioridade relevante do sistema de base é definida como nenhuma. O campo **Prioridade relevante (personalizada)** não é importado das coleções MITRE-ATT&CK TAXII, mas de um campo personalizado introduzido no Now Platform. Você pode usar as informações de prioridade relevantes para filtrar e priorizar técnicas nos painéis, durante o mapeamento da fonte de dados ou ao analisar o mapa térmico.

4. Clique em uma técnica para exibir todas as informações associadas a essa técnica.

   Na ilustração a seguir, você pode exibir os detalhes de cada técnica de Remoção de acesso à conta, seu ID, origem e outras informações relacionadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:
O elemento Fonte de dados: componente de dados introduzido por MITRE substitui o campo Fonte de dados anterior. O componente de dados fornece uma subcamada extra de contexto para as fontes de dados. Se o seu repositório MITRE-ATT&CK contiver as coleções TAXII antigas, você poderá exibir o campo Fonte de dados. Caso contrário, você pode exibir as fontes de dados com o contexto adicional de componentes de dados no campo Fonte de dados: componente de dados. Você pode exibir o novo campo de componente de dados somente quando a origem for Enterprise ATT&CK. Para obter mais informações, consulte mapeamento de componente de dados.

5. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos**.

O que Fazer Depois

Você pode estender as informações em alguns desses objetos de lista relacionados. Por exemplo, você pode adicionar novas informações para Grupo, Mitigação e Referências externas.

Gerenciar mitigações

Gerencie as mitigações que foram importadas das coleções MITRE TAXII. As mitigações permitem impedir que um adversário execute técnicas ou subtécnicas com êxito na sua organização. Em STIX, as mitigações são conhecidas como curso de ações.

Antes de Iniciar

Função necessária:

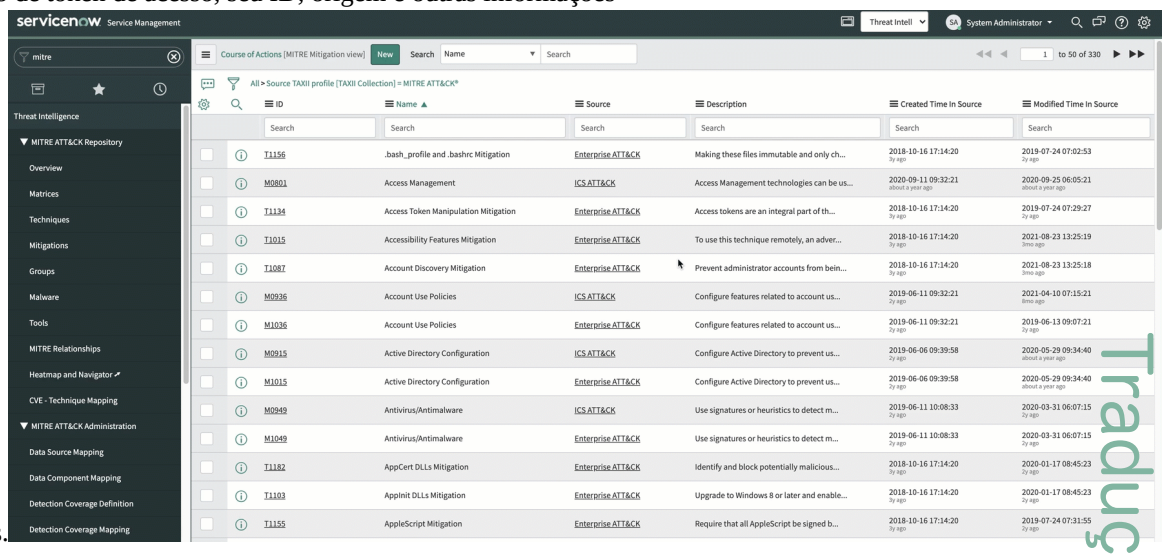
- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Mitigações**.
   As mitigações agora estão listadas.
2. Clique em uma mitigação para exibir todas as informações associadas.
   Na ilustração a seguir, você pode exibir os detalhes da mitigação da Manipulação de token de acesso, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos**.

O que Fazer Depois

Use o módulo de técnicas para adicionar ou modificar os dados de mitigações.

Gerenciar grupos

Gerencie os grupos que foram importados das coleções MITRE TAXII. Grupos são conjuntos de atividades de invasão relacionadas que são rastreadas por um nome comum na comunidade de segurança. Os analistas rastreiam clusters de atividades usando vários termos, como grupos de ameaças, grupos de atividades, agentes de ameaça, conjuntos de intrusão e campanhas. Em STIX, os grupos são conhecidos como conjuntos de intrusão.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

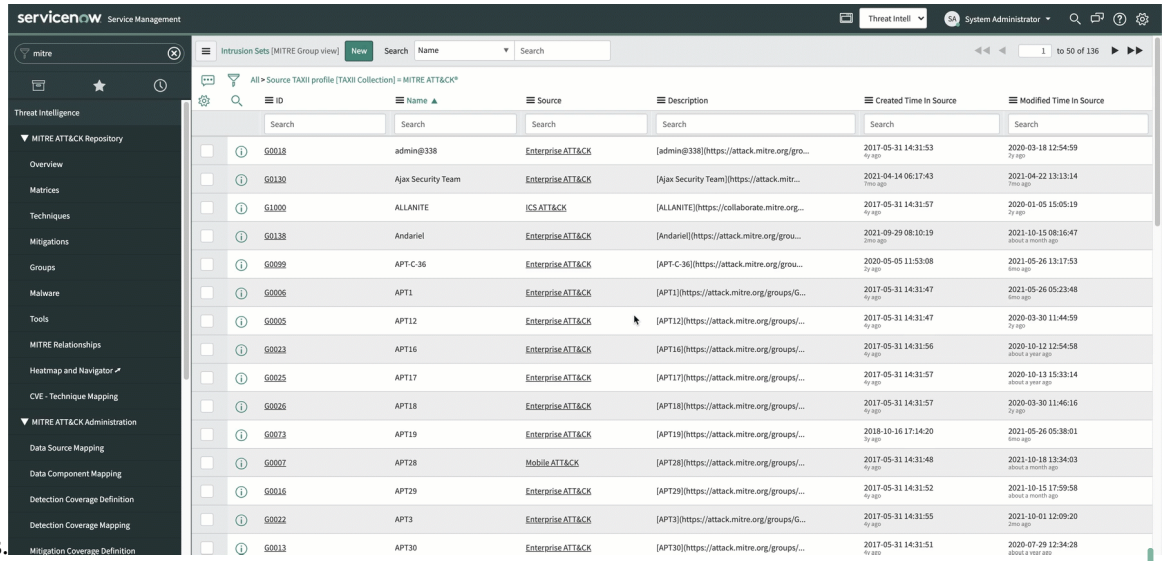
Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Grupos**.
   Você pode exibir os grupos listados.
2. Clique em um grupo para exibir todas as informações associadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes do grupo Ajax Security Team, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos**.

> **Nota:**
> Para associar os grupos de ameaça a um caso de segurança para investigação mais detalhada, clique em **Adicionar ao caso de segurança**.

O que Fazer Depois

Use o módulo de técnicas para adicionar ou modificar os dados dos grupos.

Gerenciar malware

Gerencie as informações de malware que você importou das coleções MITRE TAXII. Malware é um tipo de TTP que representa um código malicioso. Refere-se a um programa que é inserido secretamente em um sistema. A intenção de um malware é comprometer a confidencialidade, a integridade ou a disponibilidade dos dados, das aplicações ou do sistema operacional (SO) da vítima.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

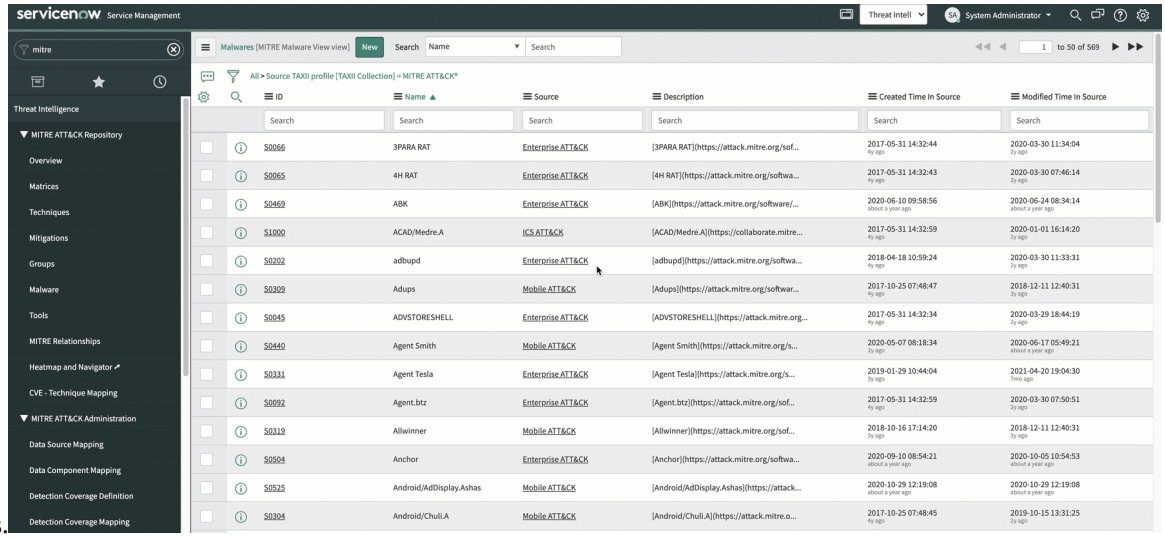
Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Malware**.
   Você pode exibir o malware listado.
2. Clique em um malware para exibir todas as informações associadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes do malware 3PARA RAT, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos**.

O que Fazer Depois

Use o módulo de técnicas para adicionar ou modificar os dados de malware.

Gerenciar ferramentas

Gerencie as informações de ferramentas que você importou das coleções MITRE TAXII. As ferramentas são softwares legítimos usados por agentes de ameaça para executar ataques.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

Por Que e Quando Desempenhar Esta Tarefa

As ferramentas permitem que você saiba como e quando os agentes de ameaça as usam para executar campanhas. Ao contrário do malware, essas ferramentas ou pacotes de software geralmente são encontrados em um sistema e têm finalidades legítimas para usuários avançados, administradores, administradores de rede ou até mesmo usuários normais.

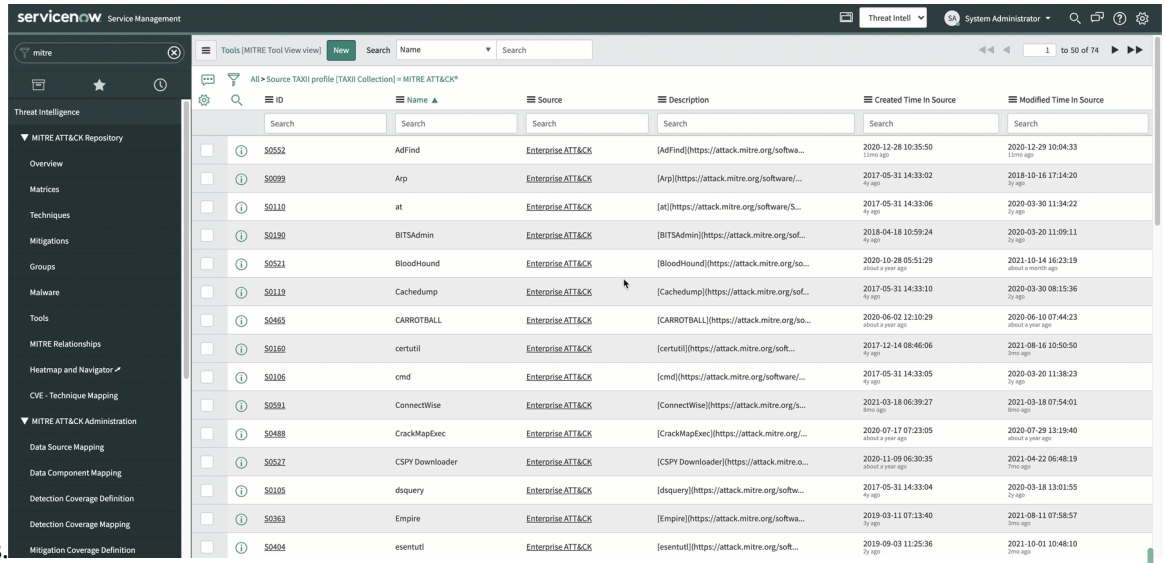
Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Ferramentas**.
   Você pode exibir as ferramentas listadas.
2. Clique em uma ferramenta para exibir todas as informações associadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes da ferramenta CARROTBALL, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos**.

O que Fazer Depois

Use o módulo de técnicas para adicionar ou modificar os dados das ferramentas.

Gerenciar MITRE relacionamentos

Gerencie as informações de relacionamentos MITRE que você importou das coleções MITRE TAXII.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

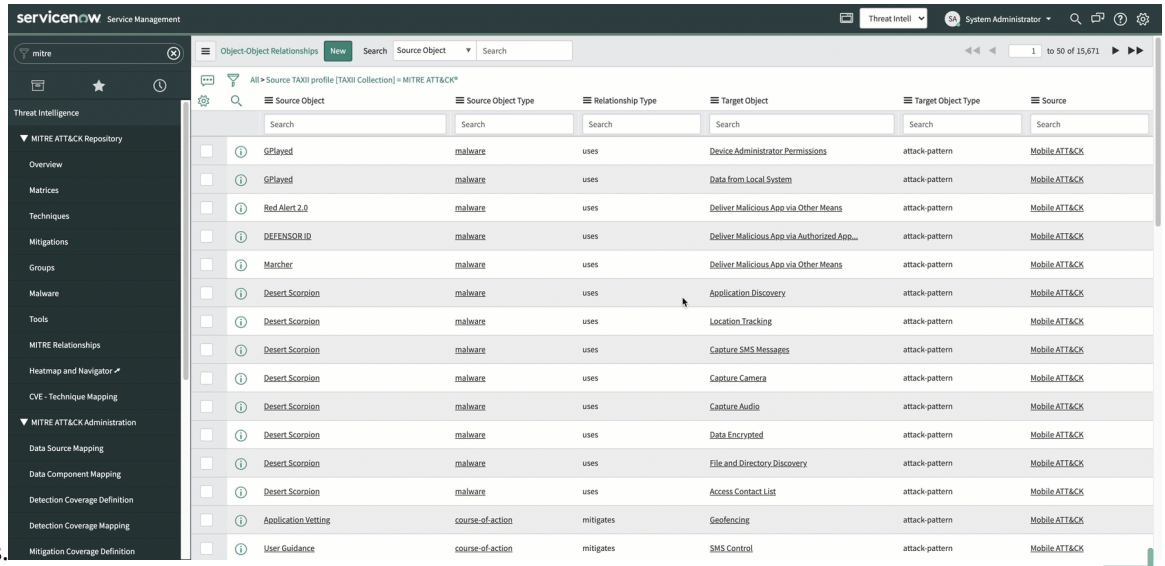
Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Relações do MITRE**.
   Você pode exibir as ferramentas listadas.
2. Clique em um objeto de origem para exibir todas as informações associadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes do objeto Red Alert 2.0, seu ID, origem e outras informações relacionadas.



3. Para exibir como esses objetos estão relacionados, clique em **Mostrar relacionamentos**.

O que Fazer Depois

Use o módulo de técnicas para adicionar ou modificar os dados de relacionamentos do MITRE.

Gerenciar CVE e mapeamento de técnica

Gerencie as informações de técnica e CVE que são mapeadas depois de importar as coleções MITRE TAXII.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

Nota:
O módulo **CVE-Technique Mapping** está disponível somente quando o produto Vulnerability Response está instalado em seu ambiente.

Por Que e Quando Desempenhar Esta Tarefa

Depois de importar as coleções MITRE TAXII, é possível exibir os CVEs em seu ambiente e o relacionamento deles com as técnicas MITRE-ATT&CK associadas. Você também pode criar associações com CVEs e os padrões de ataque.

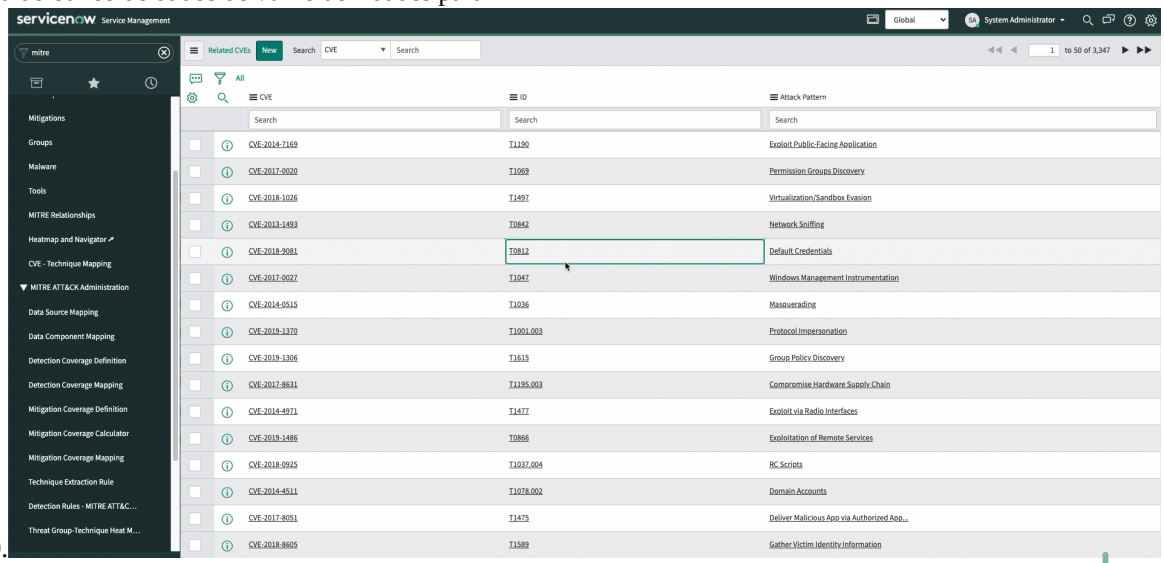
Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **CVE - Mapeamento de técnica**.
   Você pode exibir os CVEs e as técnicas listados.
2. Clique em um CVE para exibir a entrada do banco de dados de vulnerabilidades.

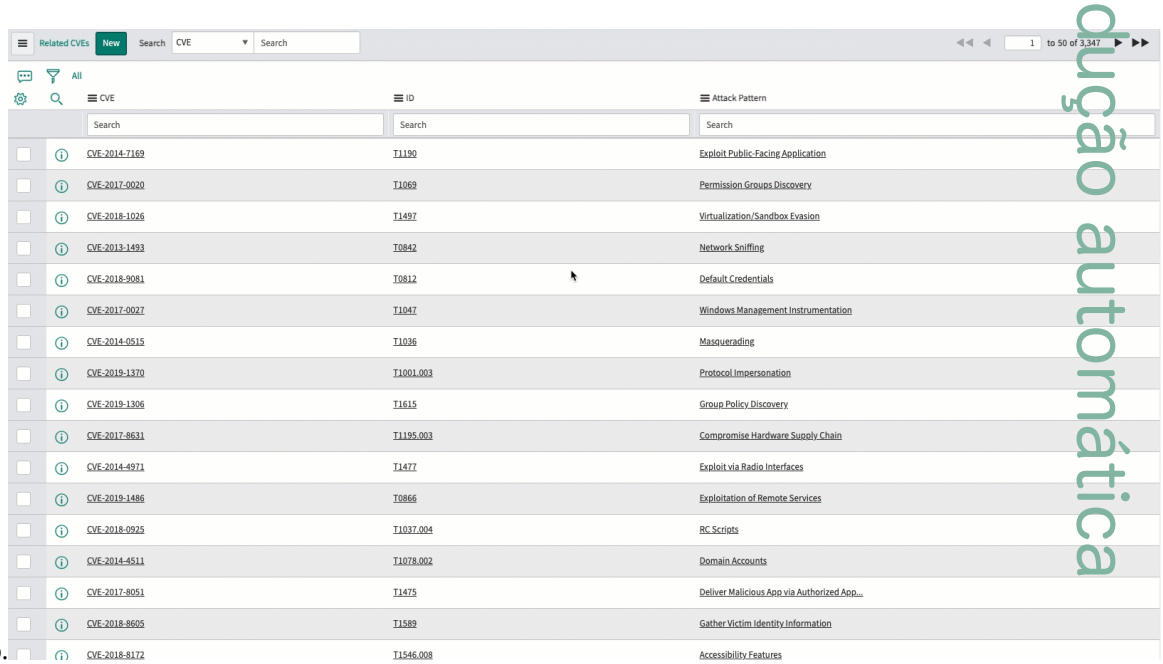
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode exibir os detalhes da lista de CVE e da entrada do banco de dados de vulnerabilidades para CVE-2014-7169.



3. Para adicionar uma entrada, clique em **Novo**, mapeie o CVE para um padrão de ataque e clique em **Enviar**.
   Na ilustração a seguir, uma nova entrada é criada pelo mapeamento de CVE-2014-0515 com o padrão de ataque de Mascaramento.



Tradução automática

Estender os dados de MITRE-ATT&CK

Estenda os dados do repositório MITRE-ATT&CK no Now Platform aprimorando-os.

Antes de Iniciar

Função necessária:

- sn_ti.admin: excluir acesso
- sn_ti.read: acesso de leitura
- sn_ti.write: criar, acesso de gravação

Por Que e Quando Desempenhar Esta Tarefa

Você pode estender os objetos Malware, Grupo, Mitigação e Ferramenta para uma técnica no repositório MITRE-ATT&CK.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode criar um novo objeto e estabelecer um relacionamento entre uma técnica e o novo objeto no módulo Repositório do MITRE ATT&CK, mas não pode definir o tipo de relacionamento neste módulo. Para obter mais informações sobre como definir tipos de relacionamento, consulte relacionamentos de objeto para objeto. Para definir um tipo de relacionamento, navegue até o **Inteligência contra ameaças** > **Repositório LOC** > **Relacionamentos objeto-objeto** módulo.

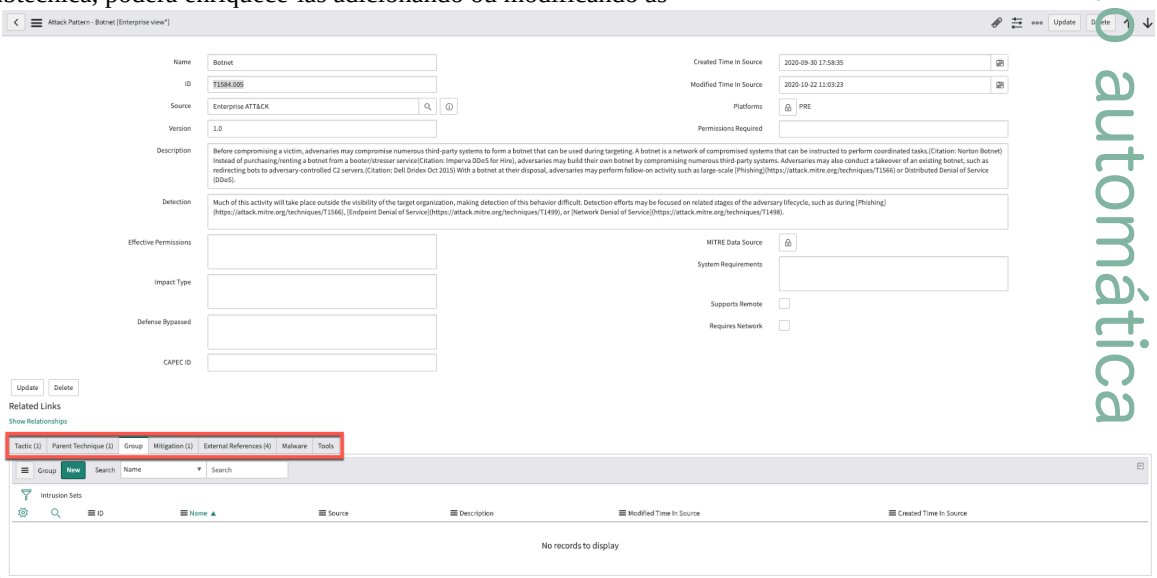
Se você mapear o tipo de relacionamento entre uma técnica existente e um objeto existente, deverá definir a técnica como o objeto de destino e o objeto como o objeto de origem. Para fazer isso, navegue até o **Repositório LOC** > **Relacionamentos objeto-objeto** módulo.

Você pode criar um grupo e associá-lo a um padrão de ataque, mas no Repositório MITRE ATT&CK, você só pode estabelecer o relacionamento entre o grupo e o padrão de ataque. Para definir o tipo de relacionamento objeto a objeto, você deve fazê-lo no Repositório IoC.

Nota:
Todas as personalizações feitas nos objetos são salvas durante as atualizações programadas.

Procedimento

1. Navegar até **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Técnicas**.
2. Clique em uma técnica ou subtécnica para exibir todas as informações associadas a essa técnica. Na ilustração a seguir, você pode ver que a técnica Botnet (T1584.005) não está associada a nenhum grupo. Se você tiver informações adicionais sobre uma técnica ou subtécnica, poderá enriquecê-las adicionando ou modificando as informações.

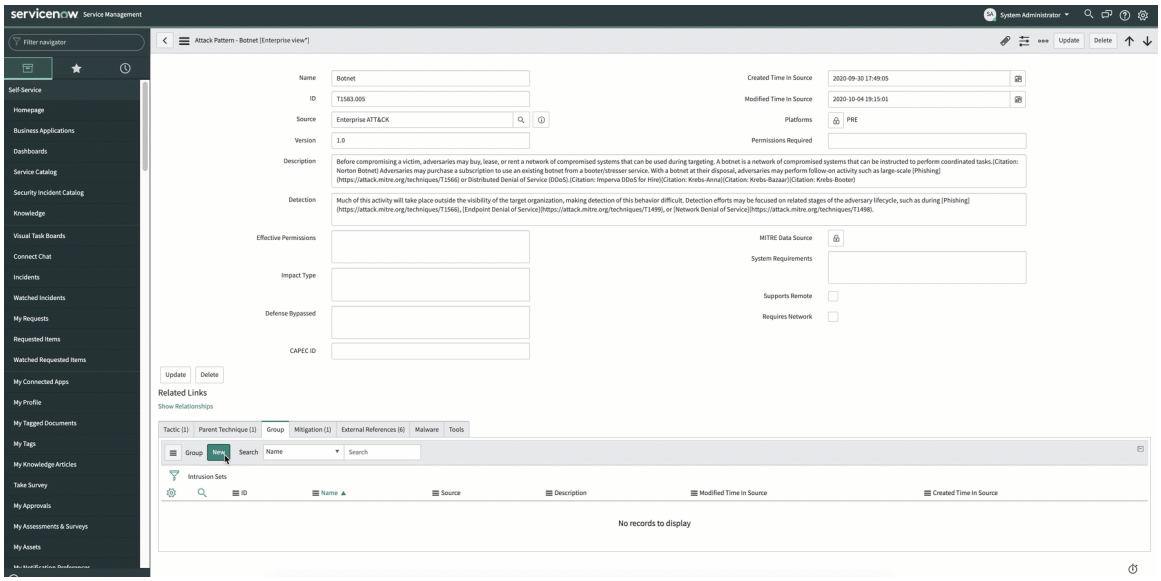


3. Clique em uma lista relacionada para aprimorar seus dados e associá-la a um novo grupo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, um grupo, Custom1, foi associado à subtécnica Botnet.



Definir a fonte de dados e o mapeamento da ferramenta de detecção

Defina a fonte de dados e o mapeamento da ferramenta de detecção para MITRE-ATT&CK táticas e técnicas. O mapeamento de fonte de dados fornece informações sobre a relevância e a disponibilidade das fontes de dados e as ferramentas de detecção para monitorar as fontes de dados em seu ambiente.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: gravação, exclusão de acesso
- sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

Você pode identificar as fontes de dados e as ferramentas de detecção de que sua organização precisa para detectar as técnicas com eficácia.

Por exemplo, se sua organização se concentra em 5 técnicas, talvez você precise de 10 fontes de dados e 10 ferramentas de detecção para monitorar essas fontes. Digamos que você identifique que sua organização não tem duas fontes de dados e cinco ferramentas de detecção. Este exercício oferece visibilidade sobre as fontes de dados, sua relevância para a organização e para identificar lacunas na cobertura. Você também pode se concentrar em aprimorar seu ambiente com as fontes de dados e as ferramentas de detecção corretas.

Todas as táticas, técnicas, ID e fontes de dados ativas são preenchidas automaticamente com base em TAXII perfil

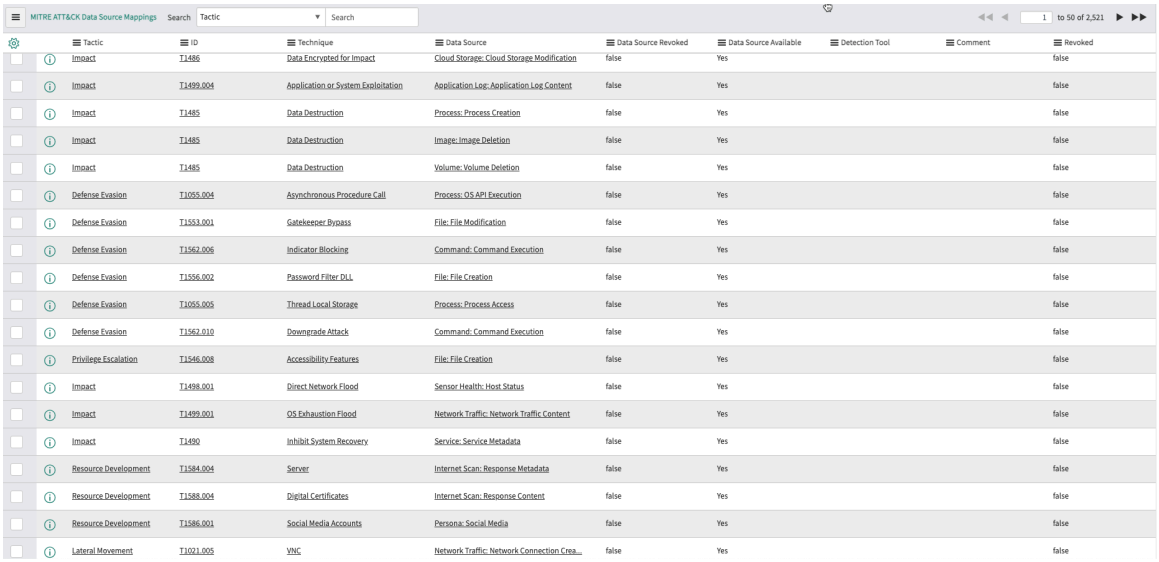
Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Mapeamento de fonte de dados**.

   A ilustração a seguir mostra a lista de táticas, técnicas e seus IDs que foram preenchidos com base nas atualizações de sua coleção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Tactic	ID	Technique	Data Source	Data Source Revoked	Data Source Available	Detection Tool	Comment	Revoked
Impact	T1486	Data Encrypted for Impact	Cloud Storage: Cloud Storage Modification	false	Yes			false
Impact	T1499.004	Application or System Exploitation	Application Log: Application Log Content	false	Yes			false
Impact	T1485	Data Destruction	Process: Process Creation	false	Yes			false
Impact	T1485	Data Destruction	Image: Image Deletion	false	Yes			false
Impact	T1485	Data Destruction	Volume: Volume Deletion	false	Yes			false
Defense Evasion	T1055.004	Asynchronous Procedure Call	Process: OS API Execution	false	Yes			false
Defense Evasion	T1553.001	Gatekeeper Bypass	File: File Modification	false	Yes			false
Defense Evasion	T1562.006	Indicator Blocking	Command: Command Execution	false	Yes			false
Defense Evasion	T1556.002	Password Filter DLL	File: File Creation	false	Yes			false
Defense Evasion	T1055.005	Thread Local Storage	Process: Process Access	false	Yes			false
Defense Evasion	T1562.010	Downgrade Attack	Command: Command Execution	false	Yes			false
Privilege Escalation	T1546.008	Accessibility Features	File: File Creation	false	Yes			false
Impact	T1498.001	Direct Network Flood	Sensor Health: Host Status	false	Yes			false
Impact	T1499.001	OS Exhaustion Flood	Network Traffic: Network Traffic Content	false	Yes			false
Impact	T1490	Inhibit System Recovery	Service: Service Metadata	false	Yes			false
Resource Development	T1584.004	Server	Internet Scan: Response Metadata	false	Yes			false
Resource Development	T1588.004	Digital Certificates	Internet Scan: Response Content	false	Yes			false
Resource Development	T1586.001	Social Media Accounts	Persona: Social Media	false	Yes			false
Lateral Movement	T1021.005	VNC	Network Traffic: Network Connection Crea...	false	Yes			false

Campo	Descrição
Tática	Objetivo do adversário ou motivo para executar uma ação.
ID	Identidade exclusiva da técnica.
Técnica	Como um adversário atinge um objetivo tático executando uma ação.
Fonte de Dados	Fonte de dados associada à técnica.
Fonte de dados revogada	A fonte de dados será revogada se definida como verdadeira, mas o mapeamento da fonte de dados ainda será retido. Se o valor da fonte de dados não for encontrado em MITRE, o valor de Fonte de dados revogada será marcado automaticamente como verdadeiro. O mapeamento de fonte de dados para um registro será revogado se a técnica e os relacionamentos de fonte de dados estiverem ausentes nos dados atualizados MITRE. Padrão: falso
Fonte de dados disponível	Disponibilidade da fonte de dados.
Ferramenta de detecção	Ferramenta que complementa a fonte de dados detectando as técnicas usadas. A ferramenta de detecção está mapeada com o sensor de alerta em SIR.
Revogado	O mapeamento de fonte de dados para um registro será revogado se a técnica e os relacionamentos de fonte de dados estiverem ausentes nos dados atualizados MITRE.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Padrão: falso

2. Revise as fontes de dados listadas e modifique o valor no campo **Fonte de dados disponível** com base no seu ambiente.

3. **Nota:**
   Você não pode editar esta entrada na exibição de lista.

   No campo **Ferramenta de detecção**, siga estas etapas:

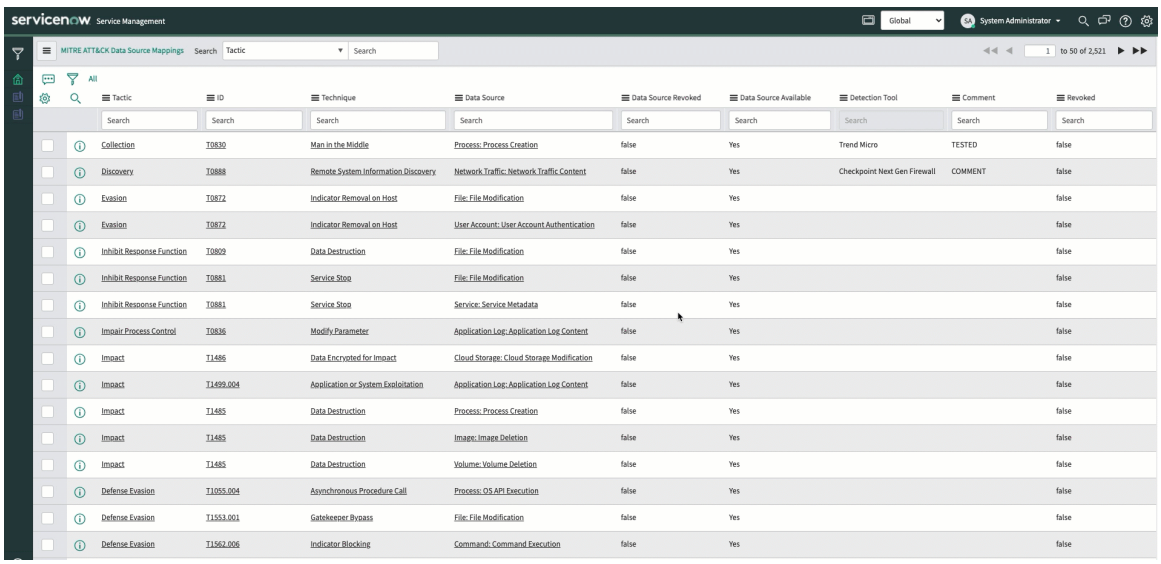
   a. Clique no ícone de informações e clique em **Abrir registro**.

   b. Desbloqueie a entrada **da Ferramenta de detecção**.

   c. Use a lista de pesquisa para selecionar uma ferramenta de detecção. Você pode selecionar várias ferramentas de detecção.

   d. Clique em **Atualizar**.

   Na ilustração a seguir, várias ferramentas de detecção são adicionadas para monitorar a fonte de dados.



Definir a fonte de dados e o mapeamento do componente de dados

Use o Mapeamento de componente de dados se você estiver usando as coleções TAXII mais recentes e quiser manter um relacionamento entre as fontes de dados, os componentes de dados e as várias técnicas. Mapeie as fontes de dados com o contexto adicional de componentes de dados que fornece uma subcamada extra de contexto para fontes de dados que permitem entender melhor os comportamentos do adversário em MITRE-ATT&CK.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: gravação, exclusão de acesso
- sn_ti.read: acesso de leitura

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

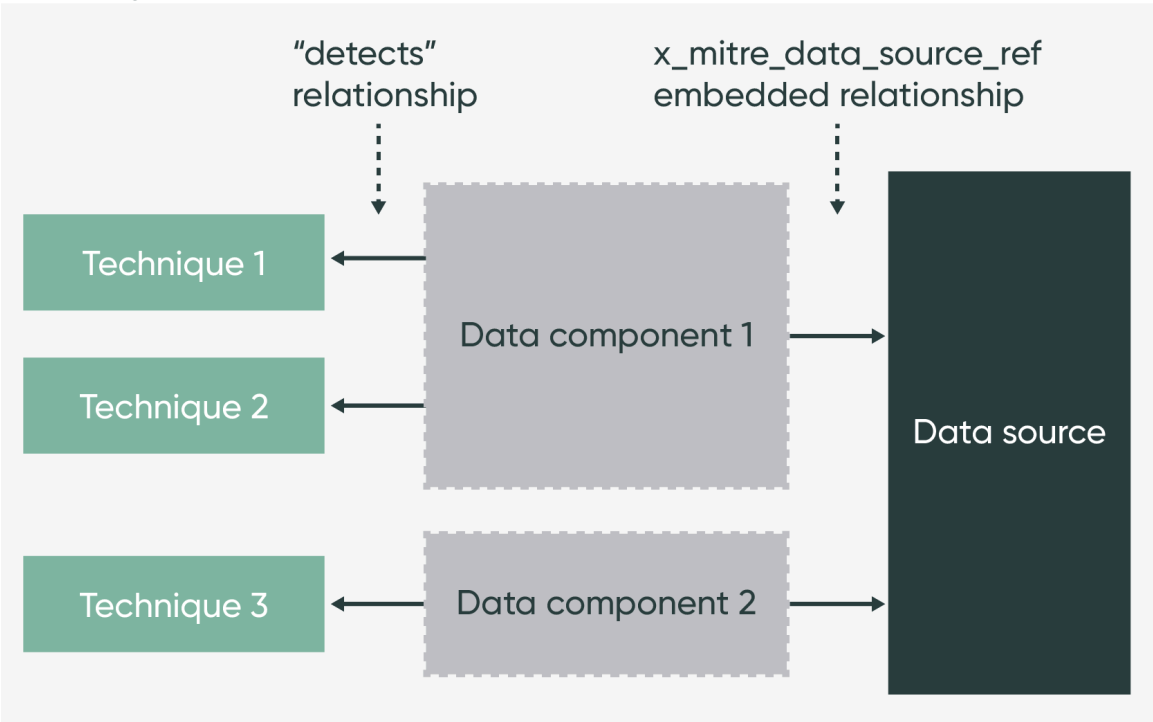
Por Que e Quando Desempenhar Esta Tarefa
O mapeamento das fontes de dados e dos componentes de dados fornece visibilidade das fontes de dados ou dos componentes e das técnicas que são relevantes para sua organização.

Por exemplo, se sua organização se concentra em 7 técnicas, talvez você precise de 5 fontes de dados e 10 componentes de dados para monitorar essas fontes. Sua avaliação das ferramentas internas revela que sua organização não tem duas fontes de dados e quatro componentes de dados. Este exercício de mapeamento fornece visibilidade sobre as fontes de dados, componentes e técnicas, sua relevância para a sua organização e para identificar as lacunas na cobertura. Assim, você pode concentrar seu investimento nas fontes de dados e nos sensores de alerta corretos para detectar e mitigar as ameaças do adversário.

A estrutura MITRE-ATT&CK contém uma estrutura atualizada para as fontes de dados - Fonte de dados: Componente de dados. Este novo formulário de fonte de dados fornece um contexto extra para as fontes de dados. O objeto de fonte de dados apresenta o nome da fonte de dados, bem como os principais detalhes sobre os dados coletados (arquivo, processo, tráfego de rede e assim por diante) e valores ou propriedades específicas necessárias para detectar comportamentos do adversário.

A ilustração a seguir mostra a representação da estrutura MITRE-ATT&CK STIX™ para fontes de dados e componentes de dados. Você pode ver as fontes de dados e os componentes de dados capturados como objetos STIX™ personalizados. A ilustração mostra que cada fonte de dados contém um ou mais componentes de dados e cada componente de dados detecta uma ou mais técnicas.

Estrutura geral de fontes de dados e componentes de dados



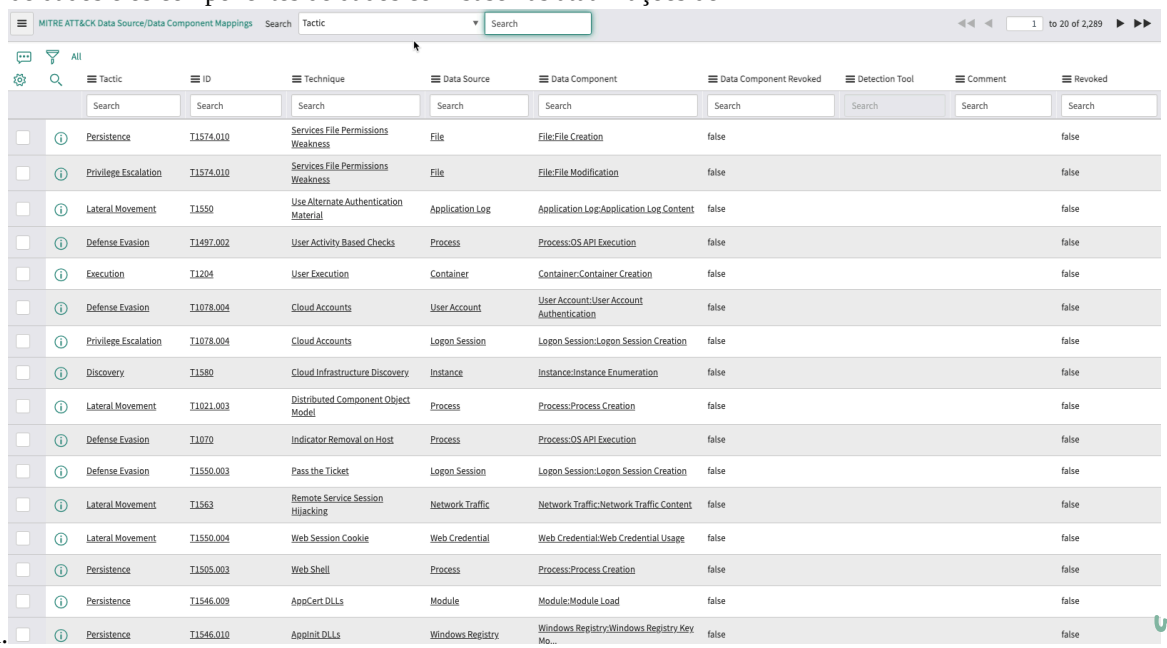
Você pode continuar usando o Mapeamento de fonte de dados se o seu repositório MITRE-ATT&CK contiver as coleções TAXII antigas e você tiver mapeado suas fontes de dados para várias técnicas. No entanto, use o Mapeamento de componente de dados se você estiver usando as coleções TAXII mais recentes e quiser manter um relacionamento entre as fontes de dados, os componentes de dados e as várias técnicas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Mapeamento de componente de dados**.
   A ilustração a seguir mostra a lista de táticas, IDs e técnicas junto com as fontes de dados e os componentes de dados com base nas atualizações de coleta.



Campo	Descrição
Tática	Objetivo do adversário ou motivo para executar uma ação.
ID	Identidade exclusiva da técnica.
Técnica	Como um adversário atinge um objetivo tático executando uma ação.
Fonte de Dados	Fonte de dados associada à técnica.
Componente de dados	Componente de dados associado à fonte de dados. Um componente de dados só pode ter uma fonte de dados primária.
Componente de dados revogado	Identifica se o componente de dados foi revogado na base de conhecimento MITRE-ATT&CK.
Ferramenta de detecção	Ferramenta que complementa a fonte de dados detectando as técnicas usadas. A ferramenta de detecção está mapeada com o sensor de alerta em SIR.
Comentário	Descrição sobre a fonte de dados e o mapeamento do componente de dados.
Revogado	Identifica se o componente de dados para mapeamento de técnica foi revogado por MITRE-ATT&CK.

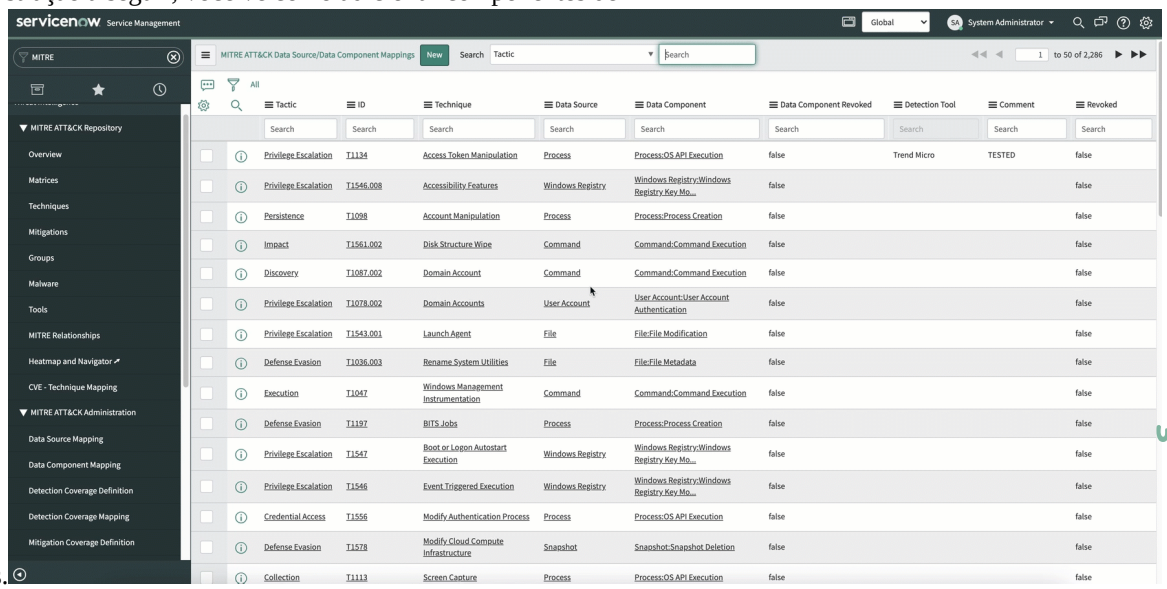
2. Revise as fontes de dados e os componentes de dados listados e modifique os valores com base no seu ambiente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Siga estas etapas para adicionar um componente de dados.
   a. Navegar até **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Técnicas**.
   b. Clique em uma técnica que você deseja modificar a fonte de dados: informações do componente de dados.
   c. Desbloquear fonte de dados: componente de dados.
   d. Use a lista de pesquisa para selecionar MITRE-ATT&CK componentes de dados.
   e. Bloqueio de fonte de dados: componente de dados.
   f. Clique em **Atualizar**.

Na ilustração a seguir, você vê como adicionar componentes de dados.



Definir a cobertura de detecção da técnica

Defina a cobertura de detecção de técnica que sua organização deve medir e detectar técnicas de adversários específicas.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: acesso de gravação
- Função necessária: sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

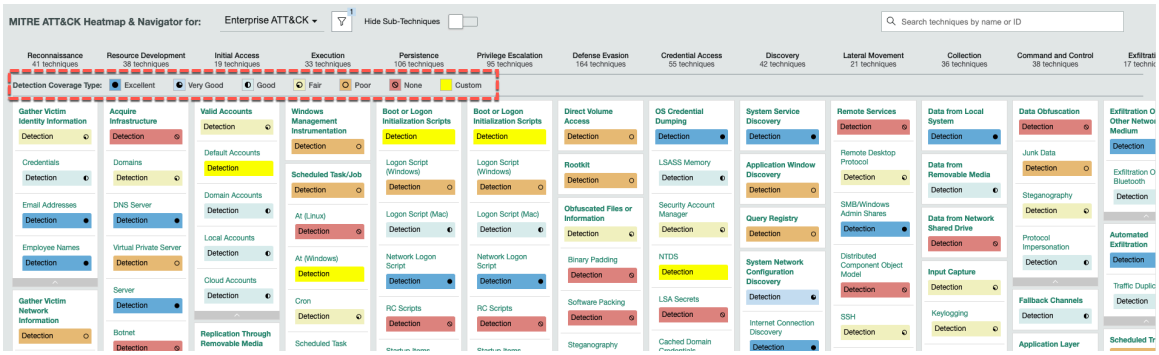
As definições de cobertura de técnica são usadas no mapeamento geral de detecção de técnica. Você pode usar a cobertura da técnica do sistema de base. A cobertura da técnica do sistema de base consiste nos tipos de cobertura Nenhum, Ruim, Justo, Bom, Muito Bom e Excelente. A cobertura da técnica do sistema de base também está associada a cores predefinidas. Você pode personalizar as entradas e as cores do tipo de cobertura ou criar suas próprias entradas. Por exemplo, você pode modificar os tipos de cobertura do sistema de base para Não aplicável, Cobertura parcial e Cobertura completa. Como alternativa, você também pode criar medidas numéricas para os tipos de cobertura, como 0-25 por cento, 25 a 50 por cento e 50 a 100 por cento. O tipo de modificações feitas na cobertura do sistema de base não se limita aos exemplos compartilhados.

As personalizações feitas no tipo de cobertura e na cor são usadas no mapeamento geral de detecção de técnica e também no mapa térmico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Se você modificar a definição de cobertura do sistema de base, os ícones de tipo de cobertura não serão exibidos com as técnicas no mapa térmico. O mapa térmico funciona conforme o esperado quando você modifica os mesmos campos que a cobertura de detecção de técnica definida pelo sistema de base e as cores de cobertura. No entanto, se você excluir os campos existentes da cobertura geral de detecção da técnica, o mapa térmico não exibirá os ícones de tipo de cobertura.



Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Definição de cobertura de detecção**.
2. Revise as entradas gerais de detecção de técnica e personalize as entradas para o seu ambiente.

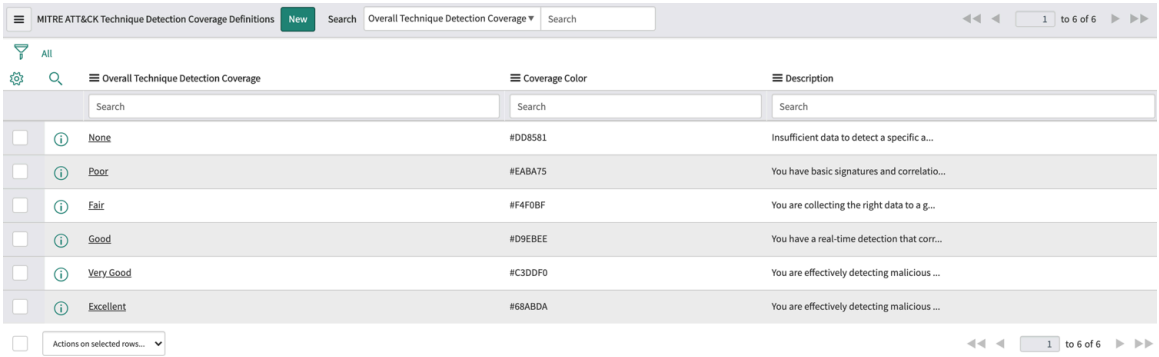
Definição de cobertura de detecção

Campo	Descrição
Cobertura geral de detecção de técnica	Nome da cobertura geral de detecção da técnica. A cobertura da técnica do sistema de base consiste em Nenhum, Ruim, Razoável, Bom, Muito Bom ou Excelente.
Cor de cobertura	Cor atribuída à pontuação de cobertura de detecção. A cor que você define é usada para a cobertura de detecção da técnica no mapa térmico. Você pode personalizar as cores usando códigos HEX e valores RGB(A).
Descrição	Cobertura geral de detecção da técnica. Consulte a definição do sistema de base na Definição de pontuação.

A ilustração a seguir mostra a lista Definição de cobertura de detecção.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Para adicionar uma entrada, clique em **Novo**, conclua as entradas e clique em **Enviar**.

MITRE-ATT&CK Definição de pontuação

Defina o sistema de pontuação MITRE-ATT&CK da sua organização para que você possa medir a eficácia com que sua organização pode detectar técnicas específicas do adversário.

Definição de pontuação

Pontuação	Mapeamento de pontuação	Descrição
Nenhum(a)	0	Dados insuficientes para detectar uma técnica adversária específica.
Ruim	1	Assinaturas básicas e regras de correlação estão em vigor para detectar técnicas de adversários específicas. A detecção de ameaças não é em tempo real e cobre apenas um número mínimo de aspectos de uma técnica. Por exemplo, a busca ocorre apenas em um endpoint de cada vez. Sua organização ainda pode ter milhares ou centenas de eventos que os buscadores devem revisar e correlacionar a outros eventos para encontrar valores atípicos. O número de falsos positivos é alto.
Justo	2	Coletando os dados corretos em grande parte e a qualidade dos dados é justa. Por exemplo, sua organização pode estar começando a adicionar logs do Sysmon, ETW, logs do PowerShell e assim por diante. No entanto, a detecção de ameaça ainda não é em tempo real. Sua organização pode não ter todas as ferramentas certas para agregar e analisar os dados com eficácia. Os Caçadores devem executar consultas manualmente e correlacionar para analisar os dados com precisão. O número de falsos positivos é alto.
Bom	3	Detecção em tempo real que correlaciona e integra vários dados em seus endpoints. A detecção de ameaças cobre muitos aspectos dos procedimentos de uma técnica. Seus adversários podem ignorar a detecção com evasão e ofuscação. Sua organização pode identificar facilmente falsos positivos e filtrá-los. Sua organização usa técnicas básicas de ciência de dados para analisar os dados no repositório central.
Muito Bom	4	Detecte com eficácia técnicas mal-intencionadas em tempo real e cubra a maioria dos aspectos dos procedimentos de uma técnica. A possibilidade de seus adversários ignorarem a detecção com métodos de evasão e ofuscação é mais difícil

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definição de pontuação

Pontuação	Mapeamento de pontuação	Descrição
		do que no nível Bom. Sua organização pode identificar facilmente falsos positivos e filtrá-los. Sua organização usa técnicas avançadas de ciência de dados para detectar as técnicas do adversário.
Excelente	5	Detecte com eficácia técnicas mal-intencionadas em tempo real e cubra todos os aspectos dos procedimentos de uma técnica. Sua organização tem uma boa compreensão do seu ambiente com a automação e a qualidade dos dados corretas. A possibilidade de seus adversários ignorarem a detecção com métodos de evasão e ofuscação não é possível neste nível. O número de falsos negativos é baixo.

Mapear a cobertura de detecção da sua técnica para uma técnica

Mapeie sua cobertura geral de detecção de técnica com a técnica que permite que sua organização detecte técnicas adversas específicas.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: acesso de gravação
- Função necessária: sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar a cobertura de detecção de técnica para obter uma visão geral da cobertura geral de detecção de técnica da sua organização. Por exemplo, se um adversário estiver atacado sua organização, você verá o tipo de cobertura que tem para detectar as técnicas do invasor.

A técnica e o ID são preenchidos automaticamente para todas as coleções e técnicas que você ativou. O tipo de cobertura e a definição de pontuação que você definiu estão disponíveis para como uma opção que você pode selecionar na cobertura geral de detecção de técnica.

Você pode mapear a cobertura geral de detecção da técnica com a técnica para concluir o mapeamento. Você pode associar uma técnica a apenas uma cobertura de detecção de técnica geral.

O mapeamento de cobertura de detecção de técnica que você define é usado na visualização de cobertura no mapa térmico.

Nota:
Você pode chegar à cobertura geral de detecção da técnica usando cálculos específicos da sua organização. Você pode usar qualquer produto de Simulação de violação e ataque (BAS), o Repositório de análise cibernética (CAR) ou qualquer outro método conforme necessário para definir a definição de pontuação e usá-lo neste procedimento para o mapeamento geral da cobertura de detecção de técnica.

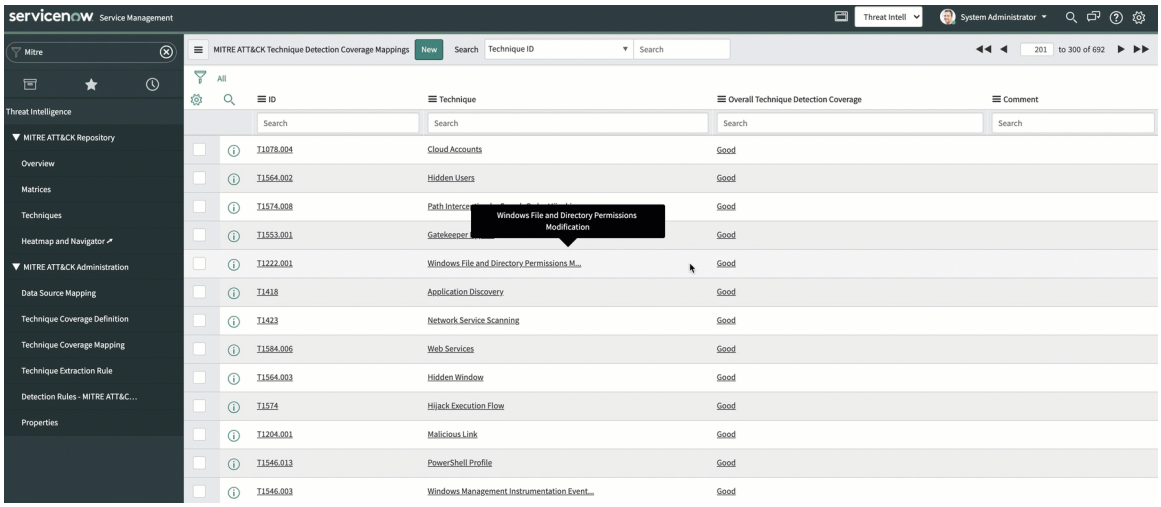
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Mapeamento de cobertura de detecção**.

   Nesta ilustração, você vê que a subtécnica Contas em nuvem (T1078.004) tem cobertura excelente na organização e que a Cobertura de detecção da técnica geral está mapeada para **Excelente**.



2. Analise cada técnica e mapeie a cobertura geral de detecção da técnica com base na definição de cobertura de detecção e na disponibilidade de cobertura da organização.

Definir a cobertura de mitigação

Defina a cobertura de mitigação para cada mitigação associada a uma técnica para que você obtenha visibilidade de como sua organização pode impedir os ataques que acontecem devido a uma técnica específica.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- Função necessária: sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

As definições de cobertura de mitigação são usadas no mapeamento geral de cobertura de mitigação e técnica. Você pode usar a cobertura de mitigação do sistema de base. A cobertura de mitigação do sistema de base consiste nos tipos de cobertura Nenhum, Ruim, Justo, Bom, Muito Bom e Excelente. A cobertura de mitigação do sistema de base também está associada a cores predefinidas e porcentagens de cobertura. Você pode personalizar os tipos de cobertura (adicionar ou remover tipos de cobertura), porcentagens de cobertura para limites inferiores e limites superiores e cores ou criar sua cobertura de mitigação personalizada.

As personalizações feitas nos tipos de cobertura, cores ou porcentagens são usadas no mapeamento de cobertura de mitigação e também no mapa térmico.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Definição de cobertura de mitigação**.
2. Revise as entradas de detecção de mitigação e personalize as entradas para o seu ambiente.

Tradução automática

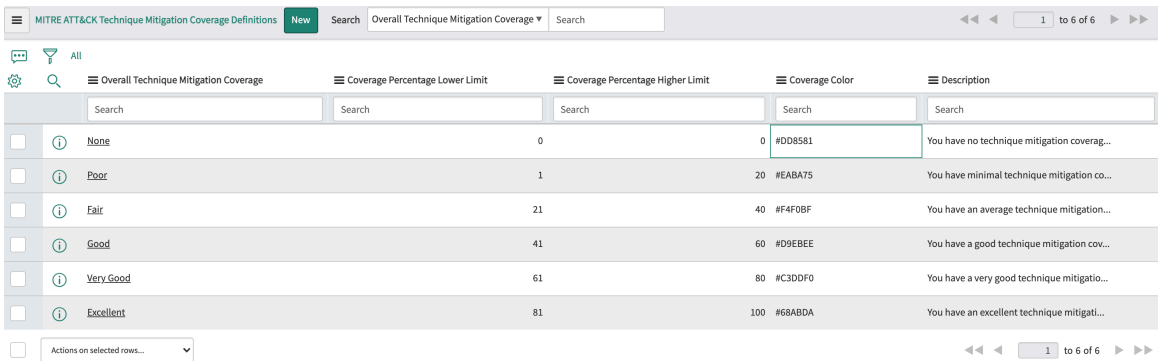
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definição de cobertura de mitigação de técnica

Campo	Descrição
Cobertura geral de mitigação da técnica	Nome da cobertura de mitigação da técnica. A cobertura de mitigação do sistema de base consiste em Nenhum, Ruim, Justo, Bom, Muito Bom ou Excelente.
Limite inferior do percentual de cobertura	O limite inferior da porcentagem da cobertura de mitigação. Defina os valores numéricos entre 0 e 100.
Limite superior do percentual de cobertura	O limite percentual mais alto da cobertura de mitigação. Defina os valores numéricos entre 0 e 100.
Cor de cobertura	Cor atribuída à pontuação de cobertura de detecção. A cor que você define é usada para a cobertura de mitigação da técnica no mapa térmico. Você pode personalizar as cores usando códigos HEX e valores RGB(A).
Descrição	Cobertura geral de detecção de mitigação. Consulte a definição do sistema de base na definição de abrangência de mitigação da técnica.

Nota:
Certifique-se de não sobrepor os intervalos de porcentagem de cobertura ao personalizar os limites de porcentagem (inferior ou superior). Por exemplo, se um registro de cobertura tiver os intervalos de 0 a 20, o próximo registro consecutivo deverá ter o intervalo de limite inferior de 21 ou superior para evitar a sobreposição do intervalo de porcentagem de cobertura.

A ilustração a seguir mostra a lista de definição de cobertura de mitigação.



3. Para adicionar uma entrada, clique em **Novo**, conclua as entradas e clique em **Enviar**.

Definições de cobertura de mitigação de técnica

Defina a cobertura de mitigação da sua organização para que você possa medir e detectar com eficácia técnicas de adversários específicas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definições de cobertura de mitigação da técnica MITRE ATT&CK

Cobertura geral de mitigação da técnica	Limite inferior do percentual de cobertura	Limite superior do percentual de cobertura	Cor de cobertura	Descrição
Nenhum(a)	0	0	#DD8581	Você não tem cobertura de mitigação de técnica e seus controles de defesa não têm a capacidade de impedir um ataque em qualquer cenário.
Ruim	1	20	#EABA75	Você tem cobertura mínima de mitigação de técnica. As chances de um ataque são muito altas e seus controles de defesa podem impedir um ataque em 0 a 20 por cento dos cenários.
Justo	21	40	#F4F0BF	Você tem uma cobertura média de mitigação de técnica. As chances de um ataque são altas e seus controles de defesa podem impedir um ataque em 21 a 40 por cento dos cenários.
Bom	41	60	#D9EBEE	Você tem uma boa cobertura de mitigação de técnica. No entanto, as chances de um ataque são relativamente altas e seus controles de defesa podem impedir um ataque em 41 a 60 por cento dos cenários.
Muito Bom	61	80	#C3DDF0	Você tem uma cobertura de mitigação de técnica muito boa. As chances de um

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definições de cobertura de mitigação da técnica MITRE ATT&CK

Cobertura geral de mitigação da técnica	Limite inferior do percentual de cobertura	Limite superior do percentual de cobertura	Cor de cobertura	Descrição
				ataque são baixas e seus controles de defesa podem impedir um ataque em 61 a 80 por cento dos cenários.
Excelente	81	100	#68ABDA	Você tem uma excelente cobertura de mitigação de técnica e as chances de um ataque usando essa técnica são muito baixas e seus controles de defesa podem impedir um ataque em 81 a 100 por cento dos cenários.

Mapear sua cobertura de mitigação para uma técnica

Mapeie sua cobertura de mitigação com a técnica que permite detectar a estratégia de mitigação geral da sua organização.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: acesso de gravação, exclusão
- Função necessária: sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

As mitigações permitem impedir que um adversário execute técnicas ou subtécnicas com êxito na sua organização. Cada técnica MITRE-ATT&CK contém mitigações que você pode implantar em sua organização para reduzir a chance de ser atacado. Você pode usar a cobertura de mitigação para obter uma visão geral da estratégia de mitigação geral da sua organização. Por exemplo, se um adversário estiver enfrentando um ataque à sua organização, você verá o tipo de cobertura que tem para atenuar as técnicas do invasor.

A técnica e as informações de mitigação são preenchidas automaticamente para todas as coleções e técnicas que você ativou. A definição de cobertura de mitigação que você definiu está disponível para seleção na cobertura de mitigação da técnica.

Você pode identificar mitigações que são relevantes para sua organização. Se uma mitigação for relevante, você poderá definir se as estratégias de mitigação foram implantadas. Você pode especificar se as estratégias são aplicadas como parte da Política SOC da sua organização. Você também pode identificar se sua organização possui ferramentas preventivas para atenuar as técnicas de um invasor e mapear todos os controles de segurança que sua organização implantou para minimizar os riscos à segurança. Preencha a cobertura de mitigação (porcentagem) para cada um dos registros.

Depois de mapear as informações para cada uma das técnicas, a calculadora de cobertura de mitigação preenche automaticamente a Cobertura de mitigação da técnica calculada. Para

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

calcular a cobertura de mitigação geral para qualquer técnica, os registros de mapeamento de mitigação de técnica devem estar ativos e relevantes para a organização. Os registros que estão inativos e não relevantes não são considerados para o cálculo da cobertura geral de mitigação da técnica. Com base nos valores da Cobertura de mitigação da técnica calculada e na definição da coberturade mitigação, sua Cobertura de mitigação da técnica geral (calculada) é preenchida.

As personalizações feitas nos tipos de cobertura, cores ou porcentagens são usadas no mapeamento de cobertura de mitigação e também no mapa térmico.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Mapeamento de cobertura de mitigação**.
2. Analise cada técnica para o mapeamento de mitigação e atualize a **Cobertura de mitigação (percentual)** para calcular a disponibilidade de cobertura da sua organização.

Mapeamentos de cobertura de mitigação de técnica

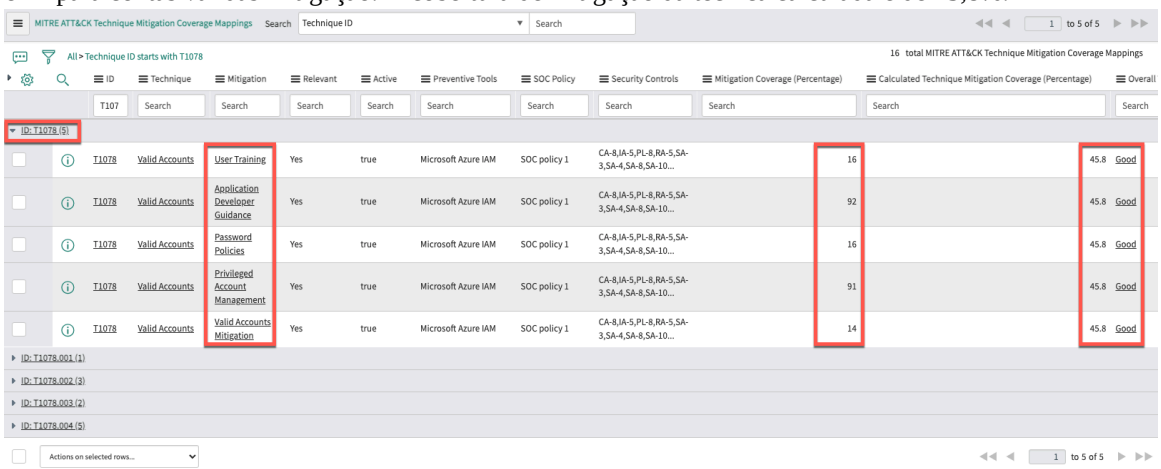
Campo	Descrição
ID	Identidade exclusiva da técnica. Os IDs são preenchidos automaticamente para todas as coleções e técnicas que você ativou.
Técnica	Como um adversário atinge um objetivo tático executando uma ação. As informações da técnica são preenchidas automaticamente para todas as coleções e técnicas que você ativou.
Mitigação	Mitigações que permitem impedir que um adversário execute técnicas ou subtécnicas com êxito na sua organização. As informações de mitigação são preenchidas automaticamente para todas as coleções e técnicas que você ativou.
Relevante	Opção para especificar se a mitigação é relevante para sua organização.
Ativo	Opção para especificar se as estratégias de mitigação são implantadas em sua organização. Esta é uma opção necessária para calcular a cobertura de mitigação da técnica.
Ferramentas preventivas	Opção para especificar se sua organização tem ferramentas preventivas para atenuar as técnicas de um invasor.
Política de SOC	As políticas SOC que definem as estratégias de mitigação em sua organização.
Controles de segurança	Os controles de segurança da sua organização contêm as estratégias de mitigação para minimizar os riscos à segurança.
Cobertura de mitigação (percentual)	Um sistema de pontuação para calcular a cobertura de mitigação da técnica. Defina valores numéricos entre 0 e 100. Esta é uma opção necessária para calcular a cobertura de mitigação da técnica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Cobertura de mitigação da técnica calculada (percentual)	A cobertura de mitigação da técnica calculada em porcentagem. Este valor é determinado com base na fórmula definida na calculadora de cobertura de mitigação.
Cobertura geral de mitigação da técnica (calculada)	A cobertura geral de mitigação da técnica. Este valor é determinado com base na cobertura de mitigação definida para sua organização.
Comentário	Descrição sobre a técnica e o mapeamento de cobertura de mitigação.
Revogado	A técnica para mapeamento de cobertura de mitigação foi revogada.

Nesta ilustração, você vê que a técnica Contas válidas tem cinco mitigações associadas, cada uma com uma cobertura de mitigação de 16 para treinamento do usuário, 92 para orientação de desenvolvedor de aplicações e 16 para políticas de senha, 91 para gestão de contas privilegiadas e 14 para contas válidas mitigação. A cobertura de mitigação da técnica calculada é de 45,8%.



Calculadora de cobertura de mitigação de técnica geral

A cobertura geral de mitigação da técnica é determinada com base na fórmula definida na calculadora de cobertura de mitigação.

Antes de Iniciar

- Função necessária: sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- Função necessária: sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

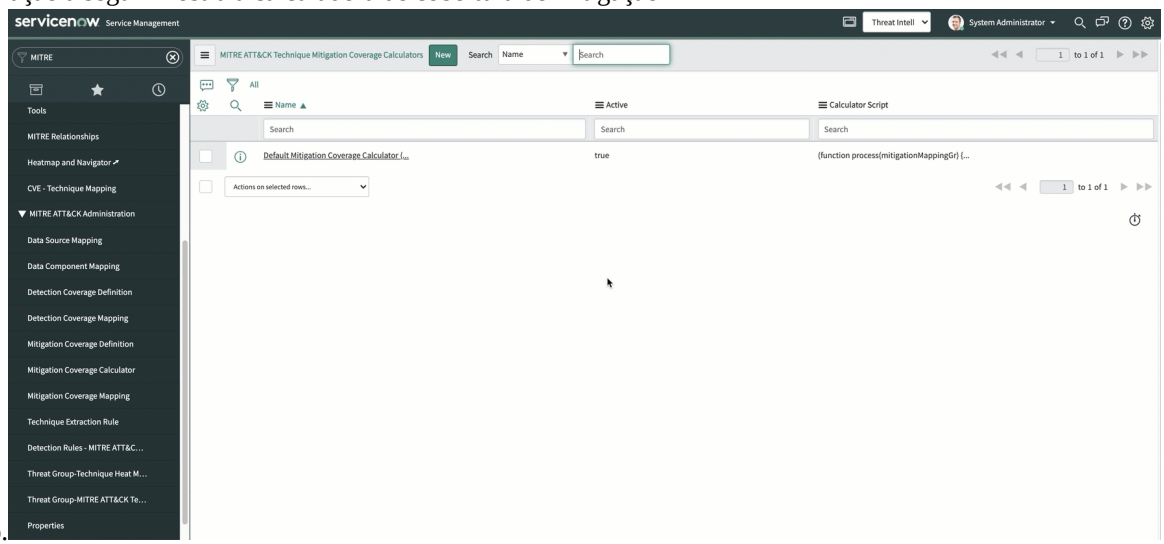
- Você pode definir como ativa apenas uma calculadora de cobertura de mitigação por domínio.
- A calculadora de cobertura de mitigação do sistema de base é uma calculadora média.
- Todas as personalizações do script da calculadora devem garantir que a saída final seja um valor numérico entre 0 e 100.
- A definição de cobertura de mitigação é aplicada com base no intervalo da saída final.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Calculadora de cobertura de mitigação**.
A ilustração a seguir mostra a calculadora de cobertura de mitigação padrão.



Criar e mapear regras de detecção

Crie regras de detecção e mapeie-as em relação às táticas e técnicas. Com este mapeamento, você pode ver a cobertura das regras de detecção em sua organização.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

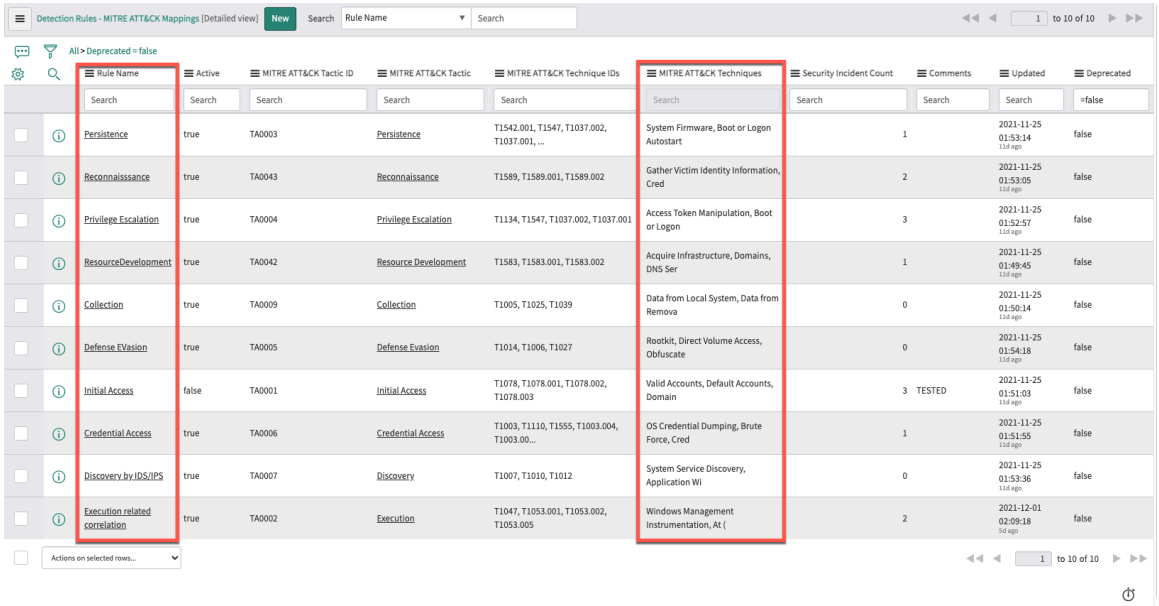
O mapeamento de regra de detecção permite que sua organização veja quais regras de detecção estão disponíveis para identificar técnicas específicas.

O objetivo primário do mapeamento é fornecer visibilidade se sua organização tiver as regras de detecção necessárias para identificar quando um alerta ou evento for acionado como resultado de um ataque de um adversário usando uma técnica específica.

Por exemplo, exiba a ilustração a seguir que mostra uma lista das regras de detecção mapeadas para várias técnicas. Você também pode exibir essas informações em o MITRE-ATT&CK navegador.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Se você não pretende usar as regras de extração automática do SIEM do sistema de base, habilite o acúmulo automático de MITRE-ATT&CK TTPs com base no mapeamento da regra de detecção. Você pode preencher o alerta ou a regra de evento que aciona o incidente de segurança no campo Nome da regra de alerta. Você também pode preencher o campo Nome da regra de alerta usando a integração de SIEM, a análise de e-mail, a criação manual etc. Para obter mais informações, consulte Informações de acúmulo MITRE-ATT&CK das regras de detecção.

Nota:

O recurso de regras de detecção foi atualizado para incluir o mapeamento de uma única tática para várias técnicas. Anteriormente, você poderia mapear uma única tática com uma única técnica. Se você estiver atualizando o plug-in Inteligência contra ameaças da versão 12.0.4 para uma versão superior, revise os pontos a seguir antes de usar as regras de detecção no módulo MITRE-ATT&CK.

- Você encontrará vários registros mesclados em um único registro se os campos - nome da regra, sensor de alerta, origem, categoria, subcategoria e MITRE-ATT&CK tática forem comuns.
- Os registros antigos são marcados como verdadeiros na coluna obsoleta e falsos na coluna ativa.
- Os novos registros mesclados estão disponíveis para uso e são marcados como falsos na coluna obsoleta e verdadeiros na coluna ativa.
- Depois de verificar a atualização e exibir que todas as suas regras de detecção foram migradas com sucesso, você pode excluir os registros antigos que estão marcados como verdadeiros na coluna obsoleta.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Regras de detecção — Mapeamentos MITRE ATT&CK**.
2. Use um dos seguintes métodos para criar sua regra de detecção:
   Método 1: crie regras de detecção manualmente.

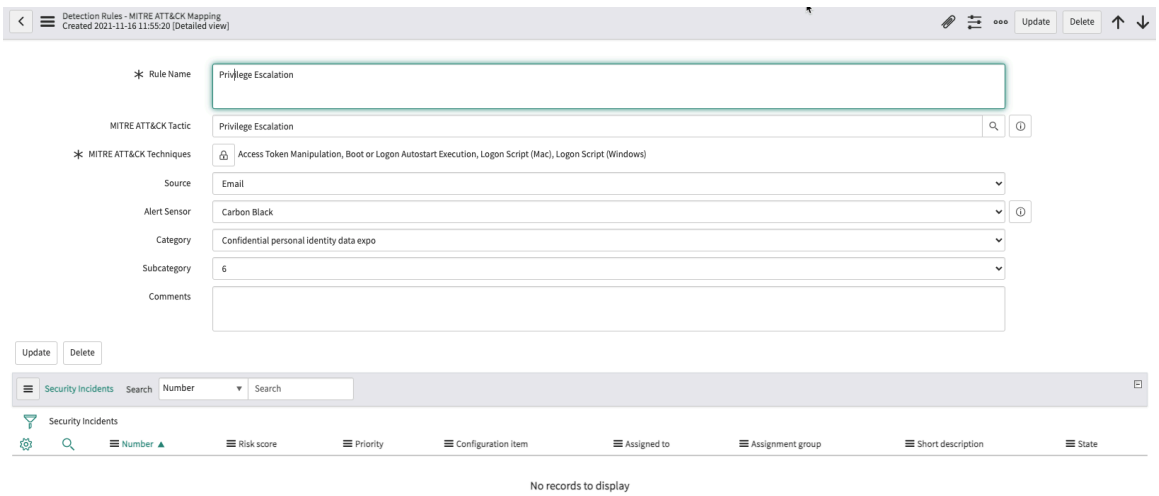
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Clique em **Novo** e preencha os campos no formulário.

Regras de detecção - Mapeamento MITRE-ATT&CK

Campo	Descrição
Nome de Regra	Nome da regra de detecção.
MITRE-ATT&CK Tática	Relevante MITRE-ATT&CK tática.
MITRE-ATT&CK Técnicas	Relevante MITRE-ATT&CK técnica. Você pode selecionar várias técnicas para uma única tática.
Fonte	Origem do incidente de segurança, como e-mail, firewall, monitoramento de rede e assim por diante.
Sensor de alerta	Integração de segurança por meio da qual você ingere os dados de alerta ou evento, como Carbonblack, CrowdStrike, McAfee e assim por diante.
Subcategoria	Subcategoria que define ainda mais o problema.
Categoria	Categoria que identifica o tipo de problema de segurança.
MITRE-ATT&CK Técnica	Relevante MITRE-ATT&CK técnica. Você pode selecionar várias técnicas para uma única tática.
Contagem de incidentes de segurança	O número de incidentes de segurança aos quais as técnicas são anexadas. Essa contagem aparece quando você habilita o acúmulo de MITRE-ATT&CK informações automaticamente de regras de alerta para incidentes de segurança.
Preterido	O mapeamento da regra de detecção está obsoleto.
Ativo	Opção para especificar se a regra de detecção está ativa e implantada em seu ambiente.



b. Clique em **Enviar**.

Método 2: importe e crie regras de detecção.

a. Clique com o botão direito do mouse no cabeçalho da coluna Nome da regra.

b. Na lista, clique em **Importar**.

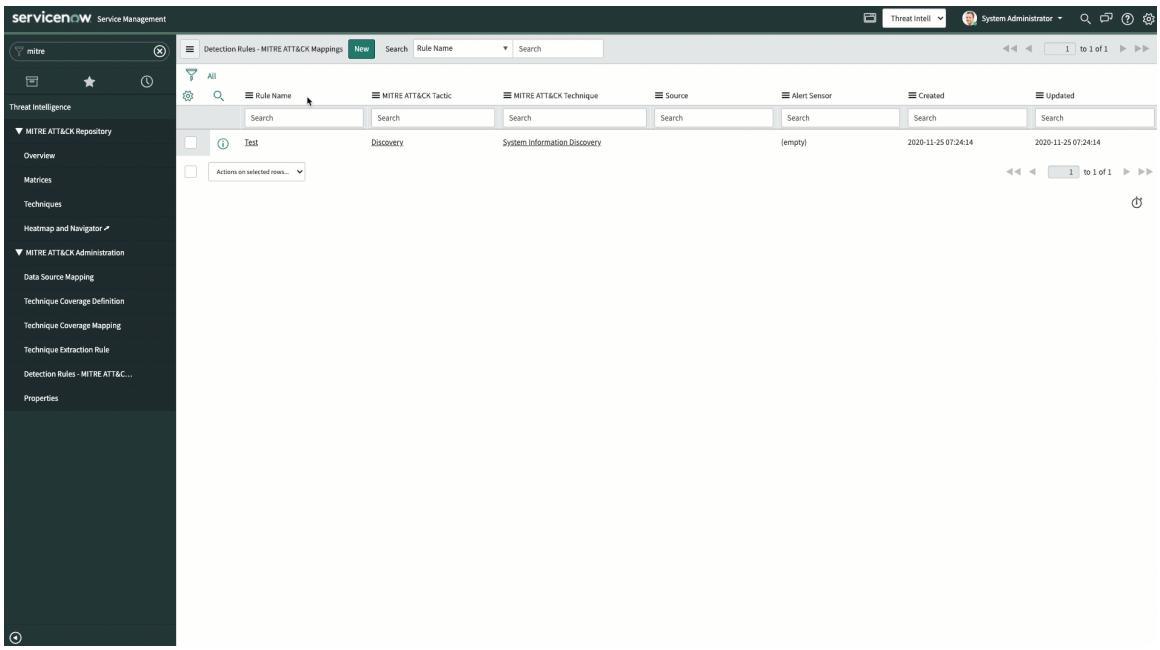
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

c. Clique **em Criar modelo do Excel**.

d. Clique em **Download** após a conclusão da exportação. Um modelo do Excel com o nome de arquivo sn_ti_alert_rules_mitre_attack_technique_mapping é baixado para o seu computador.

Na ilustração a seguir, você vê como exportar o modelo do Excel, preencher os detalhes na planilha, carregar o arquivo, visualizar os campos e importá-lo de volta para o Now Platform.



e. Abra a planilha, selecione a segunda guia da planilha e revise o que você inseriu. No formulário, preencha os campos e salve o arquivo.

Importar modelo

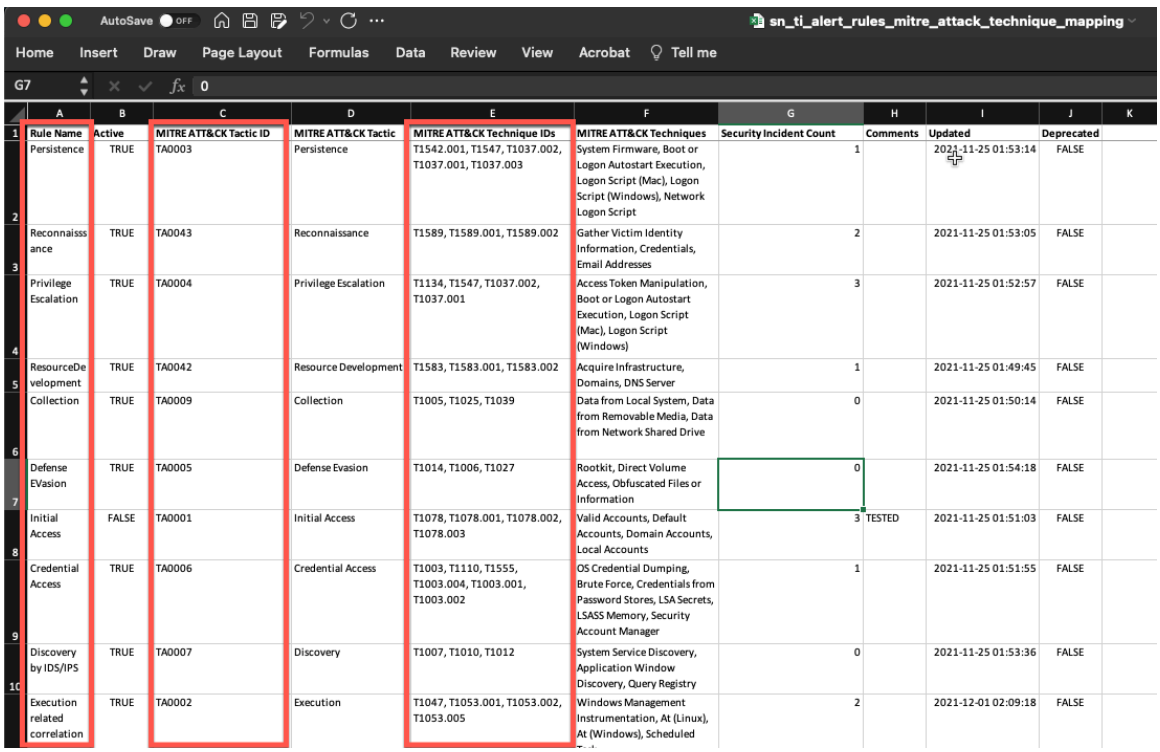
Campo	Descrição
Nome de Regra	Nome da regra de detecção.
Ativo	Opção para especificar se a regra de detecção está ativa e implantada em seu ambiente.
Sensor de alerta	Integração de segurança por meio da qual você ingere os dados de alerta ou evento, como Carbonblack, CrowdStrike, McAfee e assim por diante.
Categoria	Categoria que identifica o tipo de problema de segurança.
Comentários	Descrição sobre a regra de detecção.
Preterido	O mapeamento da regra de detecção está obsoleto.
MITRE-ATT&CK IDs de técnica	MITRE-ATT&CK ID de técnica, como T1546.008, para Recursos de acessibilidade.
MITRE-ATT&CK ID da tática	MITRE-ATT&CK ID de tática, como TA0003, para Persistência.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Contagem de incidentes de segurança	O número de incidentes de segurança aos quais as técnicas são anexadas. Esta contagem aparece quando você habilitou o acúmulo de MITRE-ATT&CK informações automaticamente de regras de alerta para incidentes de segurança e a regra de detecção está ativa.
Fonte	Origem do incidente de segurança, como e-mail, firewall, monitoramento de rede e assim por diante.
Subcategoria	Subcategoria que define ainda mais o problema.
MITRE-ATT&CK Tática	Relevante MITRE-ATT&CK tática.
MITRE-ATT&CK Técnica	Relevante MITRE-ATT&CK técnica.

A ilustração a seguir mostra o modelo de planilha. Os campos obrigatórios são destacados em vermelho - Nome da regra, MITRE-ATT&CK ID da tática e MITRE-ATT&CK ID da técnica.



Rule Name	Active	MITRE ATT&CK Tactic ID	MITRE ATT&CK Tactic	MITRE ATT&CK Technique IDs	MITRE ATT&CK Techniques	Security Incident Count	Comments	Updated	Deprecated
Persistence	TRUE	TA0003	Persistence	T1542.001, T1547, T1037.002, T1037.001, T1037.003	System Firmware, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows), Network Logon Script	1		2021-11-25 01:53:14	FALSE
Reconnaissance	TRUE	TA0043	Reconnaissance	T1589, T1589.001, T1589.002	Gather Victim Identity Information, Credentials, Email Addresses	2		2021-11-25 01:53:05	FALSE
Privilege Escalation	TRUE	TA0004	Privilege Escalation	T1134, T1547, T1037.002, T1037.001	Access Token Manipulation, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows)	3		2021-11-25 01:52:57	FALSE
ResourceDevelopment	TRUE	TA0042	Resource Development	T1583, T1583.001, T1583.002	Acquire Infrastructure, Domains, DNS Server	1		2021-11-25 01:49:45	FALSE
Collection	TRUE	TA0009	Collection	T1005, T1025, T1039	Data from Local System, Data from Removable Media, Data from Network Shared Drive	0		2021-11-25 01:50:14	FALSE
Defense EVasion	TRUE	TA0005	Defense Evasion	T1014, T1006, T1027	Rootkit, Direct Volume Access, Obfuscated Files or Information	0		2021-11-25 01:54:18	FALSE
Initial Access	FALSE	TA0001	Initial Access	T1078, T1078.001, T1078.002, T1078.003	Valid Accounts, Default Accounts, Domain Accounts, Local Accounts	3	TESTED	2021-11-25 01:51:03	FALSE
Credential Access	TRUE	TA0006	Credential Access	T1003, T1110, T1555, T1003.004, T1003.001, T1003.002	OS Credential Dumping, Brute Force, Credentials from Password Stores, LSA Secrets, LSASS Memory, Security Account Manager	1		2021-11-25 01:51:55	FALSE
Discovery by IDS/IPS	TRUE	TA0007	Discovery	T1007, T1010, T1012	System Service Discovery, Application Window Discovery, Query Registry	0		2021-11-25 01:53:36	FALSE
Execution related correlation	TRUE	TA0002	Execution	T1047, T1053.001, T1053.002, T1053.005	Windows Management Instrumentation, At (Linux), At (Windows), Scheduled	2		2021-12-01 02:09:18	FALSE

f. Clique **em Escolher arquivo** e selecione a planilha no seu computador.

g. Clique em **Carregar**.

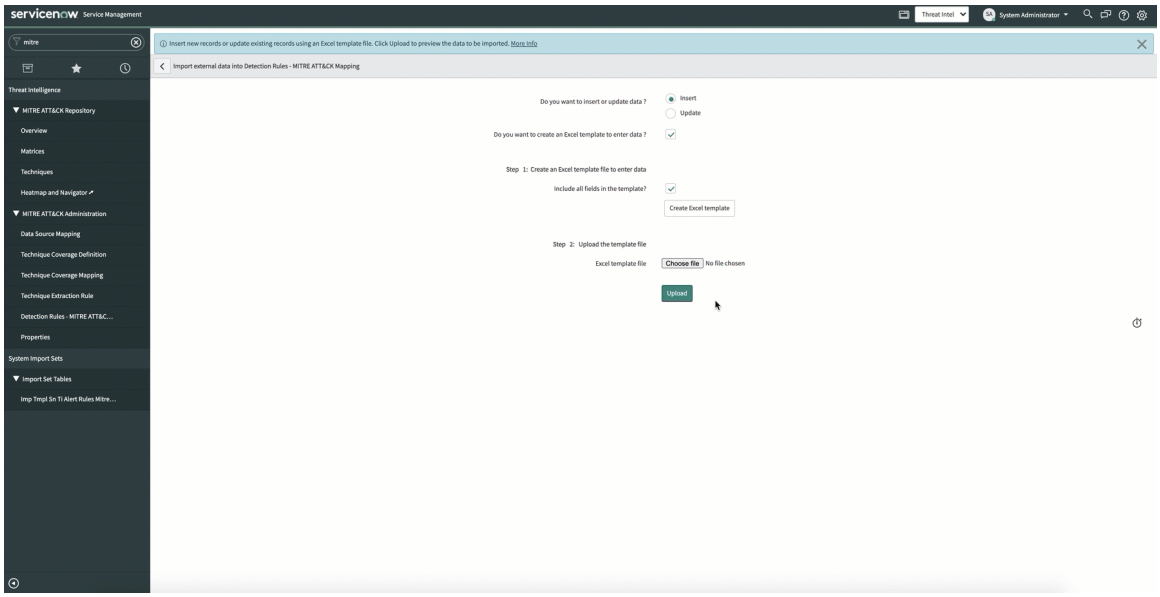
h. Clique **em Visualizar dados importados**.

i. Visualize os mapeamentos e clique em **Concluir importação**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ilustração a seguir mostra como carregar a planilha, visualizar os dados, revisar quaisquer erros e concluir o processo de importação de mapeamento de regra de detecção.



Regras de técnica de extração automática para importar informações de MITRE-ATT&CK

Use as regras de extração automática do sistema de base para importar as informações MITRE-ATT&CK de quaisquer integrações de terceiros existentes.

Usar regras de extração automática de pesquisa de ameaças

Use as regras de extração automática de pesquisa de ameaças para importar as informações MITRE-ATT&CK de quaisquer integrações de terceiros Inteligência contra ameaças existentes.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

Quando qualquer integração Inteligência contra ameaças, como Sandbox ou um TIP, oferece suporte à estrutura MITRE-ATT&CK e se as informações MITRE-ATT&CK forem analisadas em cada nível de integração, as informações serão exibidas em cada registro de resultado de pesquisa de ameaça. No entanto, nem todas as integrações Inteligência contra ameaças analisam as informações MITRE-ATT&CK. A regra de extração automática global de pesquisa de ameaças pode extrair MITRE-ATT&CK informações de todas as Inteligência contra ameaças integrações.

Você pode optar por acumular as informações MITRE-ATT&CK automaticamente dos resultados da pesquisa de ameaças para um incidente de segurança. Para acúmulo automático de resultados de pesquisa de ameaças para incidentes de segurança, habilite a propriedade do sistema. Como alternativa, você pode acumular as informações manualmente para cada pesquisa de ameaça individual.

O sistema de base Inteligência contra ameaças extrai automaticamente as MITRE-ATT&CK informações da carga bruta de integrações de terceiros para o registro de resultado de

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

pesquisa de ameaças, se a integração Inteligência contra ameaças fornecer MITRE-ATT&CK informações como a técnica ou tática.

Se as informações de MITRE-ATT&CK não estiverem disponíveis no campo de carga bruta do registro de pesquisa de ameaças, você deverá definir sua própria regra para extração automática da integração de terceiros.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Regra de extração da técnica**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de extração de técnica

Campo	Descrição
Nome	Nome da regra de extração automática.
Tipo de Regra	Tipo de regra de extração automática. Selecione **Pesquisa de ameaças**.
Ignorar extração automática	Configuração que, por padrão, está desmarcada. Esta configuração permite a extração automática de MITRE-ATT&CK técnicas.
Mecanismo de Origem	Mecanismo de origem.
Global	Configuração do mecanismo de origem. Quando você define o mecanismo de origem como **Global**, a extração é executada em todos os resultados de integração de pesquisa de ameaças.
Descrição	Descrição da regra de extração automática.
Método de processo	Regex ou um método de script que você especifica para vincular as informações da técnica da carga bruta.
Extração de Regex	Opção que você especifica para o **Campo de destino** ao usar o método de extração regex. Regex é o padrão.
Extração de script	Processo que você seleciona ao executar um script. O script revisa o seguinte: ○ ThreatLookupResultSysId:sys_id do registro do resultado da pesquisa de ameaças ○ sourceName: nome da origem da pesquisa de ameaças.
Extração de tática	Opção que você especifica para extrair informações relacionadas à tática da carga bruta. Se uma carga útil contiver informações relacionadas a táticas e

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	técnicas específicas, você poderá extrair e anexar as informações ao incidente de segurança.

4. Clique em **Enviar**.

Usar regras de extração automática do SIEM

Use as regras de extração automática do SIEM para importar as informações MITRE-ATT&CK de quaisquer integrações de terceiros do SIEM Security Operations existentes.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura

Por Que e Quando Desempenhar Esta Tarefa

A regra de extração de técnica está disponível para todas as integrações de SIEM do sistema de base Security Operations, como Splunk, IBM QRadar e integrações de ArcSight. Quando o Now Platform ingere dados de alerta ou evento dessas integrações de SIEM e eles contêm informações MITRE-ATT&CK, o Now Platform processa a carga útil bruta e extrai automaticamente as informações MITRE-ATT&CK.

Se o seu Now Platform contém integrações de SIEM do sistema de base, isso significa que as regras de extração de técnica já foram criadas no módulo MITRE-ATT&CK. Você deve revisar e modificar as regras conforme necessário.

Habilite a regra de extração automática do SIEM ou a regra de alerta de cada vez.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Regra de extração da técnica**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

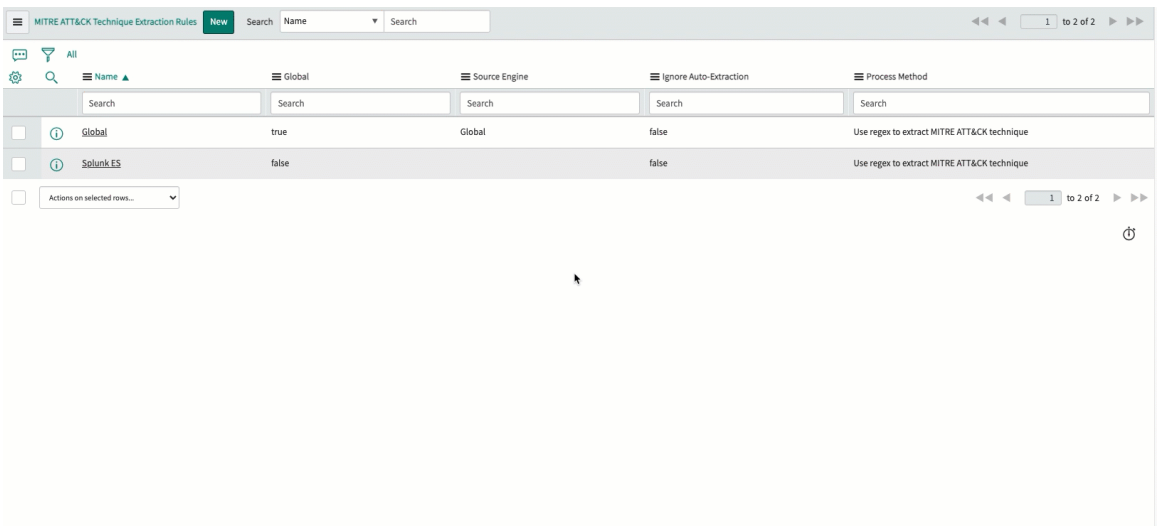
Formulário Regra de extração de técnica

Campo	Descrição
Nome	Nome da regra de extração automática.
Tipo de Regra	Tipo de regra de extração automática. Selecione **SIEM**.
Ignorar extração automática	Configuração que por padrão está desmarcada. Esta configuração permite a extração automática de MITRE-ATT&CK técnicas.
Importar Tabela	Tabela de importação que é mapeada automaticamente para integrações de SIEM do sistema de base. Revise este campo para outras integrações de SIEM para as informações de MITRE-ATT&CK e mapeie de acordo.
Importar campo	Campo de importação que é mapeado automaticamente para integrações de SIEM do

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	sistema de base. Revise este campo para outras integrações de SIEM para as informações de MITRE-ATT&CK e mapeie de acordo.
Descrição	Regra de extração automática.
Método de processo	Regex ou um método de script que você especifica para vincular as informações da técnica da carga bruta.
Extração de Regex	Opção que você especifica para o **Campo de destino** ao usar o método regex. A extração de regex é o método de processo padrão.
Extração de script	Método de processo de script que você usa se quiser personalizar como as informações de MITRE-ATT&CK são extraídas.
Extração de tática	Opção que você especifica para extrair informações relacionadas à tática da carga bruta. Se uma carga útil contiver informações relacionadas a táticas e técnicas específicas, você poderá extrair e anexar as informações ao incidente de segurança.

Na ilustração a seguir, você vê um exemplo da regra de extração da técnica SIEM Splunk Enterprise na exibição de formulário. Esta regra é semelhante a todas as outras regras de extração de técnica de SIEM.



4. Clique em **Enviar**.

Analisar o grupo de ameaças e o mapeamento de técnicas MITRE-ATT&CK

Analise o grupo de ameaças e as informações de mapeamento de objeto para objeto de técnicas que são importadas das coleções MITRE TAXII. Este mapeamento permite que você exiba o grupo de técnicas e o mapeamento de técnica correspondente.

Antes de Iniciar
Função necessária:

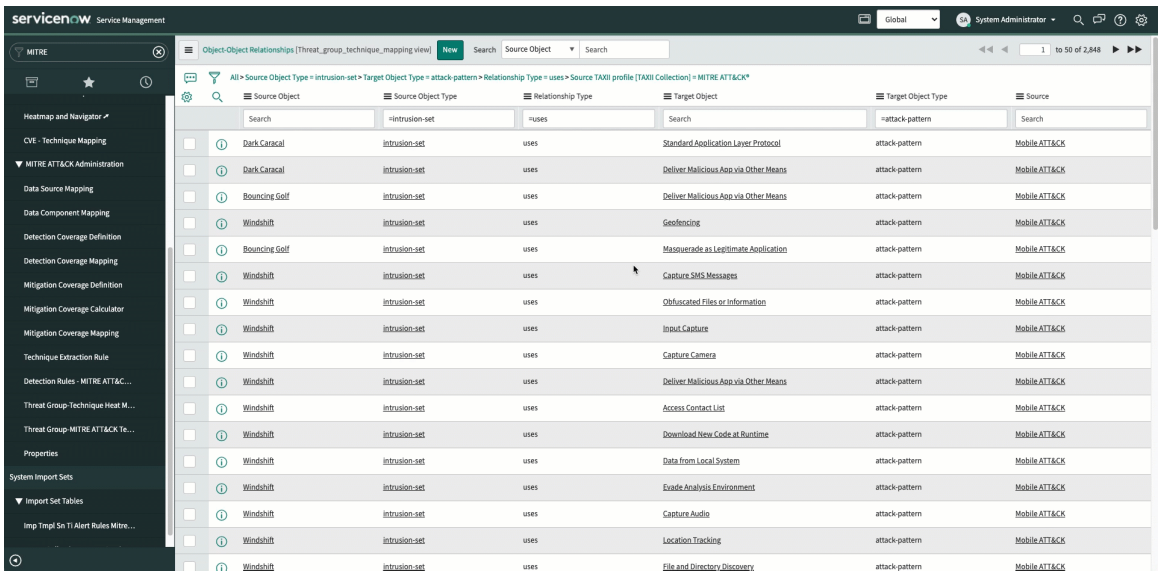
- sn_ti.admin, sn_si.admin: criar, gravar, excluir acesso
- sn_ti.read: acesso de leitura

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Grupo de ameaças - Técnicas MITRE ATT e CK**.
2. Clique com o botão direito do mouse no **Objeto de origem** e selecione **Agrupar por objeto de origem** para exibir todos os padrões de ataque associados a um grupo de ameaça.

   A ilustração a seguir mostra o grupo de ameaças admin@338 e os vários padrões de ataque adotados por esse grupo de ameaças que fazem parte da origem de ataque da empresa.



Grupo de ameaças para definição de mapa térmico de técnica

Defina o grupo de ameaças para a definição do mapa térmico da técnica para que, no mapa térmico, você possa medir e detectar os padrões de ataque que os grupos de ameaças estão usando para atacar sua organização. A probabilidade de um ataque usando uma técnica específica aumenta quando você tem um número alto de invasores.

Antes de Iniciar

Função necessária:

- sn_ti.admin, sn_si.admin: acesso de gravação
- sn_ti.read: acesso de leitura

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Definição do mapa térmico da técnica de grupo de ameaças**.
2. Revise o grupo de ameaças para a definição do mapa térmico da técnica e personalize as entradas para o seu ambiente.

Definições do mapa térmico da técnica de grupo de ameaças

Campo	Descrição
Número de grupos de ameaças (intervalo mínimo)	O número mínimo de grupos de ameaças que usam uma técnica específica.

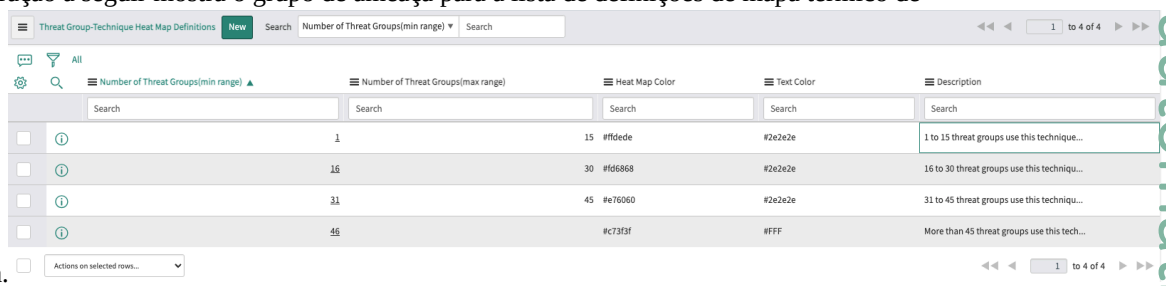
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Número de grupos de ameaças (intervalo máximo)	O número máximo de grupos de ameaças que usam uma técnica específica. A probabilidade de um ataque usando uma técnica específica aumenta quando você tem um número alto de invasores.
Cor do mapa térmico	Cor atribuída à categoria de grupo de ameaça. A cor que você define é usada para realçar a categoria do grupo de ameaça no mapa térmico. Você pode personalizar as cores usando códigos HEX e valores RGB(A).
Cor do texto	Cor atribuída ao texto do grupo de ameaça. A cor que você define é usada para realçar os grupos de ameaça no mapa térmico. Você pode personalizar as cores usando códigos HEX e valores RGB(A).
Descrição	Descrição sobre o intervalo e a definição do grupo de ameaça.

Nota:
Certifique-se de não sobrepor os intervalos de contagem do grupo de ameaça se você personalizar o intervalo do grupo de ameaça (mínimo ou máximo).

A ilustração a seguir mostra o grupo de ameaça para a lista de definições de mapa térmico de técnica.



3. Para adicionar uma entrada, clique em **Novo**, conclua as entradas e clique em **Enviar**.

Revise as propriedades do sistema MITRE-ATT&CK

Revise os valores de propriedade do sistema MITRE-ATT&CK.

Antes de Iniciar

Função necessária: sn_ti.admin, sn_si.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração do MITRE ATT&CK** > **Propriedades**.
2. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

MITRE-ATT&CK Formulário Propriedades

Campo	Descrição
Acumular informações do MITRE ATT&CK automaticamente dos observáveis para o incidente de segurança [sn_ti.rollup_mitre_att&ck_technique_observable_si]	Acúmulo de MITRE-ATT&CK informações de observáveis para o incidente de segurança. Para obter mais informações, consulte Associar informações do MITRE ATT&CK a observáveis. Valor padrão: sim
Agregar informações do MITRE ATT&CK automaticamente dos resultados da Pesquisa de ameaças para o incidente de segurança [sn_ti.rollup_mitre_att&ck_technique_threat_lookup_si]	Acúmulo de MITRE-ATT&CK informações dos resultados da pesquisa de ameaças para o incidente de segurança. Para obter mais informações, consulte Extração automática de pesquisa de ameaças. Valor padrão: sim
Agregar informações do MITRE ATT&CK automaticamente de regras de alerta para incidentes de segurança [sn_ti.rollup_mitre_att&ck_technique_alert_rule_si]	Acúmulo de MITRE-ATT&CK informações de TTP automaticamente de regras de alerta para incidentes de segurança. Para obter mais informações, consulte regras de detecção de mapa. Valor padrão: Não
Agregar informações do MITRE ATT&CK automaticamente de incidentes de segurança secundários para incidentes de segurança primários [sn_ti.rollup_mitre_att&ck_technique_child_si_sa]	Acumule MITRE-ATT&CK informações automaticamente de incidentes de segurança secundários para incidentes de segurança primários. Valor padrão: sim
A habilitação desta propriedade permite o mapeamento de campos de incidente de segurança, como categoria e subcategoria, com regras de detecção na tabela "Regras de detecção - mapeamento MITRE ATT&CK" [sn_ti.enable_category_mapping_with_alert_rule]	Categoria e subcategoria na página de mapeamento Regras de detecção - MITRE ATT&CK. Valor padrão: Não
Tempo (em horas) para calcular "CVE - Contagem de VUL" [sn_ti.time_to_calculate_cve_vits_count]	O tempo programado em horas para calcular as informações de CVE e VUL. Valor padrão: 24

3. Clique em **Salvar**.

Usando MITRE-ATT&CK para detectar e analisar ameaças

Use a estrutura MITRE-ATT&CK] nos módulos Inteligência contra ameaças e SIR para detectar e analisar ameaças à sua organização.

Associar MITRE-ATT&CK™ informações a incidentes de segurança

Associe as MITRE-ATT&CK táticas e técnicas ao incidente de segurança para obter uma melhor análise de incidentes e ameaças de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Adicione as informações de táticas e técnicas de MITRE-ATT&CK ao incidente de segurança para que você possa correlacionar suas informações de incidente de segurança e ameaça para uma melhor análise. Por exemplo, sua organização pode estar recebendo informações relacionadas a táticas, técnicas e procedimentos (TTP) de fontes de terceiros, como Inteligência contra ameaças relatórios ou outras fontes fora de Security Incident Response. Em seguida, você adiciona essas informações de volta a SIR para melhor correlação e análise de ameaças.

Você pode optar por acumular as informações MITRE-ATT&CK automaticamente dos resultados da extração automática de pesquisa de ameaças, de observáveis ou de um incidente de segurança secundário para um incidente de segurança. Para acúmulo automático de incidentes de segurança, habilite a propriedade do sistema. Como alternativa, você pode acumular as informações manualmente para cada pesquisa de ameaça individual ou observável.

Procedimento
1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja aprimorar com as informações de MITRE-ATT&CK.
3. Clique no link relacionado **Associar técnica MITRE ATT&CK**.
   O painel Associar técnica do MITRE ATT&CK é exibido.

   Esta ilustração mostra como navegar até a lista relacionada e procurar Associar MITRE-ATT&CK Técnica, revisar a origem Enterprise ATT&CK, adicionar um impacto de tática e adicionar uma técnica Desligamento/reinicialização do sistema.

   Associar informações do MITRE ao incidente de segurança
4. Selecione **Origem**.

   Nota:
   Somente as coleções e matrizes que foram ativadas aparecem na lista de origem.

   As táticas e técnicas associadas à origem estão disponíveis para seleção. Você também pode associar várias origens.
5. Selecione a **Tática** e as **Técnicas**.
6. **Opcional:** Revise as informações com base na relevância com o incidente de segurança e faça o seguinte:
   - Para remover completamente a associação, clique no ícone de lixeira. Clicar neste ícone exclui a origem e suas táticas e técnicas associadas.
   - Para remover uma tática, clique no ícone de menos ao lado da tática.
   - Para remover uma técnica, clique no ícone x ao lado da técnica.
7. Clique em **Salvar**.

Resultado
As informações de MITRE-ATT&CK estão associadas ao incidente de segurança. Agora você pode exibir as informações associadas no **cartão MITRE ATT&CK**.

Associar MITRE-ATT&CK informações a incidentes de segurança encerrados

Agora você pode associar MITRE-ATT&CK táticas e técnicas aos incidentes de segurança encerrados para obter uma melhor análise de ameaças e incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Associar informações do MITRE ao incidente de segurança

Usando o cartão MITRE-ATT&CK para ver informações relacionadas em um incidente de segurança

Você pode usar o cartão MITRE-ATT&CK para ver as informações relacionadas MITRE-ATT&CK em um incidente de segurança.

Depois que as informações são acumuladas de uma pesquisa de ameaças, um observável ou uma integração de SIEM, elas são adicionadas ao incidente de segurança. Em seguida, as informações agregadas são apresentadas no cartão MITRE-ATT&CK. O **cartão MITRE ATT&CK** fornece duas exibições:

- Exibição do navegador: esta exibição, que é semelhante ao navegador MITRE-ATT&CK, mostra todas as técnicas que foram adicionadas manualmente ou acumuladas das tabelas de pesquisa de observáveis ou ameaças. **Mostrar origem das técnicas** exibe a origem da técnica se ela tiver sido acumulada manualmente ou por meio de uma Origem. **Mostrar ID** exibe o ID da técnica.

  A ilustração a seguir mostra como navegar até a exibição do navegador **de cartão MITRE ATT&CK**. Ao clicar em qualquer um dos links disponíveis, as informações são abertas no módulo Inteligência contra ameaças.

  Cartão MITRE ATT&CK: exibição do navegador e exibição de lista

- Exibição de lista: esta exibição mostra os dados em um formato de lista ou tabela. Você pode ver todos os dados distribuídos em diferentes tabelas e grupos nesta exibição.

  A ilustração a seguir mostra como navegar até a exibição de lista do cartão MITRE ATT&CK. Ao clicar em qualquer um dos links disponíveis, as informações são abertas no módulo Inteligência contra ameaças.

Associar MITRE-ATT&CK informações a observáveis

Associe MITRE-ATT&CK táticas e técnicas a um observável para obter uma melhor análise de incidentes e ameaças de segurança em um nível granular.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Alguns SIEMs podem fornecer MITRE-ATT&CK informações com eventos, alertas ou observáveis. Para associar as informações de MITRE-ATT&CK em um nível granular, você pode adicionar as informações a um observável.

Você pode optar por acumular as informações MITRE-ATT&CK automaticamente dos observáveis para um incidente de segurança. Para acúmulo automático de observáveis para incidentes de segurança, habilite a propriedade do sistema. Como alternativa, você pode acumular as informações manualmente para cada observável.

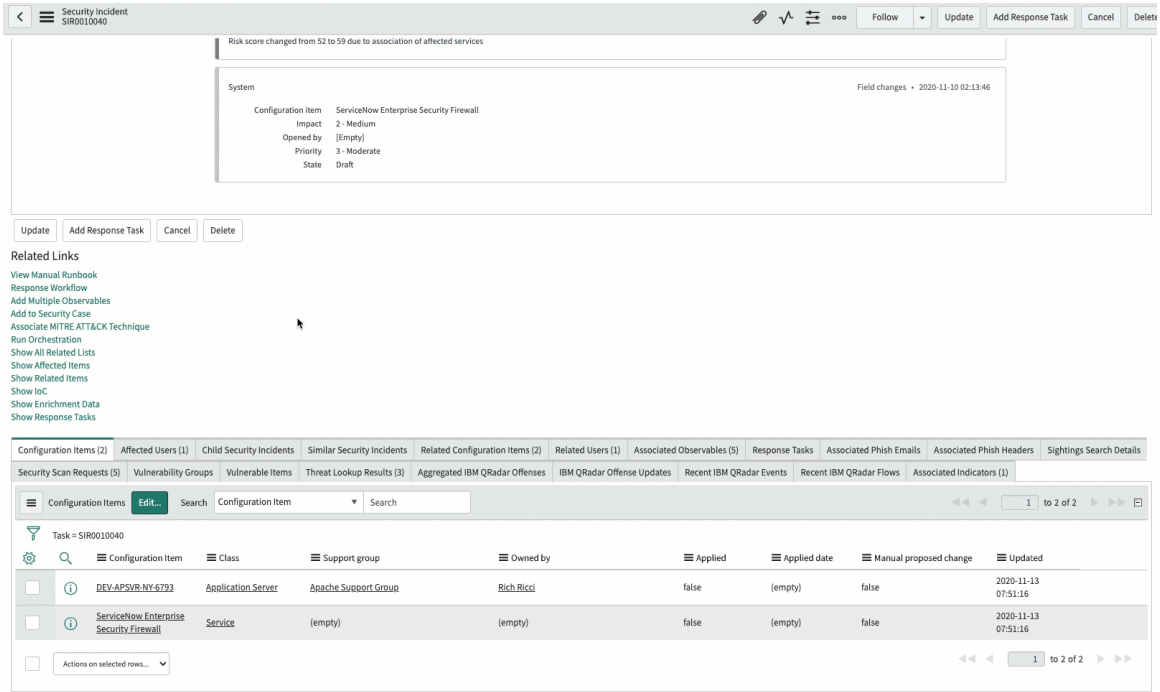
Procedimento

1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja aprimorar com as informações de MITRE-ATT&CK.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Observáveis associados**.
4. Aponte para o observável que você deseja associar, clique com o botão direito do mouse e selecione **Associar técnica MITRE ATT&CK**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Na ilustração a seguir, você pode ver como navegar na lista relacionada até **Associar técnica do MITRE ATT&CK**, revisar a origem e adicionar uma tática e uma técnica.



5. Nas listas de origem, revise a **Origem**.

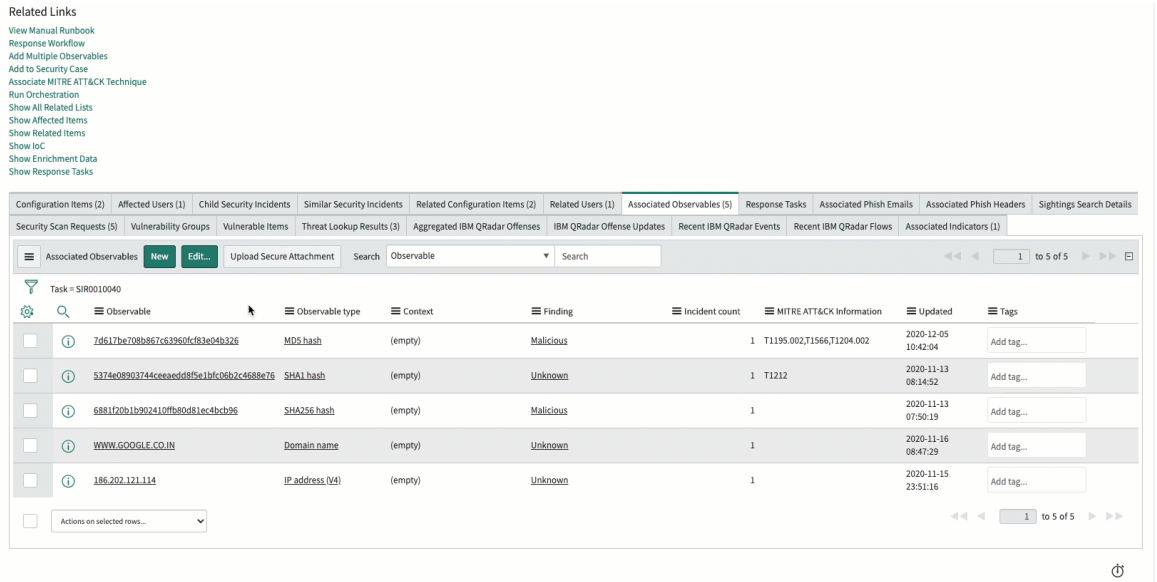
> **Nota:**
> Somente as coleções e matrizes que foram ativadas aparecem na lista de origem.

6. Revise a **tática** e as **técnicas**e adicione ou remova-as com base na relevância com o observável.
7. Clique em **Salvar**.
   As táticas e técnicas que você adicionou aparecem na coluna MITRE-ATT&CK Informações na lista relacionada de observáveis.
8. Selecione o observável e, em seguida, no menu Ações, clique **em Agregar informações do MITRE ATT&CK para SI**.
   Se você habilitou acúmulo automático de MITRE-ATT&CK informações de observáveis para incidente de segurança, as informações serão acumuladas automaticamente. Se você não habilitou o acúmulo automático, será necessário fazer isso manualmente.

   A ilustração a seguir mostra como selecionar um observável e acumular as informações de MITRE-ATT&CK para um incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



9. Para ter uma exibição agregada das técnicas associadas aos observáveis, selecione dois ou mais observáveis na lista e, em seguida, no menu **Ações** na lista de linhas selecionadas, clique em **Mostrar informações do MITRE ATT&CK**.

Resultado
Uma exibição agregada das informações do MITRE ATT&CK para os observáveis selecionados é exibida.

Associar informações MITRE-ATT&CK ao caso de segurança

Associe MITRE-ATT&CK táticas e técnicas a um caso de segurança para melhorar a gestão de casos de segurança e a análise de ameaças em um nível granular.

Antes de Iniciar
Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
2. Selecione o caso de segurança que você deseja aprimorar com as informações do MITRE-ATT&CK.
3. Na lista relacionada, clique em **Associar técnica MITRE ATT&CK**.

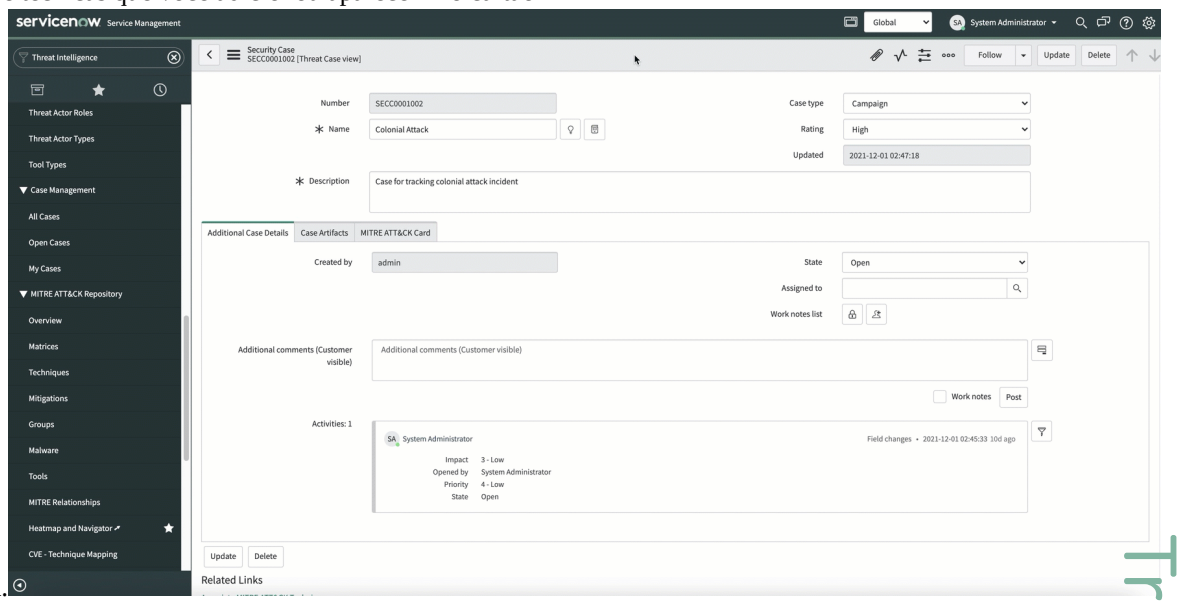
   Na ilustração a seguir, você pode ver como navegar na lista relacionada até **Associar técnica do MITRE ATT&CK**, revisar a origem e adicionar uma tática e uma técnica.

4. Nas listas de origem, revise a **Origem**.
5. Revise a **Tática** e as **Técnicas**e adicione ou remova-as com base na relevância do caso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Clique em **Salvar**.
   As táticas e técnicas que você adicionou aparecem no cartão MITRE-ATT&CK.



Acumular informações de MITRE-ATT&CK usando os resultados da Pesquisa de ameaças

Se você não habilitou o acúmulo automático de MITRE-ATT&CK informações, poderá fazer isso manualmente.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Se você habilitou acúmulo automático de MITRE-ATT&CK informações dos resultados da pesquisa de ameaças ao incidente de segurança, as informações serão acumuladas automaticamente. Se você não habilitou o acúmulo automático, poderá fazê-lo manualmente.

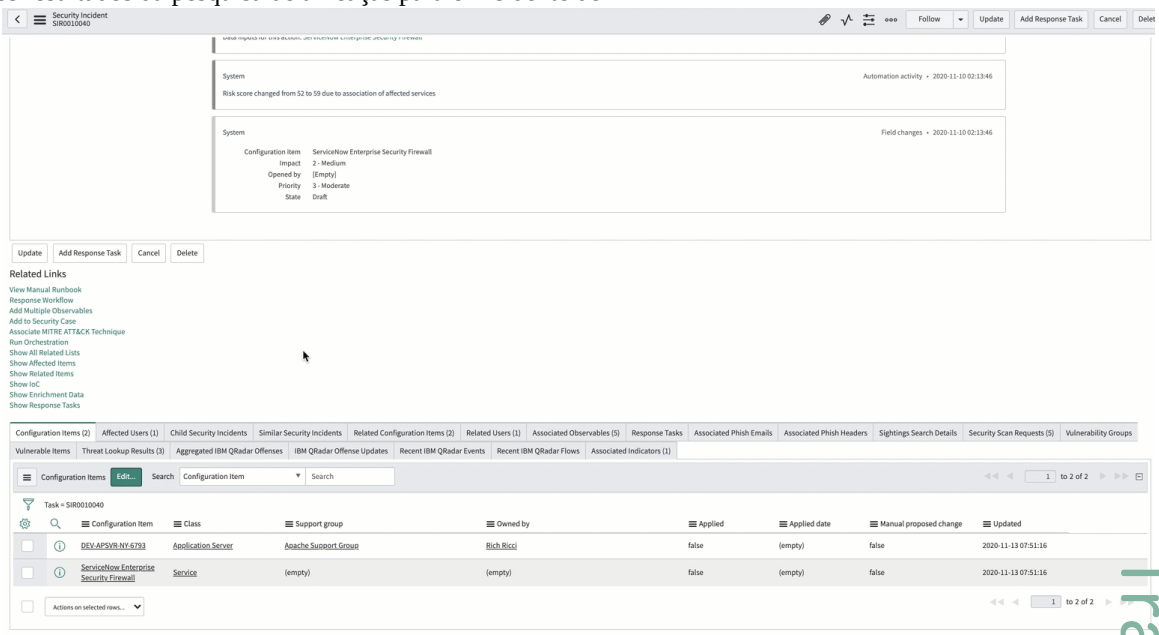
Procedimento

1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja aprimorar com as informações de MITRE-ATT&CK.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Resultados da pesquisa de ameaças**.
4. Selecione o observável e, em seguida, no menu Ações, clique **em Agregar informações do MITRE ATT&CK para SI**.
   Você pode selecionar vários observáveis e acumular as informações.
5. Clique em **Recarregar** para confirmar as mudanças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A ilustração a seguir mostra como selecionar um observável e acumular os resultados da pesquisa de ameaças para o incidente de segurança.



Você pode exibir o cartão MITRE-ATT&CK para confirmar que os resultados da pesquisa de ameaças foram acumulados para o incidente de segurança.

Informações de acúmulo MITRE-ATT&CK das regras de detecção

Habilite o acúmulo de informações de MITRE-ATT&CK das regras de detecção para os incidentes de segurança para obter uma melhor análise de ameaças e incidentes de segurança.

Antes de Iniciar

Função necessária: nenhuma

Certifique-se de ter realizado o seguinte:

- Habilite a propriedade Acumular informações do MITRE ATT e ACK automaticamente das regras de alerta para os incidentes de segurança no módulo Propriedades. Por padrão, esta opção está desabilitada. Para obter mais informações, consulte Revisar as propriedades do sistema MITRE-ATT&CK.
- Execute o mapeamento de regras de detecção para MITRE-ATT&CK TTPs no módulo Regras de detecção - MITRE ATT&CK Mapeamento de TTP. O nome da regra de detecção deve corresponder ao nome da regra de alerta que aciona o incidente de segurança. Para obter mais informações, consulte Criar e mapear regras de detecção.

Por Que e Quando Desempenhar Esta Tarefa

Se você não pretende usar as regras de extração automática do SIEM do sistema de base, habilite o acúmulo automático de MITRE-ATT&CK TTPs com base no mapeamento da regra de detecção. Você pode preencher o alerta ou a regra de evento que aciona o incidente de segurança no campo Nome da regra de alerta. Você também pode preencher o campo Nome da regra de alerta usando a integração SIEM, a análise de e-mail, a criação manual e assim por diante.

Tradução automática

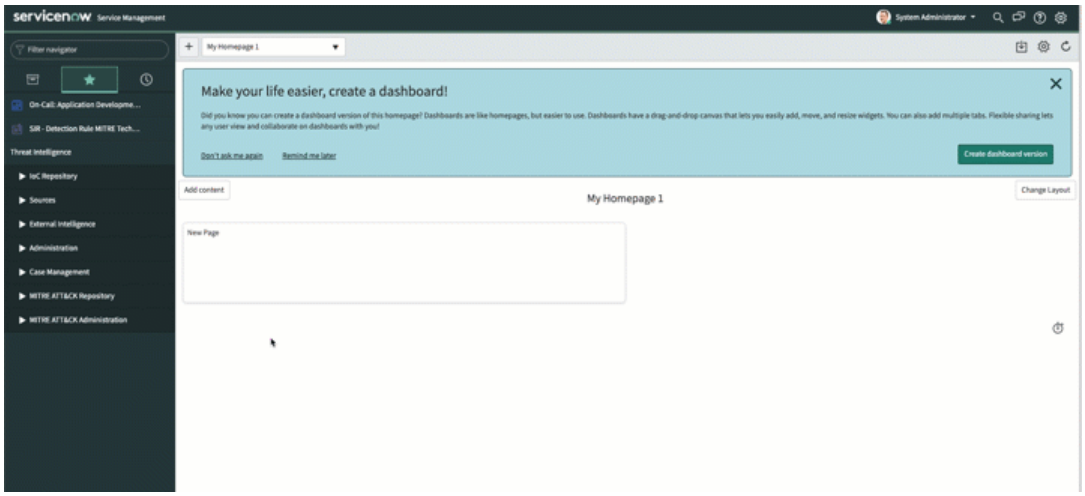
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Administração do MITRE ATT&CK** > **Propriedades**.
2. Habilite a propriedade Acumular informações do MITRE ATT&ACK automaticamente das regras de alerta para os incidentes de segurança e clique em **Salvar**.
   Por padrão, esta opção está desabilitada.
3. Você precisa preencher o campo Nome da **regra de alerta** do incidente de segurança com as regras de alerta necessárias.

   Nota:
   Certifique-se de adicionar o nome exato da Regra de alerta. Para adicionar várias regras, você precisa adicionar as regras usando um separador de vírgula.

4. Clique com o botão direito do mouse no formulário e clique em **Salvar**.
   Se o valor do nome da regra de alerta no incidente de segurança corresponder a um registro no módulo Regra de detecção - Mapeamento de TTP do MITRE ATT e CK, as técnicas e táticas correspondentes associadas à regra de alerta serão vinculadas ao incidente de segurança automaticamente.



5. Abra o incidente de segurança, selecione o **cartão MITRE ATT&CK** e valide se as técnicas foram acumuladas.
6. Habilite a opção **Mostrar origem das técnicas** para exibir a origem das técnicas.
   A origem das técnicas deve ser Regra de detecção.

Informações de acúmulo MITRE-ATT&CK de incidentes de segurança secundários

Se você não habilitou o acúmulo automático de MITRE-ATT&CK informações, poderá fazer isso manualmente.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

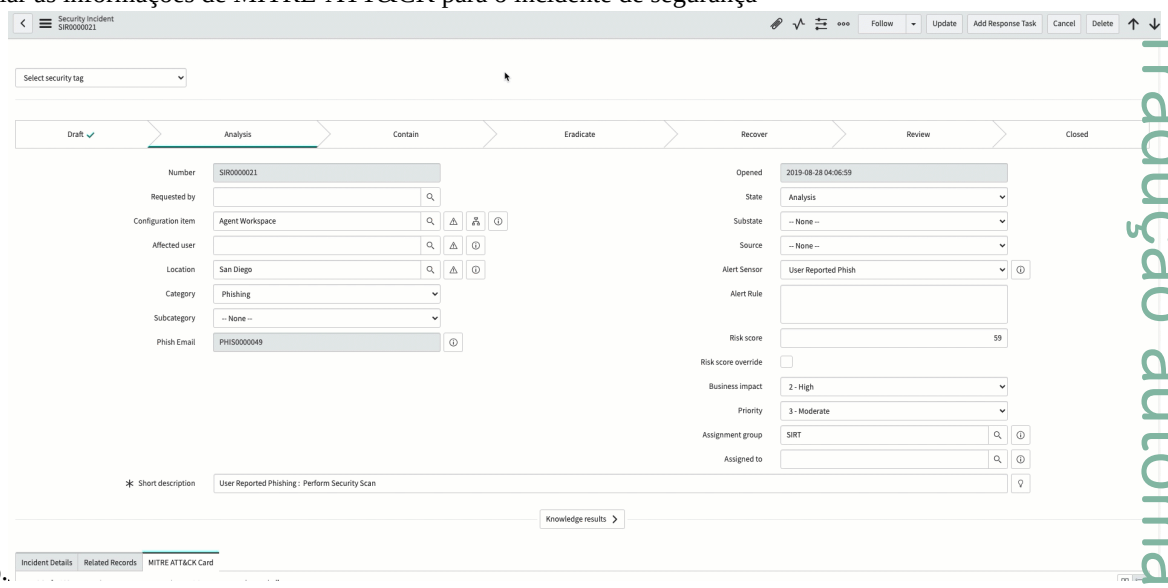
Se você habilitou acúmulo automático de MITRE-ATT&CK informações de incidentes de segurança secundários, as informações serão acumuladas automaticamente. Se você não habilitou o acúmulo automático, poderá fazê-lo manualmente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Incidentes** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança primário que você deseja aprimorar com as informações do secundário MITRE-ATT&CK.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Incidentes de segurança secundários**.
4. Selecione o incidente de segurança secundário e, no menu Ações, clique **em Agregar informações do MITRE ATT&CK para SI**.
   Você pode clicar em **Mostrar informações do MITRE ATT&CK** para exibir as informações do MITRE do incidente de segurança secundário antes de acumular as informações do MITRE ATT&CK.
5. Clique em **Recarregar** para confirmar as mudanças.
6. Clique no **cartão MITRE ATT&CK** para exibir a origem das técnicas.
   A ilustração a seguir mostra como selecionar o incidente de segurança secundário e acumular as informações de MITRE-ATT&CK para o incidente de segurança primário.



   Você pode exibir o cartão MITRE-ATT&CK para confirmar se as informações do incidente de segurança secundário MITRE-ATT&CK foram acumuladas para o incidente de segurança primário.

Realizar análise de link e busca de ameaças usando MITRE-ATT&CK filtros específicos

Correlacione e execute análises de link de observáveis, incidentes de segurança e MITRE-ATT&CK informações relacionadas para que sua organização possa começar a procurar ameaças.

Antes de Iniciar

Função necessária: sn_ti.mitre_analyst, sn_si.read

Por Que e Quando Desempenhar Esta Tarefa

Depois de associar os incidentes de segurança às informações de MITRE-ATT&CK, você pode usar os filtros específicos de MITRE-ATT&CK para a busca de ameaças. Use os filtros MITRE-ATT&CK com os filtros Security Incident Response existentes para correlacionar e executar a análise de link.

Tradução automática

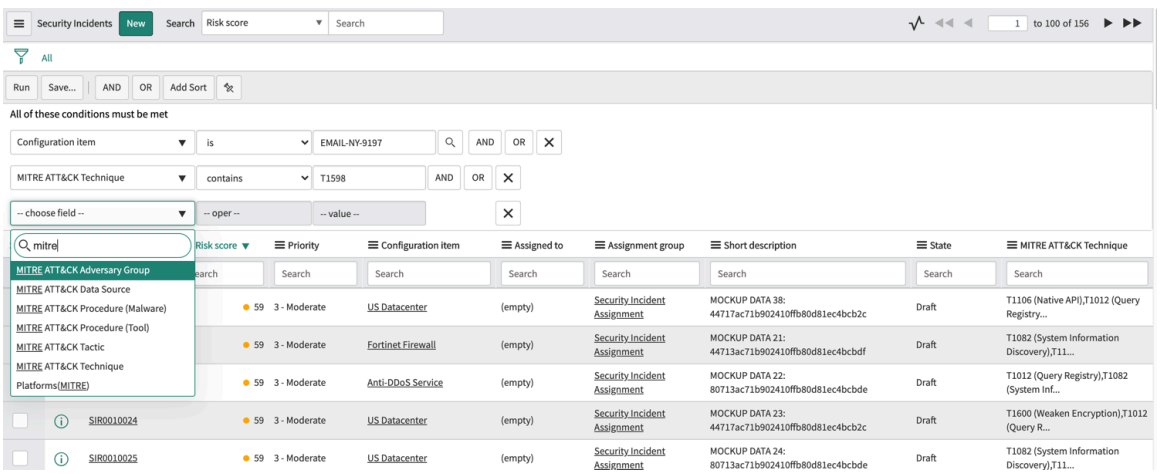
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Clique em **Atualizar lista personalizada** para adicionar as colunas MITRE.
3. Selecione uma condição de filtro para que você possa exibir MITRE informações relacionadas e associações com incidentes de segurança ou observáveis:
   - MITRE-ATT&CK Grupo adversário
   - MITRE-ATT&CK Fonte de dados
   - MITRE-ATT&CK Procedimento (malware)
   - MITRE-ATT&CK Procedimento (ferramentas)
   - MITRE-ATT&CK Tática
   - MITRE-ATT&CK Técnica
4. Crie uma condição de filtro que se baseie nos critérios acima e clique em **Executar** para executar uma análise de link ou correlação entre incidentes de segurança, observáveis e MITRE-ATT&CK informações relacionadas.

Nota:
Os dados MITRE-ATT&CK são armazenados como uma cadeia de caracteres e você só pode usar **contém** como o operador para condições de filtro.

Por exemplo, se você quiser revisar se um item de configuração (IC) está comprometido, selecione um IC. Em seguida, você correlaciona o IC com as técnicas presentes adicionando um MITRE-ATT&CK ID de técnica. Você pode continuar a criar seus critérios de filtro para correlacionar as informações e para a busca de ameaças.



MITRE-ATT&CK mapa térmico e navegador

Você pode usar o mapa térmico MITRE-ATT&CK e o navegador para navegação básica e para visualizar a cobertura geral de detecção da técnica.

Visão geral do mapa térmico e do navegador MITRE-ATT&CK

Você pode usar o navegador com os filtros primários para navegação básica e observação de matrizes ATT&CK. O mapa térmico destaca o espectro da cobertura de detecção, incluindo os pontos cegos em que sua organização não tem cobertura. Isso está disponível depois de mapear a cobertura de detecção da técnica.

Com o mapa térmico e o navegador, você pode:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Identifique de forma rápida e eficiente os recursos de detecção da sua organização e destaque as lacunas na cobertura de detecção da técnica.
- Procure ameaças e execute a correlação de ameaças usando os recursos associados.

Acessar o mapa térmico e o navegador MITRE-ATT&CK

Acesse o mapa térmico MITRE-ATT&CK e o navegador para visualizar a matriz que permite usar o ATT&CK.

Antes de Iniciar

Função necessária: sn_ti.read, sn_ti.mitre_analyst

Por Que e Quando Desempenhar Esta Tarefa

Você pode revisar o mapa térmico, usar os filtros para correlacionar e executar a análise de link de MITRE-ATT&CK informações, os observáveis e os incidentes de segurança em sua organização.

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Mapa térmico e Navegador**.
   O mapa térmico e o navegador são abertos em uma nova guia.
2. Selecione a origem para preencher o mapa térmico.

   Nota:
   Somente as coleções e matrizes que foram ativadas aparecem na lista de origem.

   Na ilustração a seguir, você vê como navegar até o mapa térmico e o navegador e como selecionar a origem, que é Enterprise ATT&CK neste exemplo.

   Navegue e selecione a origem para preencher o mapa térmico
3. Use a caixa de pesquisa para encontrar rapidamente uma tática ou técnica específica usando seu nome ou ID.

   A ilustração a seguir mostra como pesquisar uma tática, técnica ou qualquer informação contida nelas. Use a pesquisa para expandir rapidamente uma tática ou técnica específica.
4. Clique em **Filtros** e selecione um filtro entre os filtros Primário ou Avançado.
5. Clique em **Aplicar** e controle os filtros da seguinte forma:
   - Para salvar seus filtros, crie uma exibição personalizada. Você pode criar e salvar três exibições personalizadas.
   - Para remover os filtros selecionados, clique em **Restaurar filtros padrão** para carregar sua exibição salva padrão.
   - Para limpar todos os filtros e a exibição existente, clique em **Limpar todos os filtros**.

   Nota:
   As exibições que você salva são específicas para um usuário.
6. Clique **em Ocultar subtécnicas** para remover todas as subtécnicas da exibição do mapa térmico.
   Se uma técnica tiver subtécnicas, você poderá clicar no ícone expandir para exibir as subtécnicas.

Usando as exibições personalizadas

As exibições personalizadas no mapa térmico MITRE-ATT&CK e no navegador ajudam você a salvar e exibir seus filtros favoritos na próxima vez que acessar o mapa térmico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Você pode criar e salvar três exibições personalizadas para cada coleção MITRE-ATT&CK por usuário.

Criar uma exibição

Depois de selecionar os filtros necessários nos filtros Primário ou Avançado, clique no botão de reticências (...) no cabeçalho Filtros e selecione **Criar uma nova exibição**. Insira o nome da exibição personalizada e **Salvar exibição**.

Exibições padrão

Clique **em Salvar como exibição padrão** para carregar diretamente a exibição na próxima vez que acessar o mapa térmico. Você pode definir uma exibição padrão para cada uma das coleções.

Nota:
Se você estiver atualizando o plug-in Inteligência contra ameaças de uma versão mais antiga, a exibição padrão existente da versão antiga aparecerá como uma exibição personalizada.

A ilustração mostra como criar uma exibição personalizada no mapa térmico

Atualizar uma exibição

Você pode fazer atualizações em uma exibição personalizada existente modificando os filtros Primário ou Avançado necessários. Selecione uma exibição personalizada, atualize os filtros conforme necessário e clique no botão de reticências (...) no cabeçalho Filtros e selecione **Atualizar exibição** para salvar os filtros.

Esta ilustração mostra como atualizar uma exibição personalizada.

Gerenciar exibições personalizadas

Use as caixas de seleção ao lado de cada exibição personalizada para aplicar o filtro de exibição personalizado selecionado.

Clique no botão de reticências (...) ao lado de cada nome de exibição personalizado para controlar as exibições personalizadas da seguinte forma:

- Defina uma exibição padrão.
- Remova uma exibição personalizada como padrão. Isso não exclui a exibição personalizada.
- Renomeie a exibição personalizada.
- Exclua a exibição personalizada.

Esta ilustração mostra como gerenciar exibições personalizadas.

Exportar uma exibição salva

Para exportar as exibições personalizadas salvas para arquivos JSON, clique nas reticências (...) no cabeçalho Filtros e selecione **Exportar exibições salvas**. Clique no ícone de download da exibição personalizada que você deseja baixar para o seu computador local.

Esta ilustração mostra como exportar exibições personalizadas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importar uma exibição

Você pode importar somente arquivos JSON. Para importar as exibições personalizadas, clique no botão de reticências (...) no cabeçalho Filtros e selecione **Importar exibição (json)**.

Revise as seguintes condições ao importar exibições:

- Você só pode importar o formato de arquivo JSON.
- Você pode importar apenas uma exibição ou arquivo de cada vez.
- Você não pode importar se já tiver três exibições personalizadas em seus filtros. Exclua uma exibição personalizada e importe uma exibição.
- Você não pode importar uma exibição com um nome de exibição personalizado existente. Renomeie uma exibição antes de importar.

Esta ilustração mostra como importar uma exibição.

Navegador com filtros primários

Use os filtros primários para filtrar técnicas no navegador MITRE-ATT&CK. As informações no repositório MITRE-ATT&CK estão disponíveis para seleção.

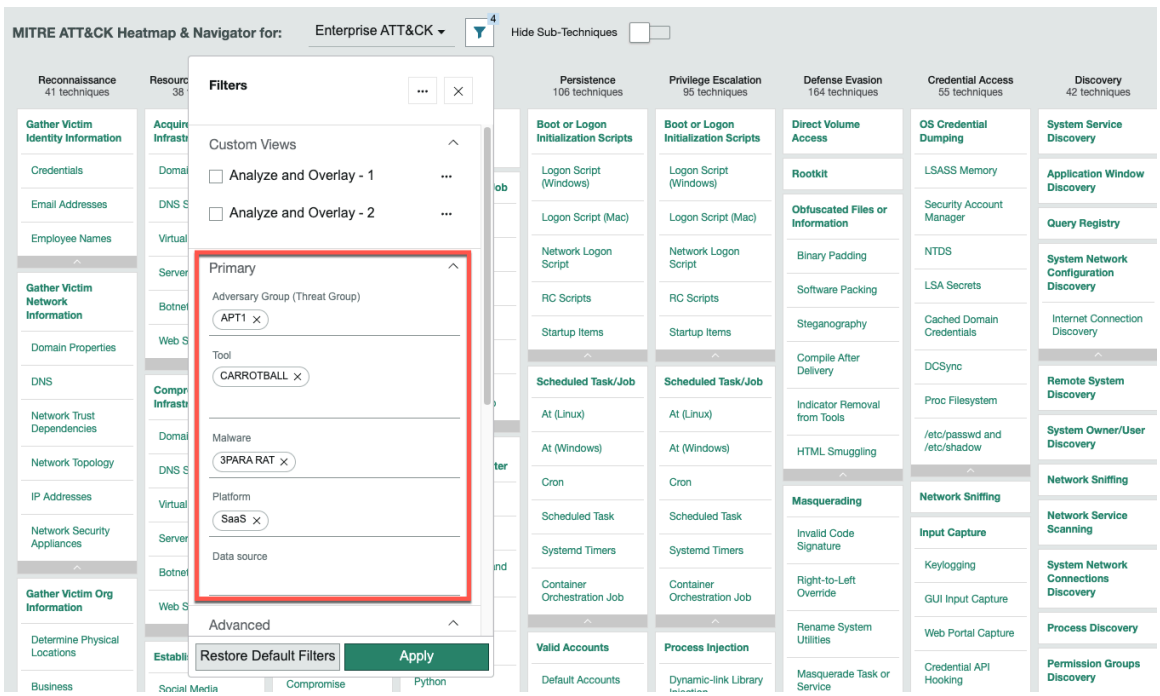
Filtro	Descrição
Grupo adversário (grupo de ameaça)	Conjuntos de atividades de invasão relacionadas que são rastreadas por um nome comum na comunidade de segurança. Grupos podem significar vários grupos de ameaças, grupos de atividades, agentes de ameaça, conjuntos de intrusão e campanhas. Você pode adicionar vários grupos ao filtro **Grupo adversário (grupo de ameaça)**. Por exemplo, você adiciona APT1 e AT12, pois ambos são grupos de ameaças atribuídos à China. Embora os dois grupos possam ter como destino origens diferentes, eles podem usar técnicas semelhantes.
Ferramenta	Software legítimo usado por agentes de ameaça para executar ataques. Você pode entender como os agentes de ameaça executam campanhas se souber como e quais ferramentas são usadas pelos agentes de ameaça. As ferramentas incluem o software que não é encontrado em um sistema corporativo e o software que está disponível como parte de um sistema operacional que já está presente em um ambiente como os utilitários do Microsoft Windows. Por exemplo, o gsecdump é um descarregador de credenciais disponível publicamente que o grupo adversário APT11 usa para obter hashes de senha e segredos de LSA (Autoridade de Segurança Local) dos sistemas operacionais Microsoft Windows.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Filtro	Descrição
Malware	Software comercial, personalizado de código fechado ou de código aberto que se destina a ser usado para fins mal-intencionados por adversários. Os exemplos são PlugX, CHOPSTICK e assim por diante
Plataforma	Táticas e técnicas que representam MITRE-ATT&CK em uma plataforma específica. Por exemplo, MITRE-ATT&CK oferece suporte a essas plataformas na matriz Enterprise ATT&CK: Microsoft Windows, macOS, Linux, PRE, AWS, GCP, Azure, Azure AD, Office 365, SaaS, Rede.
Fonte de dados	Fontes de dados que você está coletando em seu ambiente e usando para detectar MITRE-ATT&CK técnicas. Os exemplos são monitoramento de dll e extensões de navegador.

A ilustração a seguir mostra todos os filtros primários disponíveis no navegador MITRE-ATT&CK.



Uso de um mapa térmico com recursos primários e avançados

Você pode usar um mapa térmico com filtros avançados para executar uma análise correlacionando incidentes de segurança com MITRE-ATT&CK informações.

Exibir IDs de técnica

Você pode exibir os IDs de técnica MITRE-ATT&CK com os nomes das técnicas ao selecionar o filtro **Exibir IDs de técnica**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir IDs de técnica em um mapa térmico

Exibir técnicas relevantes por prioridade

Para filtrar as técnicas com base em sua prioridade relevante no navegador, selecione **Filtrar por filtro de prioridade relevante da técnica** e selecione a **Prioridade relevante** no menu. Você pode atribuir várias prioridades para filtragem. Você também pode apontar para as técnicas no mapa térmico para saber a prioridade da técnica.

As informações de prioridade relevantes são baseadas na priorização que você definiu no campo Prioridade relevante de técnicas.

Esta ilustração mostra a filtragem por prioridade relevante.

Exibir cobertura de detecção de técnica

Para exibir a cobertura geral de detecção da técnica no mapa térmico, selecione o filtro **Exibir cobertura de detecção da técnica**. O mapa térmico destaca o aspecto visual da cobertura de detecção, incluindo os pontos cegos onde você não tem cobertura. A definição de pontuação do sistema de base e as cores foram definidas na cobertura de detecção da técnica. As informações foram extraídas automaticamente da cobertura geral de detecção da técnica.

Por exemplo, as áreas do mapa térmico marcadas em vermelho indicam falta de detecção. As áreas marcadas em azul indicam a presença de recursos de detecção completos. As áreas marcadas em laranja, amarelo e azul claro refletem as capacidades de detecção parcial.

- A visualização de cores é baseada na definição da técnica e na codificação de cores que você define.
- A visualização da cobertura é baseada no mapeamento de cobertura de detecção de técnica que você define.
- Se você modificar a definição de cobertura do sistema de base, os ícones de tipo de cobertura não serão exibidos com as técnicas no mapa térmico.

Nota:
O mapa térmico funciona conforme o esperado quando você modifica os mesmos campos que a cobertura de detecção de técnica definida pelo sistema de base e as cores de cobertura.

Nesta ilustração, você vê a cobertura de detecção de técnica para todas as técnicas e subtécnicas e o tipo de cobertura com suas cores e ícones.

Cobertura de detecção da técnica de mapa térmico

Exibir cobertura de mitigação da técnica

Para exibir a cobertura geral de mitigação da técnica no mapa térmico, selecione o filtro Exibir cobertura de mitigação da técnica. O mapa térmico destaca o aspecto visual da cobertura de mitigação, incluindo áreas que você não tem cobertura. A cobertura de mitigação, as cores e os intervalos de porcentagem foram definidos na Definição de cobertura de mitigação. As informações são extraídas da Cobertura geral de mitigação da técnica.

Por exemplo, as técnicas destacadas em vermelho indicam que não há cobertura de mitigação, laranja indica cobertura de mitigação ruim e azul indica cobertura de mitigação excelente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

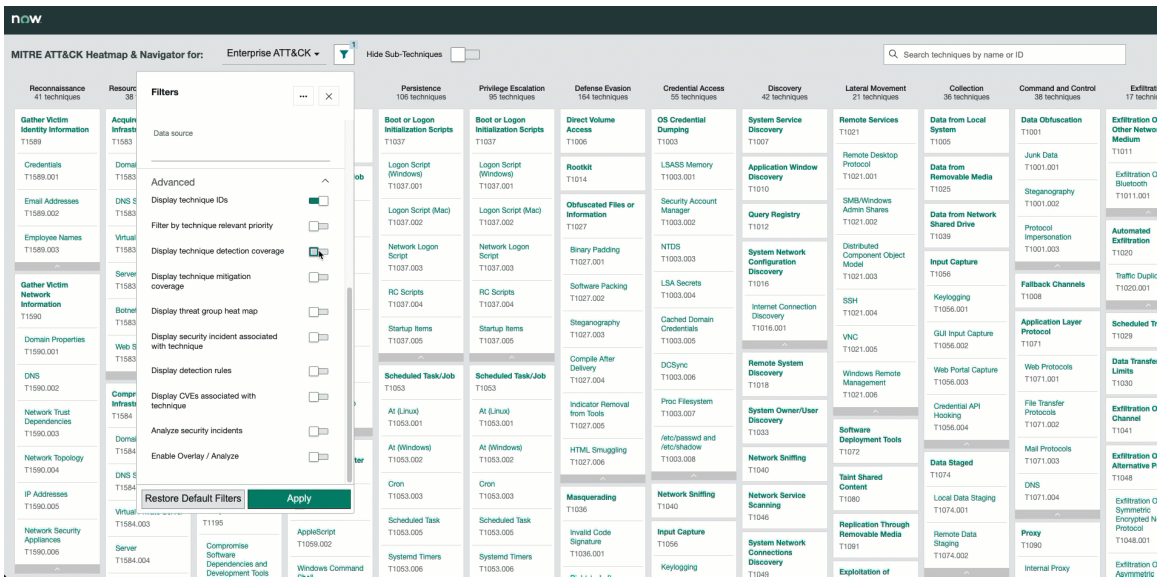
- A visualização de cores é baseada na definição de mitigação da técnica e na codificação de cores que você define.
- A visualização da cobertura é baseada no mapeamento de cobertura de mitigação de técnica que você define.
- Se você modificar a definição de cobertura de mitigação do sistema de base, os ícones de tipo de cobertura de mitigação não serão exibidos com as técnicas no mapa térmico.

Nota:
O mapa térmico funciona conforme o esperado quando você modifica os mesmos campos que a cobertura de mitigação da técnica definida pelo sistema de base e as cores de cobertura.

Esta ilustração mostra o mapa térmico de cobertura de mitigação da técnica

Exibir cobertura de detecção e mitigação

Você pode usar a detecção de técnica e os filtros de cobertura de mitigação de técnica juntos para obter informações sobre a relevância da detecção de técnica e reduzir a cobertura para sua organização.



Esta ilustração mostra como usar os filtros de detecção e mitigação juntos.

Exibir grupo de ameaças

Para exibir o grupo de ameaças para informações de técnica no mapa térmico, selecione **Exibir mapa térmico do grupo de ameaças**. Você pode medir o número de grupos de ameaças que estão usando uma técnica específica. A probabilidade de um ataque usando uma técnica específica aumenta quando você tem um número alto de invasores. Os intervalos de grupo de ameaça e as cores do mapa térmico foram definidos na Definição de mapa térmico de técnica de grupo de ameaças.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- A visualização de cores do mapa térmico e do texto é baseada no grupo de ameaça para a definição do mapa térmico da técnica.
- A visualização do intervalo do grupo de ameaças é baseada no mapeamento do grupo de ameaças para a técnica.
- Você não pode usar o filtro **Exibir mapa térmico de grupo de ameaças** quando a cobertura de detecção de técnica ou a cobertura de mitigação de técnica estão habilitadas. Esta ilustração mostra as informações do grupo de ameaça no mapa térmico.

Exibir incidentes de segurança associados à técnica

Para exibir as técnicas que são exploradas com frequência em sua organização e que resultaram em incidentes de segurança, clique em **Exibir incidente de segurança associado à técnica**. Você pode exibir mais informações sobre cada um dos incidentes de segurança associados ao clicar no link que é aberto em uma nova janela para análise. Incidentes de segurança associados a uma técnica.

- Prioridade: selecione **Prioridade de incidente de segurança** para filtrar pela prioridade do incidente de segurança.
- Intervalo de datas: selecione o **intervalo de datas do Incidente de** segurança para filtrar os problemas de segurança pelo intervalo de datas.
- Falsos positivos: selecione **Filtrar incidente de segurança de falsos positivos** para remover problemas de falsos positivos. Selecionar este filtro reduz o número de incidentes de segurança exibidos no mapa térmico.

Quando você usa este filtro com o filtro **Exibir cobertura de detecção de técnica**, ele fornece informações sobre a relevância da cobertura de detecção de técnica para sua organização até a data selecionada.

Por exemplo, ao ativar os dois filtros, você pode ver que, na tática de evasão de defesa, a técnica de mascaramento não tem cobertura. Quando você examina mais, a técnica de Mascaramento está relacionada à Tarefa ou Serviço de Mascaramento, que também tem um incidente de segurança associado a ele. Isso mostra que há uma lacuna na cobertura de detecção da técnica de Mascaramento e talvez você queira revisar a cobertura geral de detecção da técnica.

Exibir regras de detecção

Para ver se você tem as regras de detecção definidas para uma técnica específica, clique em **Exibir regras de detecção**. Você também pode ver cada regra de detecção associada com sua definição.

Essas informações são baseadas no mapeamento de regras de detecção que você definiu. Exibir regras de detecção associadas.

Exibir CVEs associados à técnica

Para exibir as informações de Vulnerabilidades e exposições comuns (CVE) associadas a cada uma das técnicas, clique em **Exibir CVEs associados à técnica**. As informações de CVE para técnica são baseadas nas informações disponíveis no módulo CVE — Mapeamento de técnica. Isso fornece informações sobre vulnerabilidades conhecidas e permite que você saiba se os adversários podem explorar sua organização.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importante:
O mapa térmico foi aprimorado para exibir somente os CVEs relevantes que estão associados aos VITs

Para exibir VITs associados a CVEs e técnicas, selecione **Exibir VITs associados a CVE e técnicas**. Além disso, para filtrar ainda mais as técnicas sem VITs, selecione **Ocultar técnicas sem VITs**. As informações de CVE e VIT exibidas são obtidas do produto Vulnerability Response em seu ambiente. Você pode exibir a lista filtrada de CVEs e VITs no mapa térmico e navegar até cada CVE ou VIT para cada técnica do mapa térmico.

Nota:

- A **técnica Exibir CVEs associados a** está disponível somente quando o produto Vulnerability Response está instalado em seu ambiente.
- As informações de VIT e CVE são calculadas com base no trabalho programado definido em MITRE-ATT&CK propriedades. O trabalho de programação do sistema de base é definido por 24 horas.

Ao usar este filtro com o filtro **Exibir incidente de segurança associado à técnica**, você pode saber se as vulnerabilidades conhecidas causaram incidentes de segurança em sua organização.

Você pode exibir mais informações sobre cada CVE para analisar se o CVE é relevante para sua organização. Para fazer isso, exiba os itens de vulnerabilidade. Se os itens de vulnerabilidade forem criados, você poderá exibir mais informações sobre qualquer informação de IC associada no módulo Vulnerability Response. Você também pode revisar a severidade e a prioridade para tomar decisões informadas. Revise os CVEs para tomar decisões fundamentadas.

Analisar incidentes de segurança

Para analisar incidentes de segurança e revisar as técnicas usadas por um adversário para um ataque, clique em **Analisar incidentes de segurança**. Você pode adicionar vários incidentes de segurança para análise usando cadeias de caracteres separadas por vírgulas.

Este filtro ajuda a analisar um incidente de segurança. Você pode saber por que o incidente ocorreu, quais técnicas foram exploradas, se algum agente de ameaça conhecido estava envolvido, se os agentes de ameaça usaram uma sequência específica para um ataque e assim por diante. Como você pode analisar vários incidentes de segurança ao mesmo tempo, é possível correlacionar as informações para ver se eles estão relacionados ou se são um incidente isolado. Se os incidentes de segurança estiverem relacionados e você observar um padrão, poderá revisar o andamento deles na cadeia de eliminação para interromper o ataque ou para formar uma estratégia de defesa para sua organização.

Ao usar o filtro **Analisar incidentes de segurança** com filtros primários, como um **Grupo adversário**, você pode correlacionar se adversários conhecidos estão envolvidos. Por exemplo, quando vários incidentes de segurança estão sendo analisados, as técnicas associadas aos incidentes de segurança estão presentes na forma de uma cadeia de eliminação. Ao sobrepor as informações com o adversário, você notará uma sobreposição entre as técnicas associadas ao incidente de segurança e as técnicas associadas ao adversário. Somente as informações da técnica sobreposta serão mostradas se ambos os filtros estiverem habilitados.

Analisar incidentes de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usando sobreposição para analisar incidentes de segurança e grupos adversários

Use o filtro **Habilitar sobreposição/Analisar** para exibir o comportamento do adversário, analisar um ou mais incidentes de segurança e correlacionar as informações para ver se um ataque é um incidente isolado ou um ataque coordenado por um adversário conhecido.

Por exemplo, agora você pode exibir os incidentes de segurança e o comportamento da cadeia de eliminação do adversário da ameaça na mesma exibição. Esta exibição fornece informações de sobreposição que informam sobre o ataque e o comportamento do adversário conhecido. Isso permite que você analise se este é um ataque isolado ou um ataque coordenado por um adversário conhecido.

Habilitar o filtro de análise de sobreposição ignora todos os filtros primários, exceto o filtro **Grupo adversário**, e ignora o filtro avançado **Filtrar por prioridade relevante da técnica** ao gerar uma exibição.

Depois de habilitar o filtro de análise de sobreposição, use a paleta de cores para atribuir cores para o seguinte:

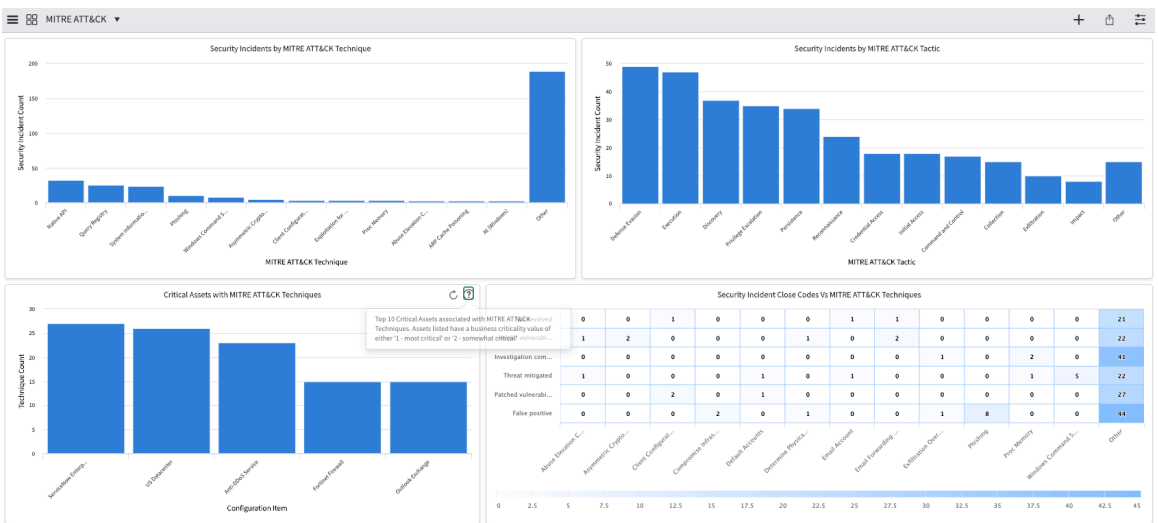
- Analisar incidente de segurança
- Grupo adversário
- Sobreposição

A ilustração a seguir mostra que o grupo adversário APT18 está espalhado por várias técnicas e táticas na cadeia de eliminação. A análise também mostra que há três técnicas que se sobrepõem ao grupo adversário e aos incidentes de segurança que você está rastreando. Esta ilustração mostra as informações de sobreposição de adversário e incidente de segurança.

Usando o painel MITRE-ATT&CK

O painel MITRE-ATT&CK fornece uma exibição executiva da cobertura da fonte de dados, táticas e técnicas que são usadas em sua organização.

O módulo MITRE-ATT&CK Visão geral exibe MITRE-ATT&CK informações sobre incidentes de segurança, incluindo tendências e relatórios. Você pode clicar em qualquer parte de um widget (barra, ponto de dados, tabela e assim por diante) para exibir dados específicos dessa parte.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Use o painel MITRE-ATT&CK para ver seus dados relacionados à segurança

Use o painel MITRE-ATT&CK para obter uma visão geral da cobertura da fonte de dados, das táticas e das técnicas usadas em sua organização.

Antes de Iniciar

Função necessária: sn_si.ciso, sn_si.analyst, sn_si.manager, sn_ti.read

Procedimento

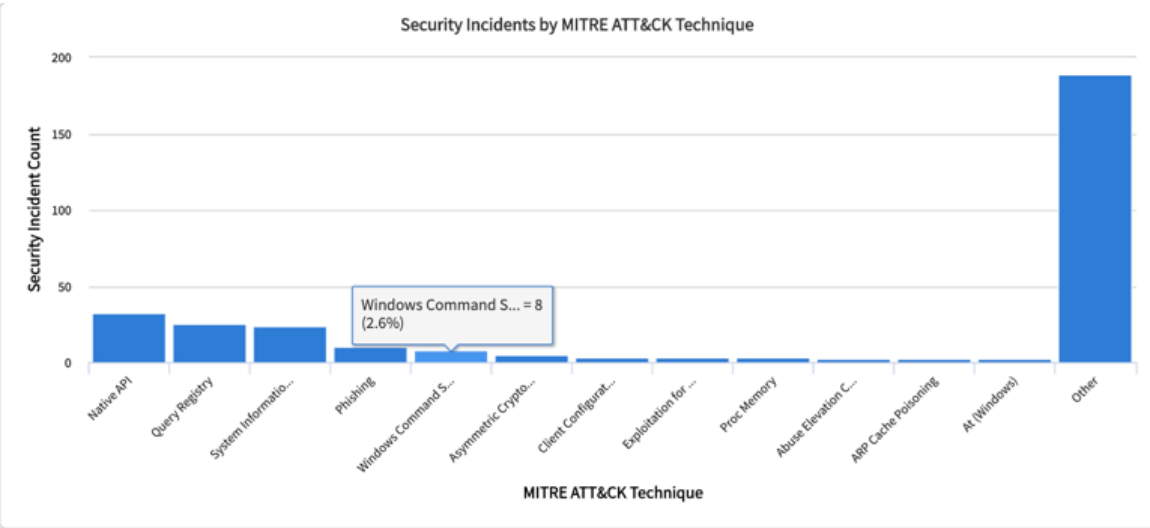
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Repositório do MITRE ATT&CK** > **Visão geral**.
2. Clique em qualquer um dos widgets a seguir para ver detalhes adicionais:
   - Incidentes de segurança por MITRE-ATT&CK técnica
   - Incidentes de segurança por MITRE-ATT&CK Tática
   - Ativos críticos com MITRE-ATT&CK técnicas
   - Códigos de encerramento de incidente de segurança versus técnicas MITRE-ATT&CK
   - Técnicas MITRE-ATT&CK por cobertura de detecção
   - Técnicas MITRE-ATT&CK por cobertura de mitigação
   - Grupos de ameaças por técnica MITRE-ATT&CK
   - CVEs por técnica MITRE-ATT&CK

Widgets do MITRE-ATT&CK

O módulo MITRE-ATT&CK Visão geral consiste em widgets que permitem correlacionar as informações MITRE-ATT&CK com as informações do incidente de segurança em seu ambiente.

Exemplo de incidentes de segurança por técnica MITRE-ATT&CK

Neste exemplo, o widget Incidentes de segurança por técnica **MITRE ATT&CK** exibe as técnicas por incidente de segurança em um ambiente de organização nos últimos 90 dias.

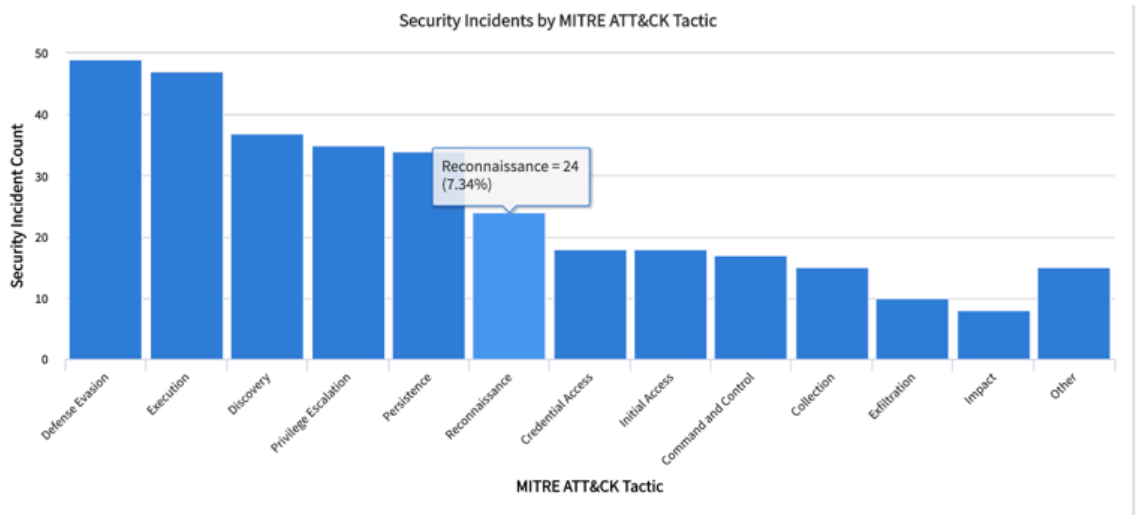


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de incidentes de segurança por tática MITRE-ATT&CK

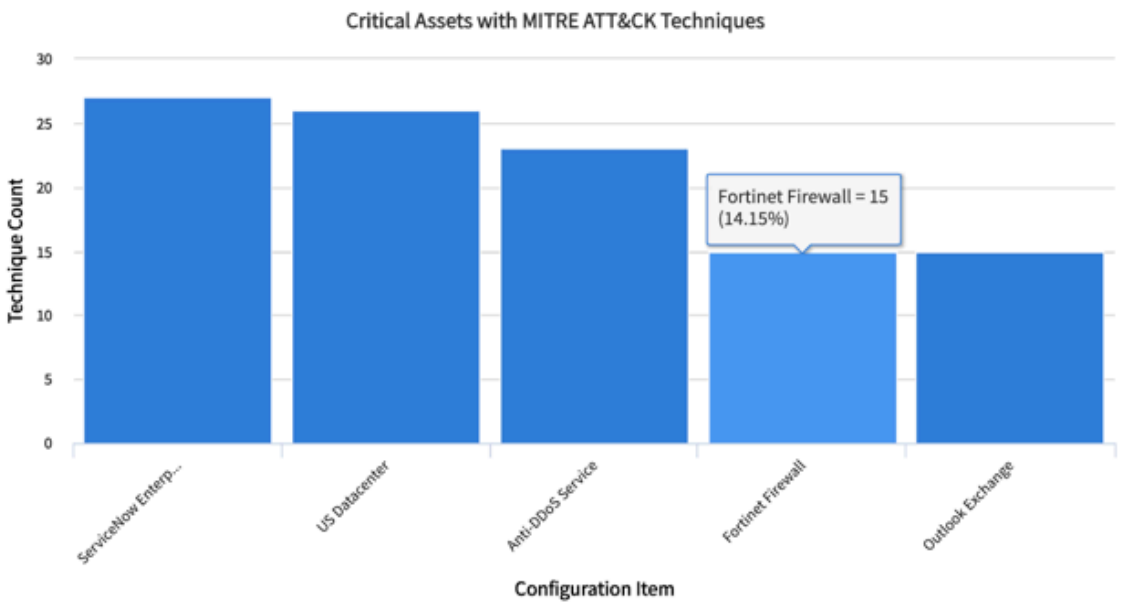
Neste exemplo, o widget **Incidentes de segurança por tática do MITRE ATT&CK** exibe as principais táticas por incidente de segurança em um ambiente de organização nos últimos 90 dias.



Exemplo de ativos críticos com MITRE-ATT&CK técnicas

Neste exemplo, o widget **Ativos críticos com técnicas MITRE ATT&CK** exibe os 10 principais ativos críticos que estão associados às técnicas MITRE-ATT&CK. Os ativos têm uma criticalidade de negócios de 1 (mais crítica) ou 2 (um pouco crítica).

Este relatório permite que uma organização veja os tipos e o número de técnicas usadas na realização de ataques contra os ativos críticos.



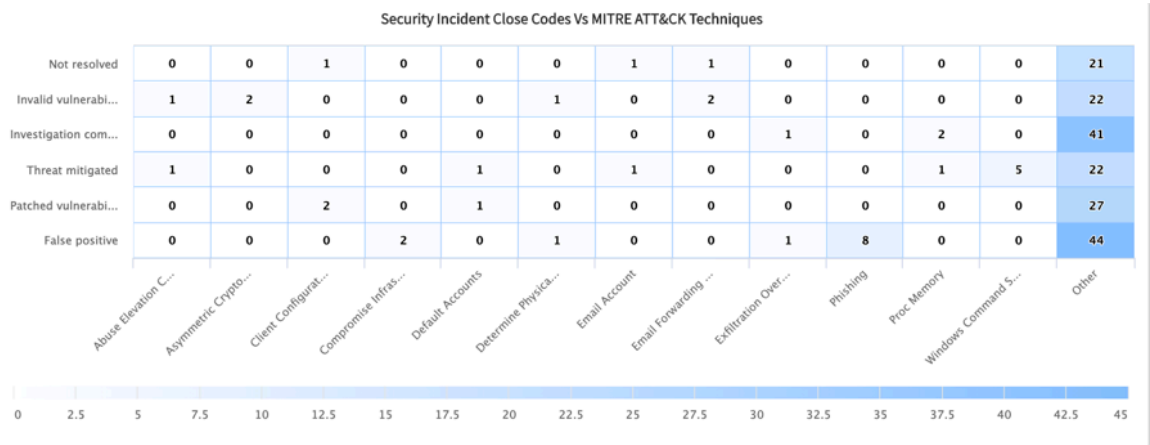
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exemplo de códigos de encerramento de incidente de segurança versus técnicas MITRE-ATT&CK

Neste exemplo, o widget Códigos de fechamento do incidente de segurança **versus técnicas** *MITRE-ATT&CK* exibe os códigos de fechamento do incidente de segurança que foram mapeados em relação às principais técnicas identificadas no ambiente de uma organização.

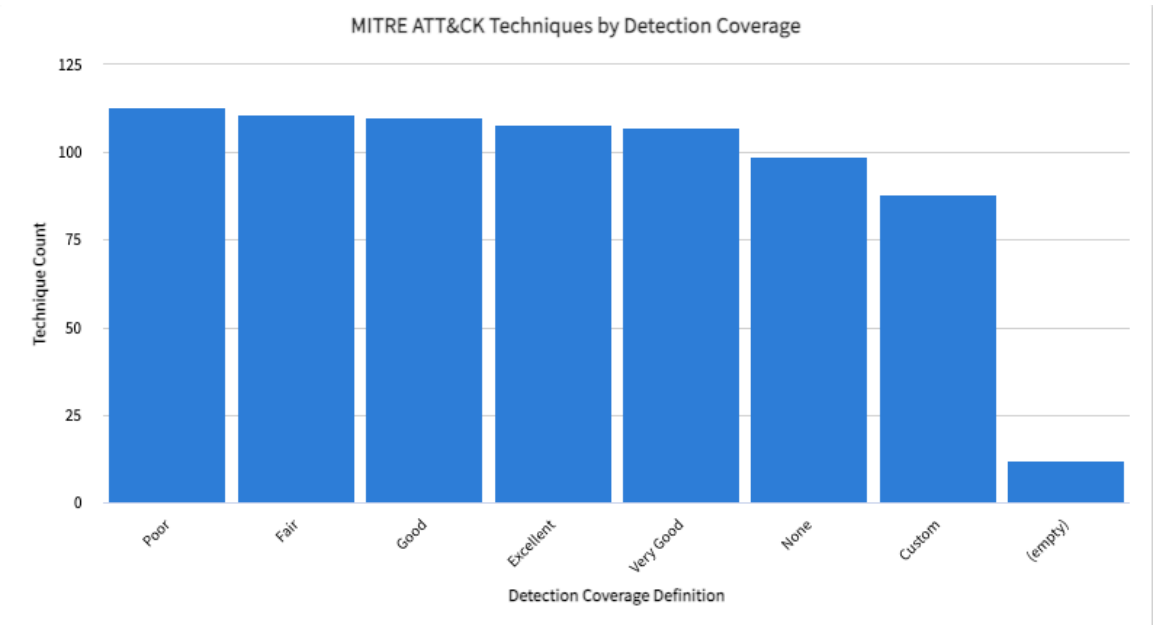
O eixo x exibe as principais técnicas que foram usadas para realizar ataques contra a empresa e o eixo y exibe os códigos encerrados.



Exemplo de cobertura de detecção por técnicas MITRE-ATT&CK

Neste exemplo, o widget **Técnicas MITRE-ATT&CK por cobertura de detecção** exibe a contagem de técnicas pela cobertura de detecção em seu ambiente.

O eixo x exibe a contagem da técnica e o eixo y exibe os tipos de cobertura de detecção.



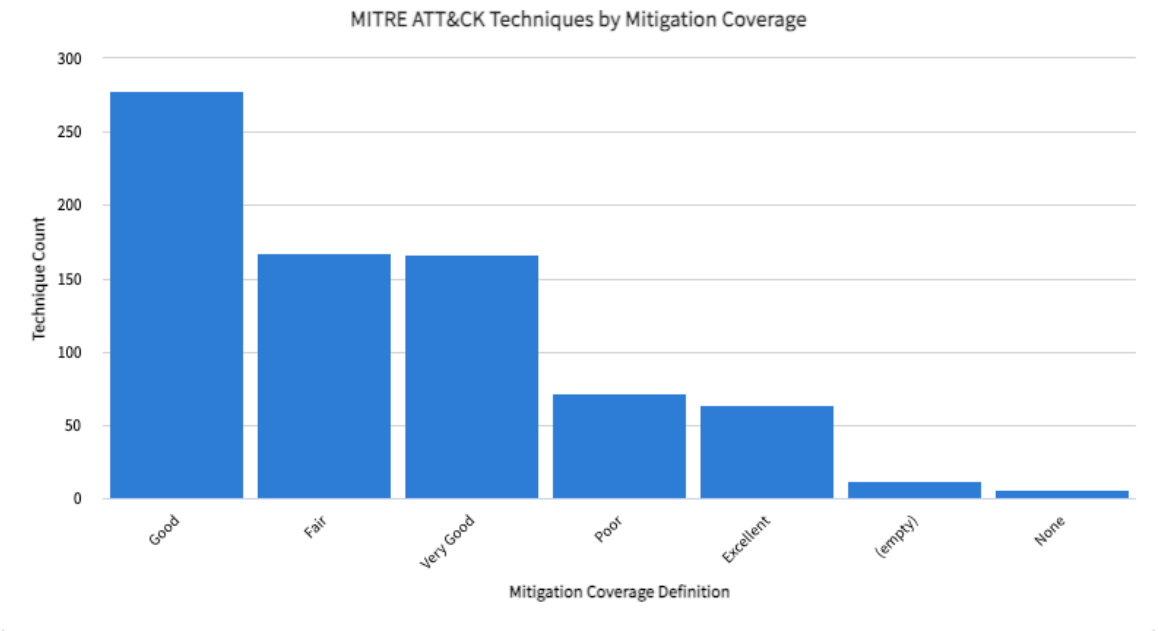
Exemplo de cobertura de mitigação por MITRE-ATT&CK técnicas

Neste exemplo, o widget **Técnicas MITRE-ATT&CK por cobertura de mitigação** exibe a contagem de técnica pela cobertura de mitigação em seu ambiente.

O eixo x exibe a contagem de técnicas e o eixo y exibe os tipos de cobertura de mitigação.

Tradução automática

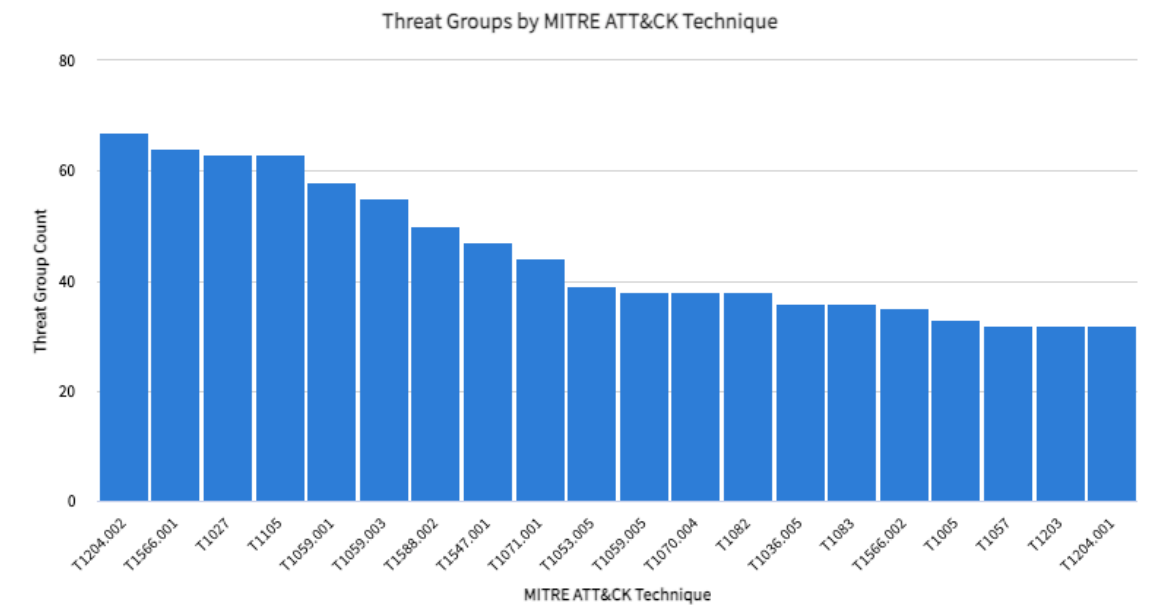
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Exemplo de grupos de ameaças por técnicas MITRE-ATT&CK

Neste exemplo, o widget **Grupos de ameaças por técnica MITRE-ATT&CK** exibe as técnicas pela contagem de grupos de ameaças. Este widget exibe 20 técnicas com a maior contagem de grupos de ameaça.

O eixo x exibe a contagem do grupo de ameaça e o eixo y exibe as técnicas MITRE-ATT&CK.



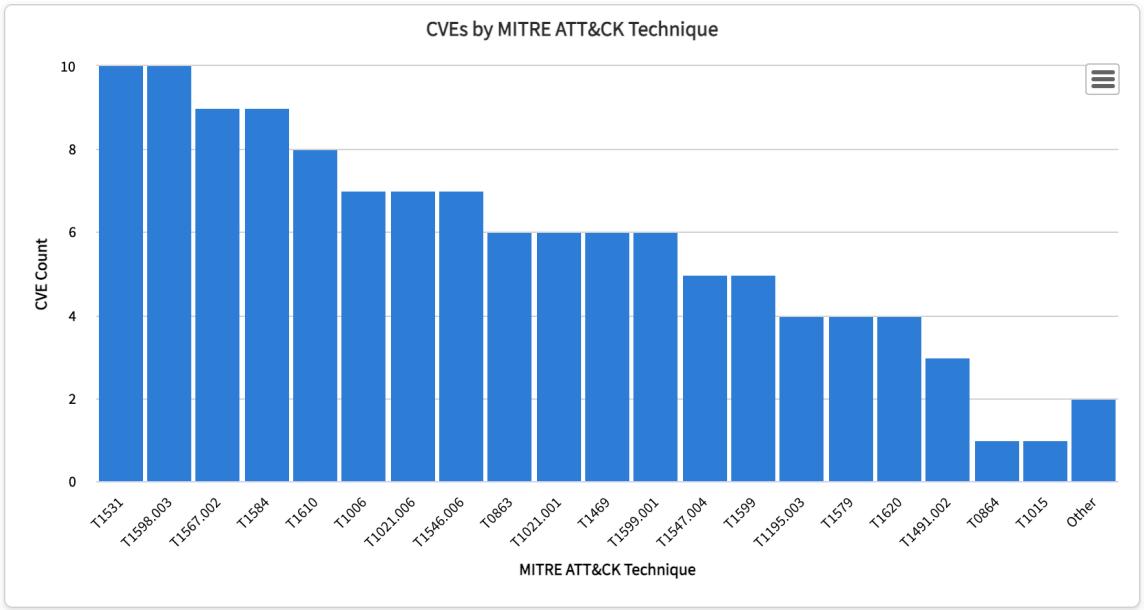
Exemplo de CVEs por técnicas MITRE-ATT&CK

Neste exemplo, o widget **CVEs por técnica MITRE-ATT&CK** exibe as técnicas com a contagem de CVE relevante em seu ambiente.

O eixo x exibe a contagem de CVE relevante e o eixo y exibe as técnicas MITRE-ATT&CK.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Administração do Inteligência contra ameaças

O sistema de base Inteligência contra ameaças está pronto para uso na ativação. Você pode adicionar registros a determinados módulos no menu da aplicação Administração, mas a maioria já está preenchida com informações padrão do setor.

As aplicações a seguir estão disponíveis no módulo **Administração** da barra de navegação Inteligência contra ameaças :

Aplicações de administração de Inteligência contra ameaças

Aplicação	Descrição
Propriedades	Inteligência contra ameaças As propriedades permitem que você controle como diferentes aspectos do sistema funcionam, incluindo a configuração de chaves de API.
Mecanismos de Ataque	Este módulo organiza os padrões de ataque hierarquicamente, com base em mecanismos que são empregados com frequência ao explorar uma vulnerabilidade.
Motivações de ataque	Este módulo lista as possíveis motivações de ataque que moldam a intensidade de um ataque por um agente de ameaça ou conjunto de intrusão.
Métodos de Descoberta	Este módulo descreve como os incidentes de segurança são descobertos.
Feeds	Este recurso foi descontinuado.
Tipos de Indicador	Este módulo é usado para caracterizar indicadores de ameaça cibernética compostos por padrões que identificam determinadas condições observáveis, bem como informações contextuais sobre o significado dos padrões e como e quando eles atuam.
Tipos de infraestrutura	Este módulo lista as possíveis classificações de infraestrutura.
Efeitos Pretendidos	Esta aplicação é usada para expressar o efeito pretendido de um agente de ameaça.
Capacidades do malware	Este módulo lista os possíveis recursos do malware.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações de administração de Inteligência contra ameaças

Aplicação	Descrição
Tipos de malware	Este módulo lista as possíveis classificações de malware.
Notificações	Este módulo é usado para criar notificações por e-mail . Isso envolve especificar quando eles são enviados, quem os recebe e o que eles contêm.
Tipos de observável	Este módulo lista as possíveis classificações de um observável, como um endereço IP ou um hash de arquivo.
Tipos de relatório	Este módulo lista as possíveis classificações de relatórios de ameaças.
Funções de agente da ameaça	Este módulo lista as funções que os agentes de ameaça desempenham.
Tipos de Agente da Ameaça	Este módulo caracteriza agentes mal-intencionados (ou adversários) que representam uma ameaça de ataque cibernético, incluindo a intenção presumida e o comportamento observado ao longo do tempo.
Calculadoras descobertas de pesquisa de ameaças	Este módulo calcula as descobertas com base nas respostas recebidas. Para integrações de terceiros que fornecem os resultados calculados, a calculadora de descoberta de pesquisa de ameaças mapeia os resultados para descobertas compatíveis no sistema. Para obter mais informações, consulte Calculadoras descobertas de pesquisa de ameaças.
Tipos de Ferramentas	Este módulo lista a possível classificação de ferramentas.

Calculadoras descobertas de pesquisa de ameaças

A Calculadora de descoberta de pesquisa de ameaças ajuda a calcular as descobertas observáveis com base nas respostas recebidas.

Você pode criar uma Calculadora de descoberta de pesquisa de ameaças para sua integração e usar um script para determinar como você deseja identificar as várias descobertas observáveis. A Calculadora de descoberta de pesquisa de ameaças inclui um script de exemplo que vem com o sistema de base, que você pode usar para identificar as descobertas observáveis ou pode modificar este script de acordo com seus requisitos.

Para integrações de terceiros que fornecem os resultados calculados, a Calculadora de descoberta de pesquisa de ameaças mapeia os resultados para descobertas compatíveis no sistema de base.

Resultados de pesquisa de ameaças de acúmulo

Quando você tem vários resultados de pesquisa de ameaças para um observável de vários fornecedores de integração, os resultados de pesquisa de ameaças recentes de todos os fornecedores são considerados e as descobertas gerais do observável são marcadas da seguinte forma:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Descobertas de pesquisa de ameaças de acúmulo

Descoberta do observável mais recente	Descoberta observável geral
Mal-intencionado	Se um dos fornecedores de integração relatar o observável como Mal-intencionado, a descoberta observável geral será marcada como Mal-intencionado.
Suspeito	Se nenhum dos fornecedores de integração relatar o observável como malicioso, um deles o relatará como suspeito e a descoberta geral do observável será marcada como suspeita.
Limpar	Se todos os fornecedores de integração relatarem o observável como Limpo, a descoberta geral do observável será marcada como Limpo.
Desconhecido	Se nenhum dos fornecedores de integração relatar o observável como Mal-intencionado ou Suspeito e um deles o relatar como Desconhecido, a descoberta geral do observável será marcada como Desconhecida.

Uso de calculadoras de descoberta de pesquisa de ameaças

Use a Calculadora de descoberta de pesquisa de ameaças para calcular as descobertas observáveis para sua integração.

Antes de Iniciar

Função necessária: sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Administração** > **Calculadoras descobertas de pesquisa de ameaças**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.
4. Clique em **Atualizar**.

Integrações do Inteligência contra ameaças

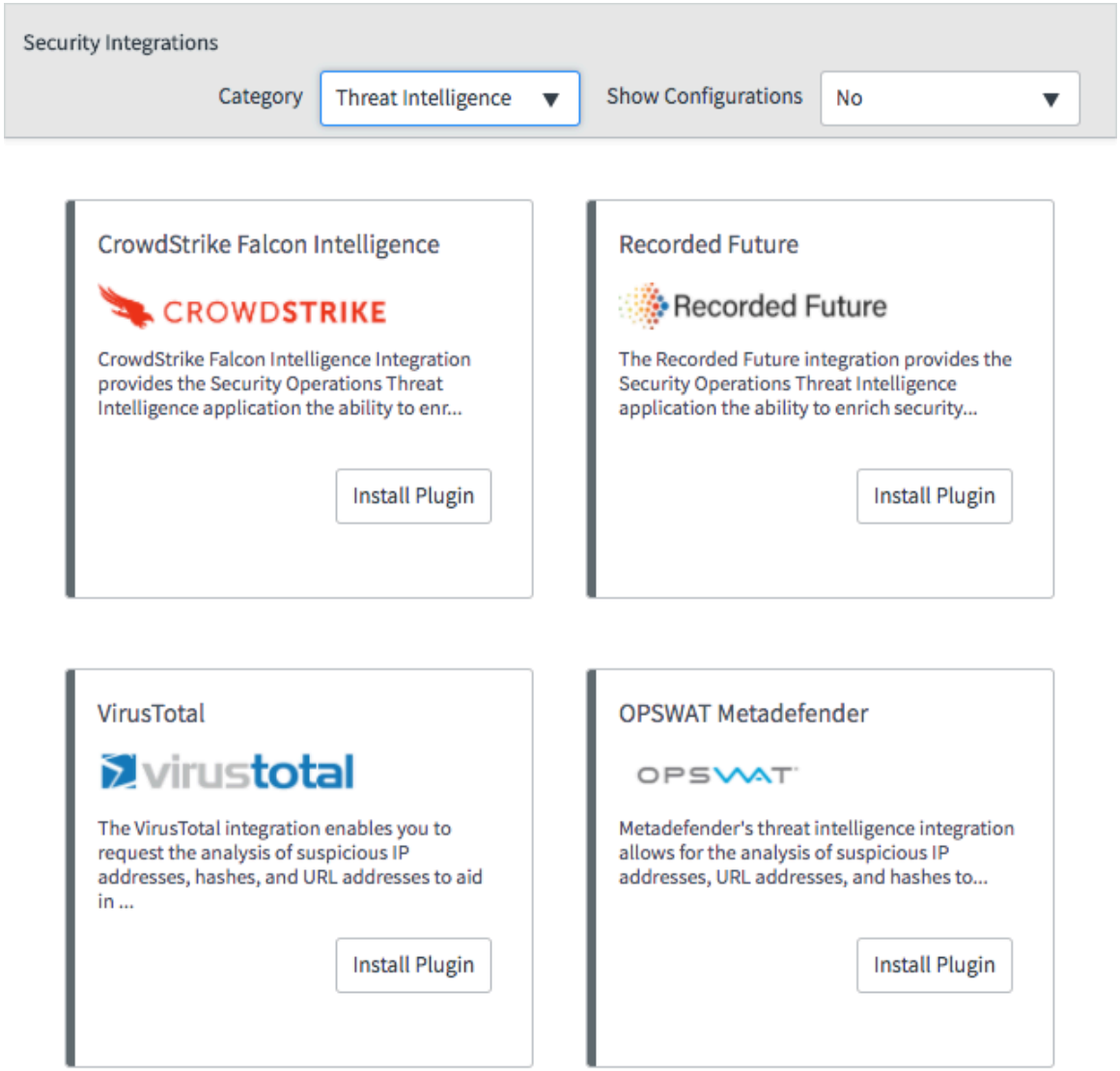
O sistema base Inteligência contra ameaças inclui integrações a pacotes de software de detecção de malware de terceiros. Esta seção fornece instruções para ativar os plug-ins e configurar ServiceNow e integrações de terceiros. Também estão incluídas algumas diretrizes básicas para desenvolver suas próprias integrações, bem como detalhes sobre integrações específicas incluídas no sistema básico.

Configurações de Integração

O sistema básico inclui uma série de "cartões" para cada uma das implementações de integração que você pode ativar e usar. Além disso, os cartões são exibidos para todas as integrações publicadas na ServiceNow Store que têm dependências nos plug-ins Security Operations. Os cartões de integração podem ser exibidos selecionando **Security Operations** > **Configurações de Integração**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Você pode filtrar as integrações visíveis usando o menu suspenso **Categoria**. O menu suspenso **Mostrar configurações** permite que você veja várias instâncias de implementações que permitem sua criação.

Botões em cartões de integração

Os cartões de integração exibem botões diferentes, dependendo do estado atual da integração e da origem do cartão.

Botão	Descrição
Instalar Plug-in	Clique neste botão para instalar o plug-in aplicável para ativar a integração. Depois que o plug-in é instalado, o botão muda para **Configurar**.
Configurar	Clique neste botão para inserir informações para configurar a integração. Para algumas integrações, pode ser necessário inserir chaves de API ou URLs adquiridos no site da integração de terceiros.
Novo	Certas integrações, como Carbon Black e IBM QRadar, permitem que você defina várias implementações da mesma integração. Para essas integrações, clique em **Novo** depois que o plug-in for ativado. Os cartões permitem instalar plug-ins (quando aplicável) e configurar as implementações para uso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Botão	Descrição
Abrir página	No sistema de base, sua instância executa uma consulta na ServiceNow Store para todas as aplicações que tenham dependências de plug-ins Security Operations. Quando essas aplicações são encontradas e os plug-ins da aplicação associados são ativados, os cartões de integração deles são exibidos com os outros cartões de integração de segurança. Clique em **Abrir página** para acessar o site da aplicação de terceiros para configurar a integração. Depois de concluir a configuração, o botão **Abrir página** muda para **Configurar**.

Integração do CrowdStrike Falcon Intelligence

CrowdStrike Falcon Intelligence enriquece Inteligência contra ameaças com dados para incidentes de segurança e observáveis associados.

Explorar

- CrowdStrike Falcon Intelligence visão geral da integração
- Integrações do Security Incident Response

Configurar

Ativar e configurar a integração CrowdStrike Falcon Intelligence

Usar

- Realizar pesquisas em observáveis
- Pesquisa de ameaças - Fluxo de trabalho CrowdStrike Falcon Intelligence

Desenvolver

- ServiceNow Security Operations diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação
- Localizar componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Faça ou responda perguntas na comunidade do Security Operations
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

CrowdStrike Falcon Intelligence visão geral da integração

CrowdStrike Falcon Intelligence fornece inteligência de segurança cibernética que se integra facilmente com Security Operations.

Nota:
O plug-in Inteligência contra ameaças é necessário para implementar a integração CrowdStrike Falcon Intelligence.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ativar e configurar a integração CrowdStrike Falcon Intelligence

O recurso Configuração de integração permite que você ative e configure rapidamente integrações de segurança de terceiros, incluindo a integração CrowdStrike Falcon Intelligence. Antes de usar o CrowdStrike Falcon Intelligence, você deve baixá-lo do ServiceNow Store e adicionar a chave de API e o ID apropriados.

Antes de Iniciar

Função necessária: administrador

- O plug-in Inteligência contra ameaças deve ser instalado e ativado antes que você possa usar a integração CrowdStrike Falcon Intelligence.
- Obtenha o ID do cliente da API e o segredo do cliente da API no seu perfil CrowdStrike Falcon Intelligence.
- Se você estiver atualizando a integração CrowdStrike Falcon Intelligence de uma versão anterior, deverá excluir a configuração existente e definir uma nova configuração. A integração oferece suporte à autenticação OAUTH2. Esta atualização requer que você insira o **ID do cliente** da **API e o segredo do cliente** da API para autenticar e concluir a configuração.
- Nos CrowdStrike Falcon Intelligence**Escopos de API**do portal, habilite a configuração de **Leitura** para **Indicadores (Falcon X)** ou **IOCs (Indicadores de compromisso)**.

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Em sua instância, navegue até **Security Operations** > **Integrações** > **Configurações de Integração**. As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão CrowdStrike Falcon Intelligence, clique em **Configurar**.
4. No formulário, preencha os campos para concluir a configuração:

CrowdStrike Falcon Intelligence Configuração

Campo	Descrição
Nome	Nome da integração, por exemplo, `demo-1`.
ID do cliente da API	O ID de cliente que você obtém na seção de configurações do perfil da sua conta no portal CrowdStrike Falcon Intelligence.
Segredo do cliente de API	A chave secreta do cliente que você obtém na seção de configurações do perfil da sua conta no portal CrowdStrike Falcon Intelligence.

5. Clique em **Enviar**.

Resultado

Depois de configurado, CrowdStrike Falcon Intelligence pode ser selecionado para executar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Realizar pesquisas em observáveis

Pesquisa de ameaças - Fluxo de trabalho CrowdStrike Falcon Intelligence

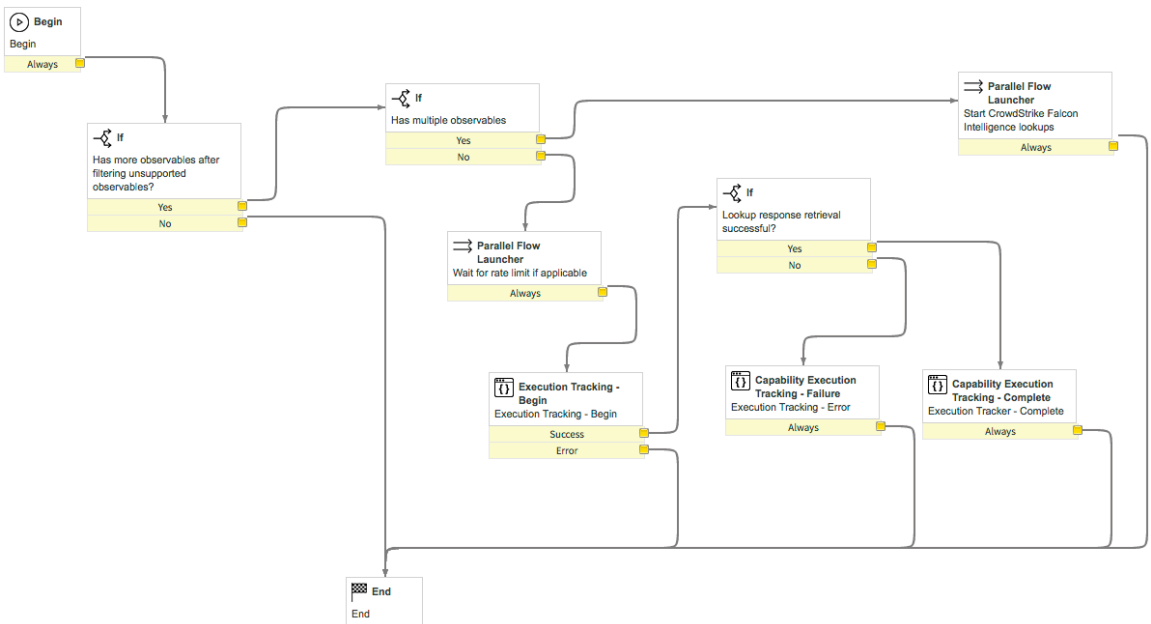
O fluxo de trabalho Pesquisa de ameaças - CrowdStrike Falcon Intelligence executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido por CrowdStrike Falcon Intelligence, eles serão verificados quanto a malware e os resultados serão retornados.

Antes de Iniciar

Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho é acionado pelo Integração do Security Operations - Pesquisa de ameaças quando você publica um ou mais observáveis em uma lista de observação e a implementação do CrowdStrike Falcon Intelligence é selecionada. Depois de publicadas, as listas de observação podem ser exibidas no software CrowdStrike Falcon Host.



Para obter informações sobre as atividades usadas por este fluxo de trabalho, consulte Atividades de fluxo de trabalho de integração comuns.

Integração de Have I been pwned?

A integração Security Operations Have I been pwned? permite que você envie pesquisas em nomes de domínio e endereços de e-mail para determinar se os dados pessoais do usuário foram comprometidos por violações de dados.

Explorar	Configurar
Integrações do Security Incident Response	• Configuração da integração do Security Operations Have I been pwned? • Ativar a integração do Security Operations Have I been pwned?

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Usar

Realizar pesquisas em observáveis Pesquisa de ameaças - Fluxo de trabalho Have I been pwned?

Desenvolver

- ServiceNow Security Operations diretrizes de desenvolvimento de integração
- Dicas para escrever integrações
- Desenvolver treinamento
- Desenvolver documentação
- Localizar componentes instalados com uma aplicação

Solucionar problemas e obter ajuda

- Solução de problemas de integração
- Faça ou responda perguntas na comunidade do Security Operations
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Configuração da integração do Security Operations Have I been pwned?

Have I been pwned? é um recurso gratuito usado para avaliar se alguém pode ter sido colocado em risco devido à violação de sua conta online ou à "pwned" em uma violação de dados. Ele se integra facilmente com Security Operations.

Antes de usar a integração Have I been pwned?, você deve ativar o plug-in. Se necessário, você também pode atualizar sua certificação SSL X509.

Os plug-ins Security Incident Response, Inteligência contra ameaçase Security Operations Have I been pwned? são necessários para implementar a integração Security Operations Have I been pwned?.

Ativar a integração do Security Operations Have I been pwned?

O recurso Configuração de integração permite que você ative e configure rapidamente integrações de segurança de terceiros, incluindo a integração Security Operations Have I been pwned?. Antes de usar a integração Have I been pwned?, você deve baixá-la do ServiceNow Store.

Antes de Iniciar

- O plug-in Inteligência contra ameaças deve ser instalado e ativado antes que você possa usar a integração Security Operations Have I been pwned?.

Função necessária: sn_si_admin

Procedimento

Baixe a integração do ServiceNow Store.
Esta integração oferece suporte a uma API aberta e não requer configuração adicional. Have I been pwned? agora pode ser selecionado para executar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tópicos relacionados

Realizar pesquisas em observáveis

Atualize seu certificado X.509

Se você precisar de uma conexão SSL para a integração, há circunstâncias em que o certificado fornecido pelo fornecedor terceirizado ainda não é confiável em ServiceNow ou expirou. Esta tarefa é opcional.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um Certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

   a. Insira o URL do endpoint na barra de endereço do navegador.
   Por exemplo: `https://<3rdparty>/`.

   b. Clique no ícone de cadeado na linha de endereço.

   c. Clique em **Mais informações** e na guia **Segurança**.

   d. Clique em **Exibir certificado** e na guia **Detalhe**.

   e. Clique em **Exportar** para salvar o PEM em seu sistema de arquivos local.

   f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
   Ele deve começar com `-----BEGIN CERTIFICATE-----` e terminar com `-----END CERTIFICATE-----`.

2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e crie um novo registro para a integração.
4. Em **Certificado PEM**, cole o certificado que você baixou e copiou para a área de transferência anteriormente.
5. Adicione o certificado ao registro do provedor de identidade.
   a. Navegar até **SSO Multiprovedor** > **Provedores de Identidade**.
   b. Selecione o provedor de identidade padrão ativo para o qual você criou o novo certificado.
   c. Role para baixo até a lista relacionada de **certificados X.509** e clique em **Editar**.
   d. Mova o certificado recém-criado para a coluna **Selecionado**.
6. Clique em **Salvar**.
   Os outros campos no registro são gerados automaticamente.

Nota:
Se você tiver um certificado que expirou, será necessário removê-lo. Para obter informações sobre como remover o certificado expirado, consulte KB0691439 Substituir um certificado SAML expirando .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de ameaças - Fluxo de trabalho Have I been pwned?

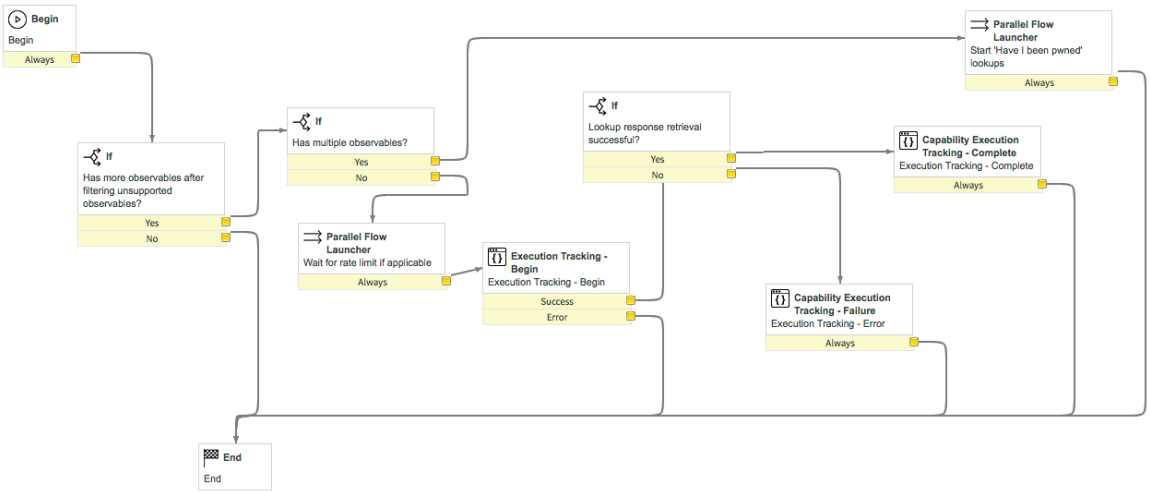
O fluxo de trabalho Pesquisa de ameaças - Have I been pwned? executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido por Have I been pwned?, eles serão verificados quanto a malware e os resultados serão retornados.

Antes de Iniciar

Função necessária: sn_si_admin

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho é acionado pelo Integração do Security Operations - Pesquisa de ameaças quando você executa uma pesquisa de ameaça em um ou mais observáveis e a implementação Have I been pwned? é selecionada. Para obter mais informações, consulte Realizar pesquisas em observáveis.



Para obter informações sobre as atividades usadas por este fluxo de trabalho, consulte Atividades de fluxo de trabalho de integração comuns.

MISP integration for Security Operations

Com MISP integration for Security Operations, você pode investigar incidentes de segurança com pesquisas de vista, enriquecimento observável e criar ou atualizar eventos em MISP. Usando MISP, você pode investigar ataques direcionados mais rapidamente, melhorar a taxa de detecção e reduzir o número de falsos positivos em seu ambiente.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral do MISP

MISP, que significa Malware Information Sharing Platform, permite trocar e compartilhar inteligência de ameaças e Indicadores de compromisso (IoCs) sobre o malware e os ataques direcionados em sua comunidade de membros confiáveis. Você também pode compartilhar MISP informações com comunidades privadas ou abertas. Ao trocar informações MISP, você pode investigar ataques direcionados mais rapidamente, melhorar a taxa de detecção e reduzir o número de falsos positivos em seu ambiente.

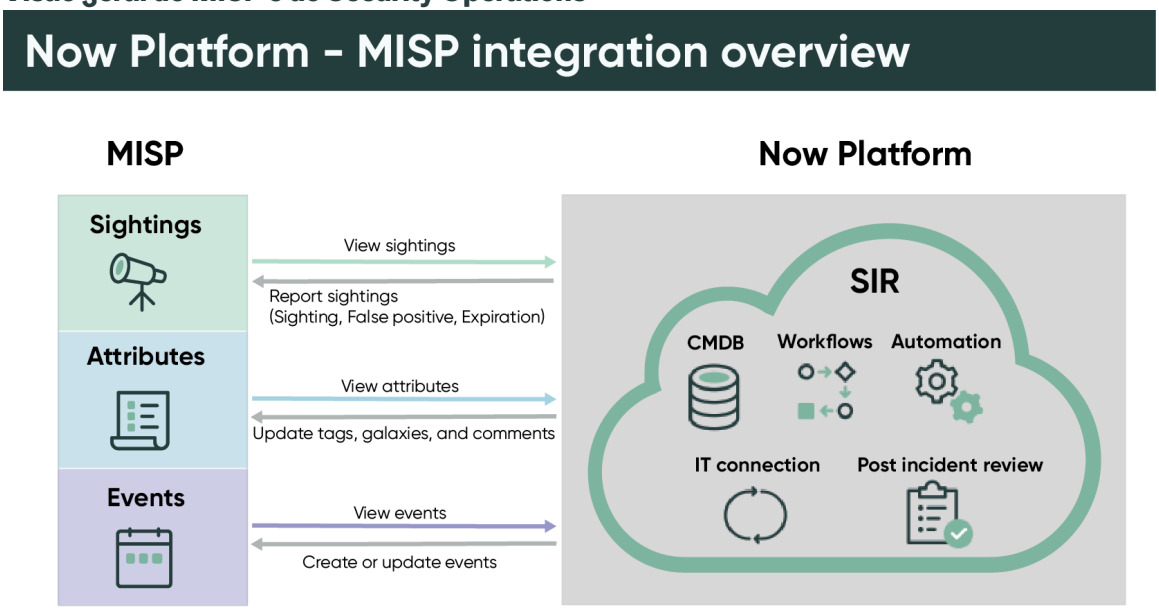
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

MISP e Security Operations

Consulte o exemplo a seguir para saber como as informações de MISP fluem com as aplicações Security Operations.

Visão geral do MISP e do Security Operations



Principais recursos

Esta integração inclui o que você pode fazer com os principais recursos MISP :

- Conectar a privado e público MISP instâncias.
- Suporte à pesquisa de vista manual e automática de observáveis.
- Executar pesquisa de vista na gestão de casos.
- Relatar ou atualizar vistas para um atributo:
  - Relatar um observável como vista (global)
  - Relatar um observável como falso positivo (global)
  - Relatar um observável como expirado
- Suporte ao enriquecimento observável manual e automático. Os resultados incluem o atributo MISP e as informações de evento associadas aos observáveis.
- Aprimoramento de atributo em MISP que inclui adicionar ou atualizar marcadores, galáxiasou comentários.
- Criação de evento no MISP de SIR: oferece suporte à criação manual e automática de eventos em MISP de SIR.
- Atualize um evento [MISP de SIR que inclui adicionar ou atualizar marcadores, galáxiasou atributos.
- Adicionar observáveis associados a incidentes de segurança como atributos a um MISP evento.
- Extrair automaticamente MITRE-ATT&CK™ informações de MISP atributos e associe as informações a SIR incidentes de segurança.
- Adicionar automaticamente SIR MITRE-ATT&CK™ informações como galáxias para um MISP evento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Principais conceitos

Esta integração inclui os seguintes conceitos-chave que você deve saber:

- MISP é uma plataforma de inteligência contra ameaças (TIP). Você usa TIPs para coletar, correlacionar, categorizar, compartilhar e integrar dados de ameaças à segurança em tempo real para oferecer suporte à priorização de ações e ajudar na prevenção, detecção e resposta de ataques.
- MISP é um TIM (Threat Intelligence Management). Você usa TIMs para transformar dados de ameaça em inteligência contra ameaças por meio de contexto e para priorizar automaticamente as ameaças por pontuação e relevância definidas pelo usuário.
- MISP Camada de dados
  - Eventos são encapsulamentos para informações vinculadas contextualmente.
  - Atributos são pontos de dados individuais, que podem ser indicadores ou dados de suporte.
  - Os objetos são composição de atributo de modelo personalizado.
  - Referências de objeto são os relacionamentos entre os outros blocos de construção.
  - Vistas são ocorrências específicas de tempo de um ponto de dados detectado.
- MISP Camada de contexto
  - Marcadores são rótulos anexados a eventos ou atributos e podem vir de taxonomias.
  - Clusters de galáxias são itens da base de conhecimento que você pode usar para rotular eventos ou atributos que vêm de galáxias.
  - Os relacionamentos de cluster denotam relacionamentos predefinidos entre clusters.
- Os indicadores contêm um padrão que você pode usar para detectar atividades cibernéticas suspeitas ou mal-intencionadas.
- Os atributos em MISP podem ser indicadores de rede (endereço IP), indicadores do sistema (uma cadeia de caracteres na memória) ou até mesmo detalhes da conta bancária. Os atributos em MISP são conhecidos como observáveis em outros SIEMs ou formatos como STIX.
  - Um tipo descreve o atributo. Por exemplo, MD5 ou um URL.
  - A categoria de atributo descreve um atributo. Por exemplo, uma entrega de carga útil.
  - Um marcador IDS determina se um atributo pode ser usado automaticamente para detecção.

Nota:
Para obter mais informações sobre conceitos MISP, consulte o site de documentação do MISP

Como sua organização pode se beneficiar do MISP integration for Security Operations

Os analistas de segurança devem obter e manter a conscientização da situação do cenário de ameaças, o que significa que eles devem consolidar e integrar manualmente uma quantidade enorme de dados de ameaças. Coletar, consolidar e integrar esses dados consome um tempo valioso, o que atrasa a detecção e a análise de ameaças. MISP integration for Security Operations permite que os analistas detectem mais ameaças e respondam mais rapidamente, integrando a inteligência de segurança MISP em uma instância Now Platform existente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ao usar o MISP integration for Security Operations, sua organização pode realizar as seguintes ações:

- Permita que seus analistas de segurança respondam rapidamente e com o contexto certo.
- Melhore a eficiência da sua equipe de segurança automatizando os fluxos de trabalho de incidentes para detectar e conter ameaças.
- Reduza o tempo de pesquisa manual e permita que os analistas de segurança operacionalizem e selecionem indicadores de dentro do Now Platform.

Conheça esta integração

Identificador de documento	Título do documento
MISP site de documentação	Site de documentação do MISP
ServiceNow site da documentação do produto	Site de documentação do produto da ServiceNow

Administração do MISP

Você pode configurar a integração MISP em Now Platform para executar uma pesquisa de vista, aprimoramento observável e para criar e atualizar eventos em MISP.

Comece com MISP integration for Security Operations

Revise as informações a seguir antes de configurar seu MISP integration for Security Operations.

Check-list

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform, Inteligência contra ameaçase Security Incident Response.	As funções a seguir são usadas nos recursos MISP no Now Platform: • O administrador (admin) instala as aplicações do ServiceNow Store e atribui as funções de administrador de incidentes de segurança (sn_si.admin) e administrador de inteligência contra ameaças (sn_ti.admin). • sn_si.admin e sn_ti.admin podem configurar a integração e configurar os perfis de criação de evento MISP automáticos. • sn_sec_misp.write — A função de analista MISP tem permissões de leitura e gravação para MISP dados que incluem os dados de evento e atributo. Para obter mais informações, consulte Configurar Inteligência contra ameaças.
Atribua as funções de usuário MISP necessárias.	Analise o MISP funções de usuário e as permissões necessárias para usar o MISP integration for Security Operations.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	Nota: Para obter mais informações sobre as funções de usuário em MISP, consulte a seção Funções no site de documentação do MISP.
Verifique se você está usando MISP versão 2.4.137 ou posterior.	O MISP integration for Security Operations foi testado com um mínimo MISP versão 2.4.137.
Verifique se as aplicações principais ServiceNow que são necessárias para oferecer suporte ao módulo MISP estão instaladas e ativadas.	Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na ordem a seguir para garantir uma instalação sem problemas. • Security Incident Response • Tempo de execução do ServiceNow IntegrationHub (com.glide.hub.integration.runtime) • Etapa de ação do ServiceNow IntegrationHub — REST (com.glide.hub.action_step.rest) Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte obter direito de um produto ou aplicação do Security Operations e ativar uma aplicação da ServiceNow Store.
Separação de Domínio	Verifique a seção de separação de domínio se você pretende separar dados, processos e tarefas administrativas.

MISP funções e permissões do usuário

Revise as funções de usuário necessárias na integração MISP integration for Security Operations.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Permissões de pesquisa de detecção e aprimoramento de observável

Nota:

- *Todos os recursos de integração de* **ServiceNow** *MISP precisam de permissões básicas para* **gerenciar eventos da organização** *e* **acesso à chave de autenticação**. *Verifique se você tem essas permissões básicas antes de prosseguir.*
- *Para adicionar galáxias locais, o usuário que configura a integração deve pertencer à organização host do servidor MISP correspondente.*

Capacidade do MISP	Marcador	Editor de marcador
Aprimoramento de observável (somente leitura)	#	#
Pesquisa de detecções (somente leitura)	#	#

Relatar Permissões de Vista

Capacidade do MISP	Criador de vistas
Relatar vista	#

Permissões de evento e atributo

Capacidade do MISP	Marcador	Editor de marcador
Editar marcadores de evento/atributo	#	#
Editar galáxias de evento/atributo	#	#
Editar Comentários do Atributo	#	#
Adicionar novo atributo ao evento	#	#
Criar evento no MISP	#	#

Instalar e configurar o MISP integration for Security Operations

Instale e configure o MISP integration for Security Operations do ServiceNow Store na sua instância Now Platform para que você possa começar a investigar incidentes de segurança usando os dados MISP.

Antes de Iniciar

Certifique-se de ter instalado os certificados SSL válidos no servidor MISP.

Função necessária: sn_si.admin

Procedimento

1. Baixe o MISP integration for Security Operations do ServiceNow Store e instale-o.
2. Navegar até **Security Operations** > **Integrações** > **Configurações de Integração**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Pesquise o bloco MISP-SIR/TI Integration e clique em **Configurar**.
4. No formulário, preencha os campos.

MISP - Formulário de configuração de integração de SIR/TI

Campo	Descrição
Nome	Nome da configuração da instância MISP.
MISP URL do servidor	URL do servidor MISP que serve como endpoint REST para o servidor MISP.
Chave de API	Chave de API configurada para sua conta de usuário no servidor MISP. A chave de API corresponde à chave de **autenticação** no servidor MISP.
Implantação no Local	Opção que você pode selecionar se o seu servidor MISP for implantado em uma instância no local. Ao selecionar a opção **Implantação no local**, você deve usar o MID Server para se conectar ao servidor MISP.
Aplicação MID	Campo de cadeia de caracteres que identifica o nome da aplicação MID usado para se comunicar com MISP. Este campo é obrigatório ao selecionar a opção **Implantação no** local. Para obter informações sobre como configurar o MID Server para sua aplicação, consulte Configurar um MID Server para cada aplicação

5. Clique em **Enviar**.

Resultado

Depois de validar e enviar a configuração com sucesso, o MISP - Integração de SIR/TI é salvo na página Integrações de segurança como um bloco.

Revisar as configurações de integração MISP

Revise as configurações de MISP integration for Security Operations e modifique as propriedades do sistema padrão para se adequar ao seu ambiente.

Antes de Iniciar

Função necessária: sn_si.admin, sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Integração MISP** > **Configurações de integração**.
2. Modifique as configurações a seguir conforme necessário.

Configurações de integração do MISP

Nome da propriedade		Descrição
Aprimoramento de Observável	Tempo (em horas) antes de buscar novos dados	Tempo em horas antes que você possa buscar novos dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da propriedade		Descrição
		Tipo: inteiro Valor padrão: 24
Pesquisa de Vistas	Executar pesquisa de vistas automaticamente quando novos observáveis forem associados ao incidente de segurança	Pesquisa de vista que é executada sempre que um novo observável é associado a um incidente de segurança. Valor padrão: sim
	Intervalo de pesquisa (em dias) para pesquisa de vista no MISP	Número de dias em que os dados de pesquisa de vista são pesquisados em MISP. Use esta opção somente para o recurso de pesquisa de vista automática. Valor padrão: 90
Sincronização de dados	Período de intervalo (em minutos) para que os marcadores sejam obtidos e sincronizados com o MISP	MISP tags que são buscadas no momento da configuração da integração. Depois que os dados estão no Now Platform, esta propriedade define a frequência com que os dados com o servidor MISP são sincronizados. O valor é definido em minutos. Valor padrão: 1440 (minutos ou 24 horas)
	Período de intervalo (em minutos) para atualizar galáxias MISP de origens configuradas	MISP galáxias que são buscadas no momento da configuração da integração. Depois que os dados estão no Now Platform, esta propriedade define a frequência com que os dados com o servidor MISP são sincronizados. O valor é definido em minutos. Valor padrão: 1440 (minutos ou 24 horas)
	Período de intervalo (em minutos) para que as organizações sejam buscadas e sincronizadas com o MISP	MISP organizações que são buscadas no momento da configuração da integração. Depois que os dados estão no Now Platform, esta propriedade define a frequência com que os dados com o servidor MISP são sincronizados. O valor é definido em minutos. Valor padrão: 1440 (minutos ou 24 horas)

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da propriedade		Descrição
MITRE™ Extração de técnica	Acumular MITRE-ATT&CK técnicas automaticamente dos Resultados de Aprimoramento Observável do MISP (Tags) para o incidente de segurança	Acúmulo de MITRE-ATT&CK informações de MISP resultados de aprimoramento observáveis (marcadores) para o incidente de segurança. Valor padrão: sim
	Acumular MITRE-ATT&CK técnicas automaticamente dos Resultados de Aprimoramento Observável do MISP (Galáxias) para o incidente de segurança	Acúmulo de MITRE-ATT&CK informações dos MISP resultados de aprimoramento observáveis (galáxias) para o incidente de segurança. Valor padrão: sim

Nota:

- Para usar os recursos de extração da técnica [MITRE™ em MISP, você deve habilitar o MITRE-ATT&CK recurso no Inteligência contra ameaças módulo.
- O MISP integration for Security Operations apresenta duas regras de extração da técnica do sistema base MITRE-ATT&CK para MISP - MISP galáxias e marcadores MISP. Para obter mais informações sobre regras de extração automática em MITRE-ATT&CK, consulte Regras de técnica de extração automática para importar informações do MITRE-ATT&CK.

3. Clique em **Salvar**.

Resultado
Suas configurações de integração modificadas serão salvas e aplicadas.

Configurar MISP pesquisas de vista

Configure o Now Platform para fazer pesquisas de vista para observáveis na instância MISP. Com essas informações, você pode determinar com que frequência as ameaças ocorrem.

Antes de Iniciar

- Analise o MISP função e permissões do usuário que são necessários para usar os recursos bidirecionais MISP.
- Função necessária: sn_si.admin, sn_ti.admin

Por Que e Quando Desempenhar Esta Tarefa
O fluxo de trabalho Security Operations Integration - Sightings Search executa as pesquisas de detecções. Este fluxo de trabalho aceita uma lista de observáveis, encontra todos os recursos de implementação, cria as consultas baseadas nas configurações de pesquisa de vista e executa as pesquisas baseadas no fluxo de trabalho configurado.

O MISP integration for Security Operations fornece um perfil de pesquisa de vista do sistema de base que permite configurar pesquisas de vista automáticas. Com este perfil, você pode acessar as informações de vista observável relacionadas de uma organização e também ver as vistas externas de outras organizações.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Integração MISP** > **Configuração de pesquisa de detecções**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de Configuração de pesquisa de vistas

Campo	Descrição
Nome	Nome do perfil de recurso.
Pesquisa salva	Configuração de pesquisa que é salva quando você seleciona esta opção. As consultas de configuração de pesquisa salvas são consultas de exemplo. Você pode substituí-los pelos parâmetros do seu ambiente e criar configurações adicionais de pesquisa salva, conforme necessário.
Origem de pesquisa de vistas	Origem da pesquisa de vistas. Selecione o armazenamento de log MISP como a origem.
Ativo	Opção que habilita a configuração de pesquisa salva. Somente configurações de pesquisa ativas podem executar uma pesquisa de vistas.
Tipo de observável	Tipo de observável, como endereço IP, valor de hash, URL e nome de domínio.
Máximo observável por pesquisa	Número máximo de observáveis que você pode exibir em uma consulta de pesquisa.
Pesquisar	Cadeia de caracteres de pesquisa padrão que é `$(observable)`. No entanto, você define sua própria consulta de pesquisa especificando os parâmetros compatíveis com o armazenamento de logs MISP.

4. Clique em **Enviar**.

Resultado
Você criou um perfil de configuração de pesquisa de detecções MISP.

Configurar como um evento automático é criado

Configure o Now Platform para criar automaticamente eventos em MISP.

Antes de Iniciar

- Analise o MISP função e permissões do usuário que são necessários para usar os recursos bidirecionais MISP.
- Função necessária: sn_si.admin, sn_ti.admin

Procedimento

1. Navegar até **Todos** > **Integração MISP** > **Perfis automáticos de criação de evento**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário de nome

Campo	Descrição
Nome	Nome do perfil de criação automática de eventos.
Descrição	Breve descrição do perfil. Uma descrição mais detalhada é compartilhada por meio dos atributos na próxima fase da criação do evento.
Ordem	Ordem do perfil quando as condições de gatilho são atendidas. O padrão é 100. Deixe esta configuração como padrão. Se você criar vários perfis, este valor fornecerá uma prioridade de execução em tempo de execução quando dois ou mais perfis compartilharem condições de gatilho. O perfil com o número mais baixo tem a prioridade mais alta.
Fonte	MISP origem para a criação do evento.
Ativo	Opção que indica se o perfil está ativo ou inativo. A opção é desmarcada por padrão para indicar que o perfil está desativado. Este perfil não está ativo até que você conclua todas as etapas de configuração do perfil e clique em **Concluir**.

4. Clique em **Continuar**.

Configurar condições do gatilho de evento

Configure as condições do gatilho de evento em Now Platform para que você possa acionar automaticamente um evento em MISP quando as condições forem atendidas.

Antes de Iniciar

Função necessária: sn_sec_misp.write

Procedimento

1. No formulário Condições do gatilho, preencha os detalhes que podem acionar um evento.
   Você pode criar uma lógica composta fornecendo as condições do gatilho que são baseadas em campos de incidente de segurança ou campos observáveis. Você também pode criar eventos em MISP se os observáveis não tiverem um evento correspondente em MISP. Você pode optar por criar uma lógica composta usando uma combinação das três condições do gatilho - Acionar com base em campos de incidente de segurança, Acionar com base em campos de observáveis e Criar evento de MISP, se um observável não tiver eventos correspondentes no MISP. Se você selecionar vários gatilhos, poderá juntá-los usando a condição AND. Considere criar um perfil com novas condições se você precisar usar a condição OU.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Formulário Condições do gatilho de evento

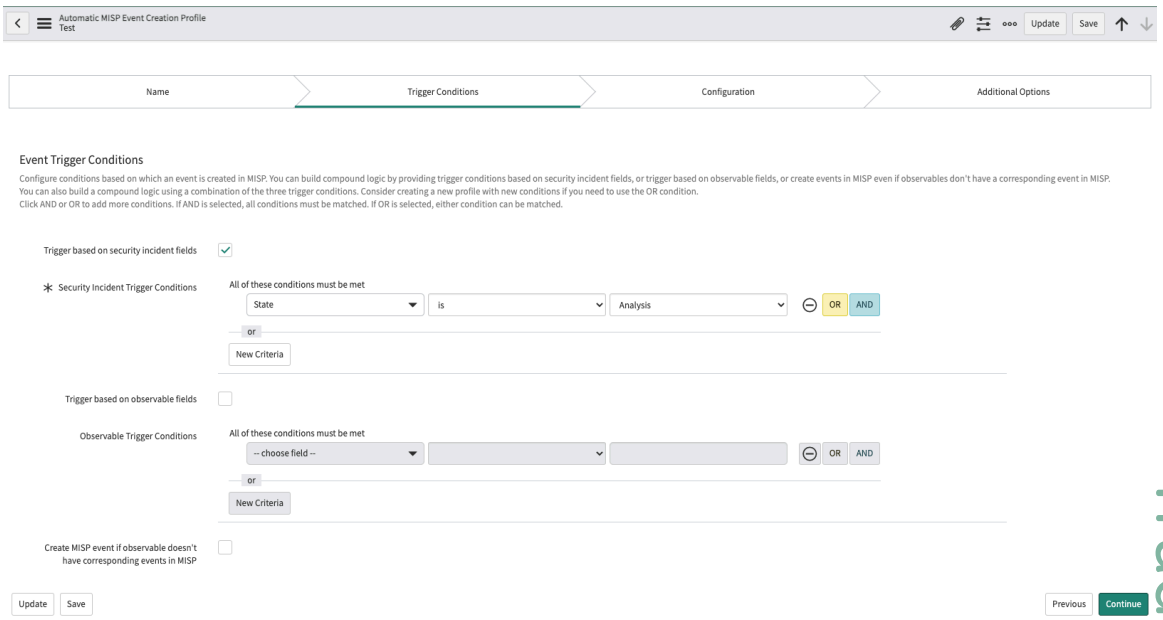
Campo	Descrição
Acionar com base nos campos de incidente de segurança	MISP evento que você pode criar se todas as condições do gatilho de incidente de segurança forem atendidas.
Condições do gatilho de incidente de segurança	Filtros na primeira linha que você pode definir usando as listas e os campos do construtor de condições. Para adicionar mais condições, clique em E ou OU. Se AND for selecionado, todas as condições deverão ser correspondidas. Se OU for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**.
Acionar com base em campos observáveis	MISP evento que você pode criar se todas as condições do gatilho observáveis forem atendidas.
Condições do gatilho observáveis	Filtros na primeira linha que você pode definir usando as listas e os campos do construtor de condições. Para adicionar mais condições, clique em E ou OU. Se AND for selecionado, todas as condições deverão ser correspondidas. Se OU for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**.
Criar evento MISP se o observável não tiver eventos correspondentes no MISP	MISP evento que você pode criar se um observável não tiver eventos correspondentes em MISP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Condições do gatilho de evento

O exemplo a seguir mostra as condições do gatilho de evento conforme você configura o perfil de criação de evento MISP.



2. Clique em **Continuar**.

Mapear os campos de evento MISP

Mapeie os campos de evento MISP no Now Platform para que as informações do incidente de segurança estejam disponíveis quando os eventos MISP forem criados.

Antes de Iniciar

Função necessária: sn_sec_misp.write

Procedimento

1. No formulário, preencha os campos.

Formulário de mapeamento de campo de evento MISP padrão

Campo	Descrição
Informações do evento	Informações do evento que são criadas automaticamente a partir de Now Platform Security Incident Response. O campo **Informações do evento** oferece suporte a variáveis de substituição usando ${SIR FIELD LABEL}$. Durante a criação de um evento, essas variáveis são substituídas pelos valores reais do campo de incidente de segurança. A variável de substituição ${URL}$ é substituída pelo URL do incidente de segurança.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Distribuição	Opção que controla quem pode exibir este evento depois que ele é publicado. Esta opção também controla se o evento é sincronizado com outros servidores. A distribuição é herdada pelos atributos e a configuração mais restritiva vence. As opções de distribuição são as seguintes: ○ Somente sua organização: permite que somente membros da sua organização exibam este evento. O evento pode ser puxado para outra instância por um dos membros da sua organização, onde somente sua organização pode ter acesso para exibi-lo. Eventos com esta configuração não são sincronizados. ○ Somente esta comunidade: permite que os usuários que fazem parte da sua comunidade MISP exibam o evento, incluindo sua própria organização, organizações neste servidor MISP e organizações que executam servidores MISP que são sincronizados com este servidor. Todas as outras organizações que se conectam aos seus servidores vinculados têm restrição para exibir o evento. ○ Comunidades conectadas: permite que os usuários que fazem parte da sua comunidade MISP exibam o evento, incluindo todas as organizações neste servidor MISP, todas as organizações nos servidores MISP que sincronizam com este servidor e as organizações de hospedagem de servidores que se conectam a qualquer servidor que está a dois saltos de distância. Quaisquer outras organizações conectadas aos servidores vinculados que estão a dois saltos de distância têm restrição para exibir o evento. ○ Todas as comunidades: compartilha o evento com todas as MISP comunidades.
Nível de ameaça	Campo que indica o nível de risco do evento. Você pode categorizar os incidentes em três categorias de ameaça diferentes (baixa, média e alta). Este campo também pode ser deixado como indefinido. A seguir estão as opções:

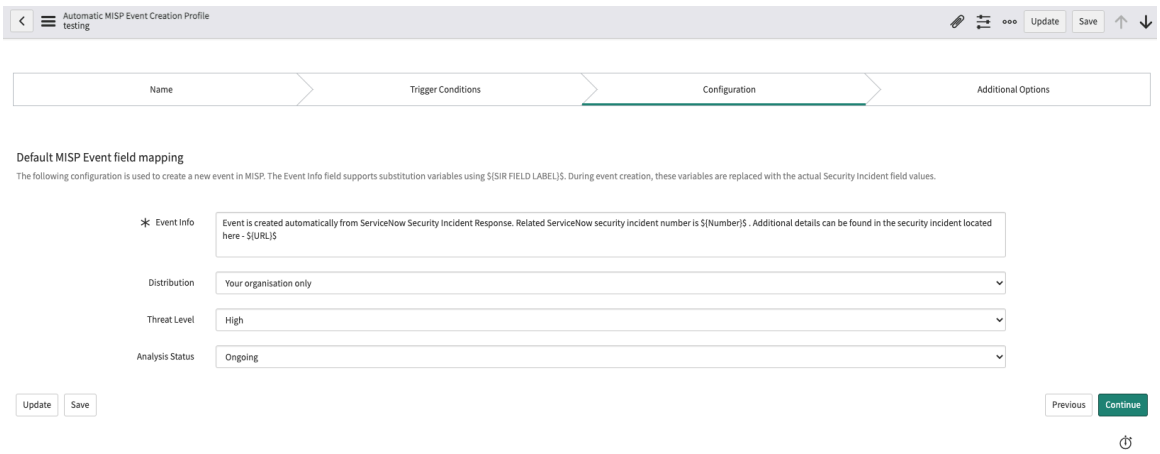
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Baixo: malware geral em massa ○ Média: ameaças persistentes avançadas (APT) ○ Alto: APTs sofisticados e ataques de dia 0
Status da análise	Fase atual da análise do evento, com as seguintes opções possíveis: ○ Inicial: a análise está apenas começando ○ Em andamento: a análise está em andamento ○ Concluído: a análise está concluída

O exemplo a seguir mostra o formulário que você pode usar para criar um evento no MISP.

Mapeamento de campo de evento MISP padrão



2. Clique em **Continuar**.

Mapear ou associar SIR observáveis como atributos para MISP eventos

Mapeie os tipos de observáveis Security Incident Response para os tipos de atributo MISP porque os tipos de atributo MISP e os observáveis SIR podem ser diferentes.

Antes de Iniciar

Função necessária: sn_sec_misp.write

Por Que e Quando Desempenhar Esta Tarefa

O MISP integration for Security Operations fornece um mapeamento do sistema de base que você usa ao adicionar SIR observáveis como atributos a um evento MISP.

Você pode optar por modificar o mapeamento do sistema de base para se adequar ao seu ambiente. Por exemplo, você pode mapear vários observáveis SIR para apenas um tipo de atributo MISP. Se algum tipo de observável não estiver mapeado, o **outro** MISP tipo de atributo será selecionado por padrão.

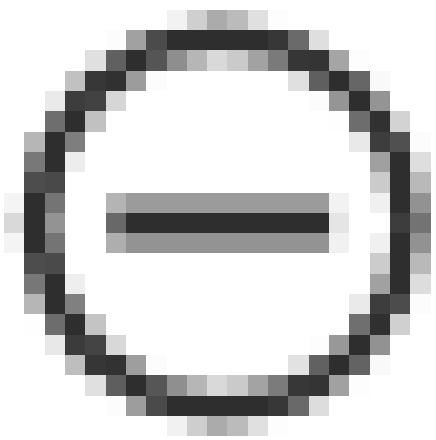
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. No formulário Opções adicionais, mapeie os tipos de atributo SIR observável e MISP.
2. Mapeie os tipos de observável Security Incident Response para os tipos de atributo MISP conforme descrito na tabela a seguir.

Mapeamento do observável de SIR e tipo de atributo do MISP

Campo	Descrição
Adicionar todos os observáveis associados como atributos	Opção que você habilita para adicionar observáveis disponíveis em um incidente de segurança a um evento MISP como atributos. Esta opção habilita o mapeamento na seção Tipo de observável para mapeamento de tipo de atributo.
Tipo de observável para mapeamento de tipo de atributo	Opção para mapear os tipos de observável SIR para os tipos de atributo MISP. Por exemplo, você pode mapear o Número CVE em SIR para o atributo de vulnerabilidade em MISP. Você pode adicionar um tipo de observável SIR a apenas um tipo de atributo MISP. O sistema de base fornece um mapeamento dos tipos de observável SIR para os tipos de atributo MISP. Se algum tipo de observável SIR não estiver mapeado para um tipo de atributo MISP, o observável será mapeado para o **outro** tipo de atributo em MISP. Para adicionar um novo mapeamento, clique em **Adicionar tipo de observável**, pesquise o tipo de observável SIR e mapeie para o tipo de atributo MISP correspondente. Clique no ícone 

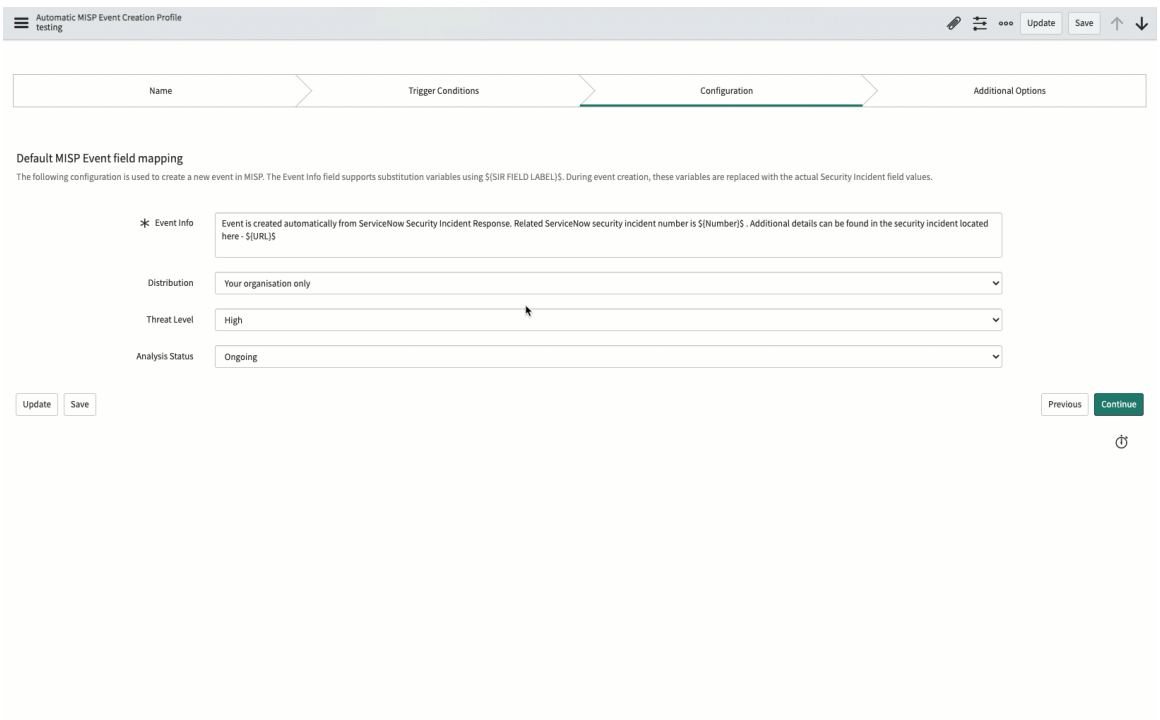
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	para remover a associação de mapeamento de atributo SIR e MISP. **Nota:** Para obter mais informações sobre os tipos de atributo MISP, consulte a documentação do MISP .
Definir sinalizador de IDS de atributo quando a descoberta observável for mal-intencionada	Opção que permite saber que se um observável estiver marcado como mal-intencionado em SIR, o atributo correspondente em MISP terá o sinalizador IDS habilitado. Se o sinalizador IDS não estiver definido, o atributo será considerado como informação contextual e não será usado para detecção automática de intrusão.

O exemplo a seguir mostra como navegar até a página de opções adicionais. Nesta página, você pode habilitar os observáveis SIR e o mapeamento de tipos de atributo MISP, adicionar novos tipos de observáveis SIR, como a rede IPV6 e a rede IPV4, e mapeá-los para o endereço IP de domínio do tipo de atributo MISP.

Mapeamento de SIR observáveis e MISP tipos de atributo



Sincronizar informações MISPMITRE-ATT&CK para eventos []

Sincronize as informações [MITRE-ATT&CK com os atributos MISP para obter uma melhor análise de ameaças e incidentes de segurança.

Antes de Iniciar
Função necessária: sn_sec_misp.write

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

No formulário Opções adicionais, revise as opções para sincronizar as informações de MITRE-ATT&CK com os atributos MISP.

Formulário Opções avançadas

Campo	Descrição
Sincronizar técnicas de Incidente de segurança MITRE-ATT&CK™ como galáxias locais para o evento MISP	Opção para sincronizar as técnicas de Now Platform SIR incidente de segurança MITRE-ATT&CK™ como galáxias locais no evento MISP. **Nota:** Para adicionar galáxias locais, o usuário que configurou a integração deve pertencer à organização host do servidor MISP correspondente.
Sincronizar técnicas de Incidente de segurança MITRE-ATT&CK™ como galáxias globais para o evento MISP	Opção para sincronizar as técnicas de Now Platform SIR incidente de segurança MITRE-ATT&CK™ como galáxias globais no evento MISP.

Resultado

Você criou um perfil que permite criar eventos automaticamente em MISP a partir de Now Platform. Agora você pode exibir os eventos na lista relacionada de eventos de MISP associados.

MISP dados do evento

Você pode revisar os dados do evento MISP para ver informações detalhadas sobre os eventos MISP.

MISP dados de evento na exibição de lista

Acessar a exibição de lista de **MISP** > **Dados do evento de MISP**.

Use a exibição de lista para obter uma visão geral rápida dos dados do evento MISP.

Exibição da lista de eventos de MISP

Campo	Descrição
ID de Evento	ID do evento atribuído por MISP quando o evento foi criado ou importado pela primeira vez para o servidor MISP.
Informações	Descrição resumida do evento.
Análise	Fase atual da análise do evento com as seguintes opções possíveis: • Inicial: a análise está apenas começando • Em andamento: a análise está em andamento • Concluído: a análise está concluída

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição da lista de eventos de MISP

Campo	Descrição
Nível de ameaça	Nível de risco do evento. Os incidentes podem ser categorizados em três categorias de ameaça diferentes (baixa, média e alta). Este campo pode ser deixado como indefinido. A seguir estão as opções: • Baixo: malware geral em massa • Média: ameaças persistentes avançadas (APT) • Alto: APTs sofisticados e ataques de dia 0
Marcadores MISP	Marcadores associados ao evento MISP.
Galáxias MISP	Galáxias associadas ao evento MISP.
Organização do proprietário	Organização que possui o evento na instância MISP. Este campo está visível somente para os administradores.
Organização do criador	Organização que criou o evento na instância MISP.
Distribuição	Distribuição do atributo individual. Um atributo pode ter um nível de distribuição diferente do evento.
Hiperlink de evento MISP	Link para o evento MISP que é armazenado no servidor MISP.
Origem do MISP	MISP origem em que o evento é criado.

MISP dados de evento na exibição de formulário

Use a exibição de formulário para obter informações detalhadas sobre os eventos MISP.

Exibição de formulário de evento de MISP

Campo	Descrição
ID de Evento	ID do evento atribuído por MISP quando o evento foi criado ou importado pela primeira vez para o servidor MISP.
UUID	ID que identifica exclusivamente eventos e atributos.
Organização do criador	Organização que criou o evento na instância MISP.
Organização do proprietário	Organização que possui o evento na instância MISP. Este campo está visível somente para os administradores.
Usuário do criador	Usuário que criou o evento em MISP.
Última mudança	Data em que o evento foi modificado pela última vez.
Origem do MISP	MISP origem em que o evento é criado.
Data de criação (no MISP)	Data em que o evento foi criado ou importado pela primeira vez no servidor MISP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de formulário de evento de MISP

Campo	Descrição
Nível de ameaça	Nível de risco do evento. Os incidentes podem ser categorizados em três categorias de ameaça diferentes (baixa, média e alta). Este campo pode ser deixado como indefinido. A seguir estão as opções: • Baixo: malware geral em massa • Média: ameaças persistentes avançadas (APT) • Alto: APTs sofisticados e ataques de dia 0
Análise	Fase atual da análise do evento com as seguintes opções possíveis: • Inicial: a análise está apenas começando • Em andamento: a análise está em andamento • Concluído: a análise está concluída
Distribuição	Distribuição do atributo individual. Um atributo pode ter um nível de distribuição diferente do evento.
Publicado	Status de se o evento foi publicado ou não. A publicação permite que os atributos do evento sejam usados para todas as exportações qualificadas e notifica os usuários que assinaram os alertas de evento.
Hiperlink de evento MISP	Link para o evento MISP que é armazenado no servidor MISP.
Informações	Descrição resumida do evento.
Marcadores (locais)	Marcadores que estão disponíveis na instância MISP da organização host para habilitar a marcação para sincronização e filtragem de exportação. MISP eventos não são modificados quando você usa marcadores locais. Marcadores locais são sempre removidos antes de serem sincronizados com outras instâncias MISP e comunidades de compartilhamento.
Marcadores (Globais)	Marcadores que estão disponíveis globalmente para serem compartilhados e sincronizados com outras instâncias MISP e comunidades de compartilhamento. Ao adicionar marcadores globais a instâncias MISP, você pode modificar eventos.
Galáxias (locais)	Galáxias que estão disponíveis na instância MISP da organização do host para sincronização e filtragem de exportação. MISP eventos não são modificados quando você usa galáxias locais. Essas galáxias locais são sempre removidas antes de serem sincronizadas com outras instâncias MISP e comunidades de compartilhamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de formulário de evento de MISP

Campo	Descrição
Galáxias (Global)	Galáxias que estão disponíveis globalmente para serem compartilhadas e sincronizadas com outras instâncias MISP e comunidades de compartilhamento. Ao adicionar galáxias globais, MISP é possível modificar eventos.

Eventos associados MISP

Você pode usar a exibição de lista de eventos MISP associada para exibir os eventos que foram criados manual ou automaticamente no contexto de um incidente de segurança.

Eventos de MISP associados

Campo	Descrição
Incidente de segurança	SIR incidente de segurança. Clique no incidente de segurança para exibi-lo.
Evento MISP	MISP ID do evento. Clique no evento MISP para exibir o evento MISP no Now Platform.
Origem do MISP	MISP origem em que o evento é criado. Clique na origem MISP para exibir a origem.
Modo de criação de evento	Status de se o evento foi criado manualmente ou automaticamente com o perfil de criação de evento. Clique no evento MISP para exibir o evento MISP associado.
Perfil de criação automática de evento	Perfil de criação de evento usado para criar o evento automático. Clique no perfil para exibir o perfil de criação automática de evento de MISP.

MISP informações do usuário

Você pode usar a página de informações do usuário MISP para exibir todos os usuários associados a Now Platform MISP integration for Security Operations.

Informação do usuário de MISP

Campo	Descrição
Fonte	Origem da conta do usuário MISP.
ID do usuário	ID do usuário que é atribuído pelo servidor MISP quando uma conta de usuário é criada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Informação do usuário de MISP

Campo	Descrição
E-mail do Usuário	Endereço de e-mail de um usuário. Somente os administradores da organização podem ver os endereços de e-mail dos usuários da própria organização.
Organização	Organização à qual um usuário pertence.
Nome da Função	Nome da função que define os privilégios do usuário que são atribuídos a um usuário. Para obter mais informações sobre funções em MISP, consulte a documentação do MISP.
ID de Função	ID da função do usuário em MISP. Por exemplo, Perm Admin, Perm Audit ou Perm Tagger e assim por diante.
Permissão	Permissões que um usuário tem. As permissões que estão disponíveis no MISP são as seguintes: • Somente Leitura • Gerenciar eventos próprios • Gerenciar eventos da organização • Gerenciar Publicar eventos da organização
Permissão de vista	Permissão que permite ao usuário realizar pesquisas de vista.
Permissão do tagger	Permissão que permite que um usuário faça marcação.

Separação de domínios e MISP

Separação de domínios é compatível com MISP. O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: Básico.

Como o Domain Separation funciona com MISP

Siga estas etapas para obter a separação de domínio:

- Crie um usuário com as funções necessárias em seu domínio.
- Execute os procedimentos MISP integration for Security Operations em seu domínio.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Solução de problemas da integração do MISP

Esta seção cobre dicas importantes de solução de problemas que podem ajudá-lo a resolver problemas comuns que podem ser encontrados ao configurar ou executar a integração do MISP.

Problemas de SSL

Ao se conectar por meio da integração MISP, certifique-se de ter instalado um certificado de CA válido no servidor MISP, que não tenha expirado. Você pode importar o RSA ou seus próprios certificados para a plataforma e garantir que o nome comum do certificado corresponda ao nome do host. Para obter mais informações, consulte Instalar e configurar o MISP integration for Security Operations e MISP funções e permissões do usuário.

Usando MISP para investigar e analisar ameaças

Você pode usar os dados MISP] no módulo Now Platform Inteligência contra ameaças e no módulo Now Platform SIR para investigar e analisar ameaças à sua organização.

Pesquisas de vista em MISP

Você pode executar pesquisas de vista em observáveis na instância MISP para determinar com que frequência determinados tipos de ataques, como ataques de phishing ou comunicações com um IP ou URL mal-intencionado, ocorrem em sua rede. Cada ocorrência é considerada uma vista.

Vistas em MISP

As vistas indicam que um indicador, objeto ou atributo foi visto e sua validade foi confirmada. Vistas em MISP é um sistema que permite responder a atributos em um evento. Ele foi projetado para fornecer um método fácil para os usuários confirmarem que viram um determinado atributo, dando a ele mais confiabilidade. Você pode visualizar um atributo várias vezes.

Nota:
Os observáveis são conhecidos como atributos no MISP.

Alguns atributos são considerados falsos positivos, o que significa que eles não são vistas válidas. Outros atributos são válidos apenas por uma determinada duração, como uma campanha de phishing que é executada por apenas uma semana. Você pode atribuir uma data de expiração aos atributos que são válidos por uma determinada duração, mas cada organização pode atribuir apenas uma data de expiração válida a um atributo.

As vistas criadas em MISP por usuários de organizações marcadas como locais no servidor MISP correspondente são conhecidas como vistas internas. As vistas criadas em MISP por usuários de organizações marcadas como remotas no servidor MISP correspondente são conhecidas como vistas externas.

Pesquisas de vista em SIR

O fluxo de trabalho Security Operations Integration - Sightings Search executa a pesquisa de detecções. Este fluxo de trabalho aceita uma lista de observáveis, encontra todos os recursos de implementação, cria as consultas baseadas nas configurações de pesquisa de vista e executa as pesquisas baseadas no fluxo de trabalho configurado.

As pesquisas de detecções ajudam os analistas a determinar a predominância de uma ameaça ao longo do tempo. Você pode selecionar observáveis individuais ou vários e o intervalo de datas para sua pesquisa de um incidente de segurança. Os resultados são

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

incluídos nas listas relacionadas Detecçõesde incidentes de segurança , Resultadosda pesquisa de detecções e Detalhes da pesquisa de detecções.

Ao começar a analisar um incidente, você pode configurar seu Now Platform para executar automaticamente uma pesquisa de vistas ou executar manualmente uma pesquisa de vistas observáveis para identificar outros usuários em sua organização que foram afetados pelo mesmo ataque de phishing.

Habilitar pesquisas de vista automáticas no MISP

Habilite a pesquisa de detecções em MISP para ser executada automaticamente para que o fluxo de trabalho Integração do Security Operations - Pesquisa de detecções seja acionado sempre que novos observáveis forem associados a um incidente de segurança.

Antes de Iniciar

Verifique se o Perfil de configuração de pesquisa de vistas para MISP está ativo.

Função necessária: sn_si.analyst

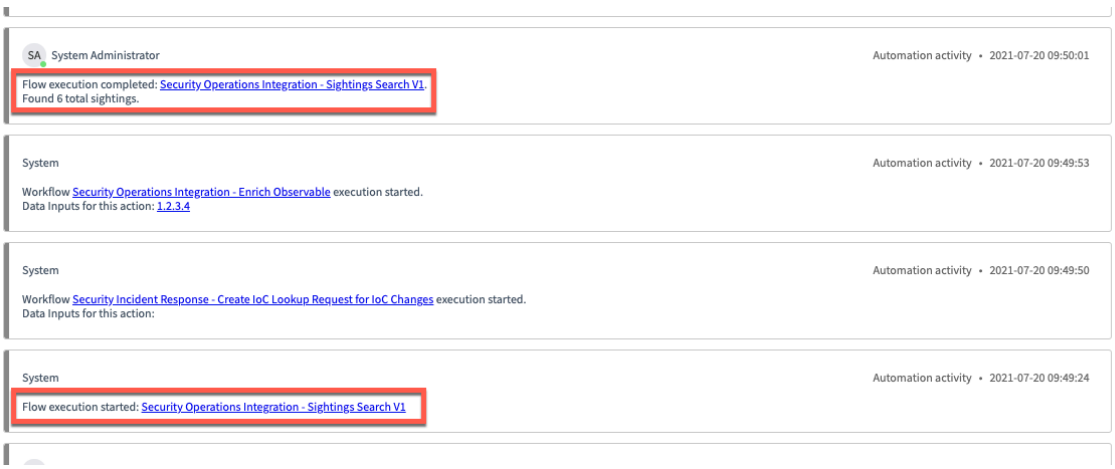
Por Que e Quando Desempenhar Esta Tarefa

Se você habilitar a capacidade de pesquisa de vista seja executada automaticamente no MISP configuração de integração do, a pesquisa de vista em MISP é acionada quando novos observáveis são associados a um incidente de segurança. Por padrão, a opção **Executar pesquisa de vista automaticamente quando novos observáveis são associados ao incidente de segurança** está habilitada.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que contém os observáveis que você deseja exibir nos dados de pesquisa de detecções MISP.
3. Revise as anotações de trabalho depois que novos observáveis forem associados ao incidente de segurança. Uma anotação de trabalho é publicada quando o fluxo de trabalho Integração do Security Operations - Pesquisa de detecções é acionado.

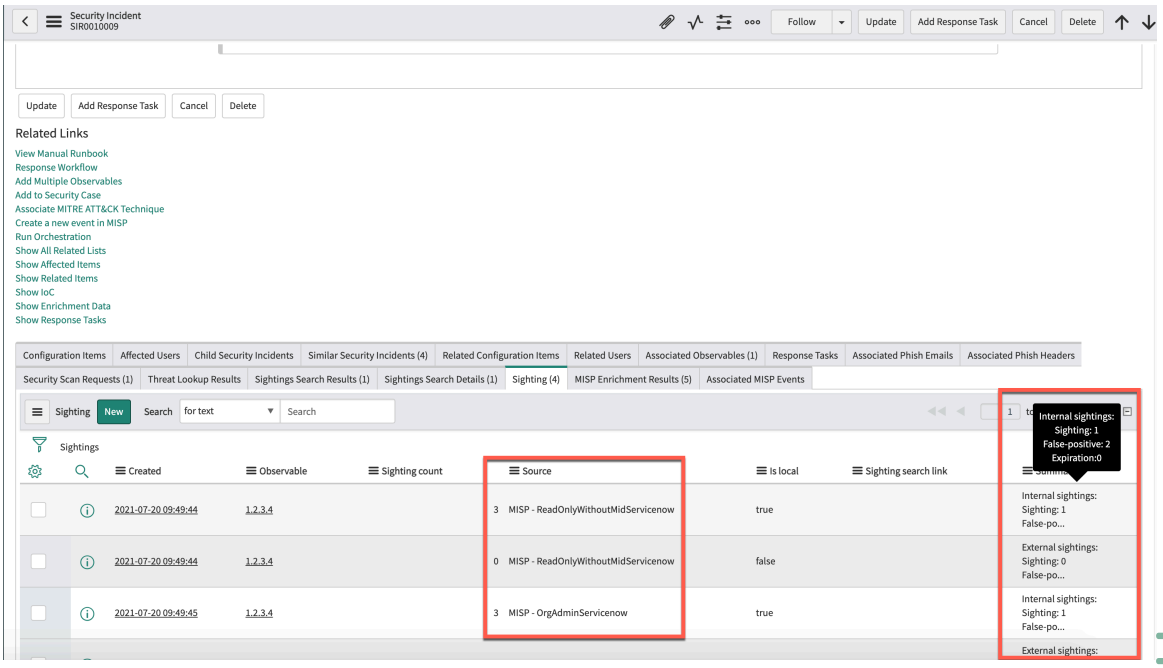
   O exemplo a seguir mostra a seção de anotações de trabalho.



4. Exiba as informações agregadas de observáveis que são vistos em todos os eventos (globais) e categorizados por suas vistas internas ou externas após a conclusão da execução do fluxo de trabalho.
   Exiba as informações nas listas relacionadas Vistas, Resultadosda pesquisa de vistas e Detalhes da pesquisa de vistas.O exemplo a seguir mostra o registro de pesquisa de vistas que foi criado na lista relacionada Vistas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Registro de pesquisa de detecções

Campo	Descrição
Criado em	Data e hora em que o registro de pesquisa de vistas foi criado.
Observável	Observável que é pesquisado pela consulta.
Contagem de vista	Contagem de avistamentos internos e externos.
Fonte	Origem do observável. Se o observável for de uma organização MISP, o registro será precedido pelas palavras MISP.
É local	Status de se a vista foi relatada por um usuário interno.
Link de pesquisa de vista	Link de pesquisa de detecções na instância MISP.
Resumo	Tipo de vistas associadas ao registro. Os três tipos de Detecções são Detecção, Falso-positivo e Vencimento. A coluna Resumo aparece somente quando o MISP integration for Security Operations está instalado. Se outras fontes além de MISP forem exibidas, a entrada da coluna Resumo estará vazia para esse registro.

Executar uma pesquisa de vista manual no MISP

Selecione um ou vários observáveis e execute uma pesquisa de vista manual na aplicação Now Platform MISP integration for Security Operations para determinar a predominância de uma ameaça ao longo do tempo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Analise o MISP função e permissões do usuário para usar os recursos bidirecionais MISP.
- Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja executar a pesquisa de detecções MISP.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Observáveis associados**.
4. Selecione o observável e, no menu Ações, clique em **Executar pesquisa de detecções**.
   Você pode selecionar vários observáveis para uma pesquisa de vista.
   A caixa de diálogo Executar pesquisa de vistas é aberta.
5. Especifique o intervalo de datas para pesquisar os dados de pesquisa de detecções.

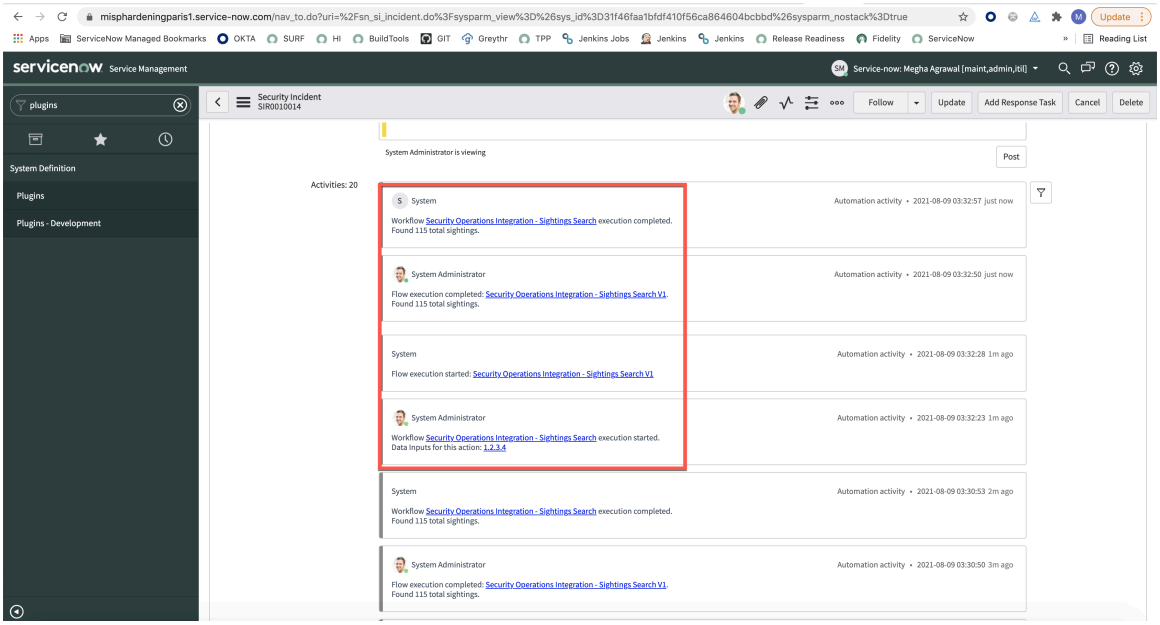
Caixa de diálogo Executar pesquisa de vistas

Campo	Descrição
Último	Número de horas ou dias anteriores à criação do incidente a ser pesquisado. O padrão é 7 dias. O limite é de 99 horas ou dias.
entre	Intervalo de datas para pesquisa. As datas padrão são as seguintes: ○ A data e a hora em que o incidente foi criado. ○ A data e a hora que são sete dias antes da abertura do incidente.

6. Clique em **Pesquisar**.
   O exemplo a seguir mostra os resultados da pesquisa de vista manual nas anotações de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Resultado

Um registro de pesquisa de detecções é criado. Depois que a execução do fluxo de trabalho for concluída, você poderá exibir as informações agregadas dos observáveis que são vistos em todos os eventos (globais) e categorizados por suas vistas internas ou externas. Os dados agregados e de avistamentos associados são exibidos no incidente de segurança nas listas relacionadas Avistamentos, Resultadosda pesquisa de avistamentos e Detalhes da pesquisa de detecções.

Relatar vistas para MISP

Relate avistamentos de dados de ameaças para que você possa reagir a falsos positivos em seus dados e aumentar sua conscientização quando ocorrer uma ameaça verdadeira. Você também pode adicionar uma data de expiração para um observável ou atributo específico.

Antes de Iniciar

- Analise o MISP função e permissões do usuário para usar os recursos bidirecionais MISP.
- Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

O MISP integration for Security Operations permite que você relate avistamentos para MISP globalmente em todos os eventos. Para relatar um avistamento para um evento específico, você deve usar a instância MISP e relatar o avistamento localmente.

Para relatar uma vista para MISP, o observável ou o atributo deve estar disponível na instância MISP.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja relatar as vistas para MISP.
3. Clique **em Mostrar todas as listas relacionadas** e na lista relacionada de Vistas.
4. Selecione o observável e, no menu Ações, selecione uma das opções a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se você selecionar observáveis que não sejam específicos de uma origem MISP, o menu Ações mostrará a contagem de origens MISP relevantes. O exemplo a seguir mostra quatro de oito observáveis relevantes para MISP.O exemplo a seguir mostra o menu de ações e os observáveis relevantes para envio.

Menu Ações que mostra os observáveis relevantes para envio

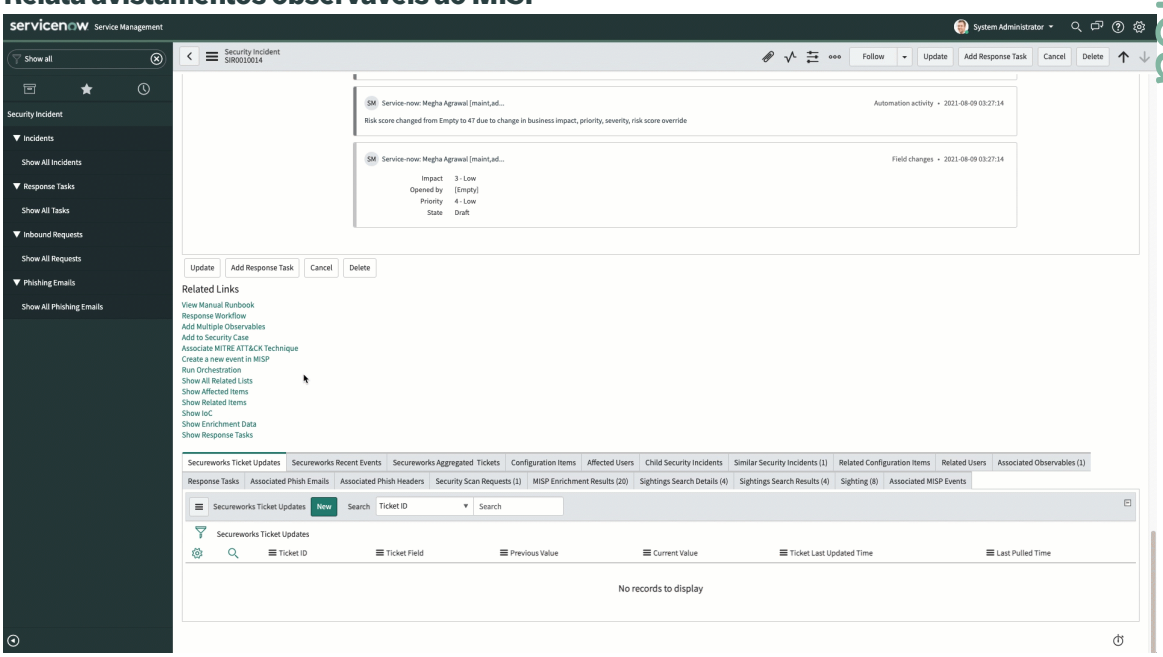
5. **Opcional:** Se você selecionou a opção **MISP: Relatar vista observável**, deverá preencher os campos da caixa de diálogo Relatar vista observável para MISP.

Caixa de diálogo Relatar vista observável para MISP

Campo	Descrição
Fonte	Campo de origem que corresponde à origem MISP da vista.
Data	Campo de data que corresponde à data em que o observável foi avistado. Se a data estiver vazia, a data e a hora atuais serão preenchidas em MISP.

O exemplo a seguir mostra como navegar até a lista relacionada de Vistas no incidente de segurança. Nessa lista, você pode selecionar um observável e relatar a vista do observável para MISP. A mensagem de sucesso mostra que a vista foi enviada com sucesso para MISP.

Relata avistamentos observáveis ao MISP



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Clique **em Relatar vista**.

6. **Opcional:** Se você selecionou a opção **MISP: Relatar observável como falso positivo**, preencha os campos da caixa de diálogo Relatar observável como falso positivo para MISP.

Caixa de diálogo Relatar observável como falso-positivo para MISP

Campo	Descrição
Origem (opcional)	Campo de origem que corresponde à origem MISP. Use este campo para declarar o observável como um falso positivo.
Data	Campo de data que corresponde à data em que o observável foi considerado um falso positivo. Se a data estiver vazia, a data e a hora atuais serão preenchidas em MISP.

a. Clique **em Relatar falso-positivo**.

7. **Opcional:** Se você selecionou a opção **MISP: Relatar observável como expirado**, deverá preencher os campos da caixa de diálogo Relatar expiração do observável para MISP.

Caixa de diálogo Relatar expiração do observável ao MISP

Campo	Descrição
Fonte	Campo de origem que corresponde à origem MISP. Use este campo para definir um observável como expirado.
Data	Campo de data que corresponde à data em que o observável expirou. Se a data estiver vazia, a data e a hora atuais serão preenchidas em MISP.

a. Clique **em Relatar expiração**.

Resultado

As vistas foram atualizadas com sucesso para o servidor MISP.

Aprimoramento de observável em MISP

Ao aprimorar os observáveis com informações adicionais de várias fontes MISP durante as investigações de resposta do incidente, você pode conter as ameaças identificadas.

Habilitar aprimoramento observável automático em MISP

Habilite o aprimoramento observável automático no Now Platform MISP quando novos observáveis forem associados ao incidente de segurança.

Antes de Iniciar

- Habilite a propriedade do sistema Security Incident Response para a opção **Habilita ou desabilita o trabalho programado, Pesquisar observáveis de incidente de segurança** para acionar a capacidade de aprimoramento do observável em SIR.
- Função necessária: sn_si.analyst

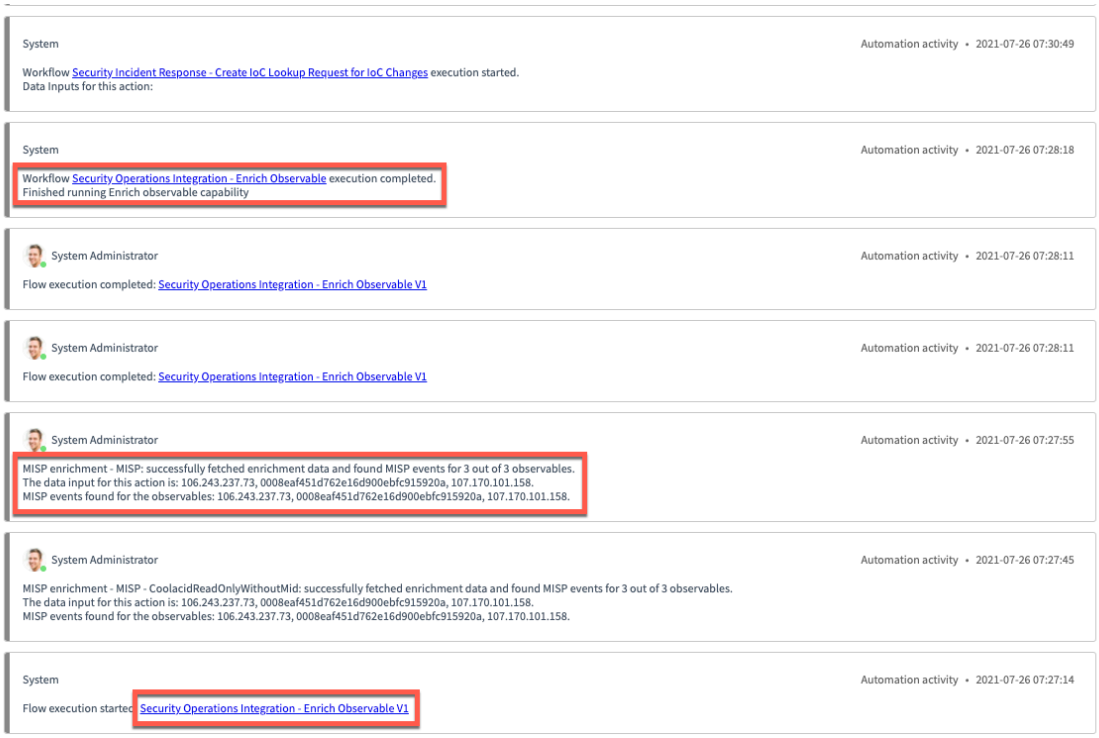
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que contém os observáveis que você deseja aprimorar os dados observáveis em MISP para.
3. Revise as anotações de trabalho depois que novos observáveis forem associados ao incidente de segurança.

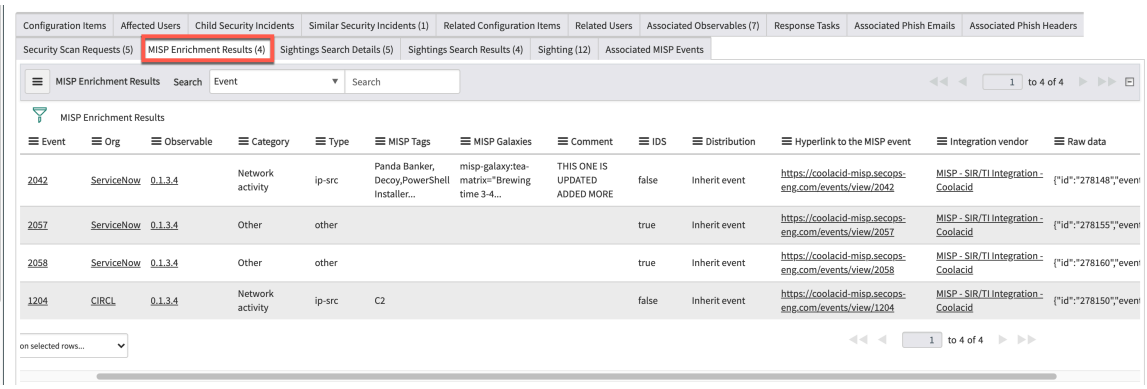
   O exemplo a seguir mostra que uma anotação de trabalho é publicada quando o fluxo de trabalho Integração do Security Operations - Aprimorar observável é acionado.



4. Na lista relacionada MISP Resultados de aprimoramento do incidente de segurança, exiba os resultados de aprimoramento após a conclusão da execução do fluxo de trabalho.

   Nota:
   Você deve configurar que a lista relacionada Resultados de aprimoramento MISP apareça nas listas relacionadas a incidentes de segurança. Para obter mais informações, consulte a configuração da lista relacionada.

   O exemplo a seguir mostra os resultados de aprimoramento no MISP.



   A tabela a seguir mostra os resultados de aprimoramento do MISP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados do aprimoramento de MISP

Campo	Descrição
Evento	ID do evento. Clique em abrir para exibir o registro na instância Now Platform.
Organização	Organização que criou originalmente o evento.
Observável	Observável que está associado ao evento.
Categoria	Categoria do atributo. Exiba a lista de categorias na documentação do MISP.
Tipo	Tipo do atributo. Exiba a lista de tipos na documentação do MISP.
Marcadores MISP	Lista de marcadores associados ao atributo MISP.
Galáxias MISP	Lista de galáxias associadas ao atributo MISP.
Comentário	Comentário contextual para descrever melhor o atributo. Esses comentários não são usados para correlação e são puramente informativos.
IDS	Indicador de comprometimento, o que permite que ele seja incluído em todas as exportações qualificadas.
Distribuição	Distribuição do atributo depois que ele é publicado. Um atributo pode ter um nível de distribuição diferente do evento. Em ambos os casos, o nível de distribuição mais baixo é usado.
Hiperlink para o evento MISP	Link para o evento MISP, que é armazenado no servidor MISP.
Fornecedor de integração	Fornecedor de integração que fornece os dados para aprimoramento.
Dados brutos	Dados brutos associados ao atributo MISP.

Executar um aprimoramento observável manual no MISP

Selecione observáveis individuais ou vários e execute um aprimoramento de observável manual para que você possa aprimorar os observáveis com informações adicionais de várias fontes MISP.

Antes de Iniciar

- Analise o MISP função e permissões do usuário para usar os recursos bidirecionais MISP.
- Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja executar o aprimoramento.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Observáveis associados**.
4. Selecione o observável e, no menu Ações, clique em **Executar aprimoramento de observável**.
   Você pode selecionar vários observáveis para uma pesquisa de vista.
   A caixa de diálogo Executar aprimoramento de observável é exibida.

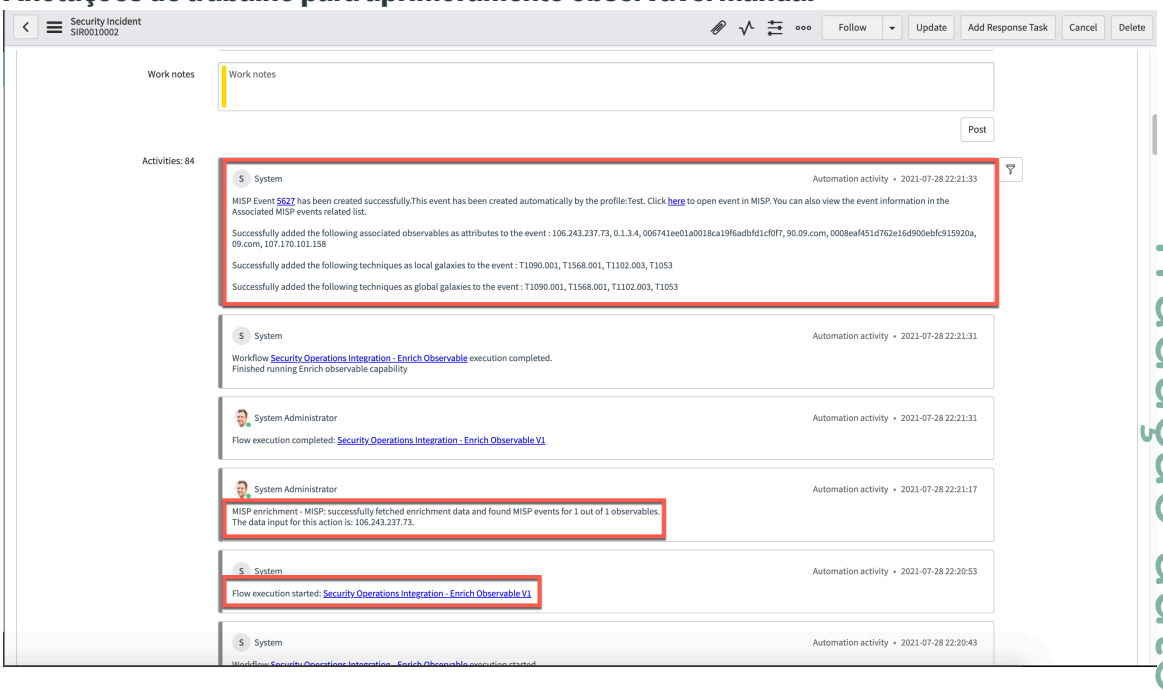
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Selecione uma origem MISP e, na coluna Selecionado, selecione uma implementação para aprimorar os observáveis selecionados.
6. Clique em **Enviar**.
   Uma anotação de trabalho mostra que o fluxo de trabalho Security Operations Integration - Enrich Observable foi acionado. Os fluxos de trabalho de implementação associados são executados para realizar o aprimoramento. Você pode exibir as anotações de trabalho no incidente de segurança para exibir o status.

   O exemplo a seguir mostra como exibir as anotações de trabalho para um aprimoramento observável manual.

Anotações de trabalho para aprimoramento observável manual



A mensagem de aprimoramento lista o evento criado. Você pode exibir o evento na instância Now Platform ou na instância MISP e exibir os detalhes do registro na guia Resultados de aprimoramento do MISP.

Adicionar ou remover marcadores a atributos MISP

Adicione ou remova marcadores em MISP para classificar eventos ou atributos. Você pode usar marcadores globalmente para habilitar sua classificação ou usar marcadores localmente quando não quiser que os eventos MISP sejam modificados durante sua classificação.

Antes de Iniciar

- Analise o MISP função e permissões do usuário para usar os recursos bidirecionais MISP.
- Verifique se o atributo que você está editando pertence à mesma organização que o usuário MISP.
- Observe que os marcadores e galáxias disponíveis para você são baseados na origem MISP e em suas permissões de distribuição.
- Função necessária: sn_sec_misp.write

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que contém os observáveis, atributos ou eventos para os quais você deseja adicionar os marcadores.
3. Clique **em Mostrar todas as listas relacionadas** e na lista relacionada Resultados de aprimoramento do MISP.
4. Clique no ícone de ⓘ ao lado de um registro e clique em **Abrir registro**.
   O exemplo a seguir mostra como revisar os **resultados de aprimoramento do MISP** e como abrir um registro de aprimoramento MISP.

   Registro de resultado de aprimoramento do MISP
   Abrindo o registro do resultado de aprimoramento do MISP

5. Revise o registro do resultado de aprimoramento do MISP.

Resultado do aprimoramento de MISP

Campo	Descrição
Observável	
Evento	ID do evento atribuído pelo servidor MISP quando o evento foi criado ou importado pela primeira vez para o MISP. Visualize o evento ou clique no registro para exibir os dados do evento na MISP página Dados do evento.
Organização	Organização que criou o atributo MISP.
Categoria	Categoria do atributo que você adiciona ao evento específico em MISP. Você pode selecionar uma opção como referência interna, atividade de rede, fraude financeira e assim por diante.
Tipo	Tipo de atributo MISP.
Fornecedor de integração	Fornecedor de integração que fornece os dados para o aprimoramento observável.
Data de criação (no MISP)	Data em que o evento foi criado ou importado pela primeira vez para MISP.
IDS	Status de um observável marcado como malicioso em SIR. O atributo correspondente em MISP também está marcado como verdadeiro.
Distribuição	Controles de opção de distribuição, como quem pode exibir este evento depois que ele for publicado. Esta opção também controla se o evento é sincronizado com outros servidores. A distribuição é herdada pelos atributos e a configuração mais restritiva vence. As opções de distribuição são as seguintes: ○ Somente sua organização: permite que somente membros da sua organização exibam este evento. O evento pode

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	ser puxado para outra instância por um dos membros da sua organização, onde somente sua organização tem acesso para exibi-lo. Eventos com esta configuração não são sincronizados. ○ Somente esta comunidade: permite que os usuários que fazem parte da sua comunidade MISP exibam o evento, incluindo sua própria organização, organizações neste servidor MISP e organizações que executam servidores MISP que são sincronizados com este servidor. Quaisquer outras organizações conectadas a esses servidores vinculados têm restrição para exibir o evento. ○ Comunidades conectadas: permite que os usuários que fazem parte da sua comunidade MISP exibam o evento, incluindo todas as organizações neste servidor MISP, todas as organizações em servidores MISP que sincronizam com este servidor e as organizações de hospedagem de servidores que se conectam a qualquer servidor ou seja, dois saltos de distância). Quaisquer outras organizações conectadas aos servidores vinculados que estão a dois saltos de distância têm restrição para exibir o evento. ○ Todas as comunidades: compartilha o evento com todas as MISP comunidades, o que permite que o evento fique disponível gratuitamente.
Hiperlink para o evento MISP	Link para o evento MISP que é armazenado no servidor MISP.
Dados brutos	Detalhes brutos do registro de dados de aprimoramento do observável.
Comentário	Comentários que você adiciona aos atributos. Esses comentários são apenas para fins informativos e não são usados para correlação.
Marcadores (locais)	Marcadores que estão disponíveis na instância MISP da organização host para habilitar a marcação para sincronização e filtragem de exportação. MISP eventos não são modificados quando você usa marcadores locais. Esses marcadores são sempre removidos antes de serem sincronizados com outras instâncias MISP e comunidades de compartilhamento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Marcadores (Globais)	Marcadores que estão disponíveis globalmente para serem compartilhados e sincronizados com outras instâncias MISP e comunidades de compartilhamento. Ao adicionar marcadores globais a instâncias MISP, você modifica eventos.
Galáxias (locais)	Galáxias que estão disponíveis na instância MISP da organização do host para sincronização e filtragem de exportação. MISP eventos não são modificados quando você usa galáxias locais. Essas galáxias são sempre removidas antes de serem sincronizadas com outras instâncias MISP e comunidades de compartilhamento.
Galáxias (Global)	Galáxias que estão disponíveis globalmente para serem compartilhadas e sincronizadas com outras instâncias MISP e comunidades de compartilhamento. Quando você adiciona galáxias globais, os eventos MISP são modificados.

6. Para editar um marcador local ou global, clique no ícone de edição ícone de em uma das seguintes opções:

   - **Marcadores (locais)**
   - **Marcadores (Globais)**

7. Na caixa de diálogo Marcadores de atributo do MISP, insira o nome do marcador a ser pesquisado e adicionado.
8. Clique **em Atualizar marcadores para atributo MISP**.

   O exemplo a seguir mostra que, ao clicar no ícone de edição dos marcadores locais, você pode pesquisar e adicionar os marcadores C3, Adware, C2 e Botnet 3101 e atualizar o servidor MISP com os marcadores. A mensagem de confirmação mostra que todos os marcadores foram atualizados em MISP.

   Adicionar marcadores locais no atributo MISP.
   Os marcadores são atualizados com sucesso no servidor MISP.

9. Para exibir as mudanças no registro, clique em **Recarregar formulário** na mensagem de sucesso.

Adicionar ou remover galáxias de um evento ou atributo MISP

Adicione ou remova galáxias em MISP para que você possa classificar esses objetos como um cluster em MISP e anexá-los a MISP eventos ou atributos.

Antes de Iniciar

- Analise o MISP função e permissões do usuário para usar os recursos bidirecionais MISP.
- Para adicionar galáxias locais, o usuário que configurou a integração deve pertencer à organização host do servidor MISP correspondente.
- Observe que os marcadores e galáxias disponíveis para você são baseados na origem MISP e em suas permissões de distribuição.
- Função necessária: sn_sec_misp.write

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Clique no ícone de edição ícone de em uma das seguintes opções.

- **Galáxias (locais)**
- **Galáxias (Global)**

2. Na caixa de diálogo Galáxias de evento do MISP, preencha os detalhes.

Caixa de diálogo Galáxias de evento do MISP

Campo	Descrição
ID de Evento	ID do evento atribuído pelo servidor MISP quando o evento foi criado ou importado pela primeira vez para o MISP.
Namespace	Namespace onde a galáxia está armazenada. Você pode usar namespaces para agrupar galáxias semelhantes.
Galáxias	Galáxia em que você armazena as informações do cluster.
Clusters	Informações sobre os clusters na galáxia.

3. Clique **em Atualizar galáxias para atributo MISP**.
   O exemplo a seguir mostra que, ao clicar no ícone de edição das galáxias locais, você pode selecionar o namespace obsoleto, selecionar a galáxia Ataque empresarial - Padrão de ataque e adicionar as informações do cluster. Depois que as informações da galáxia forem atualizadas, você poderá exibir a mensagem de sucesso.

   Como adicionar informações da galáxia no MISP por meio da Now Platform

4. Para exibir as mudanças no registro, clique em **Recarregar formulário** na mensagem de sucesso.

Resultado

As informações da galáxia foram atualizadas com sucesso no servidor MISP.

Adicionar comentários ao atributo MISP

Adicione comentários para os atributos MISP. Os comentários adicionados são apenas para fins informativos e não são usados para correlação de dados MISP.

Antes de Iniciar

- Analise o MISP função e permissões do usuário para usar os recursos bidirecionais MISP.
- Verifique se o atributo que você está editando pertence à mesma organização que o usuário MISP.
- Função necessária: sn_sec_misp.write

Procedimento

1. Clique no ícone de edição ícone de no campo Comentário.
2. Insira seu comentário no campo Comentário do atributo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique **em Atualizar comentário para atributo MISP**.
   O exemplo a seguir mostra que, clicando no ícone de edição ao lado do campo de comentário, você pode adicionar um comentário e atualizar o atributo MISP. Depois que o comentário for atualizado, você poderá exibir a mensagem de sucesso.

   Adicionando informações da galáxia no MISP por meio da Now Platform.

4. Para exibir as mudanças no registro, clique em **Recarregar formulário** na mensagem de sucesso.

Resultado
O comentário foi atualizado com sucesso no servidor MISP.

Gerenciamento de eventos no MISP

Você pode criar eventos em MISP automaticamente ou manualmente a partir de Now Platform. Você também pode editar os dados do evento em MISP a partir de Now Platform.

Verificando eventos criados automaticamente no MISP

Você pode verificar os eventos criados automaticamente depois de configurar o perfil de criação de evento em sua instância Now Platform.

Perfil de criação automática de evento

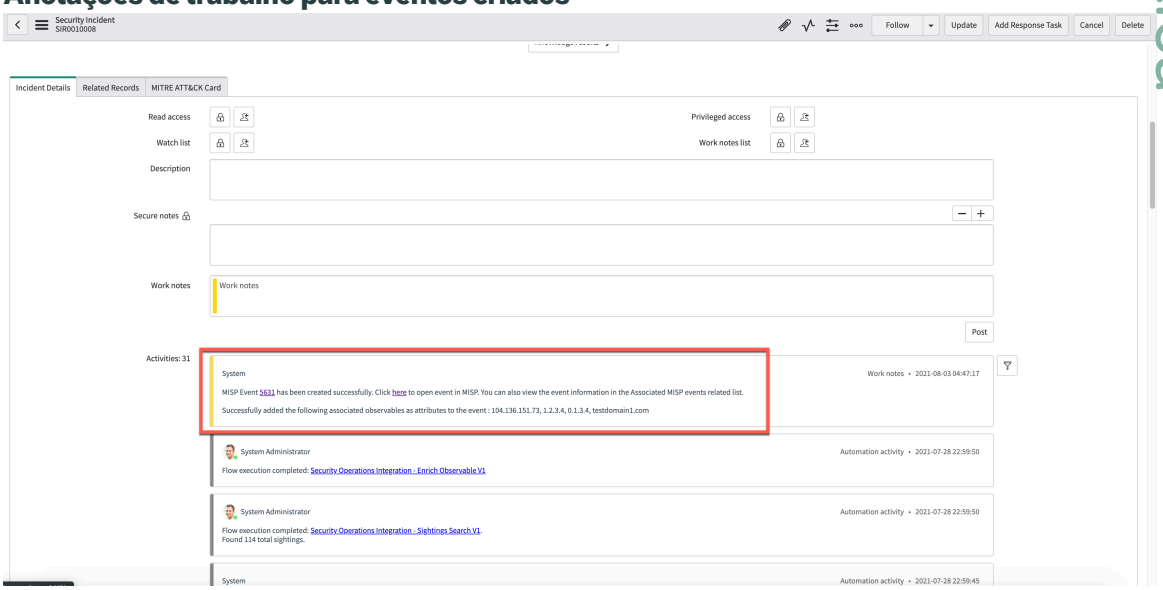
A configuração do perfil de criação automática de eventos é feita pelas funções de usuário sn_si.admin ou sn_ti.admin no **Integração MISP** > **Perfis automáticos de criação de evento** módulo.

Exibindo os dados do evento MISP

Você pode exibir os eventos criados das seguintes maneiras:

- Exiba as anotações de trabalho dos eventos criados. Você pode exibir os detalhes do evento na instância Now Platform e também como ele aparece no servidor MISP, conforme mostrado no exemplo a seguir.

Anotações de trabalho para eventos criados

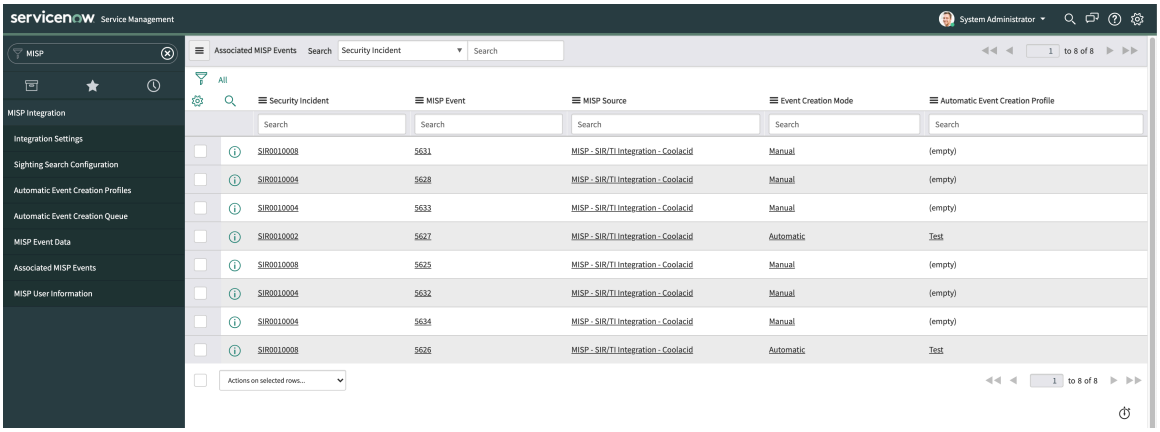


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

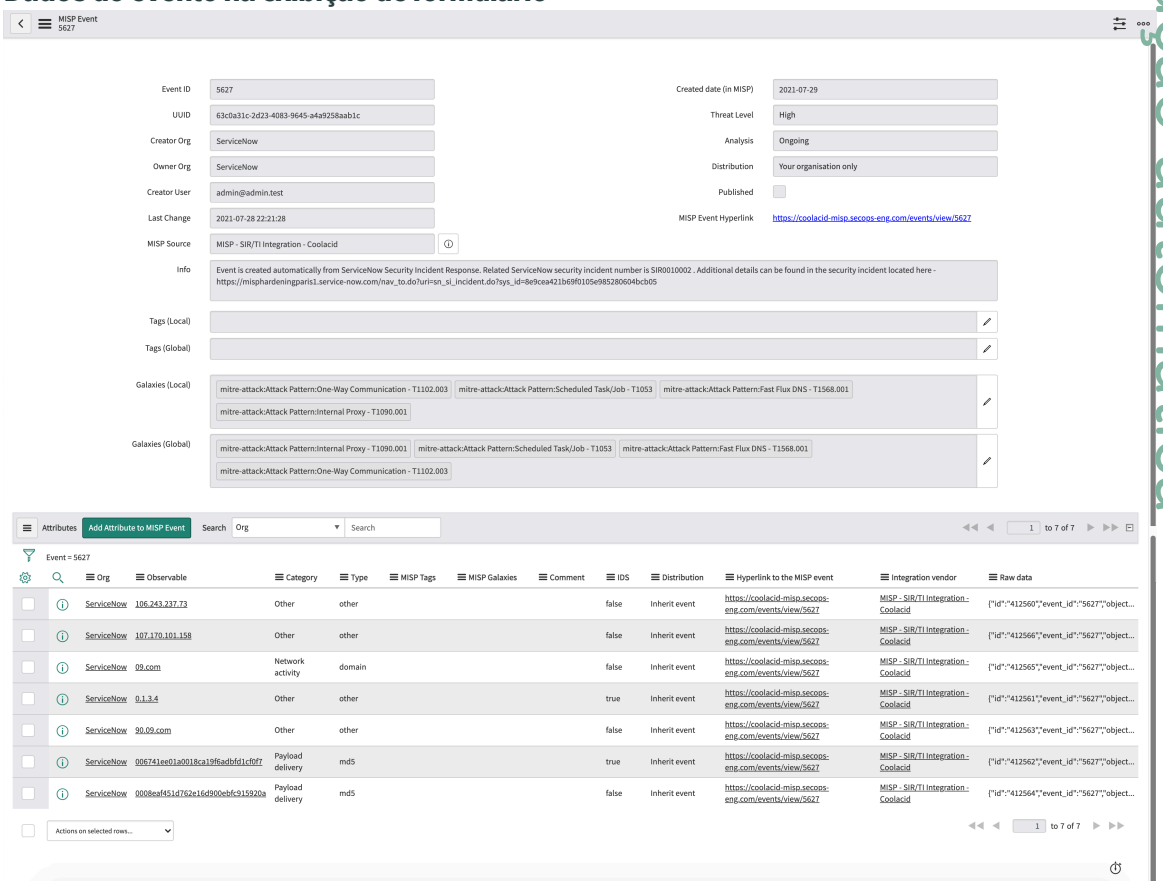
- Clique na lista relacionada Eventos de MISP associados. Aqui, você pode exibir o evento em relação ao incidente de segurança e aos recursos MISP conforme mostrado no exemplo a seguir.

Lista de eventos associados



- Exiba os dados do evento MISP na exibição de formulário para revisar as informações detalhadas sobre os eventos MISP, conforme mostrado no exemplo a seguir.

Dados do evento na exibição de formulário



Criar manualmente um evento no MISP

Crie manualmente eventos em MISP a partir de Now Platform para capturar informações contextualmente relacionadas representadas como atributos e objetos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

- Analise o MISP função e permissões do usuário para usar os recursos bidirecionais MISP.
- Função necessária: sn_sec_misp.write

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que contém os observáveis para os quais você deseja criar um evento.
3. Clique **em Criar um novo evento no MISP**.
4. Na caixa de diálogo Criar um novo evento no MISP, preencha os detalhes.

Criar um evento na caixa de diálogo do MISP

Campo	Descrição
Data	Data de criação do evento em MISP.
Informações do evento	Informações do evento que são criadas automaticamente a partir de Now Platform Security Incident Response.
Nível de ameaça	Nível de risco do evento. Você pode categorizar os incidentes em três categorias de ameaça diferentes (baixa, média e alta). Este campo também pode ser deixado como indefinido. A seguir estão as opções: ○ Baixo: malware geral em massa ○ Média: ameaças persistentes avançadas (APT) ○ Alto: APTs sofisticados e ataques de dia 0
Fonte	MISP origem para a criação do evento.
Distribuição	Opção que controla quem pode exibir este evento depois que ele é publicado. Esta opção também controla se o evento é sincronizado com outros servidores. A distribuição é herdada pelos atributos. A configuração mais restritiva vence. As opções de distribuição são as seguintes: ○ Somente sua organização: permite que somente os membros da sua

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	organização exibam este evento. O evento pode ser puxado para outra instância por um dos membros da sua organização, onde somente sua organização tem acesso para exibi-lo. Eventos com esta configuração não são sincronizados. ○ Somente esta comunidade: permite que os usuários que fazem parte da sua comunidade MISP exibam o evento, incluindo sua própria organização, organizações neste servidor MISP e organizações que executam servidores MISP que são sincronizados com este servidor. Outras organizações conectadas a servidores vinculados têm restrição para exibir o evento. ○ Comunidades conectadas: permite que os usuários que fazem parte da sua comunidade MISP exibam o evento, incluindo todas as organizações neste servidor MISP, todas as organizações em servidores MISP que sincronizam com este servidor e as organizações de hospedagem de servidores que se conectam a qualquer servidor que está a dois saltos de distância. Quaisquer outras organizações conectadas aos servidores vinculados que estão a dois saltos deste servidor têm restrição para exibir o evento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo		Descrição
		○ Todas as comunidades: compartilha o evento com todas as MISP comunidades.
Análise		Fase atual da análise do evento com as seguintes opções possíveis: ○ Inicial: a análise está apenas começando ○ Em andamento: a análise está em andamento ○ Concluído: a análise está concluída
Opções avançadas	Adicionar observáveis associados do SIR como atributos ao evento MISP	Opção para adicionar observáveis disponíveis em um incidente de segurança a um evento MISP como atributos. Esta opção habilita o **sinalizador Definir atributo IDS quando a descoberta observável for mal-intencionada**.
	Definir sinalizador de IDS de atributo quando a descoberta observável for mal-intencionada	Observável marcado como malicioso em SIR. O atributo correspondente em MISP também está marcado como verdadeiro.
	Sincronizar técnicas de incidente de segurança MITRE ATT e CK como galáxias locais para evento MISP	Opção para sincronizar as técnicas de Now Platform SIR incidente de segurança MITRE-ATT&CK™ como galáxias locais no evento MISP.
	Sincronizar técnicas de incidente de segurança MITRE ATT e CK como galáxias globais para evento MISP	Opção para sincronizar as técnicas de Now Platform SIR incidente de segurança MITRE-ATT&CK™ como galáxias globais no evento MISP.

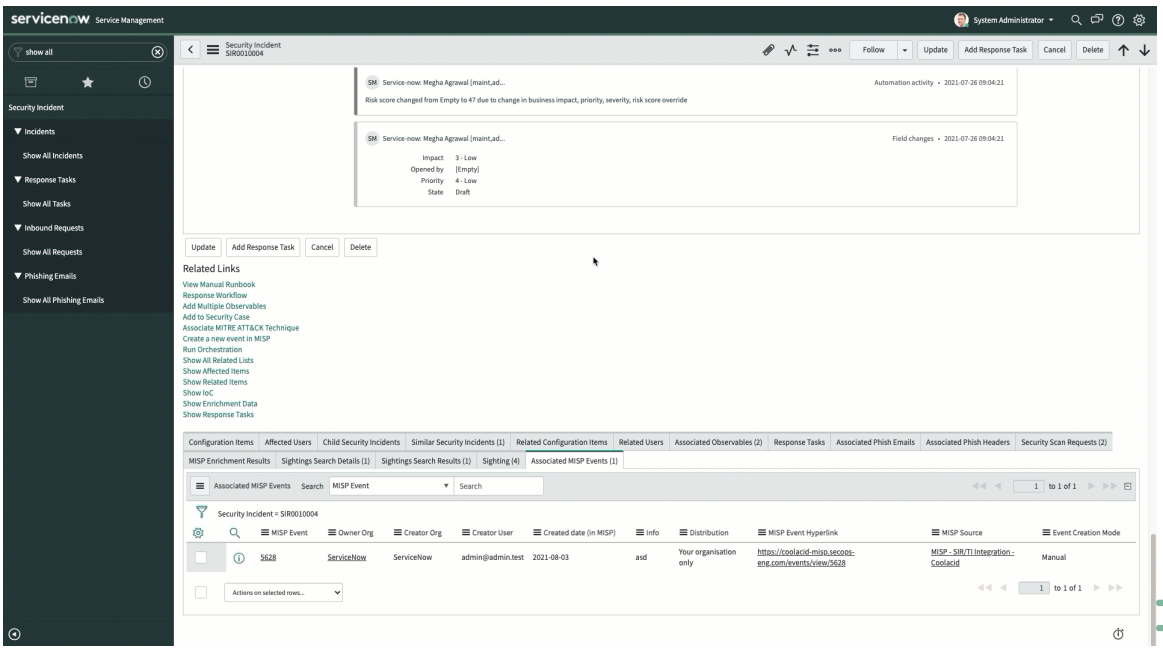
5. Clique **em Criar novo evento MISP**.

O exemplo a seguir mostra que, ao criar um evento em MISP, você pode exibir os resultados no incidente de segurança. Você também pode exibir as anotações de trabalho, o evento na instância Now Platform e o evento no servidor MISP, conforme mostrado no exemplo a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar manualmente um evento no MISP da Now Platform



Você pode exibir os resultados das seguintes maneiras:

- Uma mensagem de sucesso aparece na parte superior da página do incidente de segurança. Você pode exibir os detalhes do evento na instância Now Platform e também como ele aparece no servidor MISP.
- Nas anotações de trabalho, você pode exibir a mensagem de sucesso com mais detalhes. Você também pode exibir os detalhes do evento na instância Now Platform e também como ele aparece no servidor MISP.
- Na lista relacionada Eventos de MISP associados, você pode exibir o evento em relação ao incidente de segurança e aos recursos MISP.

Adicionar atributos a um evento MISP

Adicione atributos a um evento, como tipo, categoria e outras informações contextuais sobre o evento.

Antes de Iniciar

- Analise o MISP função e permissões do usuário para usar os recursos bidirecionais MISP.
- Verifique se o evento ao qual você está adicionando ou atualizando o atributo pertence à mesma organização que o usuário MISP.
- Função necessária: sn_sec_misp.write

Procedimento

1. Navegar até **Todos** > **MISP** > **Eventos de MISP associados**.
   Você também pode navegar até a lista relacionada de Evento de MISP associado em qualquer incidente de segurança.
2. Clique no evento MISP para o qual você deseja adicionar um atributo.
3. Clique **em Adicionar atributo ao evento MISP**.
4. Na caixa de diálogo Adicionar atributo ao evento, preencha os detalhes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionar atributo à caixa de diálogo de evento

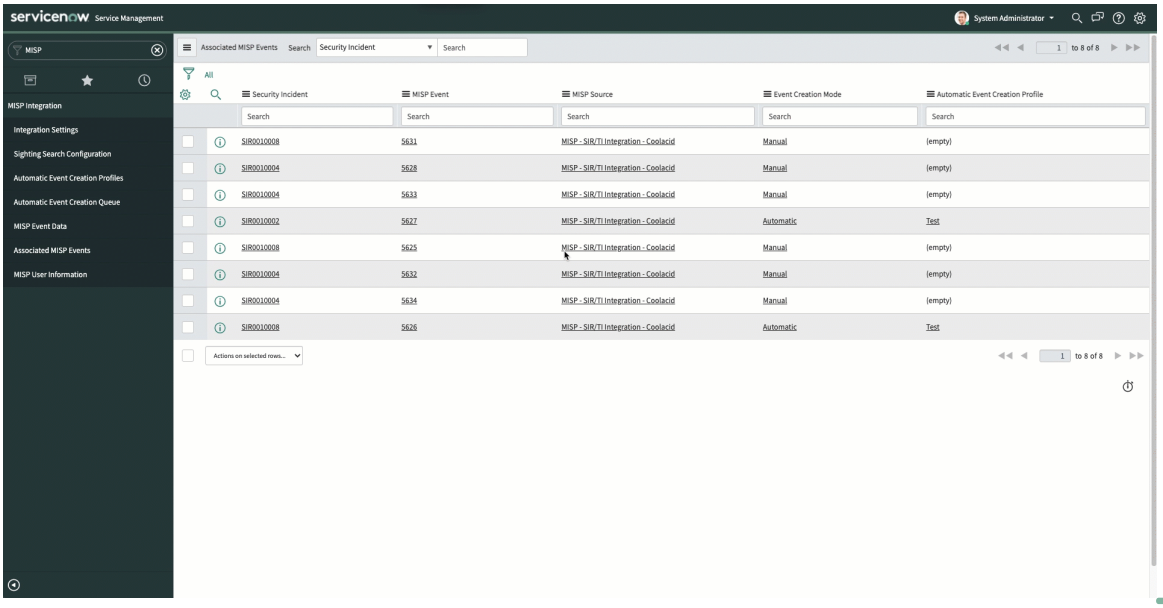
Campo	Descrição
Valor	Valor real do atributo. Insira dados sobre o valor que é baseado no que é válido para o tipo de atributo escolhido. Por exemplo, para um atributo do tipo ip-src (endereço IP de origem), 11.11.11.11 é um valor válido. **Nota:** Você só pode selecionar atributos ou observáveis que compartilham contexto com o evento. Os observáveis ainda não podem ter um atributo em MISP.
Categoria	Categoria do atributo. A categoria descreve o aspecto do malware para este atributo. Um exemplo seriam os mecanismos de persistência do malware ou da atividade de rede.
Tipo	Tipo que explica a categoria. Por exemplo, se um invasor usar um endereço IP para um ataque, um endereço de e-mail de origem ou um arquivo enviado por meio de um anexo poderá descrever a entrega de carga de um malware. Esses tipos de atributos têm a categoria de entrega de carga.
Distribuição	Usuários que podem exibir este atributo. A distribuição é herdada por atributos. A configuração mais restritiva vence.
Usar atributo como uma assinatura de IDS	Observável marcado como malicioso em SIR. O atributo correspondente em MISP também está marcado como verdadeiro.
Comentários	Comentários que você adiciona aos atributos.

O exemplo a seguir mostra que, navegando na lista Eventos de MISP associados, você pode exibir o registro de evento 5627 e adicionar atributos ao evento. Os atributos incluem o valor (testdomain.com), categoria como análise externa, tipo como domínio. Você também pode habilitar o IDS. A mensagem de sucesso no registro do evento mostra que o atributo foi adicionado ao evento, conforme mostrado no exemplo a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionar atributo a um evento MISP



5. Clique **em Adicionar atributo ao evento MISP**.

Resultado

Você pode exibir o atributo adicionado na seção Atributos.

Adicionar marcadores a um evento MISP

Adicione marcadores em Now Platform MISP para classificar eventos ou atributos. Você pode usar marcadores globalmente para habilitar sua classificação ou usar marcadores localmente quando não quiser que os eventos MISP sejam modificados durante sua classificação.

Antes de Iniciar

- Analise o MISP função e permissões do usuário para usar os recursos bidirecionais MISP.
- Verifique se o evento que você está editando pertence à mesma organização que o usuário MISP.
- Observe que os marcadores e galáxias disponíveis para você são baseados na origem MISP e em suas permissões de distribuição.
- Função necessária: sn_sec_misp.write

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que contém o evento ao qual você deseja adicionar marcadores.
3. Clique **em Mostrar todas as listas relacionadas** e na lista relacionada Resultados de aprimoramento do MISP.
4. Clique no ID do evento na lista de resultados de aprimoramento.
   Você também pode navegar a partir de **MISP** > **Eventos de MISP associados** módulo.
5. Revise o registro do evento de MISP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibição de formulário de evento de MISP

Campo	Descrição
ID de Evento	ID do evento atribuído por MISP quando o evento foi criado ou importado pela primeira vez para o servidor MISP.
UUID	ID que identifica exclusivamente eventos e atributos.
Organização do criador	Organização que criou o evento na instância MISP.
Organização do proprietário	Organização que possui o evento na instância MISP. Este campo está visível somente para os administradores.
Usuário do criador	Usuário que criou o evento em MISP.
Última mudança	Data em que o evento foi modificado pela última vez.
Origem do MISP	MISP origem em que o evento é criado.
Data de criação (no MISP)	Data em que o evento foi criado ou importado pela primeira vez no servidor MISP.
Nível de ameaça	Nível de risco do evento. Os incidentes podem ser categorizados em três categorias de ameaça diferentes (baixa, média e alta). Este campo pode ser deixado como indefinido. A seguir estão as opções: ○ Baixo: malware geral em massa ○ Média: ameaças persistentes avançadas (APT) ○ Alto: APTs sofisticados e ataques de dia 0
Análise	Fase atual da análise do evento com as seguintes opções possíveis: ○ Inicial: a análise está apenas começando ○ Em andamento: a análise está em andamento ○ Concluído: a análise está concluída
Distribuição	Distribuição do atributo individual. Um atributo pode ter um nível de distribuição diferente do evento.
Publicado	Status de se o evento foi publicado ou não. A publicação permite que os atributos do evento sejam usados para todas as exportações qualificadas e notifica os usuários que assinaram os alertas de evento.
Hiperlink de evento MISP	Link para o evento MISP que é armazenado no servidor MISP.
Informações	Descrição resumida do evento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Marcadores (locais)	Marcadores que estão disponíveis na instância MISP da organização host para habilitar a marcação para sincronização e filtragem de exportação. MISP eventos não são modificados quando você usa marcadores locais. Marcadores locais são sempre removidos antes de serem sincronizados com outras instâncias MISP e comunidades de compartilhamento.
Marcadores (Globais)	Marcadores que estão disponíveis globalmente para serem compartilhados e sincronizados com outras instâncias MISP e comunidades de compartilhamento. Ao adicionar marcadores globais a instâncias MISP, você pode modificar eventos.
Galáxias (locais)	Galáxias que estão disponíveis na instância MISP da organização do host para sincronização e filtragem de exportação. MISP eventos não são modificados quando você usa galáxias locais. Essas galáxias locais são sempre removidas antes de serem sincronizadas com outras instâncias MISP e comunidades de compartilhamento.
Galáxias (Global)	Galáxias que estão disponíveis globalmente para serem compartilhadas e sincronizadas com outras instâncias MISP e comunidades de compartilhamento. Ao adicionar galáxias globais, MISP é possível modificar eventos.

6. Para editar um marcador local ou global, clique no ícone de edição ícone de em uma das seguintes opções:

   - **Marcadores (locais)**
   - **Marcadores (Globais)**

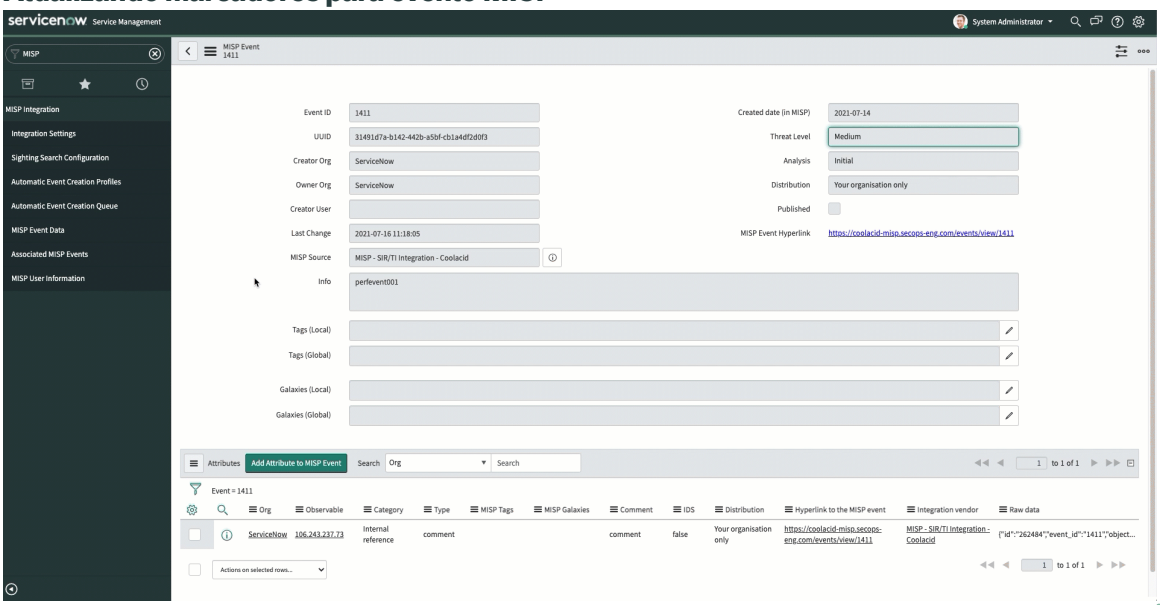
7. Na caixa de diálogo Marcadores de evento do MISP, insira o nome do marcador para pesquisar e adicionar os marcadores.
8. Clique **em Atualizar marcadores para evento MISP**.

   O exemplo a seguir mostra que, ao clicar no ícone de edição dos marcadores locais, você pode pesquisar e adicionar os marcadores C3, Adware, C2 e Botnet 3101 e atualizar o servidor MISP com os marcadores. A mensagem de confirmação mostra que todos os marcadores foram atualizados em MISP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atualizando marcadores para evento MISP



9. Clique em **Recarregar formulário** na mensagem de sucesso para exibir as mudanças no registro.

Resultado

Os marcadores foram atualizados com sucesso no servidor MISP.

Atualizar galáxias para um evento ou atributo MISP

Adicione ou remova galáxias em Now Platform MISP para que você possa classificar esses objetos como um cluster na instância MISP e anexá-los a MISP eventos ou atributos.

Antes de Iniciar

- Analise o MISP função e permissões do usuário necessário para usar os recursos bidirecionais MISP.
- Para adicionar galáxias locais, o usuário que configurou a integração deve pertencer à organização do host do servidor MISP correspondente.
- Os marcadores e galáxias disponíveis para você são baseados na origem MISP e em suas permissões de distribuição.
- Função necessária: sn_sec_misp.write

Procedimento

1. Clique no ícone de edição ícone de em uma das seguintes opções.

- **Galáxias (locais)**
- **Galáxias (Global)**

2. Na caixa de diálogo Galáxias de evento do MISP, digite e pesquise para adicionar os marcadores.

3. Clique **em Atualizar galáxias para evento MISP**.

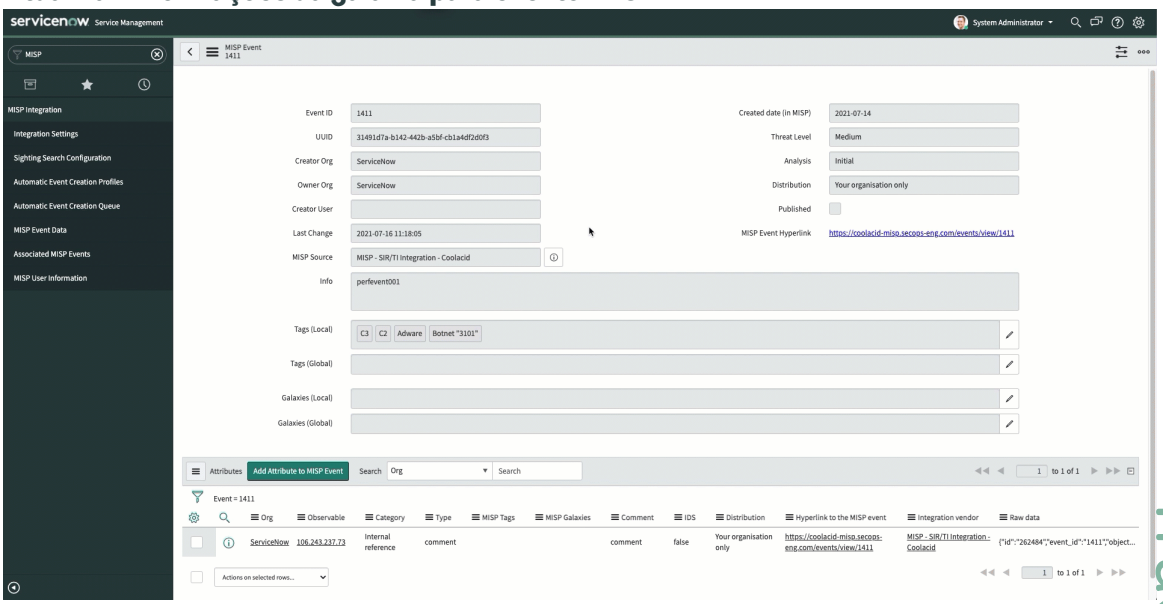
O exemplo a seguir mostra como clicar no ícone de edição das galáxias locais, selecionar o namespace obsoleto, selecionar a galáxia Ataque empresarial - Padrão de ataque

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e adicionar informações do cluster. Depois que as informações da galáxia forem atualizadas, você poderá exibir a mensagem de sucesso.

Atualizar informações da galáxia para evento MISP



As galáxias foram atualizadas com sucesso no servidor MISP.

4. Clique em **Recarregar formulário** na mensagem de sucesso para exibir as mudanças no registro.

Agregar MITRE-ATT&CK informações usando MISP resultados de aprimoramento

Acumule os resultados de aprimoramento do MISP manualmente se você não tiver habilitado o acúmulo automático de MISP informações.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Use as regras de extração automática do sistema de base para importar as informações MITRE-ATT&CKMISP da integração []. O MISP integration for Security Operations apresenta duas regras de extração da técnica do sistema base MITRE-ATT&CK para MISP - MISP galáxias e marcadores MISP. Para obter mais informações sobre regras de extração automática em MITRE-ATT&CK, consulte Regras de técnica de extração automática para importar informações do MITRE-ATT&CK.

Se você habilitou acúmulo automático de MITRE-ATT&CK informações usando MISP resultados de aprimoramento a um incidente de segurança, as informações são acumuladas automaticamente. Se você não habilitou o acúmulo automático, poderá fazer esta tarefa manualmente.

Procedimento

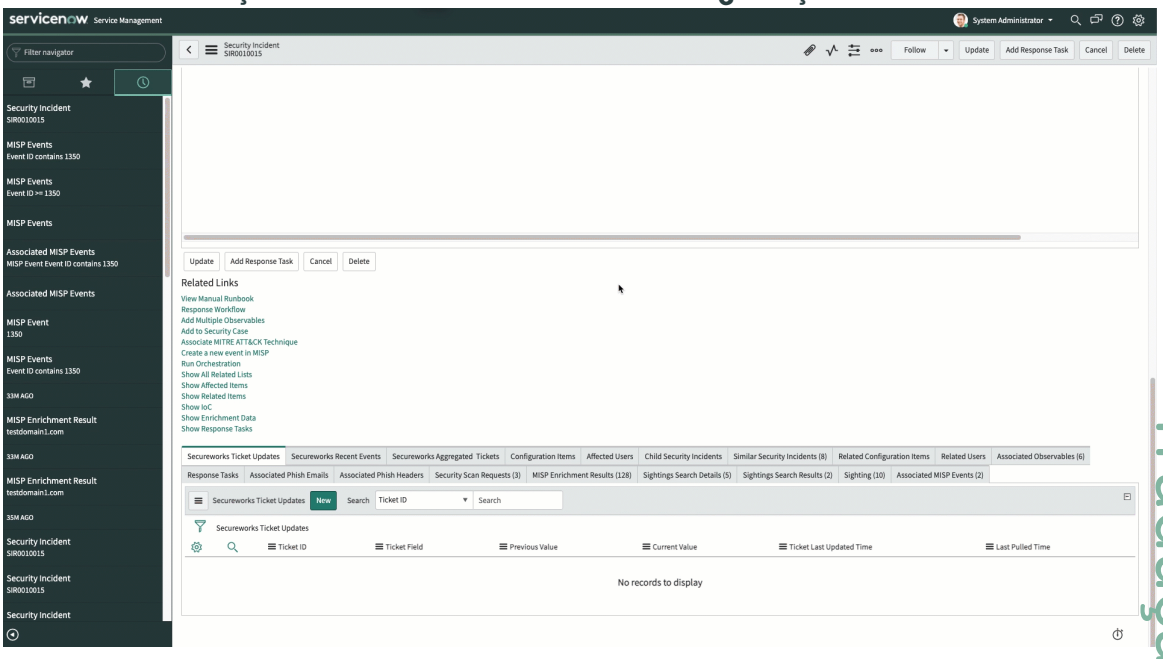
1. Navegar até **Todos** > **Incidentes de segurança** > **Mostrar Todos os Incidentes**.
2. Selecione o incidente de segurança que você deseja aprimorar com as informações de MITRE-ATT&CK.
3. Clique **em Mostrar todas as listas relacionadas** e na guia **Resultados de aprimoramento do MISP**.
4. Selecione o observável e, no menu Ações, clique **em Agregar informações do MITRE ATT&CK para SI**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode selecionar vários observáveis e acumular as informações.

5. Para confirmar as mudanças, clique em **Recarregar**.
   O exemplo a seguir mostra como selecionar um observável e acumular os resultados de aprimoramento MISP para o incidente de segurança.

Acumular informações do MITRE em um incidente de segurança



Resultado

Você pode exibir o cartão MITRE-ATT&CK para confirmar que os resultados de aprimoramento do MISP foram acumulados para o incidente de segurança.

OPSWAT Metadefender Integration

OPSWAT Metadefender permite que os dados de ameaça, detectados pelo scanner Metadefender de terceiros, sejam baixados para a aplicação Inteligência contra ameaças para acompanhamento, priorização e resolução.

Explorar • OPSWAT Metadefender visão geral da integração • Integrações do Inteligência contra ameaças	Configuração Ativar e configurar a integração OPSWAT Metadefender
Usar • Realizar pesquisas em observáveis • Pesquisa de ameaças - Fluxo de trabalho do Metadefender OPSWAT	Desenvolver • ServiceNow Security Operations diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Solução de problemas de integração
- Faça ou responda perguntas na comunidade do Security Operations
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

OPSWAT Metadefender visão geral da integração

OPSWAT Metadefender é uma solução de segurança que fornece acesso a várias máquinas antimalware e se integra facilmente com Security Operations.

Antes de usar a integração OPSWAT Metadefender, você deve ativar o plug-in e configurar a integração. Se necessário, você também pode atualizar sua certificação SSL X509.

Ativar e configurar a integração OPSWAT Metadefender

Antes de usar a integração OPSWAT Metadefender, você deve baixá-la do ServiceNow Store.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a integração estiver concluída, acesse o portal OPSWAT e obtenha a chave de API do Metadefender Cloud
3. Em sua instância, navegue até **Security Operations** > **Integrações** > **Configuração de Integração**. As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão OPSWAT Metadefender, clique em **Configurar**.
5. Insira (ou cole) a **Chave de API** que você adquiriu no portal OPSWAT.
6. Clique em **Enviar**.

Resultado

Depois de configurado, o OPSWAT Metadefender pode ser selecionado para executar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Tópicos relacionados

Realizar pesquisas em observáveis

Atualize seu certificado X.509

Se você precisar de uma conexão SSL para a integração, há circunstâncias em que o certificado fornecido pelo fornecedor terceirizado ainda não é confiável em ServiceNow ou expirou. Esta tarefa é opcional.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um Certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Insira o URL do endpoint na barra de endereço do navegador.
Por exemplo: `https://<3rdparty>/`.

b. Clique no ícone de cadeado na linha de endereço.

c. Clique em **Mais informações** e na guia **Segurança**.

d. Clique em **Exibir certificado** e na guia **Detalhe**.

e. Clique em **Exportar** para salvar o PEM em seu sistema de arquivos local.

f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
Ele deve começar com `-----BEGIN CERTIFICATE-----` e terminar com `-----END CERTIFICATE-----`.

2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e crie um novo registro para a integração.
4. Em **Certificado PEM**, cole o certificado que você baixou e copiou para a área de transferência anteriormente.
5. Adicione o certificado ao registro do provedor de identidade.
   a. Navegar até **SSO Multiprovedor** > **Provedores de Identidade**.
   b. Selecione o provedor de identidade padrão ativo para o qual você criou o novo certificado.
   c. Role para baixo até a lista relacionada de **certificados X.509** e clique em **Editar**.
   d. Mova o certificado recém-criado para a coluna **Selecionado**.
6. Clique em **Salvar**.
Os outros campos no registro são gerados automaticamente.

Nota:
Se você tiver um certificado que expirou, será necessário removê-lo. Para obter informações sobre como remover o certificado expirado, consulte KB0691439 Substituir um certificado SAML expirando .

Pesquisa de ameaças - Fluxo de trabalho do Metadefender OPSWAT

O fluxo de trabalho Pesquisa de ameaças - OPSWAT Metadefender executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido pelo OPSWAT Metadefender, os observáveis serão verificados quanto a malware e os resultados serão retornados.

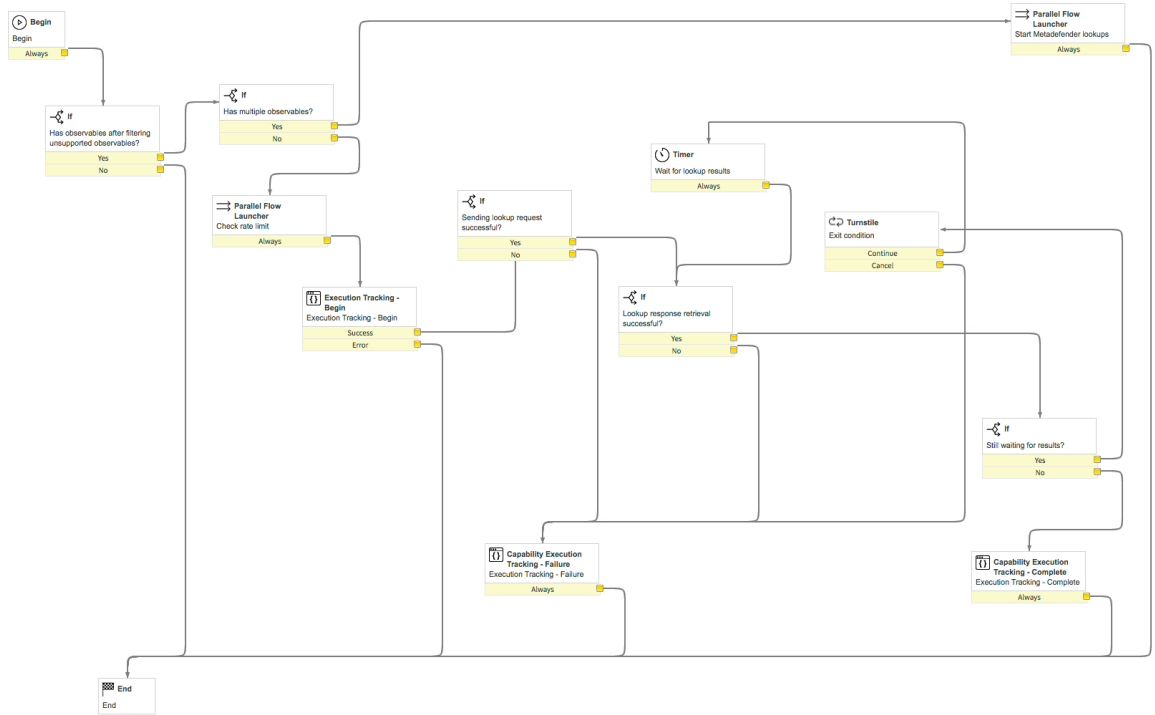
Antes de Iniciar
Função necessária: sn_si.admin

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado pelo Integração do Security Operations - Pesquisa de ameaças quando você executa uma pesquisa de ameaça em um ou mais observáveis e a implementação do OPSWAT Metadefender é selecionada. Para obter mais informações, consulte Realizar pesquisas em observáveis.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de ameaças - Fluxo de trabalho do Metadefender OPSWAT



Para obter informações sobre as atividades usadas por este fluxo de trabalho, consulte Atividades de fluxo de trabalho de integração comuns.

Integração do VirusTotal

A integração VirusTotal permite que você solicite a análise de endereços IP, arquivos, hashes de arquivo e endereços URL suspeitos para ajudar em sua investigação para determinar se eles são mal-intencionados.

Explorar Integrações do Inteligência contra ameaças	Configurar • VirusTotal configuração de integração • Ativar e configurar a integração VirusTotal
Usar • Realizar pesquisas em observáveis • Pesquisa de ameaças - Fluxo de trabalho do VirusTotal	Desenvolver • ServiceNow Security Operations diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento • Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Solução de problemas de integração
- Faça ou responda perguntas na comunidade do Security Operations
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

VirusTotal configuração de integração

VirusTotal é um serviço gratuito que analisa arquivos e URLs suspeitos e facilita a detecção rápida de vírus, worms, trojans e todos os tipos de malware. Ele se integra facilmente com Security Operations.

Antes de usar a integração VirusTotal, você deve ativar o plug-in e adicionar a chave de API apropriada. Se necessário, você também pode atualizar sua certificação SSL X509.

Se a origem de pesquisa VirusTotal for usada e o malware for encontrado, um observável será criado. Para pesquisas de IP, uma lista adicional de URLs que compartilham o endereço IP é criada e observáveis são criados para cada um dos URLs.

Nota:

- O plug-in Inteligência contra ameaças é necessário para implementar a integração VirusTotal.
- A integração VirusTotal foi atualizada para APIs da versão 3.

Ativar e configurar a integração VirusTotal

Antes de usar a integração VirusTotal, você deve baixá-la do ServiceNow Store.

Antes de Iniciar

Função necessária: administrador
Inteligência contra ameaças O deve ser instalado e ativado antes que você possa usar o VirusTotal. A integração VirusTotal foi atualizada para as APIs da versão 3.

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, acesse o VirusTotal e obtenha a chave de API no seu perfil do VirusTotal.
3. Em sua instância, navegue até **Security Operations** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
4. No cartão VirusTotal, clique em **Configurar**.

Configuração do VirusTotal

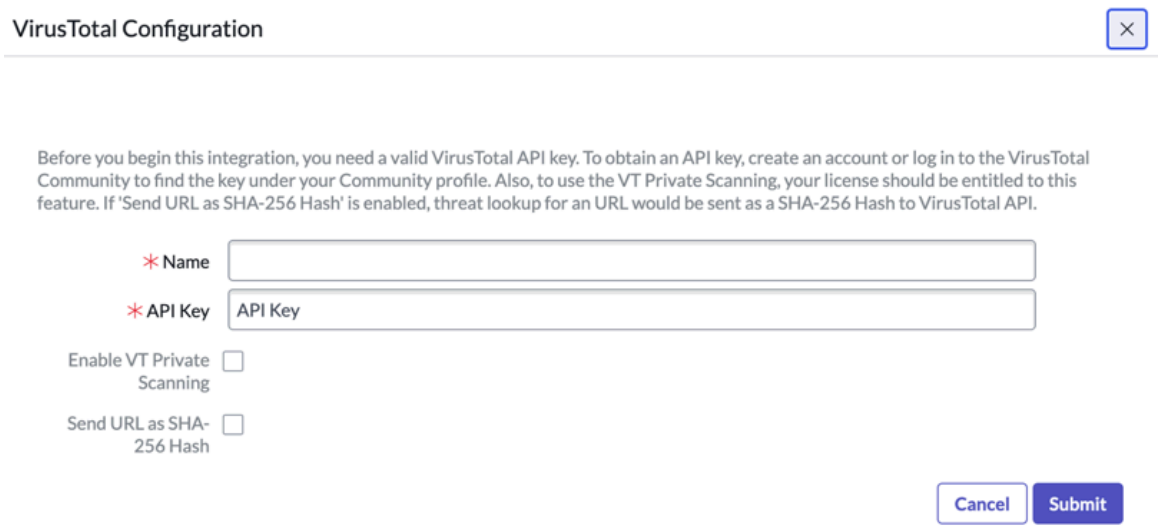
Campo	Descrição
Nome	Nome da integração. Por exemplo, VirusTotal.
Chave de API	Insira (ou cole) a **chave de API** que você adquiriu no site VirusTotal.
Habilitar verificação privada de VT	Marque esta caixa de seleção para analisar arquivos com VirusTotal preservando a privacidade. Os

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	arquivos carregados por meio desta oferta não serão compartilhados com ninguém além da sua organização e permanecerão no VirusTotal apenas por um breve período. As análises resultantes também serão efêmeras e visíveis somente para o seu grupo VirusTotal. **Importante:** Para usar o VT Private Scanning, sua licença do VirusTotal deve ter direito a este recurso.
Enviar URL como hash SHA-256	Marque esta caixa de seleção para enviar os URLs como hashes para pesquisa de ameaças e proteger a privacidade dos usuários na integração. **Nota:** Se desabilitado, o URL será enviado como codificação Base64 para a API VirusTotal.

5. Clique em **Enviar**.



Resultado

Depois de configurado, o VirusTotal pode ser selecionado para executar pesquisas em observáveis em Inteligência contra ameaças e em observáveis em incidentes de segurança.

Tópicos relacionados

Realizar pesquisas em observáveis

Pesquisa de ameaças - Fluxo de trabalho do VirusTotal

O fluxo de trabalho Pesquisa de ameaças - VirusTotal executa uma pesquisa em observáveis selecionados. Se os observáveis forem de um tipo reconhecido por VirusTotal, eles serão verificados quanto a malware e os resultados serão retornados.

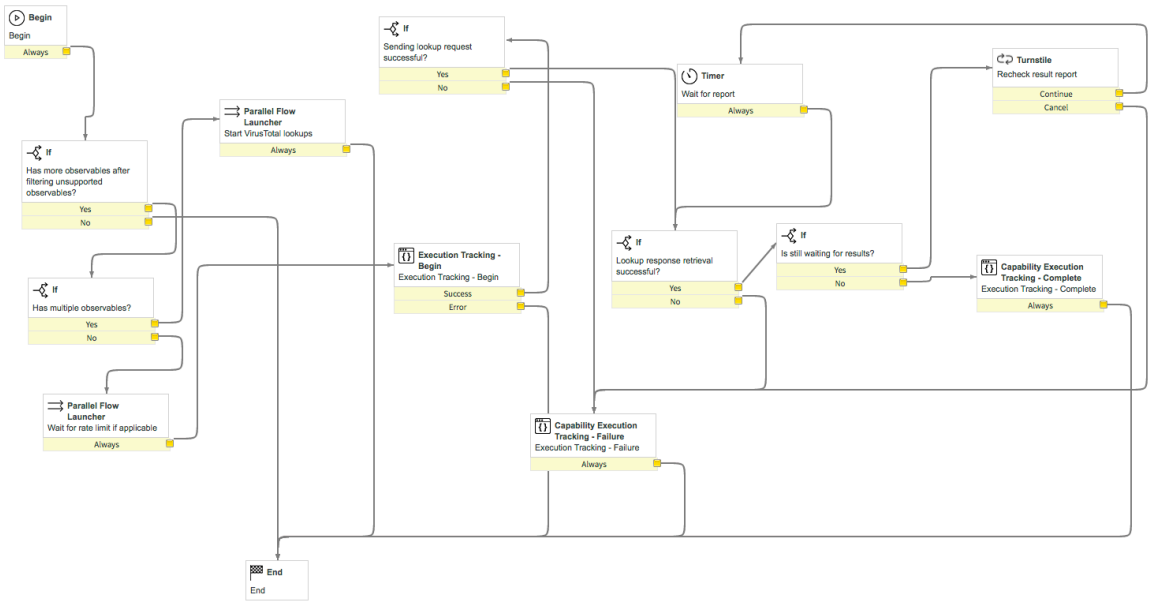
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: administrador

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado pelo Integração do Security Operations - Pesquisa de ameaças quando você executa uma pesquisa de ameaça em um ou mais observáveis e a implementação VirusTotal é selecionada. Para obter mais informações, consulte Realizar pesquisas em observáveis.

Pesquisa de ameaças - Fluxo de trabalho do VirusTotal



Para obter informações sobre as atividades usadas por este fluxo de trabalho, consulte Atividades de fluxo de trabalho de integração comuns.

Integração da API WhoisXML

A integração da API WhoisXML permite que você envie pesquisas de Whois em nomes de domínio e URLs para obter contexto em observáveis de URL e para fazer uma melhor determinação sobre ameaças.

Explorar Integrações do Inteligência contra ameaças	Configurar • Configuração da integração da API WhoisXML • Ativar e configurar a integração Whois do Security Operations
Usar Inteligência contra ameaças - Executar fluxo de trabalho de pesquisa de IoC	Desenvolver • ServiceNow Security Operations diretrizes de desenvolvimento de integração • Dicas para escrever integrações • Desenvolver treinamento

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

	• Desenvolver documentação • Localizar componentes instalados com uma aplicação
Solucionar problemas e obter ajuda • Solução de problemas de integração • Faça ou responda perguntas na comunidade do Security Operations • Pesquise artigos de erros conhecidos no portal de erros conhecidos • Contato Suporte e atendimento ao cliente	

Configuração da integração da API WhoisXML

Antes de usar a integração Whois, você deve ativar o plug-in e adicionar as credenciais. Se necessário, você também pode atualizar sua certificação SSL X509.

Os plug-ins Inteligência contra ameaças e WhoisXML API Integration são necessários para implementar a integração de API WhoisXML.

Ativar e configurar a integração Whois do Security Operations

O recurso Configuração de integração permite que você ative e configure rapidamente integrações de segurança de terceiros, incluindo a integração Security Operations Whois. Antes de usar a integração Whois do Security Operations, você deve baixá-la do ServiceNow Storee deve ter uma conta válida da API WhoisXML.

Antes de Iniciar

Inteligência contra ameaças O deve ser instalado e ativado para que você possa usar a integração Whois do Security Operations.

Função necessária: administrador

Procedimento

1. Baixe a integração do ServiceNow Store.
2. Quando a instalação estiver concluída, navegue até **Security Operations** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões.
3. No cartão da API Whois, clique em **Configurar**.
4. Insira o Nome de usuário e a Senha da sua conta da API WhoisXML.
5. Clique em **Enviar**.

Atualize seu certificado X.509

Se você precisar de uma conexão SSL para a integração, há circunstâncias em que o certificado fornecido pelo fornecedor terceirizado ainda não é confiável em ServiceNow ou expirou. Esta tarefa é opcional.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um Certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

   a. Insira o URL do endpoint na barra de endereço do navegador.
   Por exemplo: `https://<3rdparty>/`.

   b. Clique no ícone de cadeado na linha de endereço.

   c. Clique em **Mais informações** e na guia **Segurança**.

   d. Clique em **Exibir certificado** e na guia **Detalhe**.

   e. Clique em **Exportar** para salvar o PEM em seu sistema de arquivos local.

   f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
   Ele deve começar com `-----BEGIN CERTIFICATE-----` e terminar com `-----END CERTIFICATE-----`.

2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e crie um novo registro para a integração.
4. Em **Certificado PEM**, cole o certificado que você baixou e copiou para a área de transferência anteriormente.
5. Adicione o certificado ao registro do provedor de identidade.
   a. Navegar até **SSO Multiprovedor** > **Provedores de Identidade**.
   b. Selecione o provedor de identidade padrão ativo para o qual você criou o novo certificado.
   c. Role para baixo até a lista relacionada de **certificados X.509** e clique em **Editar**.
   d. Mova o certificado recém-criado para a coluna **Selecionado**.
6. Clique em **Salvar**.
   Os outros campos no registro são gerados automaticamente.

Nota:
Se você tiver um certificado que expirou, será necessário removê-lo. Para obter informações sobre como remover o certificado expirado, consulte KB0691439 Substituir um certificado SAML expirando .

Aprimorar fluxo de trabalho WhoIs do observável

O fluxo de trabalho **Aprimorar observáveis WhoIs** executa o aprimoramento em observáveis selecionados. Se os observáveis forem de um tipo reconhecido pelo WhoisXML API Integration, os observáveis serão aprimorados.

Antes de Iniciar

Função necessária: administrador

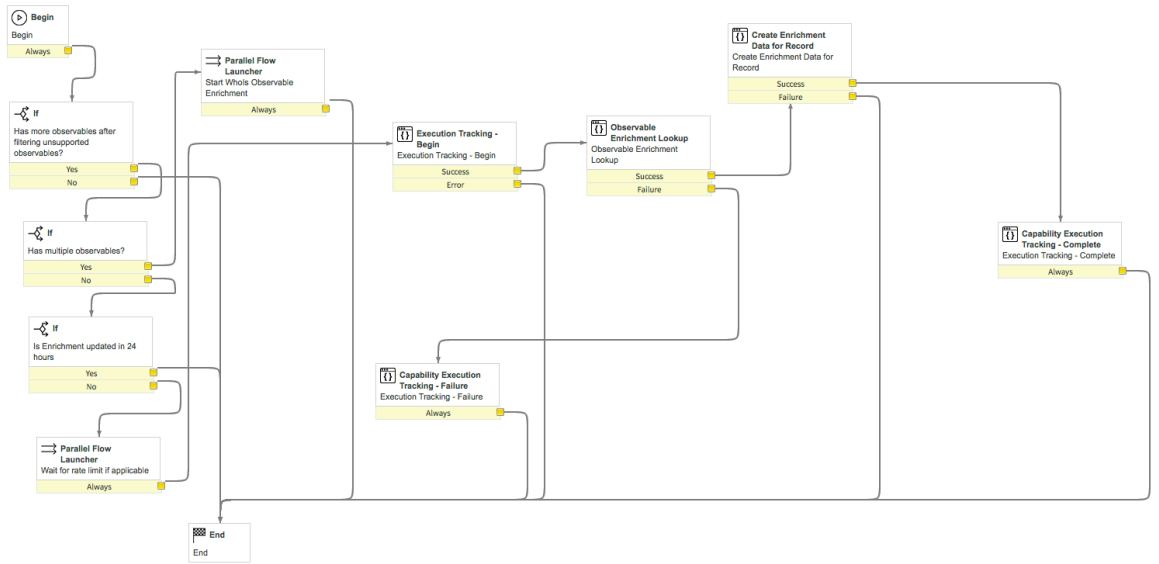
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho é acionado pelo Integração do Security Operations - Capacidade Aprimorar observável quando você executa o aprimoramento em um ou mais observáveis e a implementação de WhoIs é selecionada.

Aprimorar fluxo de trabalho WhoIs do observável



Atividades específicas para esta integração são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Atividade Pesquisa de aprimoramento de observável

A atividade de fluxo de trabalho **Pesquisa de aprimoramento de observável** inicia o processo de aprimoramento de observável.

A atividade **Pesquisa de aprimoramento de observável** pode ser usada com qualquer fluxo de trabalho de observáveis para iniciar o aprimoramento.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	A pesquisa foi bem-sucedida.
Falha	Ocorreu um erro ao tentar executar a pesquisa. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
Id_implementação	Identificador do sistema da implementação usada para executar a pesquisa.
domain_id	O identificador de domínio para o domínio no qual a pesquisa está sendo realizada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
observável_ids	Um ou mais observáveis para executar a ação desejada. Os IDs são usados como uma entrada de fluxo de trabalho.
capacidadeExcutionId	Identificador do sistema da capacidade que iniciou o fluxo de trabalho de implementação. Necessário somente para fluxos de trabalho de implementação da capacidade de integração, como Splunk, Elasticsearch.
task_sys_id	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta_dados	Dados brutos retornados pelo endpoint da API da implementação para o domínio fornecido.
mapeamento_id	O identificador do mapeamento de aprimoramento. Por exemplo, a integração WhoIs retorna dados em dois formatos diferentes, IP e URL, com um ID de mapeamento para cada um.

Orquestração de inteligência contra ameaças

Orquestração de inteligência contra ameaças As atividades permitem que os usuários determinem se uma ameaça foi vista antes em outros incidentes de segurança ou em outros sistemas usando a orquestração de fluxo de trabalho.

Para obter mais informações sobre como editar fluxos de trabalho Orquestração de resposta de incidente de segurança ou criar fluxos de trabalho personalizados, consulte Introdução a fluxos de trabalho e ao Editor de fluxo de trabalho Editor de fluxo de trabalho.

Configurar Orquestração de inteligência contra ameaças

Antes de usar Orquestração de inteligência contra ameaças, execute as etapas para configurar várias partes do sistema, incluindo o preenchimento do CMDB, a configuração do MID Server e a configuração de credenciais.

Antes de Iniciar

Função necessária: administrador

Para usar Orquestração de inteligência contra ameaças, você precisa de um CMDB totalmente preenchido com nomes de domínio. Para obter mais informações, consulte Descoberta.

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Ativar o plug-in do Inteligência contra ameaças.
2. Configurar o MID Server
3. Configurar credenciais de serviço do MID Server
   Agora você está pronto para usar Orquestração de inteligência contra ameaças atividades em um fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxos de trabalho e atividades de Orquestração de inteligência contra ameaças

O sistema básico inclui fluxos de trabalho e atividades de fluxo de trabalho que você pode usar para automatizar ações em sua instância.

Inteligência contra ameaças - Executar fluxo de trabalho de pesquisa de IoC

O fluxo de trabalho **Inteligência contra ameaças - Executar pesquisa de IoC** verifica se há um observável não expirado e, em caso afirmativo, a pesquisa é definida como **Concluída** e atualizada com os dados do observável.

Antes de Iniciar

Função necessária: sn_si.basic

Nota:
Este fluxo de trabalho substitui Orquestração de inteligência contra ameaças regras de negócio (**Preencher com tabelas IoC existentes**, **Enfileirar a pesquisa**e **Atualizar observável**) por atividades.

Se uma pesquisa for inserida ou atualizada e atender às condições, a regra de negócios de pesquisa acionará este fluxo de trabalho.

Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho **Inteligência contra ameaças - Executar pesquisa de IoC** verifica se há um observável não expirado e, em caso afirmativo, a pesquisa é definida como **Concluída** e atualizada com os dados do observável. Todos os indicadores associados ao observável são reativados.

Se o observável estiver expirado, o fluxo de trabalho executará as pesquisas e incrementará a **contagem** de vistas no observável expirado existente.

Se não houver nenhum observável correlativo, um novo observável com indicador será criado.

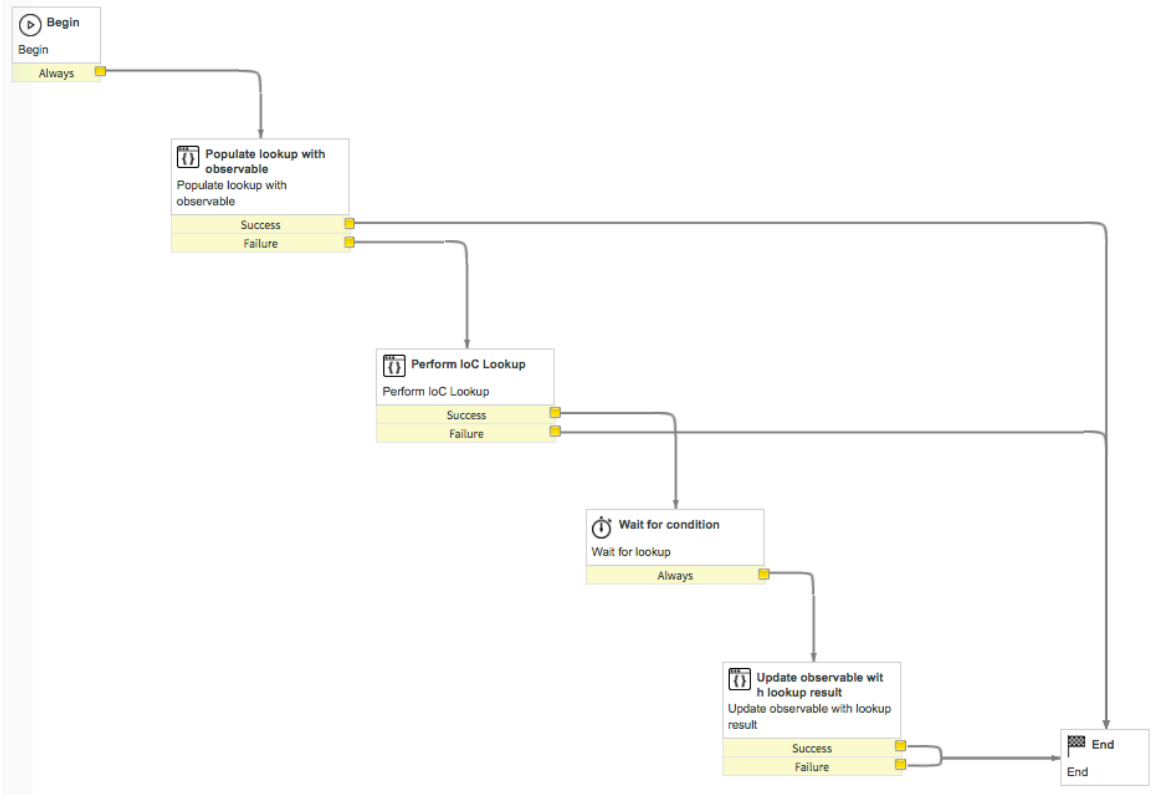
As atividades do processo de fluxo de trabalho incluem:

- Preencher pesquisa com atividade observável
- Executar atividade de pesquisa de IoC
- Aguardar pesquisa (atividade principal)
- Atualizar observável com atividade de resultado de pesquisa

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Inteligência contra ameaças - Executar fluxo de trabalho de pesquisa de IoC



Preencher pesquisa com atividade observável

Se um observável não expirado for encontrado, a atividade de fluxo de trabalho **Orquestração de inteligência contra ameaças - Preencher pesquisa com observável** fornecerá dados de um observável existente para uma pesquisa. Esta atividade pode acelerar o processo de investigação e correção.

Quando acionado por uma **pesquisa Preencher pesquisa com observável** de fluxo de trabalho, tenta encontrar um observável existente para uma pesquisa que corresponda ao **valor** e ao **tipo** da pesquisa fornecida para a atividade como entrada.

Se o observável existir e não estiver expirado, esta atividade:

- Atualiza a pesquisa com as informações encontradas no observável
- Reativa um indicador se ele estiver inativo, incrementa a **contagem de Encontrados**e atualiza a data da **última exibição**
- Define **o Estado** como Concluído.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável de entrada	Descrição
scanID[cadeia de caracteres]	identificador de pesquisa

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída	Descrição
Verdadeiro	Observável válido encontrado e pesquisa atualizada.
Falso	Observável válido não encontrado. O observável está ausente ou expirou.

Executar atividade de pesquisa de IoC

A atividade de fluxo de trabalho **Orquestração de inteligência contra ameaças - Executar pesquisa de IoC** realiza uma determinada pesquisa. Esta atividade pode acelerar o processo de investigação e correção.

Quando acionado por um fluxo de trabalho, **Executar pesquisa de IoC** obtém um scanID, pesquisa o registro de pesquisa e adiciona a pesquisa à fila criando uma entrada de fila de pesquisa.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
scanID[cadeia de caracteres]	identificador de pesquisa

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
Verdadeiro	Acionou a pesquisa.
Falso	Não acionou a pesquisa.

Atualizar observável com atividade de resultado de pesquisa

A atividade de fluxo de trabalho **Orquestração de inteligência contra ameaças - Atualizar observável com resultado de pesquisa** atualiza o registro do observável. Se não existir, ele criará um novo observável. Esta atividade é útil para registrar informações.

Quando acionado por um fluxo de trabalho, **Atualizar observável com resultado de pesquisa** atualiza um observável existente para incluir a nova **Contagem**de vistas , adiciona uma anotação e, se inativo, reativa todos os indicadores. A **contagem de encontrados** e a data da **última exibição** no indicador também são atualizadas.

Se não houver nenhum observável correlativo, o fluxo de trabalho criará um novo observável com o indicador da seguinte forma:

- Executa as pesquisas de IoC
- Cria um novo observável
- Cria um indicador para o observável
- Adiciona uma **contagem** de vistas ao observável

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Adiciona uma **contagem de encontrados** e a data da **última exibição** ao indicador
- Adiciona uma mensagem indicando a partir da qual a pesquisa foi criada

.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
scanID[cadeia de caracteres]	Identificador de pesquisa.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
Verdadeiro	Atualização ou criação do observável bem-sucedida.
Falso	Falha na atualização ou criação do observável.

Atividade Executar origens de pesquisa de IoC padrão

Quando acionado por um fluxo de trabalho, Inteligência contra ameaças - **Executar origens de pesquisa IoC padrão** obtém um ID de solicitação de pesquisa e cria várias pesquisas, dependendo dos valores de dados inseridos.

Para cada tipo de dados, a coluna de **verificação include_in_bulk** da tabela de tipo de pesquisa compatível de cada origem de pesquisa é avaliada. Se verdadeiro, uma pesquisa será adicionada à solicitação de pesquisa.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
id_scan_request	Pesquisar identificador do sistema de solicitação

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
Número de verificações criadas	Inteiro

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Security Case Management

Security Case Management fornece um meio para os analistas de segurança que estão envolvidos na busca de ameaças coletarem informações sobre atividades suspeitas em seu ambiente. Registros relacionados a casos, como incidentes de segurança, observáveis, ICs e usuários afetados, podem ser adicionados a casos para acomodar análises amplas e específicas.

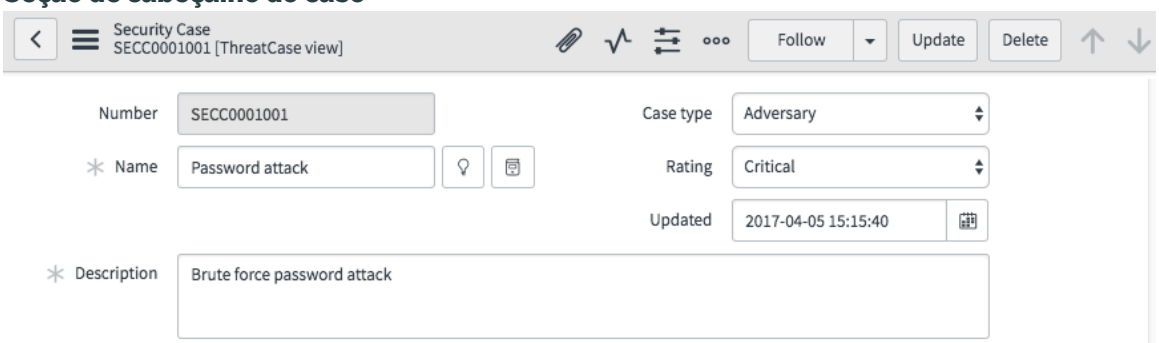
Com a capacidade de alternar facilmente os registros e as informações relacionadas, os analistas podem avaliar se estão enfrentando uma campanha direcionada, uma ameaça persistente avançada e assim por diante.

Os casos de segurança podem ser criados a partir de várias origens na sua instância, incluindo Security Case Management, Security Incident Responsee Inteligência contra ameaças. Você também pode criar casos a partir de itens de configuração e usuários afetados nas tabelas Itens de configuração [cmdb.ci] e Usuários [sys.user], respectivamente. Depois que os casos foram criados, cada uma dessas origens também pode ser usada para adicionar recursos de análise valiosos aos casos existentes.

Cada caso de segurança consiste em três seções principais, uma seção de cabeçalho, uma seção com detalhes adicionais do caso e uma seção de artefatos de caso que contém uma coleção de registros que ajudam a criar um argumento para identificar e lidar com ameaças específicas.

Cabeçalho do caso

Seção de cabeçalho do caso



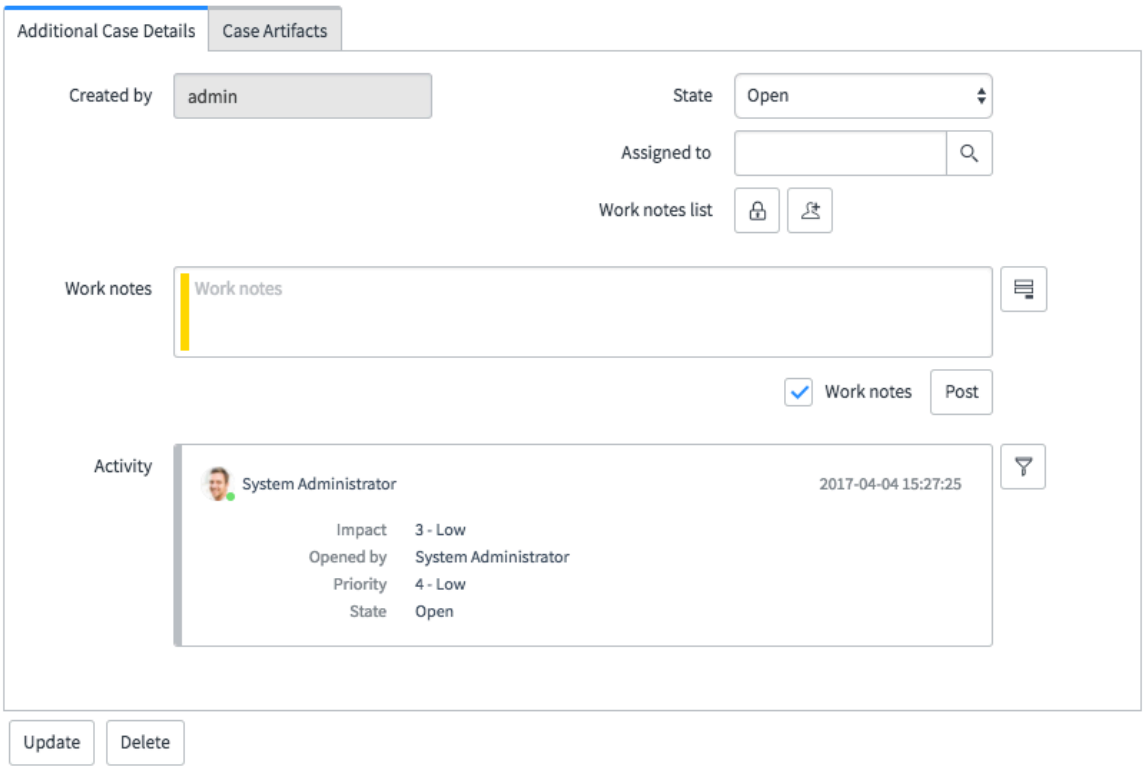
O cabeçalho do caso fornece informações básicas usadas para identificar e classificar o caso de segurança. O número do caso usa o prefixo SECC.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhes adicionais do caso

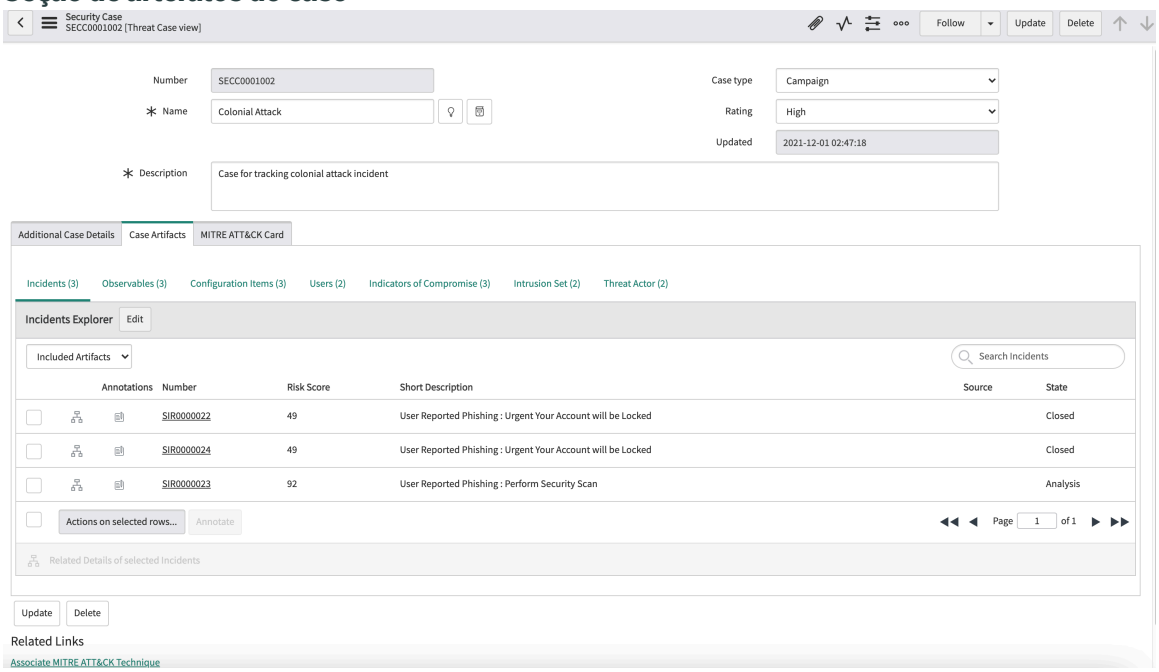
Seção de detalhes adicionais do caso



A seção **Detalhes adicionais do caso** fornece informações específicas para a análise que já foi realizada no caso, incluindo seu estado atual e anotações de trabalho e atividades registradas para o caso.

Artefatos de caso

Seção de artefatos do caso



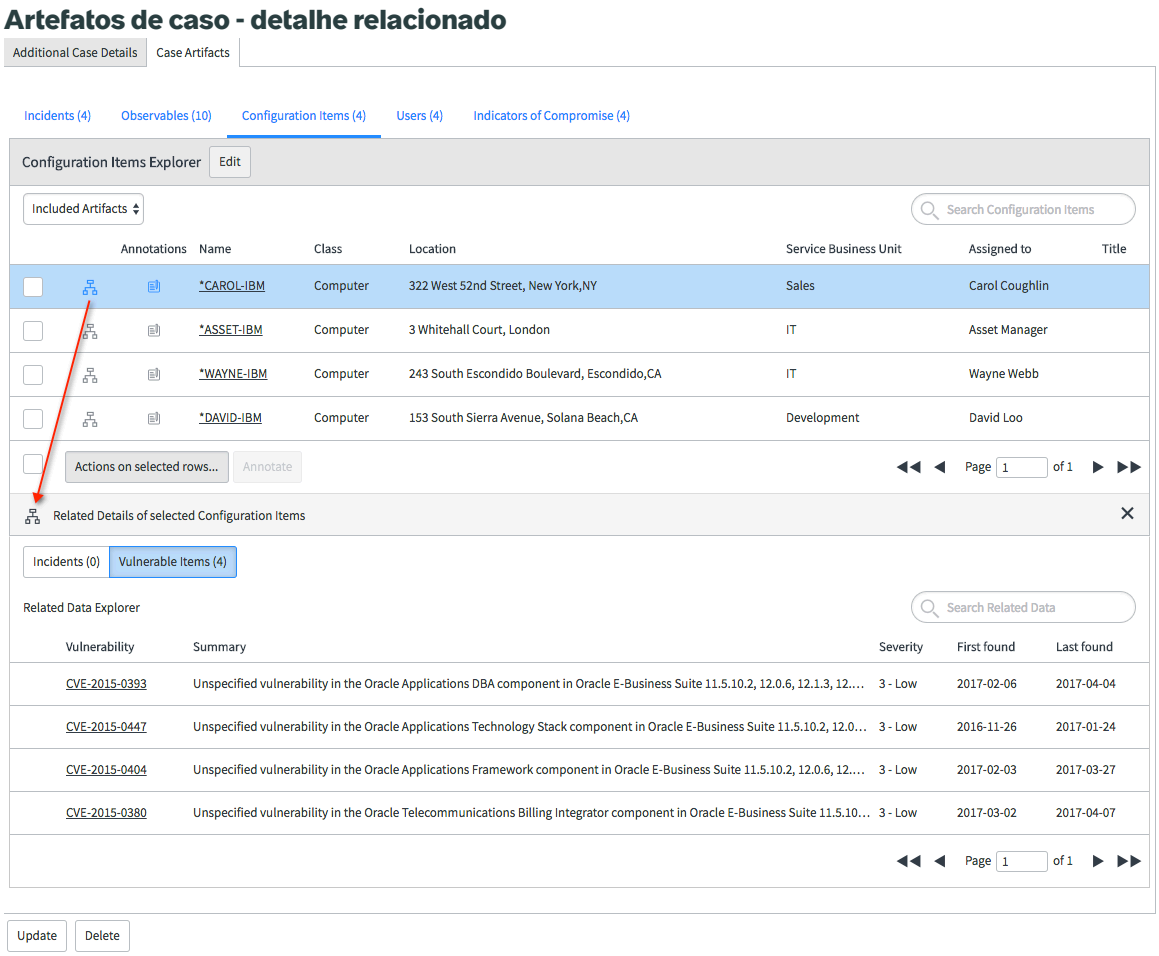
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A seção **Artefatos do caso** fornece uma série de guias de informações contidas no caso de segurança.

Você pode realizar pesquisas no conteúdo de cada guia. Você também pode excluir registros específicos que já avaliou como seguros ou que não têm valor em sua investigação. Os registros excluídos não são excluídos, mas ficam ocultos na exibição. Se necessário, você pode exibir registros excluídos e adicioná-los de volta.

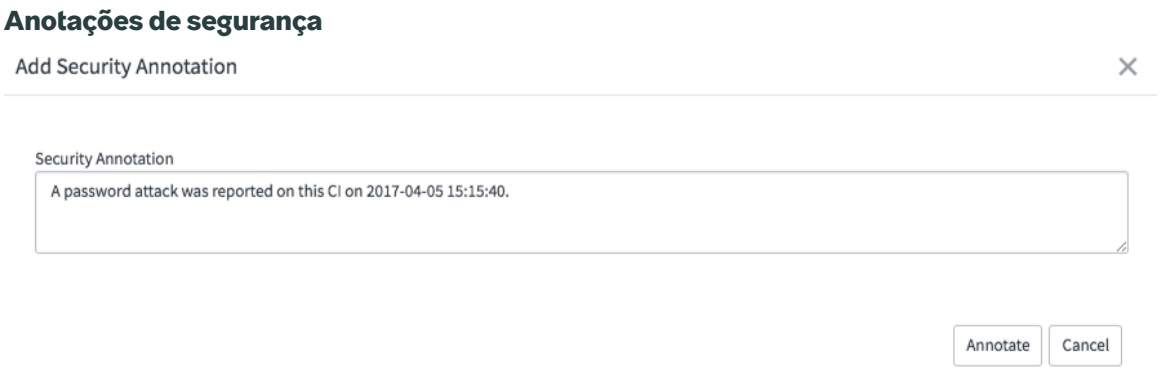
Em cada guia, você pode clicar no ícone Detalhes adicionais para mostrar informações relacionadas ao registro selecionado. Por exemplo, se você clicar na guia **Itens de configuração** para exibir o Gerenciador de itens de configuração e clicar em Detalhes adicionais para um IC específico, poderá exibir incidentes, itens vulneráveis e anotações associadas a esse IC.



Você também pode selecionar um registro e clicar no botão **Anotar** de um artefato relacionado ao caso para adicionar anotações ao registro. As anotações são simplesmente anotações que cada analista pode fazer em um artefato específico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Outras ferramentas que o analista pode usar para examinar casos incluem:

- Executar uma pesquisa de vistas em observáveis em um caso
- Pesquisar artefatos de segurança

Criar casos na Gestão de casos de segurança

Os casos são usados para rastrear informações sobre uma campanha ou agente de estado que ameaça sua organização. Depois que um caso é criado, você pode adicionar artefatos que permitem revisar e analisar todas as informações relacionadas em um único registro de caso.

Antes de Iniciar

Função necessária: sn_ti.case_use

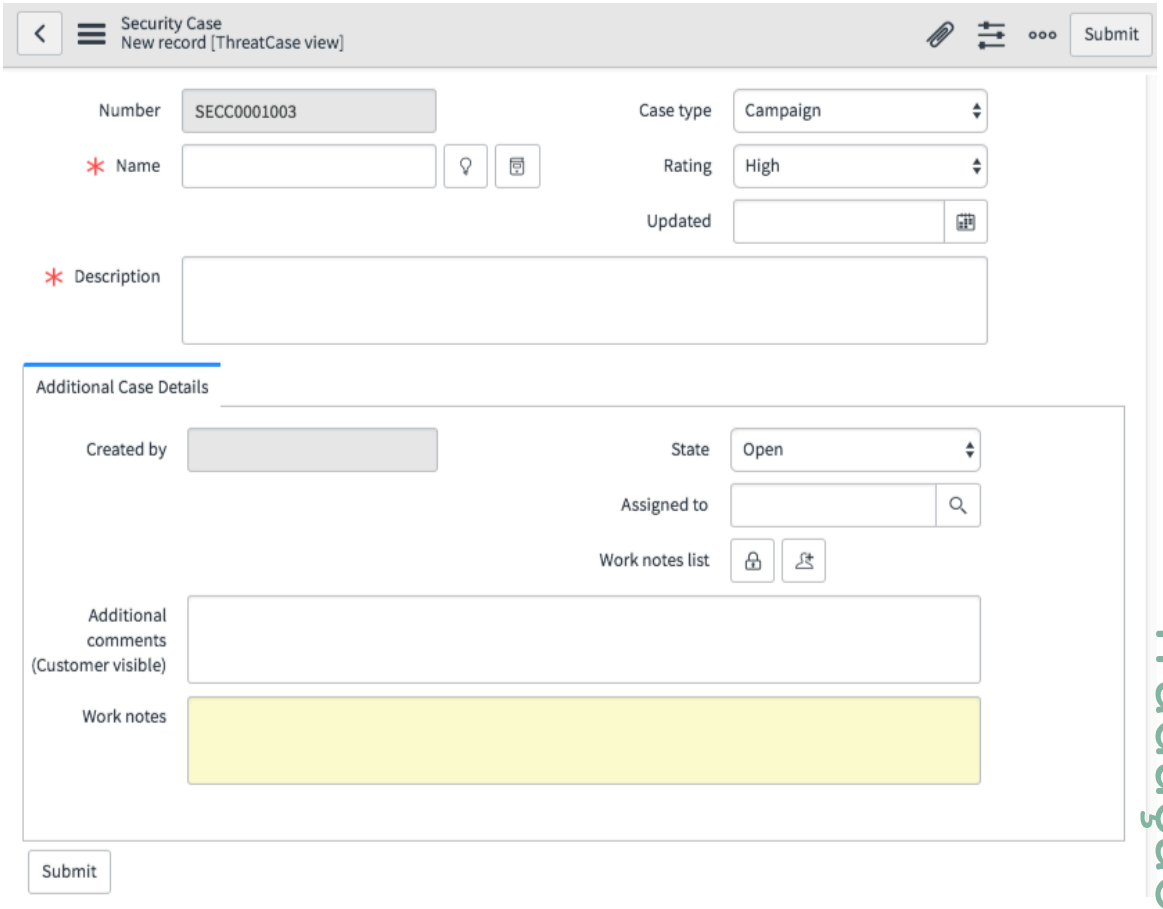
r

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
   A lista Casos de segurança é aberta.
2. Clique em **Nova**.
   A tela Casos de segurança é aberta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



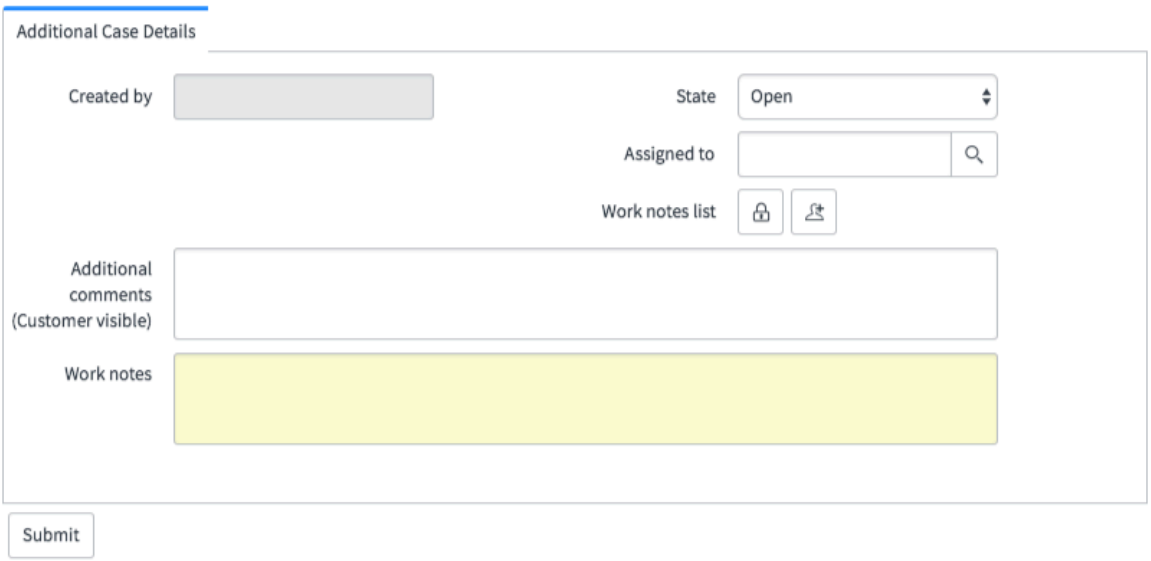
3. Preencha os campos, se for o caso.

Campo	Descrição
Número do caso	[Somente leitura] O número do caso.
Nome de Caso	Insira um nome descritivo para o caso.
Tipo de Caso	Selecione o tipo de caso que está sendo investigado.
Classificação	Selecione a importância deste caso (de Crítica a Baixa).
Última atualização	[Somente leitura] A data e a hora em que o caso foi atualizado pela última vez.
Descrição resumida	Uma breve descrição do caso.

4. Clique na guia **Detalhes adicionais do caso**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Preencha os campos, se for o caso.

Campo	Descrição
Criado por	[Somente leitura] O nome do usuário que criou este caso.
Estado	O estado atual do caso. Na criação do caso, o Estado é padronizado como Rascunho.
Atribuído a	Clique no ícone de pesquisa e atribua o caso a um analista.
Lista de Anotações de trabalho	Clique no ícone de cadeado e adicione usuários internos que podem exibir anotações de trabalho.
Comentários adicionais	Conforme necessário, insira anotações no caso que ficarão visíveis para o cliente.
Anotações de trabalho	Se necessário, digite uma anotação de trabalho para o caso.

6. Clique em **Enviar**.
Depois que o registro tiver sido salvo, você poderá clicar na guia **Artefatos do caso** e adicionar artefatos ao caso.

Adicionar artefatos a um caso

Depois de criar um caso, você pode adicionar artefatos, como incidentes de segurança, ICs e indicadores de comprometimento, ao caso. Esses artefatos atuam como pistas na resolução do caso.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

Função necessária: sn_ti.case_user_write

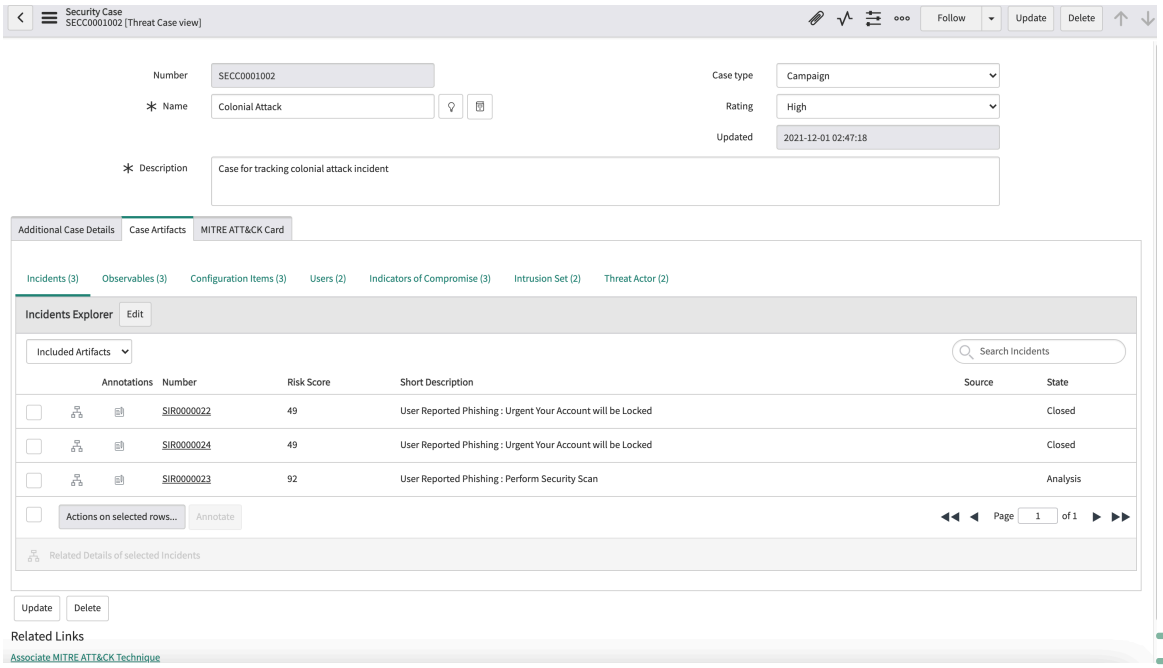
Procedimento

1. Abra um caso ao qual você deseja adicionar artefatos.

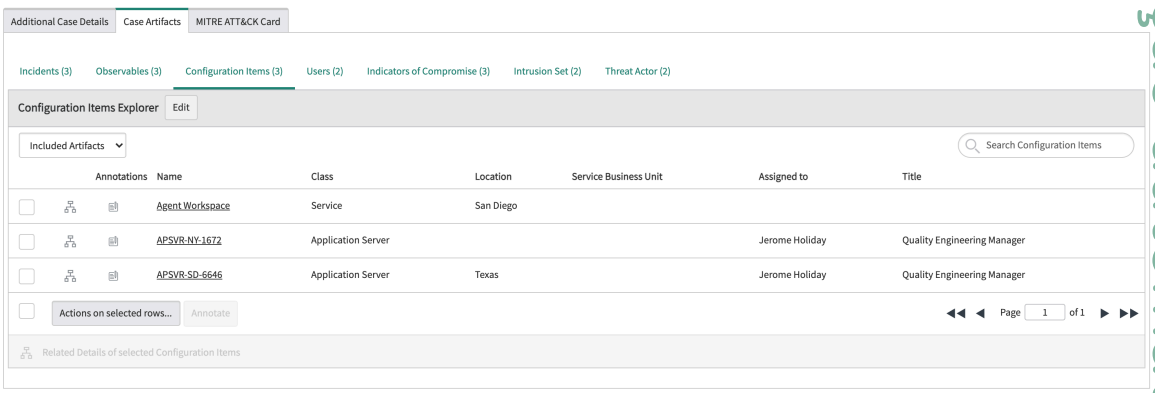
2. Clique na lista relacionada **Artefatos do caso**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



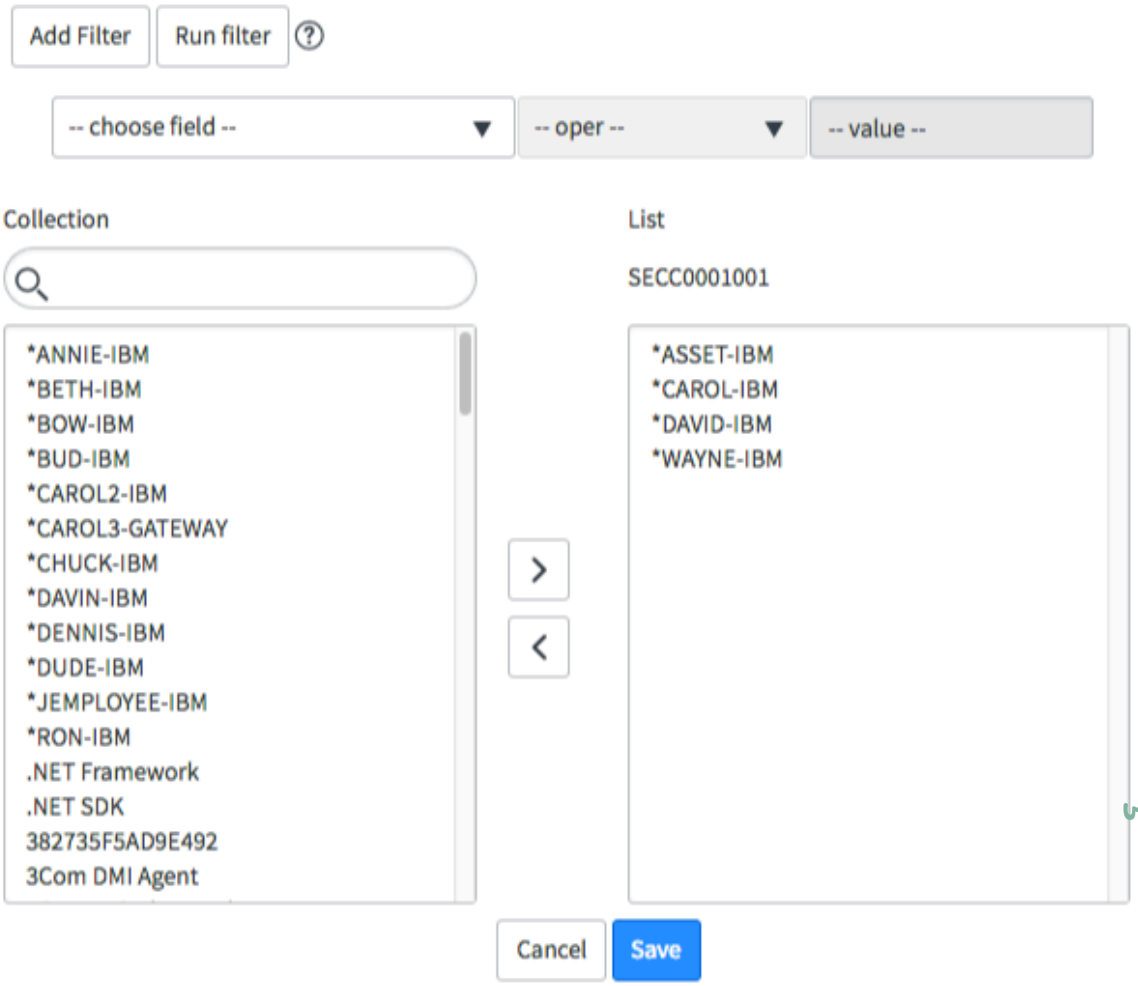
3. Clique na guia associada ao tipo de artefato que você deseja adicionar ao caso.
Por exemplo, clique em **Itens de configuração** para adicionar um ou mais ICs ao caso.



4. Clique em **Editar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Usando a interface de caixa de listagem dupla e os filtros, localize os registros de artefato que você deseja adicionar ao caso, mova-os do bucket Coleção para o bucket Lista e clique em **Salvar**.
   A lista aparece na guia selecionada e os artefatos selecionados são adicionados à lista.

Tópicos relacionados

- Adicionar IoCs e observáveis a um caso existente
- Adicionar incidentes de segurança a um caso existente
- Adicionar ICs a casos existentes
- Adicionar usuários afetados a casos existentes

Associar informações MITRE-ATT&CK ao caso de segurança

Associe MITRE-ATT&CK táticas e técnicas a um caso de segurança para melhorar a gestão de casos de segurança e a análise de ameaças em um nível granular.

Antes de Iniciar

Função necessária: sn_si.analyst

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
2. Selecione o caso de segurança que você deseja aprimorar com as informações do MITRE-ATT&CK.

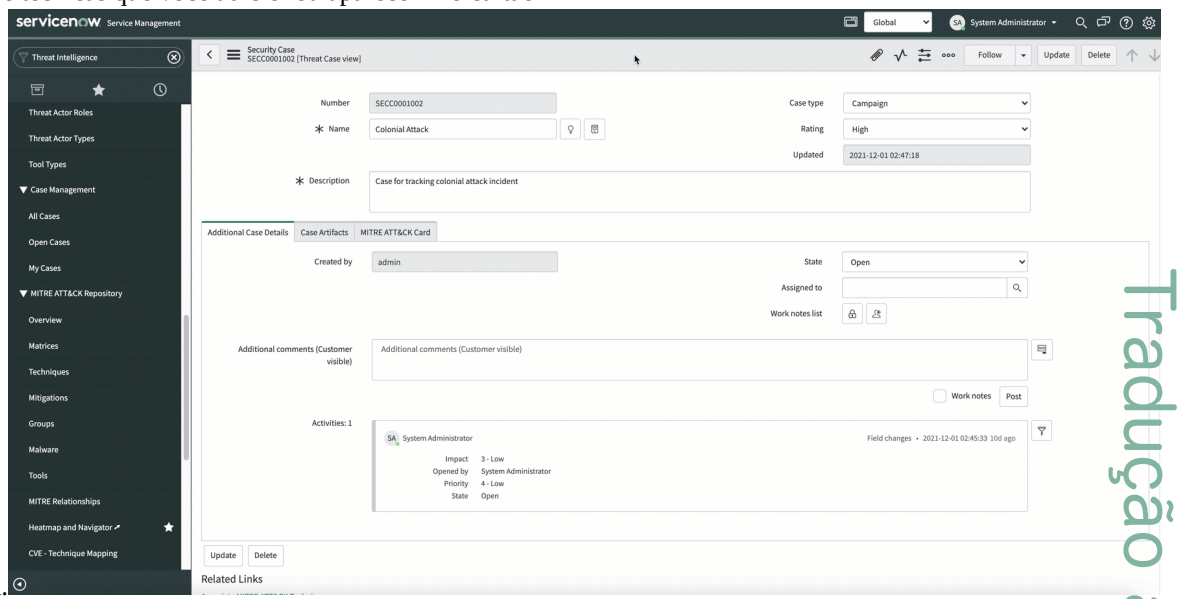
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na lista relacionada, clique em **Associar técnica MITRE ATT&CK**.

   Na ilustração a seguir, você pode ver como navegar na lista relacionada até **Associar técnica do MITRE ATT&CK**, revisar a origem e adicionar uma tática e uma técnica.

4. Nas listas de origem, revise a **Origem**.
5. Revise a **Tática** e as **Técnicas**e adicione ou remova-as com base na relevância do caso.
6. Clique em **Salvar**.
   As táticas e técnicas que você adicionou aparecem no cartão MITRE-ATT&CK.



Criação de caso a partir de artefatos de segurança

Além de criar casos manualmente a partir de Security Case Management, você também pode criar casos a partir de artefatos de segurança, como incidentes de segurança, indicadores de comprometimento, usuários afetados e itens de configuração.

IoCs e observáveis em casos

Em Inteligência contra ameaças, você pode criar casos de IoCs e observáveis, bem como adicionar IoCs e observáveis a casos existentes. Você também pode criar observáveis diretamente de um caso.

Criar um caso a partir de IoCs ou observáveis

Em Inteligência contra ameaças, você pode criar um caso a partir de artefatos (IoCs ou observáveis). Depois que os IoCs ou os observáveis forem usados para criar um caso, você poderá usar Security Case Management para analisar os dados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

Função necessária: sn_ti.case_user_write

Tradução automática

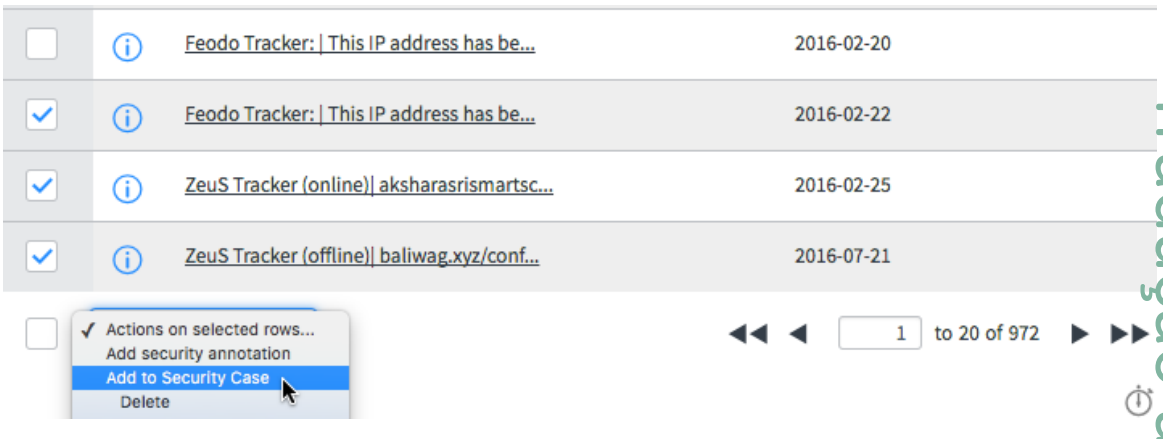
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

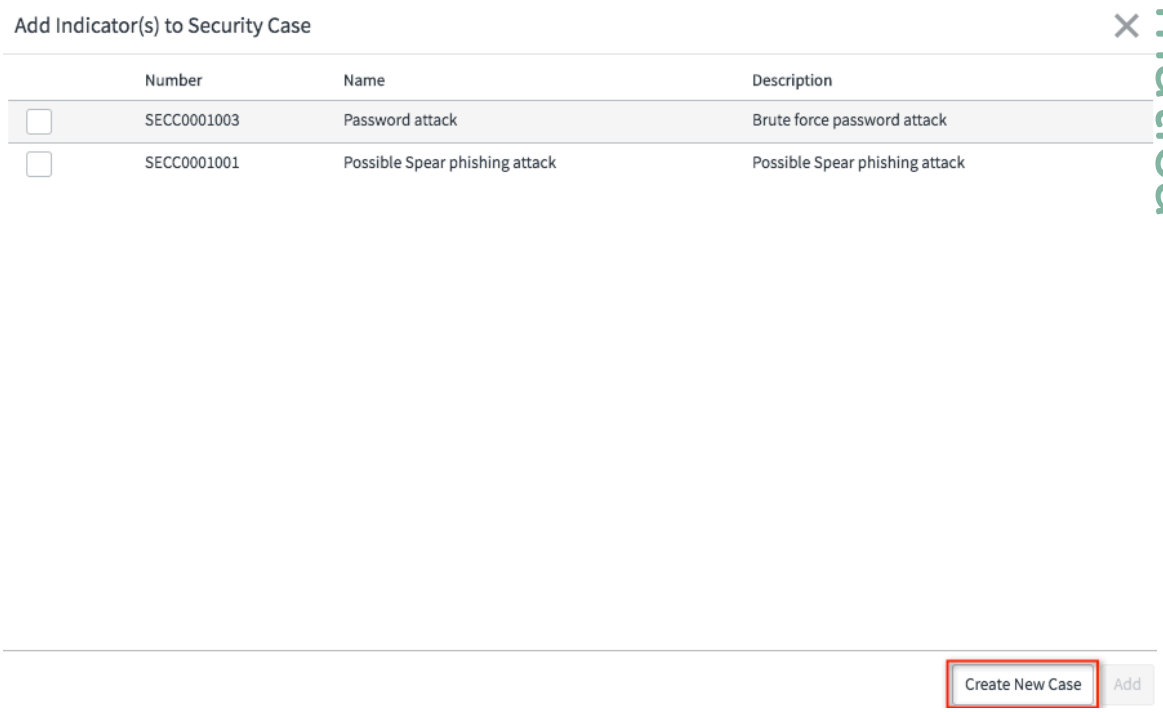
1. Navegue até os artefatos (IoCs ou observáveis) que você deseja usar para criar um caso.
   - Para criar um caso a partir de IoCs, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
   - Para criar um caso a partir de observáveis, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Na lista, selecione os artefatos que você deseja adicionar a um novo caso.

   Nota:
   Se você selecionar vários IoCs ou observáveis, todos eles serão adicionados ao caso.

3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.



A caixa de diálogo **Adicionar ao caso de segurança** é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.



4. Clique **em Criar novo caso**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. Preencha os campos.

Campo	Descrição
Nome de Caso	Insira um nome para este caso.
Descrição	Insira uma descrição que seja valiosa para o analista de caso.

6. Clique em **Enviar**.
   Uma mensagem na parte superior da lista indica que um novo caso foi criado, junto com um link para o caso em Security Case Management.
7. Clique no link para exibir o novo caso.

Adicionar IoCs e observáveis a um caso existente

Você pode adicionar IoCs e observáveis a casos existentes. Depois que os incidentes de segurança forem adicionados aos casos, você poderá usar Security Case Management para analisar os dados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

Função necessária: sn_ti.case_user_write

Procedimento

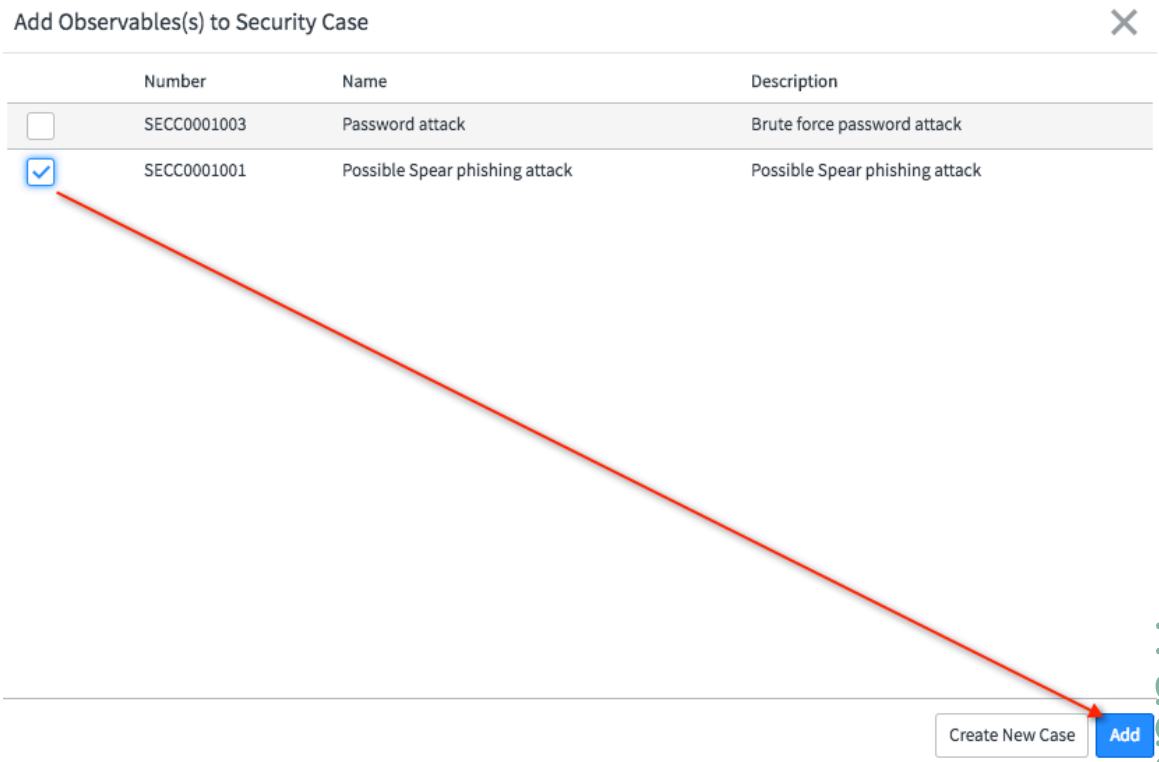
1. Navegue até os artefatos (IoCs ou observáveis) que você deseja adicionar aos casos existentes.
   - Para adicionar IoCs a um ou mais casos, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Indicadores**.
   - Para adicionar observáveis a um ou mais casos, navegue até **Inteligência contra ameaças** > **Repositório LOC** > **Observáveis**.
2. Na lista, selecione os registros de artefato que você deseja adicionar aos casos existentes.

   Nota:
   Se você selecionar vários casos, os IoCs ou observáveis selecionados serão adicionados a cada um dos casos selecionados.

3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.
   A caixa de diálogo **Adicionar ao caso de segurança** é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.
4. Selecione os casos aos quais você deseja adicionar os IoCs ou observáveis selecionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Adicionar**.
   Uma mensagem indica que os registros selecionados foram adicionados aos casos, junto com um link para os casos em Security Case Management.

Criar um observável a partir de um caso

Novos observáveis podem ser criados a partir de casos em Security Case Management.

Antes de Iniciar

Função necessária: sn_ti.case_user

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
   A lista Casos de segurança é aberta.
2. Abra um caso existente ou clique em **Novo** para criar um novo caso.
3. Clique no link relacionado **Artefatos do caso** e clique na guia **Observáveis**.
4. Clique em **Novo** e insira as informações solicitadas.

Campo	Descrição
Valor	[Somente leitura] O número do caso.
Tipo de observável	Insira um nome descritivo para o caso.
Categoria de tipo de observável	Selecione o tipo de caso que está sendo investigado.
Contagem de incidentes	Selecione a importância deste caso (de Crítica a Baixa).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Descoberta	[Somente leitura] A data e a hora em que o caso foi atualizado pela última vez.
Anotações	Uma breve descrição do caso.

5. Clique na guia **Detalhes adicionais do caso**.
6. Preencha os campos, se for o caso.

Campo	Descrição
Criado por	[Somente leitura] O nome do usuário que criou este caso.
Estado	O estado atual do caso. Na criação do caso, o Estado é padronizado como Rascunho.
Lista de Anotações de trabalho	Clique na caixa de seleção para exibir as anotações de trabalho na seção Detalhes adicionais do caso do registro do caso.
Anotações de trabalho	Se necessário, digite uma anotação de trabalho para o caso. Se a **lista Anotações de trabalho** for selecionada, a anotação de trabalho aparecerá na seção Detalhes adicionais do caso do registro do caso.

7. Clique em **Enviar**.
   Conforme necessário, você pode clicar na guia **Artefatos do caso** e adicionar artefatos ao caso.

Executar uma pesquisa de vistas em observáveis em um caso

Você pode pesquisar observáveis usando o recurso Pesquisa de detecções para determinar com que frequência eles ocorrem. Cada ocorrência é considerada uma *vista*. Você pode limitar a pesquisa ao número de vistas em um número selecionado de dias ou em um intervalo de datas.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

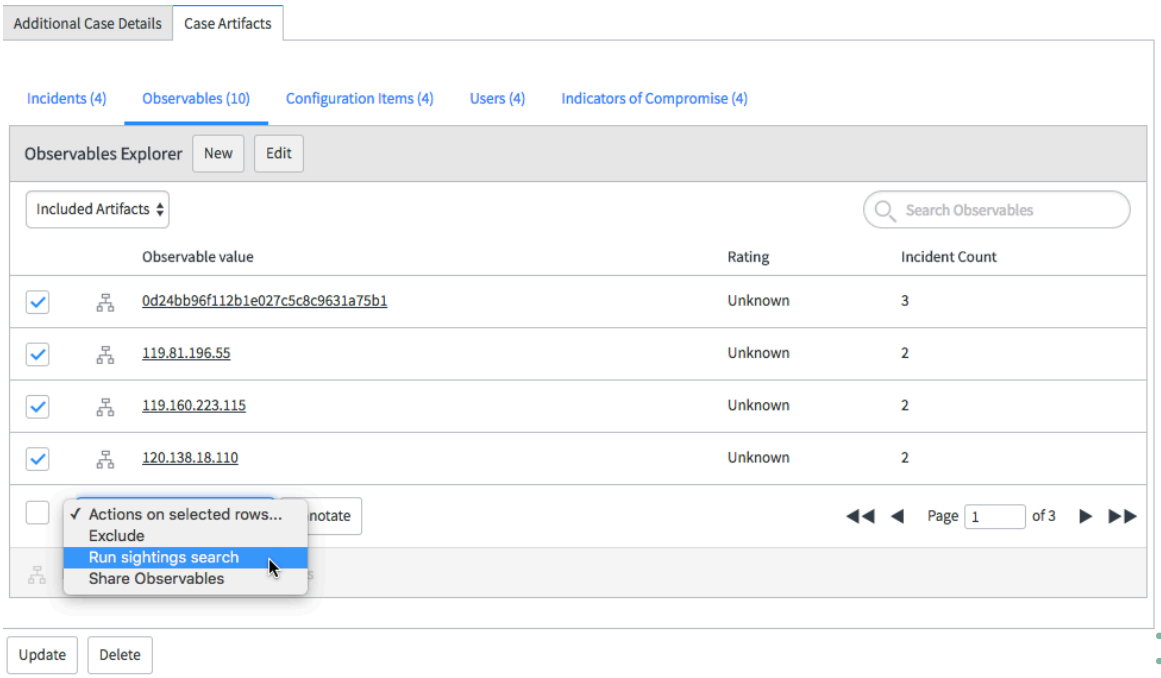
Função necessária: sn_ti.case_user_write

Procedimento

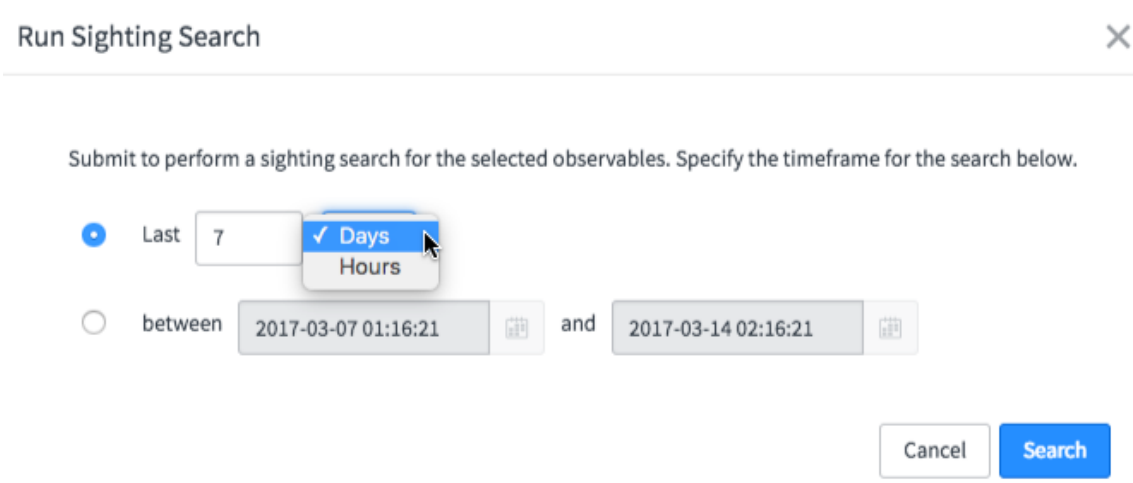
1. Navegar até **Todos** > **Inteligência contra ameaças** > **Gestão de casos** > **Todos os Casos**.
2. Abra o caso que contém observáveis para os quais você deseja executar uma pesquisa de vistas.
3. Clique no link relacionado **Artefatos do caso**.
4. Clique na guia **Observáveis**.
5. Selecione um ou mais observáveis para os quais você deseja pesquisar vistas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Na lista suspensa **Ações nos itens selecionados**, selecione **Executar pesquisa**de vistas.
   A caixa de diálogo **Executar pesquisa** de detecções é exibida.



7. Insira o número de dias ou horas que você deseja pesquisar vistas dos observáveis selecionados ou selecione um intervalo de datas.
8. Clique em **Pesquisar**.

Incidentes de segurança em casos

Em Security Incident Response, você pode criar casos a partir de incidentes de segurança, ICs e usuários afetados, bem como adicionar esses artefatos a casos existentes.

Criar um caso a partir de incidentes de segurança

Em Security Incident Response, você pode criar casos a partir de incidentes de segurança. Depois que os incidentes de segurança forem usados para criar um novo caso, você poderá usar Security Case Management para analisar os dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

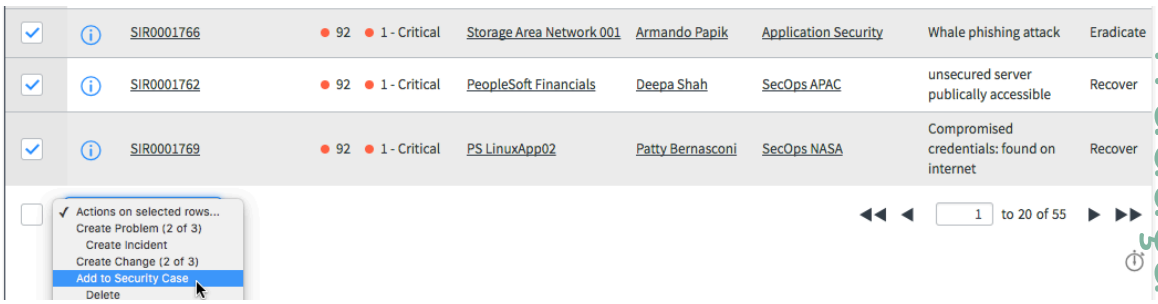
Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

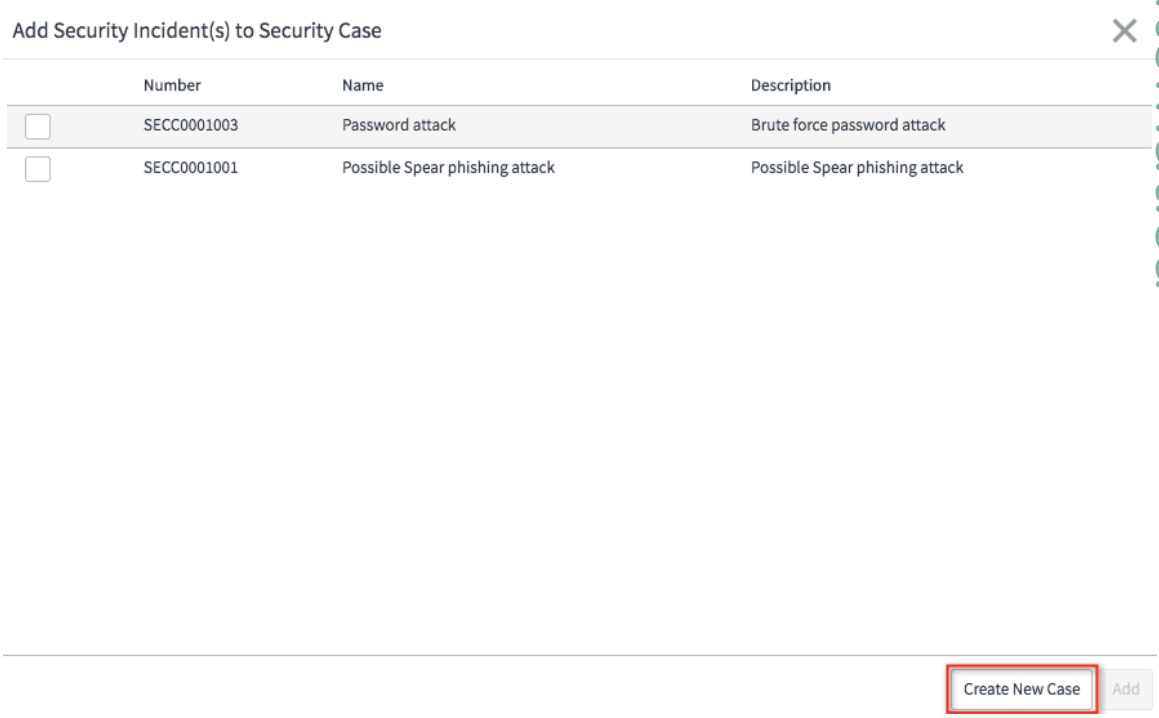
Você precisa navegar até os incidentes de segurança que deseja usar para criar casos.

Procedimento

1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar incidentes em aberto**.
   A lista de Incidentes de segurança é aberta. Na lista, você pode criar um novo caso a partir de um ou mais incidentes de segurança ou pode selecionar um incidente de segurança específico e criar um novo caso a partir do formulário.
2. Para criar um caso na lista, selecione os artefatos que você deseja adicionar a um novo caso.
3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.



A caixa de diálogo **Adicionar ao caso de segurança** é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.



4. Clique **em Criar novo caso**.
5. Preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome de Caso	Insira um nome para este caso.
Descrição	Insira uma descrição que seja valiosa para o analista de caso.

6. Clique em **Enviar**.
   Uma mensagem na parte superior da lista indica que um novo caso foi criado, junto com um link para o caso em Security Case Management.
7. Clique no link para exibir o novo caso.

Adicionar incidentes de segurança a um caso existente

Você pode adicionar incidentes de segurança a um ou mais casos existentes. Depois que os incidentes de segurança forem adicionados aos casos, você poderá usar Security Case Management para analisar os dados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

Você precisa navegar até os incidentes de segurança que deseja adicionar aos casos existentes.

Procedimento

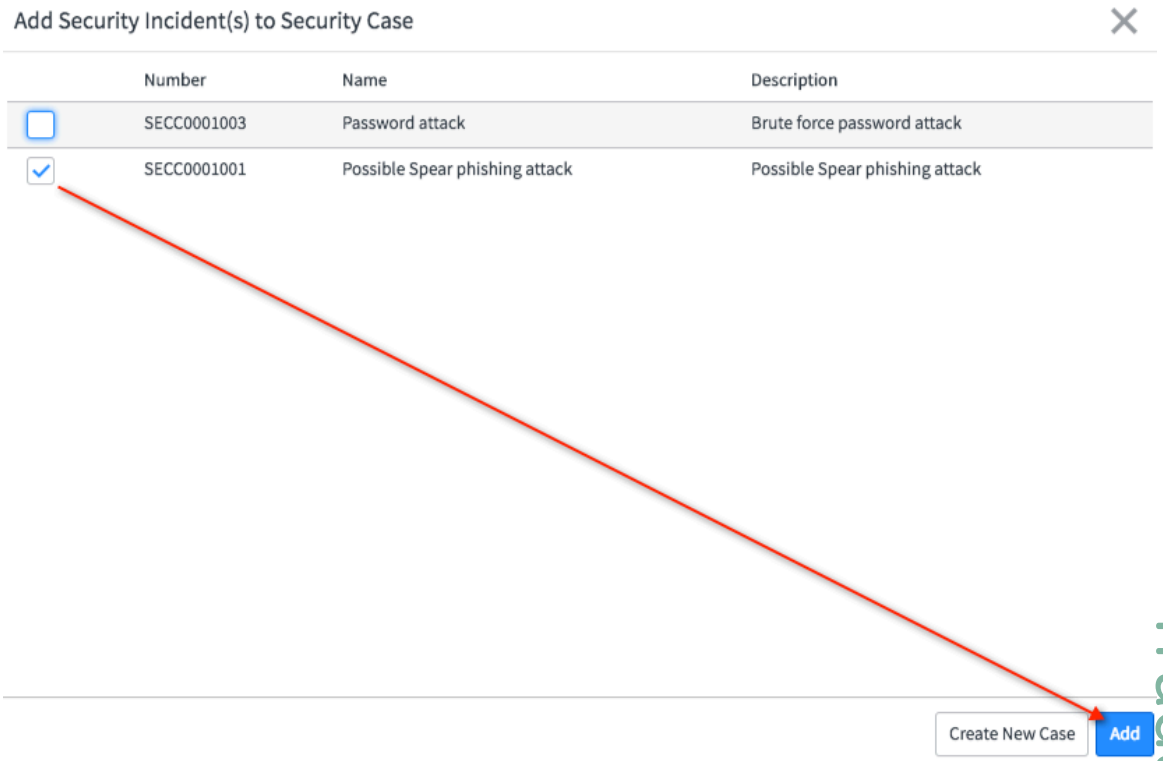
1. Navegar até **Todos** > **Incidente de segurança** > **Incidentes** > **Mostrar incidentes em aberto**.
   A lista de Incidentes de segurança é aberta.
2. Na lista, selecione um ou mais incidentes de segurança que você deseja adicionar aos casos existentes.

   Nota:
   Se você selecionar vários incidentes de segurança, os incidentes de segurança selecionados serão adicionados a cada um dos casos selecionados.

3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.
   A caixa de diálogo **Adicionar ao caso de segurança** é aberta e exibe os casos atribuídos a você.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Selecione os casos aos quais você deseja adicionar os incidentes de segurança selecionados.
5. Clique em **Adicionar**.
   Uma mensagem indica que os registros selecionados foram adicionados aos casos, junto com um link para os casos em Security Case Management.

Itens de configuração em casos

Você pode criar um novo caso a partir de um ou mais itens de configuração (IC) na tabela Item de configuração [cmdb_ci]. Você também pode adicionar ICs a casos existentes.

Criar um caso a partir de ICs

Você pode criar um caso de segurança a partir de itens de configuração na tabela Item de configuração [cmdb_ci]. Depois que os ICs forem usados para criar um novo caso, você poderá usar Security Case Management para analisar os dados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

Você precisa navegar até os itens de configuração que deseja usar para criar um caso.

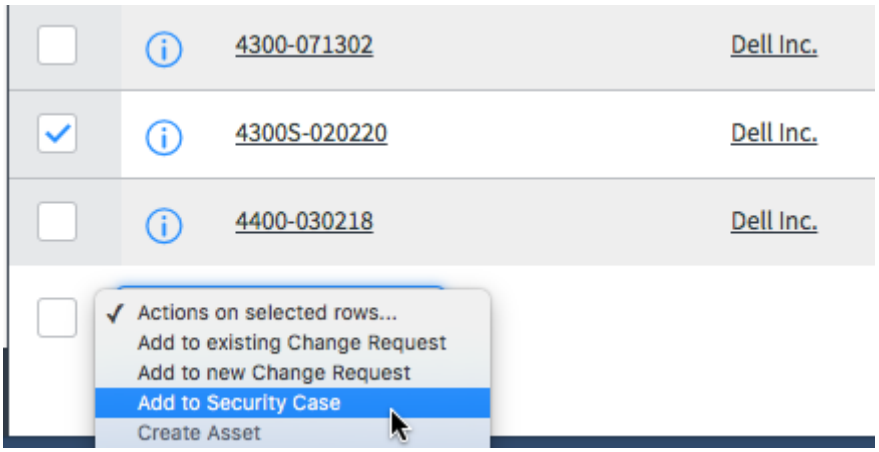
Procedimento

1. Navegar até **Todos** > **Configuração** > **Itens de Base** > **Computadores** para exibir ICs para computadores.
   A lista do tipo de IC selecionado é aberta. Na lista, você pode criar um novo caso a partir de um ou mais ICs ou pode selecionar um IC específico e criar um novo caso a partir do formulário.
2. Na lista, selecione os ICs que você deseja adicionar a um novo caso.

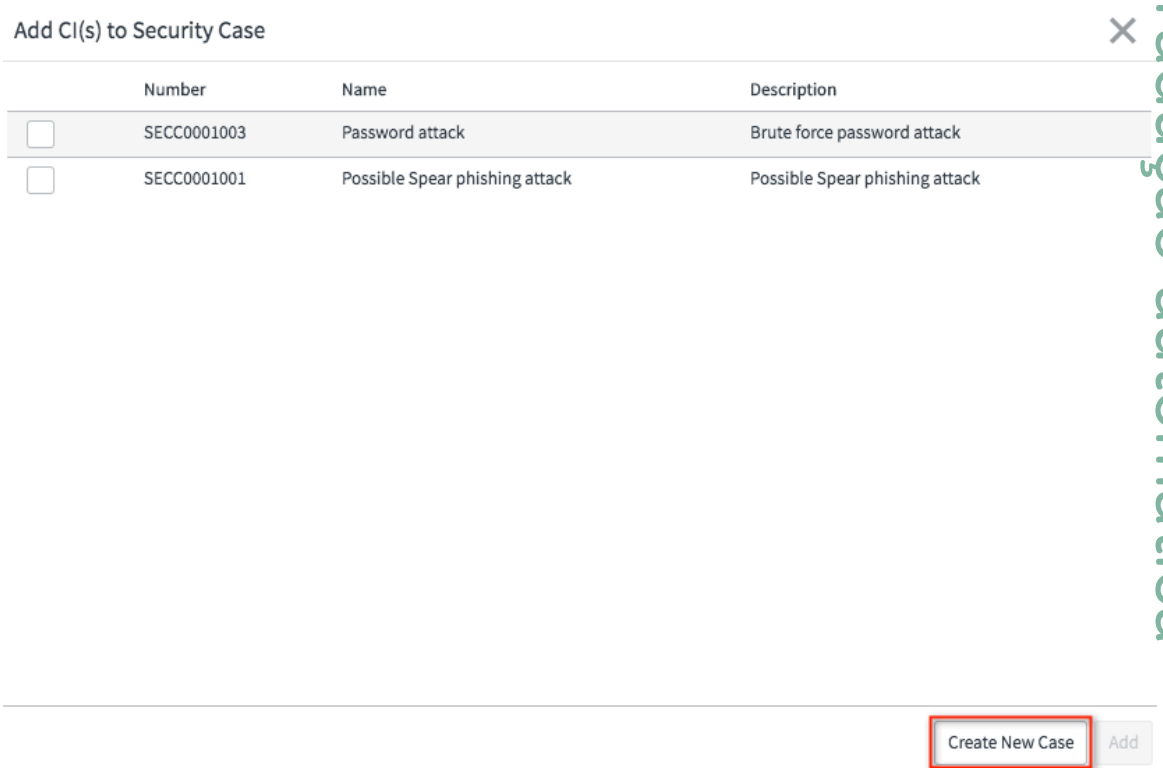
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.



A caixa de diálogo **Adicionar ao caso de segurança** é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.



4. Clique **em Criar novo caso**.
5. Preencha os campos.

Campo	Descrição
Nome de Caso	Insira um nome para este caso.
Descrição	Insira uma descrição que seja valiosa para o analista de caso.

6. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Uma mensagem na parte superior da lista indica que um novo caso foi criado, junto com um link para o caso em Security Case Management.

7. Clique no link para exibir o novo caso.

Adicionar ICs a casos existentes

Você pode adicionar itens de configuração a um ou mais casos existentes. Depois que os ICs forem adicionados aos casos, você poderá usar Security Case Management para analisar os dados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

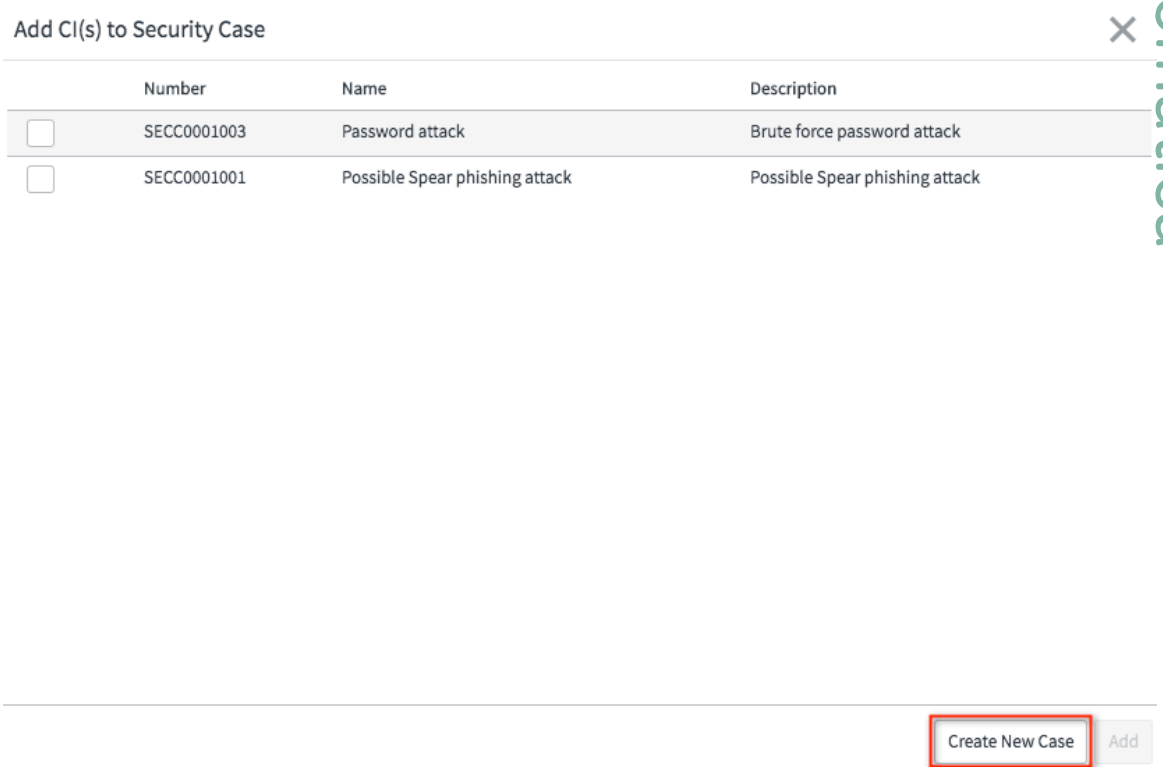
Você precisa navegar até os ICs que deseja adicionar aos casos existentes.

Procedimento

1. Navegar até **Todos** > **Configuração** > **Itens de Base** > **Computadores** para exibir ICs para computadores.
   A lista de ICs selecionados é aberta.
2. Na lista, selecione um ou mais ICs que você deseja adicionar aos casos existentes.

   Nota:
   Se você selecionar vários ICs, os ICs selecionados serão adicionados a cada um dos casos selecionados.

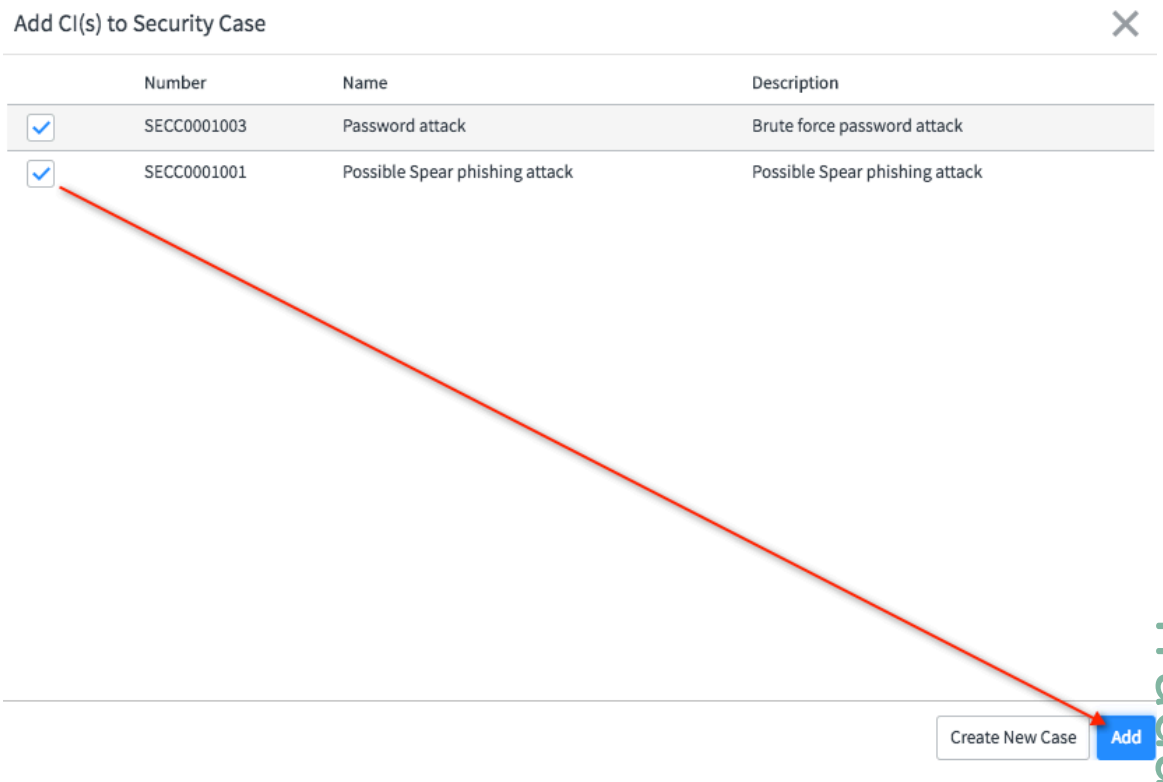
3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.
   A caixa de diálogo **Adicionar ao caso de segurança** é aberta e exibe os casos atribuídos a você.



4. Selecione os casos aos quais você deseja adicionar os ICs selecionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Adicionar**.
   Uma mensagem indica que os registros selecionados foram adicionados aos casos, junto com um link para os casos em Security Case Management.

Usuários afetados nos casos

Você pode criar um novo caso a partir de um ou mais usuários afetados na tabela Usuário [sys_user]. Você também pode adicionar usuários a casos existentes.

Criar um caso a partir de usuários afetados

Você pode criar um caso de segurança de usuários afetados na tabela Usuário [sys_user]. Depois que os usuários afetados forem usados para criar um novo caso, você poderá usar Security Case Management para analisar os dados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

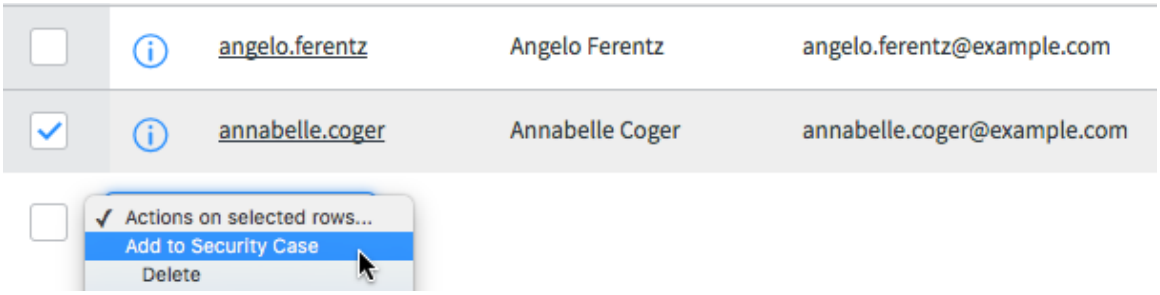
Você precisa navegar até os usuários que deseja usar para criar um caso.

Procedimento

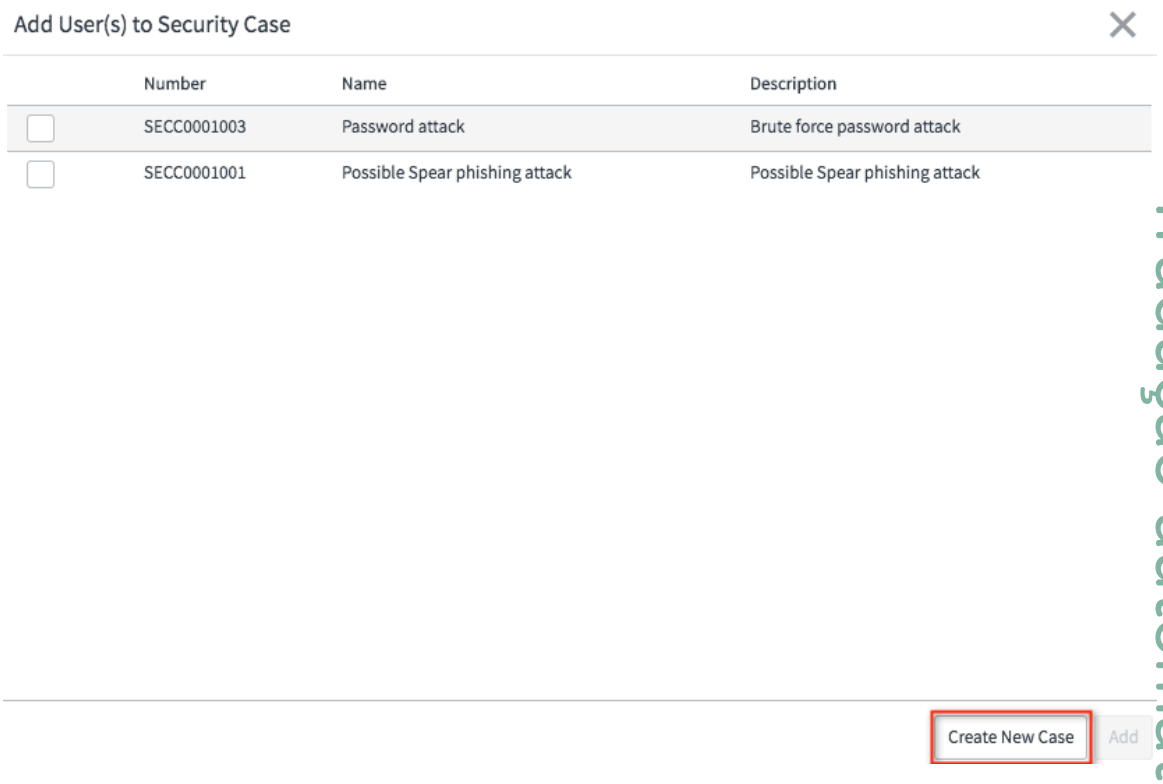
1. Navegar até **Todos** > **Administração de usuários** > **Usuários**.
   A lista dos usuários selecionados é aberta. Na lista, você pode criar um novo caso a partir de um ou mais registros de usuário ou pode selecionar um registro de usuário específico e criar um novo caso a partir do formulário.
2. Na lista, selecione os usuários que você deseja adicionar a um novo caso.
3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A caixa de diálogo **Adicionar ao caso de segurança** é aberta. Se você já tiver casos atribuídos a você, eles serão exibidos na lista.



4. Clique **em Criar novo caso**.
5. Preencha os campos.

Campo	Descrição
Nome de Caso	Insira um nome para este caso.
Descrição	Insira uma descrição que seja valiosa para o analista de caso.

6. Clique em **Enviar**.
   Uma mensagem na parte superior da lista indica que um novo caso foi criado, junto com um link para o caso em Security Case Management.
7. Clique no link para exibir o novo caso.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Adicionar usuários afetados a casos existentes

Você pode adicionar usuários afetados a um ou mais casos existentes. Depois que os registros do usuário forem adicionados aos casos, você poderá usar Security Case Management para analisar os dados.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

Função necessária: sn_ti.case_user_write

Por Que e Quando Desempenhar Esta Tarefa

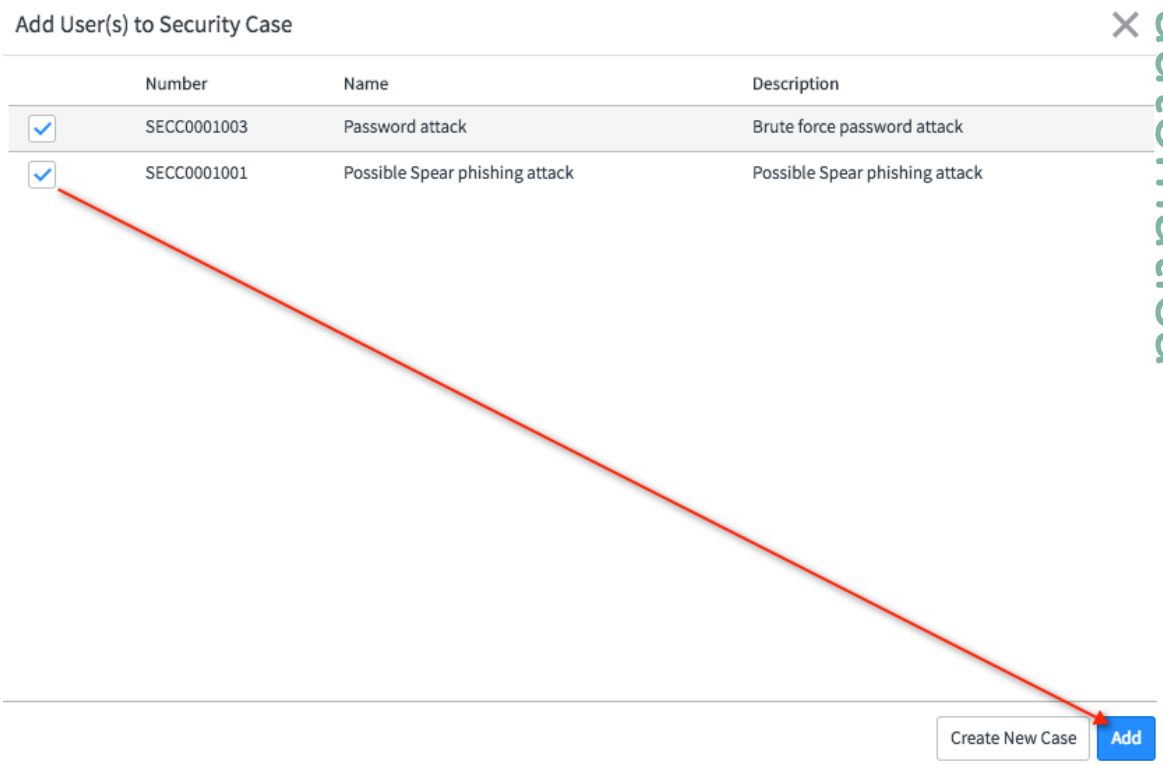
Você precisa navegar até os registros de usuário que deseja adicionar aos casos existentes.

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Usuários**.
   A lista de registros do usuário é aberta.
2. Na lista, selecione um ou mais usuários que você deseja adicionar aos casos existentes.

   Nota:
   Se você selecionar vários usuários, os registros do usuário selecionados serão adicionados a cada um dos casos selecionados.

3. Na lista suspensa **Ações em itens selecionados**, selecione **Adicionar ao caso de segurança**.
   A caixa de diálogo **Adicionar ao caso de segurança** é aberta e exibe os casos atribuídos a você.



4. Selecione os casos aos quais você deseja adicionar os usuários selecionados.
5. Clique em **Adicionar**.
   Uma mensagem indica que os registros selecionados foram adicionados aos casos, junto com um link para os casos em Security Case Management.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Análise de artefato de segurança

Depois de criar casos, usando Security Case Managementou de artefatos como IoCs, observáveis, incidentes de segurança e assim por diante, você pode continuar a adicionar artefatos para ajudar na análise das ameaças identificadas.

Detalhes relacionados aos artefatos de caso

Conforme você adiciona artefatos a um caso, detalhes adicionais relacionados a cada artefato também podem ser adicionados automaticamente. Por exemplo, se você adicionar um incidente de segurança, ele poderá conter ICs afetados e registros de usuário. Você pode exibir rapidamente os detalhes relacionados a um artefato selecionado sem sair da lista de artefatos.

Exibir detalhes relacionados a um artefato de incidente de segurança

Se o seu caso incluir artefatos de incidente de segurança, você poderá exibir todos os detalhes relacionados contidos em cada incidente de segurança referenciado pelo caso.

Antes de Iniciar

- O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

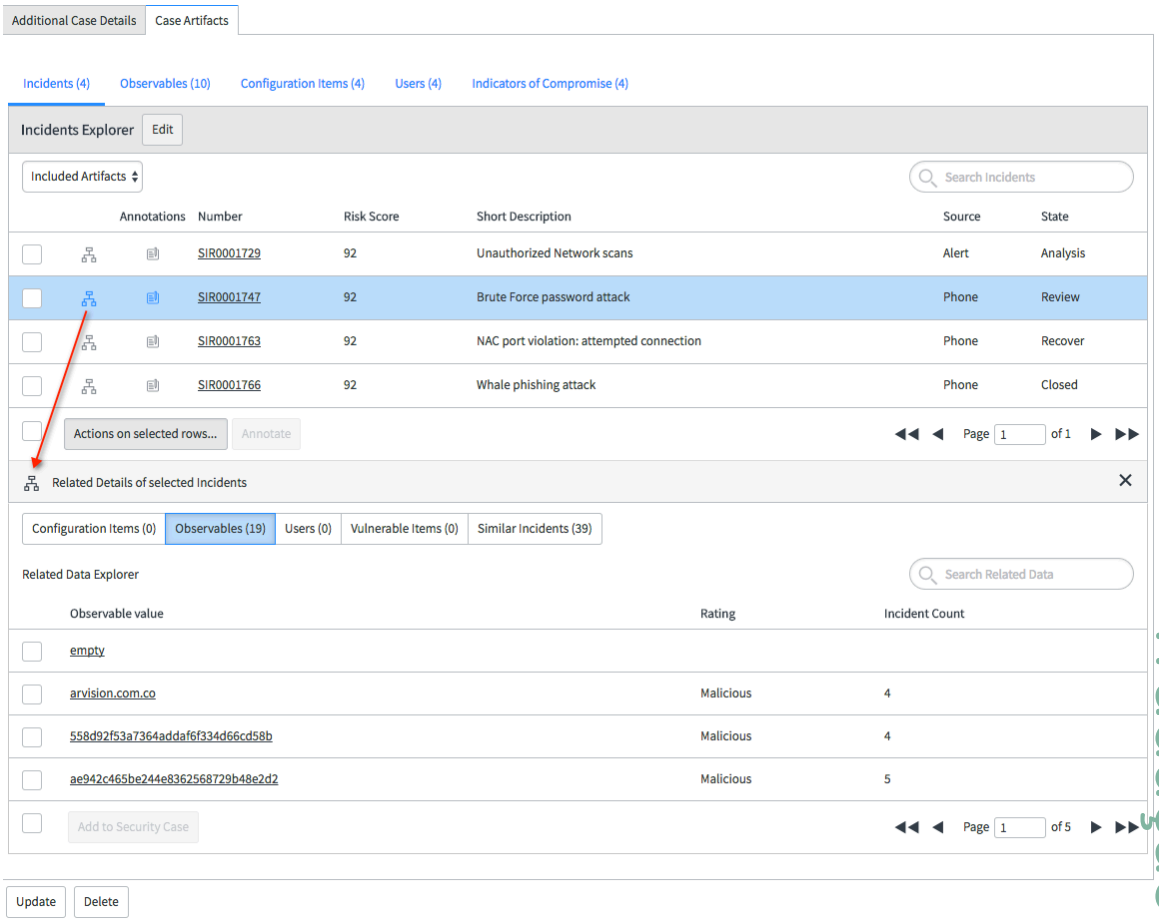
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contenha artefatos de incidente de segurança.
2. Clique na guia **Incidentes**.
3. Clique no ícone Detalhes adicionais do incidente de segurança para o qual você deseja exibir os detalhes relacionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar na guia **Anotação de segurança** para exibir anotações do artefato selecionado.

Exibir detalhes relacionados a um artefato de item de configuração

Se o seu caso incluir artefatos de item de configuração, você poderá exibir todos os detalhes relacionados contidos em cada IC referenciado pelo caso.

Antes de Iniciar

- O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

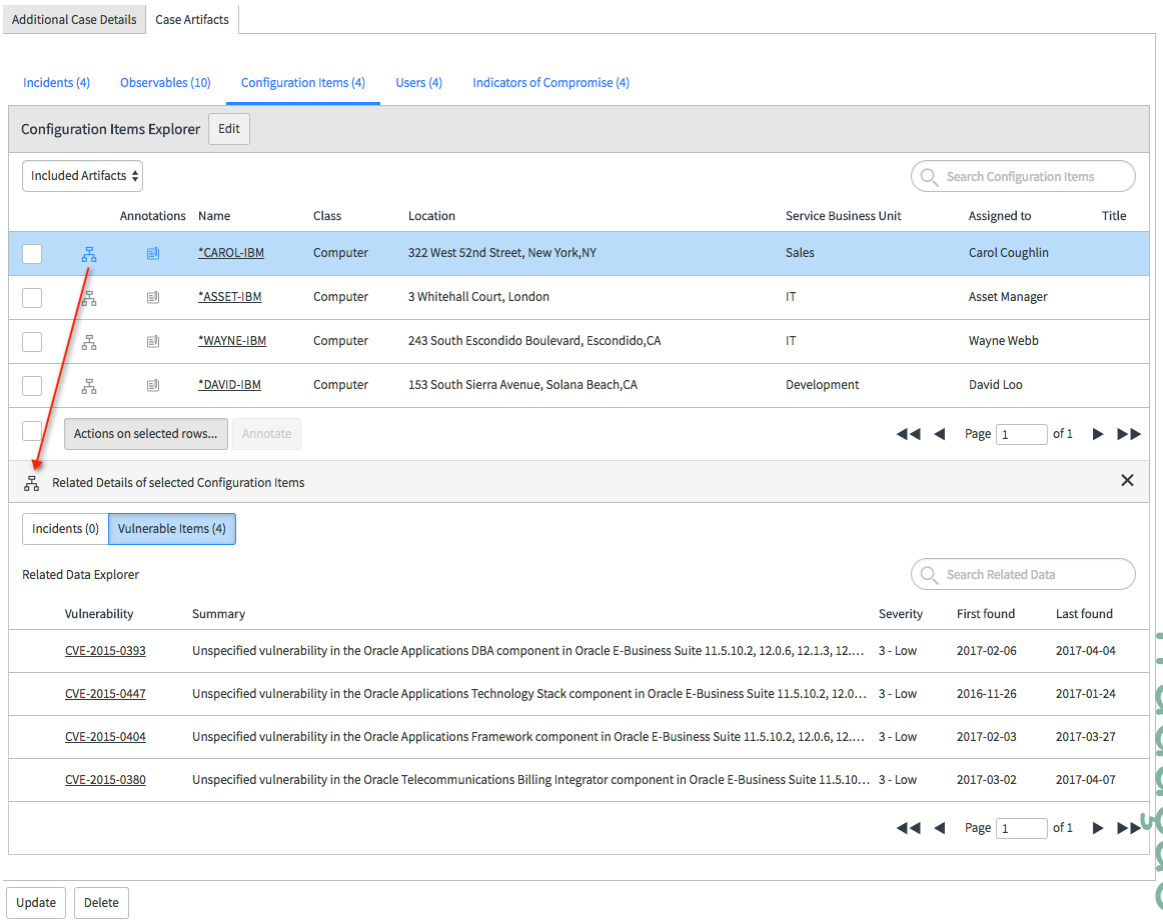
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contenha artefatos de IC.
2. Clique na guia **Itens de configuração**.
3. Clique em Detalhes adicionais para o artefato de IC para o qual você deseja exibir os detalhes relacionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar na guia **Anotação de segurança** para exibir as anotações do artefato selecionado.

Exibir detalhes relacionados a um artefato IoC

Se o seu caso incluir indicadores de artefatos de comprometimento (IoC), você poderá exibir todos os detalhes relacionados contidos em cada IoC referenciado pelo caso.

Antes de Iniciar

- O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

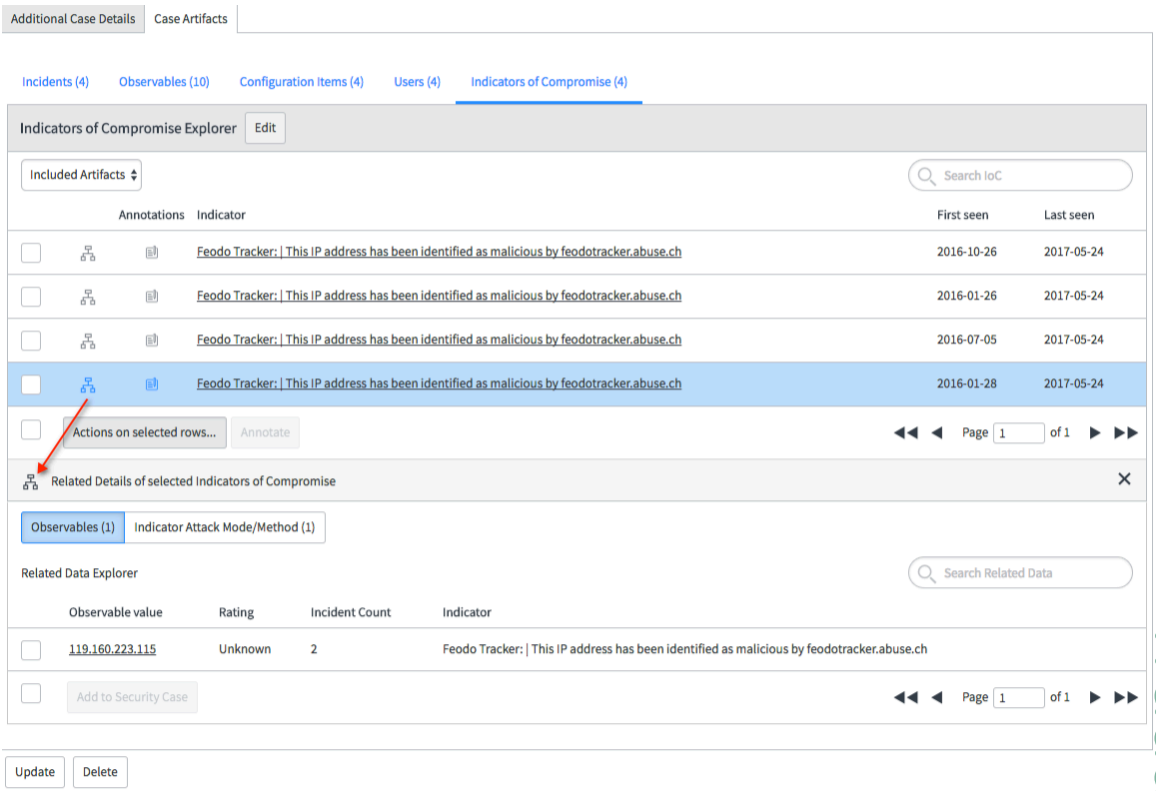
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contenha artefatos IoC.
2. Clique na guia **Indicadores de compromisso**.
3. Clique no ícone Detalhes adicionais do artefato IoC para o qual você deseja exibir os detalhes relacionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar na guia **Anotação de segurança** para exibir anotações do artefato selecionado.

Exibir detalhes relacionados a um artefato de usuário afetado

Se o seu caso incluir artefatos de usuário afetado, você poderá exibir todos os detalhes relacionados contidos em cada usuário afetado referenciado pelo caso.

Antes de Iniciar

- O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

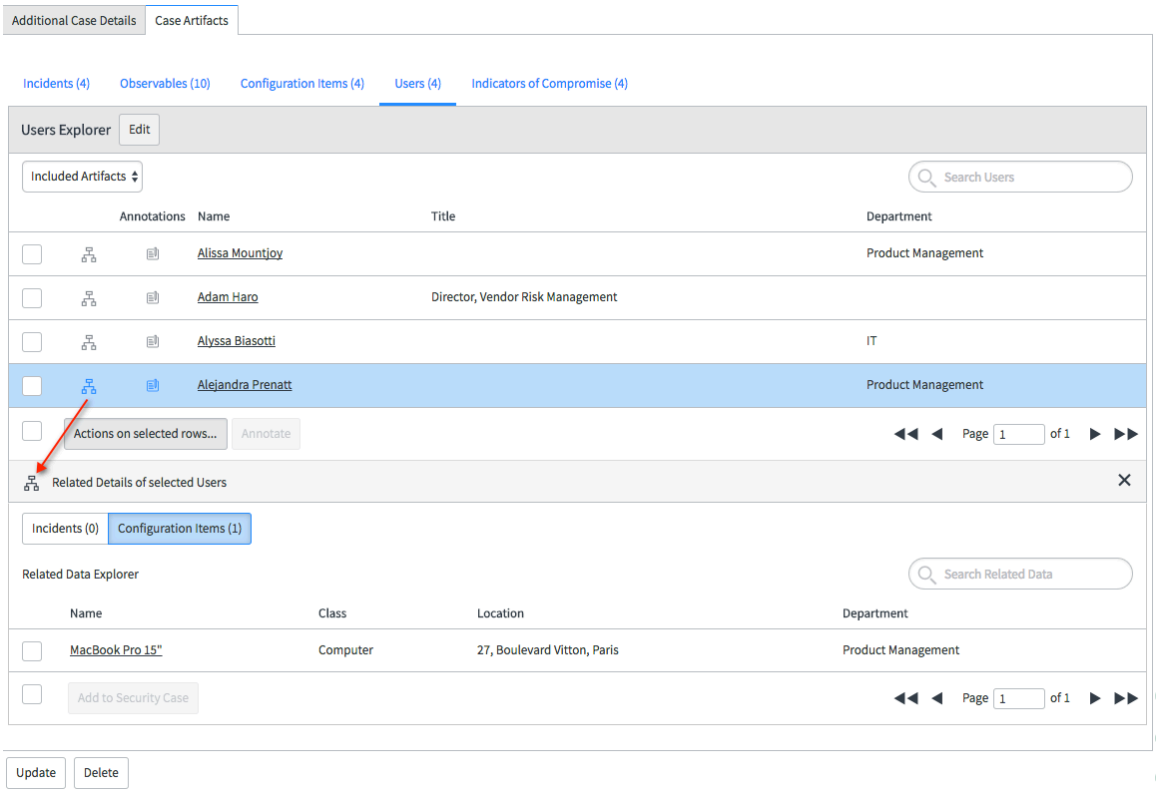
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contenha artefatos do usuário afetados.
2. Clique na guia **Usuários**.
3. Clique em Detalhes relacionados para o artefato do usuário afetado para o qual você deseja exibir os detalhes relacionados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar na guia **Anotação de segurança** para exibir anotações do artefato selecionado.

Exibir detalhes relacionados a um artefato observável

Se o seu caso incluir artefatos observáveis, você poderá exibir todos os detalhes relacionados contidos em cada observável referenciado pelo caso.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

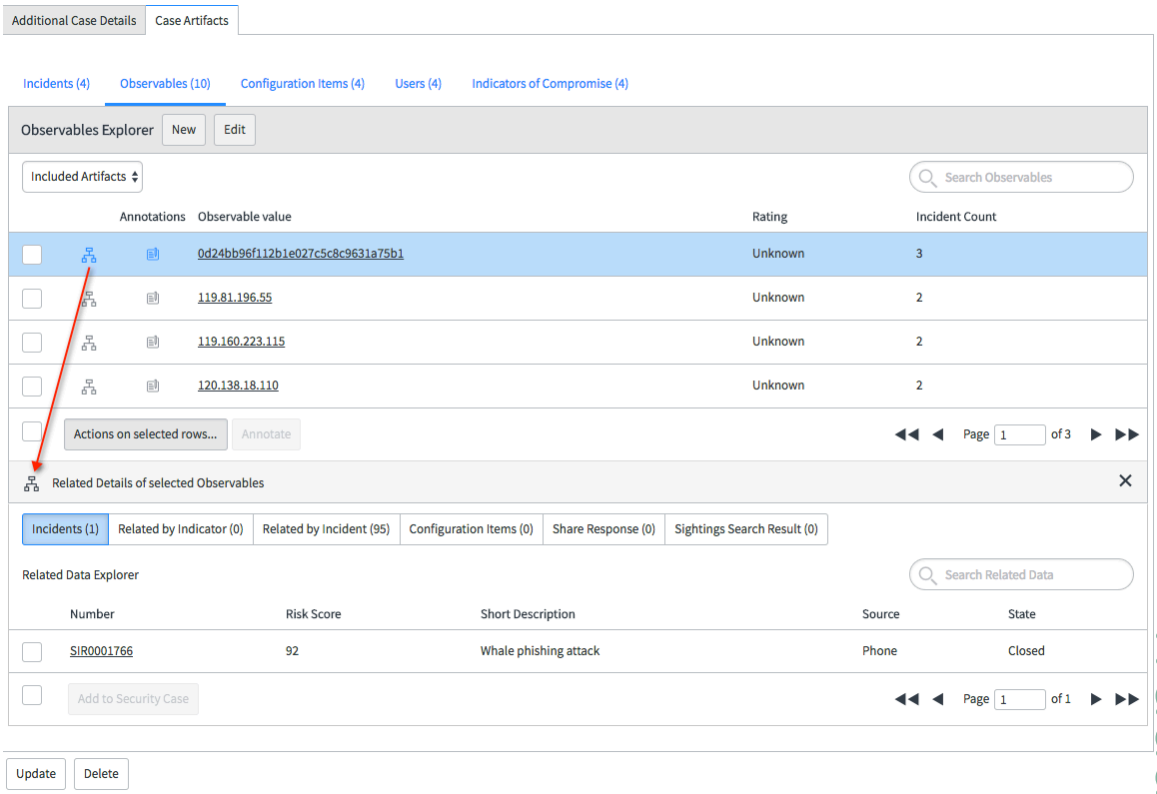
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contenha artefatos observáveis.
2. Clique na guia **Observáveis**.
3. Clique no ícone Detalhes adicionais do artefato observável cujos detalhes relacionados você deseja exibir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Clique em qualquer uma das guias para exibir tipos específicos de detalhes do artefato selecionado.
5. Você também pode clicar na guia **Anotação de segurança** para exibir anotações do artefato selecionado.

Exclusão e inclusão de artefato de segurança

As listas de artefatos de suporte atribuídos a um caso podem às vezes ficar longas e pode haver instâncias em que você deseja remover artefatos específicos de uma lista. Em vez de remover permanentemente os artefatos, você pode excluí-los da lista e, conforme necessário, retorná-los à lista posteriormente.

Excluir artefatos de segurança de um caso

Você pode remover artefatos das listas de artefatos de suporte. Eles não são removidos permanentemente e podem ser retornados ao caso conforme necessário.

Antes de Iniciar

- O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

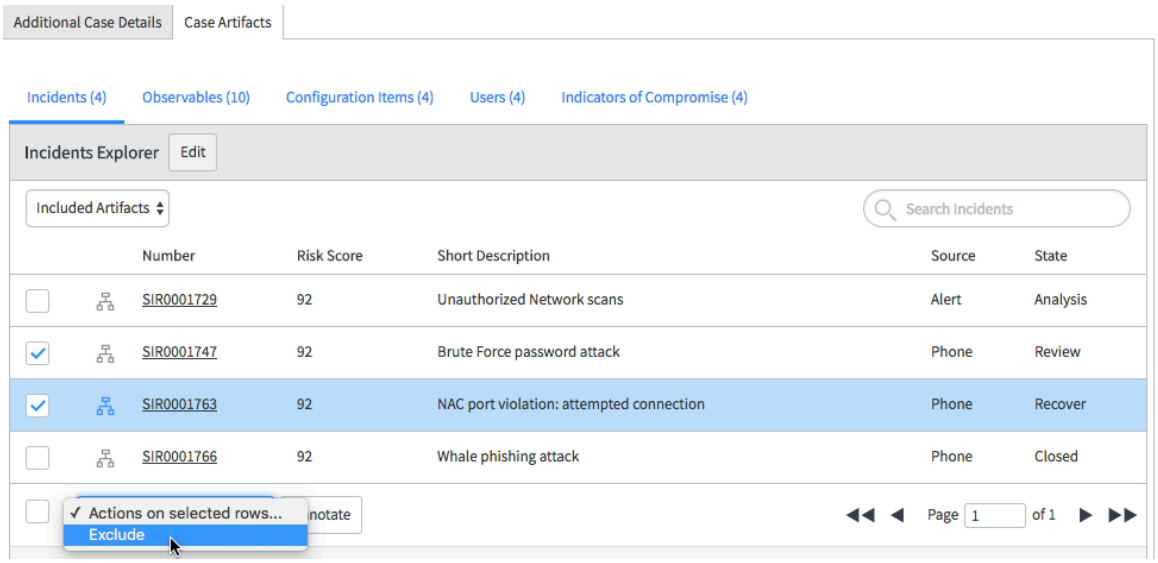
Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contenha artefatos que você deseja excluir de uma lista.
2. Clique na lista relacionada **Artefatos do caso**.
3. Clique na guia associada aos artefatos que você deseja excluir.
   Por exemplo, clique em **Incidentes** para excluir incidentes de segurança da lista.
4. Selecione um ou mais registros de artefato que você deseja excluir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Na lista suspensa **Ações em itens selecionados**, selecione **Excluir**.
6. Clique em **Excluir** na caixa de confirmação.
   Os artefatos selecionados são removidos da lista.

Retornar artefatos de segurança excluídos para um caso

Depois de excluir artefatos de uma lista em um caso, você pode retorná-los ao caso em que pode continuar trabalhando neles.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

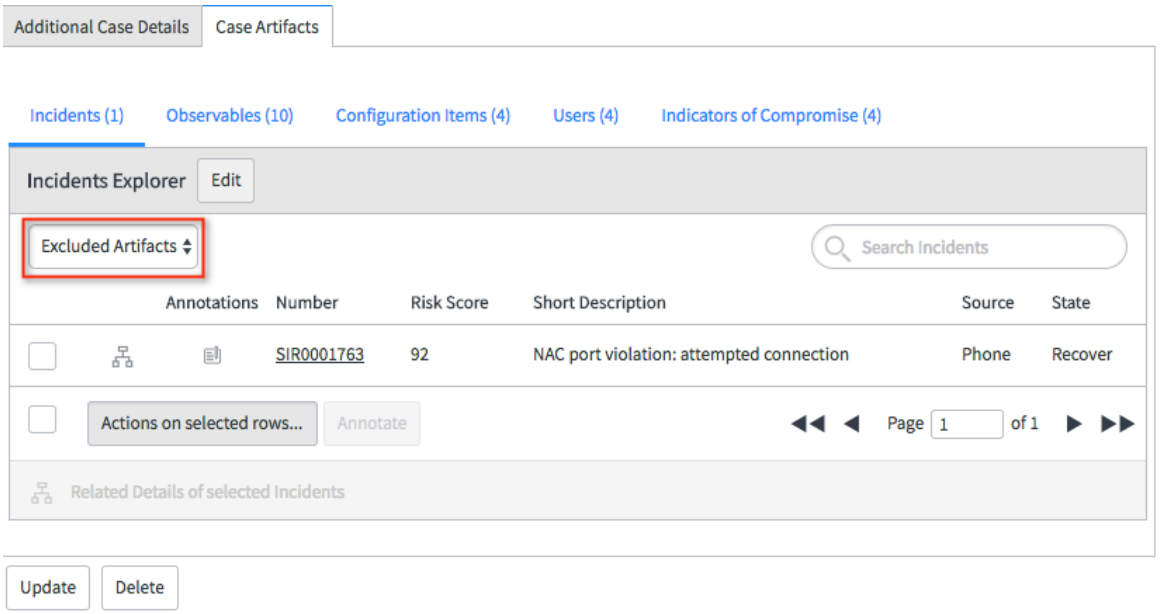
Função necessária: sn_ti.case_user_write

Procedimento

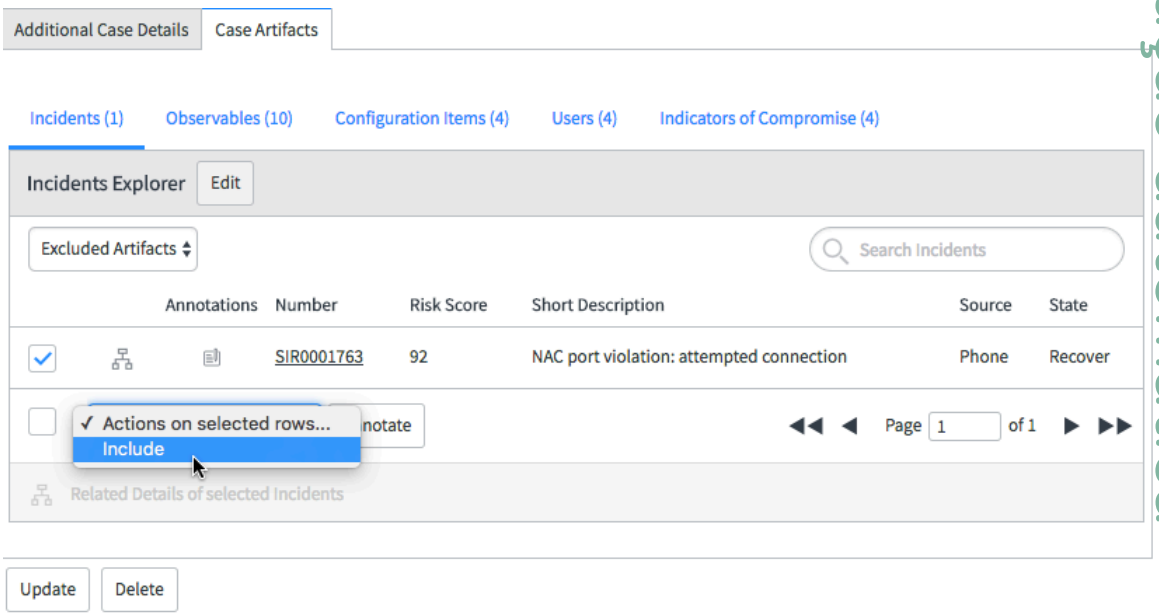
1. Abra um caso que contenha artefatos que você excluiu anteriormente de uma lista que você deseja retornar à lista.
2. Clique na lista relacionada **Artefatos do caso**.
3. Clique na guia associada aos artefatos que você deseja retornar à lista.
4. Clique na lista suspensa Filtro de artefato e selecione **Artefatos excluídos**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Selecione um ou mais registros de artefato que você deseja retornar à lista Incluir.
6. Na lista suspensa **Ações em itens selecionados**, selecione **Incluir**.



7. Clique em **Incluir** na caixa de confirmação.
   Os artefatos selecionados são removidos da lista de artefatos excluídos e retornados à lista de artefatos incluídos no caso.

Anotar artefatos de segurança

Ao analisar um caso, você pode adicionar anotações a qualquer artefato.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

Função necessária:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

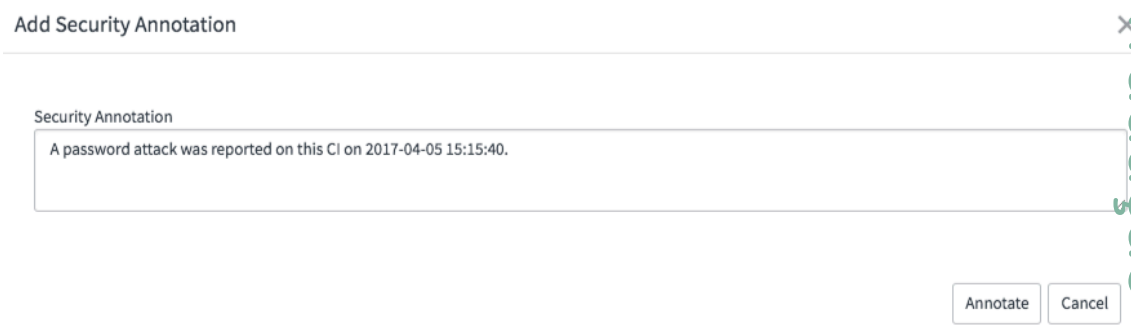
- sn_ti.case_user_write para adicionar anotações
- sn_ti.case_user_read para exibir anotações

Procedimento

1. Abra um caso que contenha artefatos que você deseja anotar.
2. Clique na lista relacionada **Artefatos do caso**.
3. Clique na guia associada aos artefatos que você deseja anotar.
   Por exemplo, clique em **Indicadores de compromisso** para adicionar anotações aos IoCs.
4. Para adicionar uma anotação a um ou mais artefatos, execute as seguintes etapas:

   a. Selecione os artefatos aos quais você deseja adicionar uma anotação.

   b. Clique **em Anotar**.

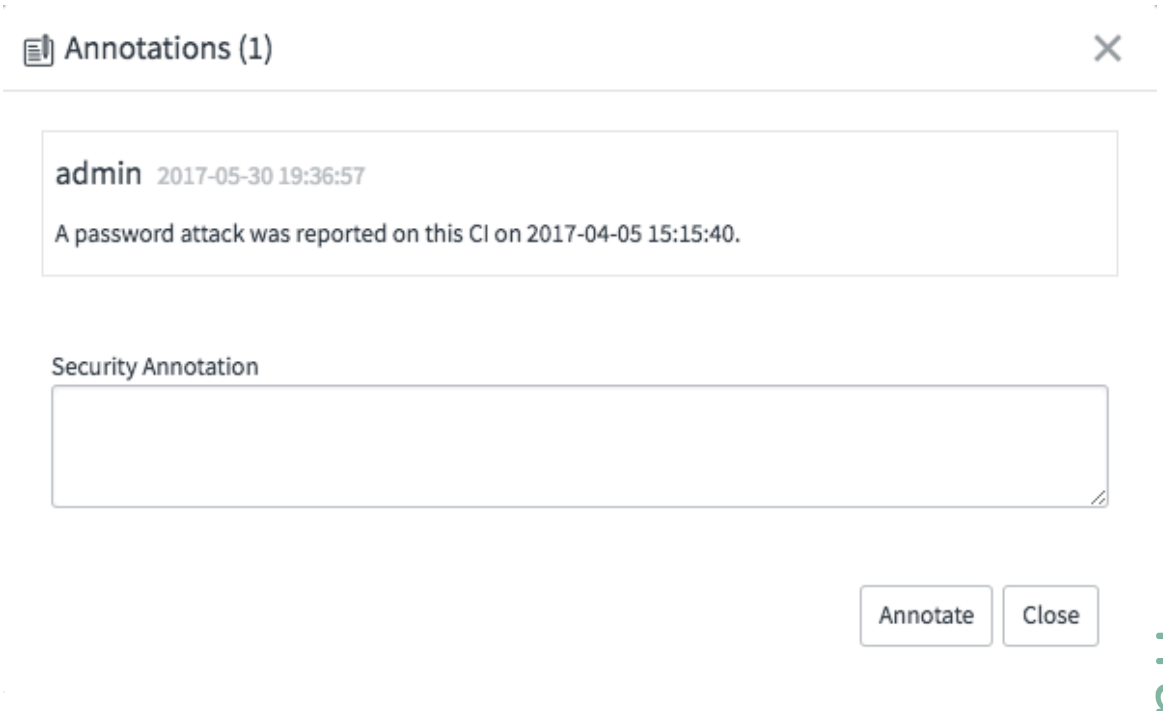


   c. Digite a anotação e clique em **Anotar**.
   A anotação é adicionada aos artefatos selecionados.

5. Para exibir anotações de um artefato, clique no ícone Exibir anotações ( ).
   As anotações existentes aparecem na caixa de diálogo Anotações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



6. Você também pode inserir uma nova anotação para o artefato na caixa **Anotação de segurança** e clicar em **Anotar**.

Pesquisar artefatos de segurança

Você pode executar uma pesquisa de palavra-chave em qualquer lista de artefatos de segurança.

Antes de Iniciar

O plug-in Inteligência contra ameaças deve ser ativado para usar Security Case Management.

Função necessária: sn_ti.case_user_write

Procedimento

1. Abra um caso que contenha artefatos de segurança.
2. Clique na guia dos artefatos de segurança nos quais você deseja executar uma pesquisa de palavra-chave.
3. Na caixa de **pesquisa de palavra** -chave, comece a digitar o nome do artefato que você deseja localizar. Quando artefatos que correspondem à sua entrada forem encontrados, eles serão exibidos.

Security Operations funcionalidade comum

Sempre que qualquer um dos plug-ins das aplicações [Security Operations principais (Security Incident Response, Vulnerability Response, Inteligência contra ameaçasou Configuration Compliance) for ativado, o plug-in Security Support Common será ativado. Este plug-in carrega vários módulos que fornecem funcionalidade comum a todas as aplicações Security Operations.

Nota:
Somente usuários com [sn_sec_cmn.admin] podem exibir e usar o módulo Security Operations. Esta função é herdada quando uma função administrativa é atribuída a você em qualquer uma das aplicações Security Operations.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulos do Security Operations

Recurso	Descrição
Referência do Security Operations Integrations, Integrações do Inteligência contra ameaças, Integrações do Vulnerability Response	Várias integrações estão incluídas com as aplicações [Security Operations (Security Incident Response, Inteligência contra ameaçase Vulnerability Response). Esta seção fornece instruções para ativar os plug-ins e configurar ServiceNow e integrações de terceiros. Também estão incluídas algumas diretrizes básicas para desenvolver suas próprias integrações, bem como detalhes sobre integrações específicas incluídas no sistema básico.
Security Operations processamento de e-mail	Você pode configurar a integração de informações de sistemas de detecção externos, fornecer granularidade no processamento de registros de operações de segurança, lidar com e-mails incompatíveis e impedir a duplicação de registros usando Processamento de E-mails.
Grupos	• **Grupos de Filtros** Crie e use grupos de filtros para localizar registros de qualquer tabela em sua instância. Por exemplo, você pode criar um grupo de todos os computadores do mesmo fabricante. Você também pode filtrar itens de configuração (ICs) que tenham vulnerabilidades semelhantes ou que se enquadrem em um intervalo de endereços IP de sub-rede específico. • **Escalações** Você pode criar um caminho de escalação para incidentes de segurança em caso de problemas que exigem mais atenção ou experiência. Quando um grupo de escalação existe, um botão aparece em qualquer incidente de segurança nesse grupo.
Marcadores de Segurança	**Marcadores**: as regras de marcador de segurança fornecem filtragem para o acesso ao marcador de segurança.
Workflows	• **Exibir Fluxos de Trabalho de Segurança** Você pode exibir os diversos fluxos de trabalho incluídos nas aplicações Security Operations. Você pode criar fluxos de trabalho a partir de modelos e no Editor de fluxo de trabalho. • **Gatilhos de Fluxo de Trabalho** Security Operations Os gatilhos de fluxo de trabalho contêm uma condição em uma tabela.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recurso	Descrição
	Todos os fluxos de trabalho anexados ao registro do gatilho de fluxo de trabalho são executados quando a condição é atendida.
Utilitários	• **Mapeamento de Dados de Aprimoramento** Mapeamento de Dados de Aprimoramento transforma dados de arquivos XML, JSON ou Propriedades em registros ServiceNow. Security Operations fluxos de trabalho usam mapas de dados de aprimoramento e fornecem dados de saída para incidentes de segurança. • **Transformações de Valores de campos** Transforma valores de campo exclusivos do cliente em valores de campo reconhecidos por análise de e-mail Security Operations, aprimoramento de dados ou tabelas usando mapas de campo. Oferece suporte a campos de escolha, faz referência e alinha dados externos na terminologia e no formato padrão do seu novo registro. • **Mapeamento de Campos** TabelasSecurity Operations podem ser mapeadas de e para outras tabelas, vinculando um incidente de segurança a um caso de atendimento ao cliente ou um problema a outras partes do sistema Security Operations. Por exemplo, você pode integrar um plug-in a uma tarefa Security Incident Response. • **Orquestração sob Demanda** Durante a análise de Security Incident Response, um analista de segurança pode executar uma tarefa orientada por um fluxo de trabalho de incidente de segurança. Por exemplo, execute um despejo de processo em um IC específico. Isso pode ser realizado com a orquestração sob demanda. • **Grupos de Sistemas Operacionais** N/D. • **Registro da aplicação SecOps** N/D.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Recurso	Descrição
CMDB	**Regras de Identificador de**IC: identificadores de IC são regras usadas para pesquisar um item de configuração (IC) no CMDB que contém informações correspondentes de uma integração de terceiros. Essas regras definem os campos que contêm dados correspondentes e a ordem de precedência pela qual eles são avaliados. O valor de **Ordem** mais baixo é avaliado primeiro.

Criar e definir grupos de filtros no Security Operations

Crie e use grupos de filtros para localizar registros de qualquer tabela em sua instância. Por exemplo, você pode criar um grupo de todos os computadores do mesmo fabricante. Você também pode filtrar itens de configuração (ICs) que tenham vulnerabilidades semelhantes ou que se enquadrem em um intervalo de endereços IP de sub-rede específico.

Antes de Iniciar

Função necessária: sn_sec_cmn.write

Por Que e Quando Desempenhar Esta Tarefa

Os grupos de filtros podem conter registros atualizados dinamicamente, uma série de registros estáticos que não são filtrados usando condições ou uma combinação de registros estáticos e atualizados dinamicamente. Alguns grupos de filtros estão incluídos no sistema de base, por exemplo, exclusões de IC.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Grupos** > **Grupos de Filtros**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Nome	O nome do grupo de filtros.
Ativo	Caixa para ativar o grupo.
Descrição	Descrição do grupo de filtros.
Endereço IP da Rede	O endereço IP da rede que contém os endereços IP dos ICs que você deseja adicionar ao grupo. Este campo aparecerá somente se você selecionou Item de configuração [cmdb_ci] ou uma tabela que estende o item de configuração no campo **Tabela**.
Máscara de sub-rede	A sub-rede que contém os endereços IP dos ICs que você deseja adicionar ao grupo, por exemplo, 255.255.255.0. Este campo aparecerá somente se você selecionou Item de configuração [cmdb_ci] ou uma tabela que estende o item de configuração no campo **Tabela**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tabela	A tabela a ser filtrada.
Condição	Use o construtor de condição para definir os critérios a serem filtrados.

4. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
   Uma guia **Condições avançadas** é exibida.

   Mais guias aparecem dependendo do tipo de tabela que você especificou no campo **Tabela**, da seguinte forma:

Tabela	Guias exibidas
Item de configuração [cmdb_ci] ou uma tabela que estende a tabela do item de configuração	**ICs adicionados manualmente** e **ICs correspondentes**
Tarefa [task] ou uma tabela que estende a tabela de tarefas	**Tarefas adicionadas manualmente** e **tarefas correspondentes**
Uma tabela não relacionada a um IC ou tarefa	**Registro Adicionado Manualmente**

5. Para definir mais condições para o seu grupo de filtros:

   a. Clique **em Condições avançadas**.

   b. Insira uma nova linha na lista integrada **Condições adicionais do grupo de filtros** para selecionar outros grupos de filtros pré-criados que você deseja combinar com o grupo de filtros que está sendo atualizado.
   Se você quiser que o grupo de filtros selecionado filtre registros com base em um campo de referência, um campo mapeado será selecionado automaticamente quando o registro atual for salvo.

   Nota:
   O valor do **campo mapeado** não pode ser editado na lista integrada **Condições adicionais do grupo de filtros**. Para mudar o campo, clique no ícone de informações para abrir o registro.

   c. Clique em **Atualizar**.

6. Para adicionar manualmente mais ICs ou tarefas ao grupo de filtros:

   a. Clique na guia **ICs adicionadosmanualmente ou Tarefas adicionadas manualmente**.

   b. Clique em **Editar**.

   c. Selecione os ICs ou tarefas que você deseja adicionar.

   d. Clique em **Salvar**.

7. Para exibir os ICs ou tarefas que correspondem aos seus critérios de seleção:

   a. Clique na guia **ICs** correspondentes ou **Tarefas correspondentes**.

   b. Se você alterou os critérios, atualize a lista clicando com o botão direito do mouse no cabeçalho do formulário e selecionando **Atualizar lista**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Transformação de dados compartilhados

Os plug-ins Security Incident Response, Vulnerability Responsee Inteligência contra ameaças compartilham recursos comuns, para dados de relacionamento e regras de duplicação, usados para importar informações externas e internas para Security Operations.

Análise de E-mails, Regras de Duplicaçãoe Mapeamento de Campos obtêm dados de entrada (um e-mail, arquivo JSON ou XML ou um registro) e transformam esses dados no formato correto para criar um novo registro. Cada um desses recursos extrai dados à sua maneira, mas eles são transformados no novo registro usando muitos dos mesmos processos.

Dados de relacionamento

Ao adicionar informações a uma lista relacionada (como um observável associado em um incidente de segurança), você pode criar um registro de relacionamento que consiste em uma tabela m2m. Às vezes, há dados adicionais nesse registro de relacionamento a serem definidos. Por exemplo, um observável sendo um IP de origem (em oposição a um IP de destino). Essas informações vão para o campo de **dados de relacionamento** no formulário de **transformação** de campo usado pela **análise de e-mail** ou para uma lista relacionada de **campos de mapeamento** de campo no formulário **de mapeamento** de campo.

O campo **Dados de relacionamento** geralmente está vazio. É mais comumente usado para endereços IP em observáveis na **Análise de e-mail**.

Você pode transformar dados de qualquer registro ServiceNow em qualquer outro registro ServiceNow usando **Campos de mapeamento** de campo no recurso **Mapeamento** de campo. Por exemplo, para transformar dados de um incidente em um incidente de segurança ou um incidente de segurança em um PRB.

Regras de duplicação do Security Operations

Use Regras de Duplicação para lidar com registros duplicados de segurança, vulnerabilidade, IoCs e assim por diante.

As regras de duplicação têm duas finalidades. Eles impedem que muitos registros duplicados sejam criados e, quando uma duplicata é detectada, eles especificam quais campos no registro são atualizados. Somente duplicatas ativas são procuradas. Se o registro não estiver ativo, por exemplo, se o incidente for encerrado, qualquer novo problema idêntico se tornará um novo incidente.

As regras de duplicação são usadas por **Análise de e-mail**, Mapeamento de **campo**e **Mapeamento de dados de aprimoramento**.

Tópicos relacionados

- Criar analisadores de e-mail no Security Operations
- Mapear tabelas para tabelas com mapeamento de campo do Security Operations

Criar regras de duplicação no Security Operations

Você pode usar Regras de Duplicação para identificar novos e-mails, dados de aprimoramento ou mapas de campo com registros duplicados ativos e processá-los adequadamente.

Antes de Iniciar

Função necessária: sn_sec_cmn.write

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Regras de Duplicação**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado:

Regra de duplicação

Campo	Descrição
Nome	O nome da regra de duplicação.
Tabela	Tabela em que os registros são criados e usados para determinar a duplicação.
Campos de identificação	Selecione um conjunto de campos que indicam um incidente de segurança duplicado, observável, vulnerabilidade e assim por diante, quando os valores nesses campos forem idênticos.
Ação duplicada	Controla como lidar com e-mails duplicados. As opções são: **Criar como secundário** Cria um registro como secundário do original. O campo que vincula o secundário ao primário é o campo **Primário**. **Não criar nem atualizar registros** (padrão) Não faz nada. Ignora duplicatas. **Atualizar registro duplicado** Atualiza os campos no registro existente conforme especificado em **Ações de duplicação.** **Nota:** Se você escolher **Atualizar registro duplicado**, a lista relacionada **Ações** de duplicação será exibida.
Ativo	Marque esta caixa de seleção para ativar a regra.
Descrição	Descreve a finalidade e a aplicação desta regra de duplicação; quando deve ser usado, por exemplo, uma regra projetada para observável baseado em IP ou incidentes de segurança do firewall.

4. Clique com o botão direito do mouse no cabeçalho do registro e selecione **Salvar** ou clique em **Atualizar**.
5. Para definir ações de duplicação, se você tiver escolhido **Atualizar registro duplicado**, clique em **Novo** para criar ações de duplicação para cada campo que deseja atualizar no incidente.
6. Preencha ou edite os campos no formulário para descrever como atualizar o campo:

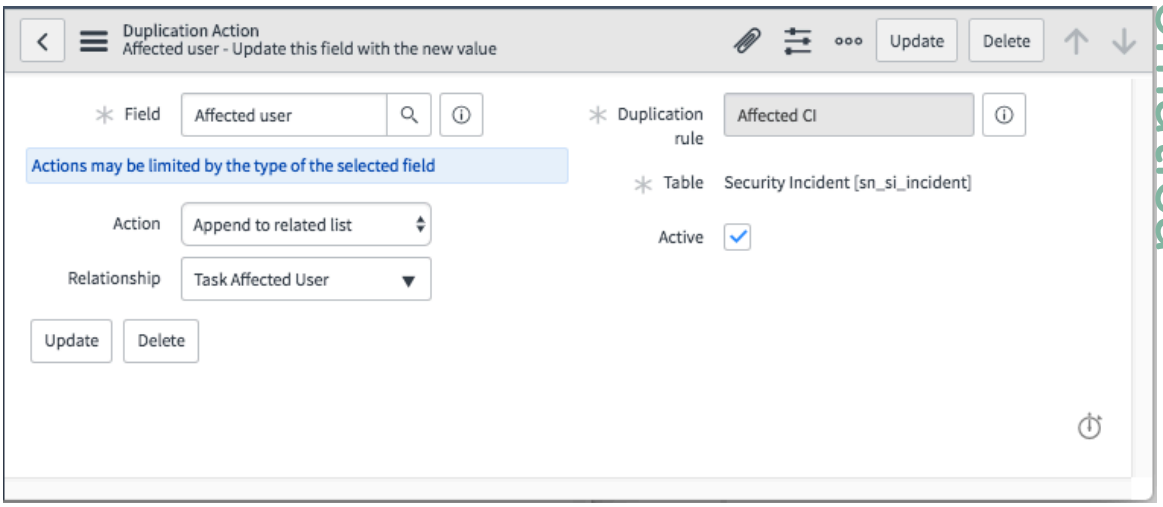
Ações de duplicação

Campo	Descrição
Campo	O nome do campo a ser usado para a ação de duplicação.
Ação	As ações compatíveis variam de acordo com o tipo de campo. As opções são: **Atualizar este campo com o novo valor** Substitui o valor anterior no registro existente por este valor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

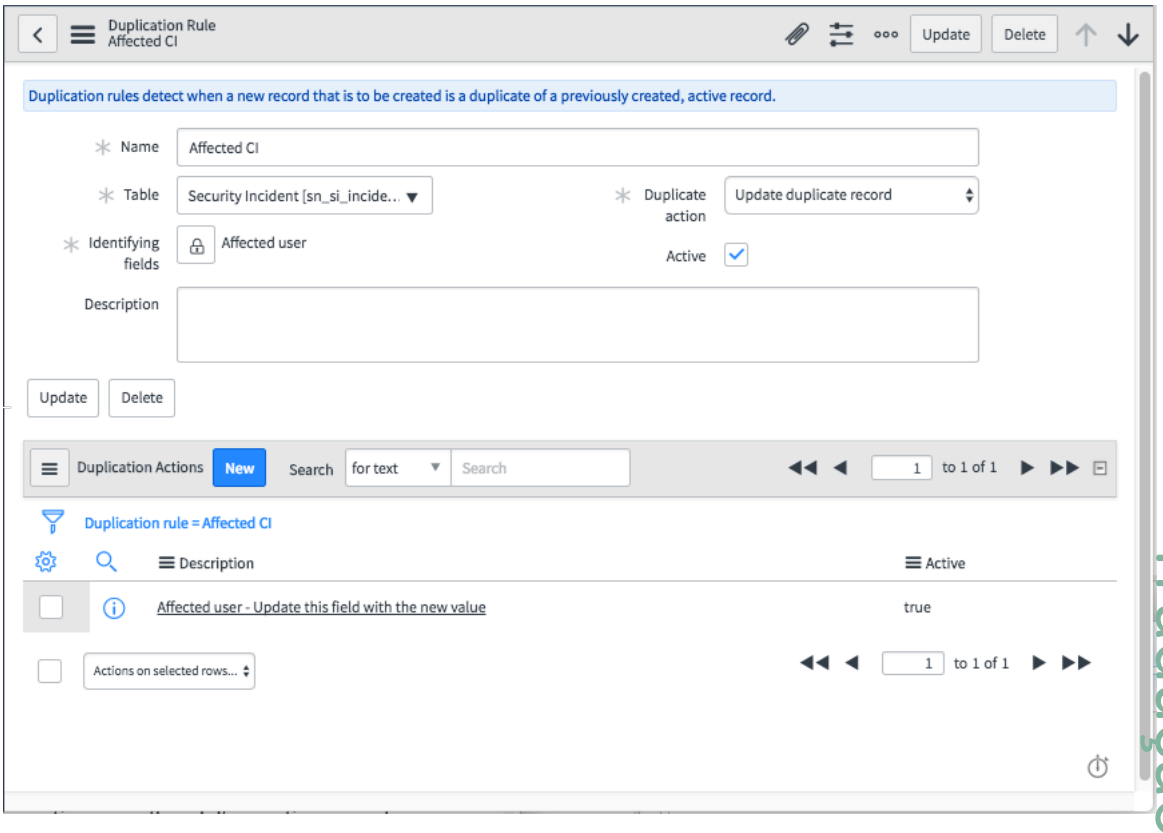
Campo	Descrição
	Anexar o novo valor a uma lista separada por vírgulas, se exclusivo Trata o valor como uma entrada em uma lista separada por vírgulas e adiciona os novos dados (se houver) como uma nova entrada nessa lista. Se os dados já estiverem na lista, eles não serão adicionados duas vezes. **Anexar o novo valor a este campo** Acrescenta o novo valor ao final do texto existente no campo. **Adicionar um a um campo de contador** Adiciona um ao campo numérico. **Definir o campo como hoje** Define o campo para a data e hora atuais. **Anexar à lista relacionada** Adiciona o registro relacionado com este valor à lista relacionada do registro atual. Aparece quando há uma tabela de muitos para muitos, com uma coluna do mesmo tipo, vinculada à tabela que está sendo atualizada. Por exemplo, **IC** afetado ou **Usuário afetado**.
Relacionamento	[Opcional] Este campo é exibido somente quando a ação **Acrescentar à lista relacionada** é selecionada. É o nome da lista relacionada que você deseja associar a esta regra.
Regra de duplicação	Regra da qual esta ação faz parte.
Tabela	Tabela em que os registros são criados. Exibe somente como informação.
Ativo	Marque esta caixa de seleção para ativar a ação.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

7. Clique em **Enviar**.



Security Operations processamento de e-mail

Você pode configurar a integração de informações de sistemas de detecção externos, fornecer granularidade no processamento de registros de operações de segurança, lidar com e-mails incompatíveis e impedir a duplicação de registros usando Processamento de E-mails.

Processamento de E-mails consiste nestes recursos:

Recurso	Descrição
Análise de E-mails	Gere novos registros Security Operations de e-mails do sistema externo.
Regras de Duplicação	Identifica novo e-mail com incidentes conhecidos e os processa adequadamente.
Propriedades	Especifica contas usadas como entrada em Análise de E-mails para segurança, vulnerabilidade e IoCs. Fornece granularidade no processamento de registros Security Operations.
E-mails Incompatíveis	Lista os e-mails que não correspondem a nenhum registro Security Operations.

Security Operations propriedades de e-mail

E-mail Propriedades especifica quais caixas de entrada são usadas como entrada em Análise de E-mails para importar informações de sistemas de detecção externos para criar registros de segurança, vulnerabilidade e IoCs. Você pode configurar uma conta geral para todos os

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

sistemas de detecção externos usarem ou contas de e-mail individuais para Security Incident Response, Inteligência contra ameaçasou Vulnerability Response.

Criar Security Operations propriedades de e-mail

Você pode especificar endereços de e-mail para relatórios e controlar comportamentos automáticos de e-mail usando e-mail Propriedades.

Antes de Iniciar

Função necessária: sn_sec_cmn.admin

Configure ferramentas de detecção externas para enviar e-mails para sua caixa de entrada de análise de e-mail.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Processamento de E-mails** > **Propriedades**.
2. Insira as caixas de correio dos destinatários conforme apropriado:
   Estes são os endereços de e-mail de entrada a serem processados pela **Análise de E-mail**, em vez de **Ações de Entrada**.

Propriedades de análise de e-mail

Campo	Descrição
Caixa de entrada para Security Operations ferramentas	Endereço de e-mail completo para Security Operations. Por exemplo, secops_support@yourcompany.com.
Caixa de entrada para ferramentas de Incidente de segurança	Endereço de e-mail completo para Security Incident Response. Por exemplo, sir_support@your.company.com.
Caixa de entrada para Vulnerability Response ferramentas	Endereço de e-mail completo para Vulnerability Response. Por exemplo, vuln_resp@yourcompany.com.
Caixa de entrada para Inteligência contra ameaças ferramentas	Endereço de e-mail completo para Inteligência contra ameaças. Por exemplo, Threat_intel@yourcompany.com.

3. Clique em **Salvar**.

Security Operations análise de e-mail

Gere novos Security Operations registros de sistemas de detecção externos usando Análise de E-mails. Este recurso fornece um método para integrar informações de ferramentas externas, como detecção de malware, detecção de vulnerabilidade, firewalls, inteligência contra ameaças e muito mais.

Como os e-mails são analisados

Qualquer sistema que pode enviar um e-mail, pode criar Security Operations registros, por exemplo, incidentes de segurança, solicitações, itens vulneráveis, vulnerabilidades, observáveis de incidente de segurança, métodos de ataque e muito mais.

Todos os plug-ins [Security Operations (Security Incident Response, Inteligência contra ameaçase Vulnerability Response) têm uma propriedade (**email_to**) que define o endereço de e-mail para o qual as integrações externas devem enviar e-mails, a serem analisados pelos analisadores de e-mail. Confira **Processamento de E-mails** > **Propriedades** para obter mais informações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O e-mail enviado para qualquer um dos Security Operations endereços de e-mail é armazenado em uma tabela de eventos de e-mail. Esses e-mails são processados para determinar se eles correspondem a algum analisador de e-mail.

Os e-mails que têm uma correspondência são sinalizados e as regras de transformação e duplicação criam ou atualizam um registro Security Operations. O e-mail é vinculado a esse registro e sinalizado como correspondente.

Os e-mails que não correspondem são listados em E-mails Incompatíveis como um registro Security Operations. Eles podem ser revisados para ajudar a criar analisadores de e-mail para lidar com esses e-mails. Uma ação Reprocessar permite que você execute o e-mail incompatível por meio dos analisadores novamente. O log de e-mail original está vinculado a esse registro.

As regras de duplicação para a transformação de e-mail gerenciam vários e-mails relacionados ao mesmo problema. Essas regras definem o que torna um registro duplicado e podem impedir que registros duplicados sejam criados. Quando uma duplicata é detectada, a regra especifica qual ação tomar: nenhuma ação (não criar um novo registro), criar o novo registro como um registro secundário do registro existente ou atualizar o registro existente. Ao atualizar a regra duplicada, especifica quais campos no registro existente são atualizados.

Nota:
Um analisador de e-mail Security Operations funciona em conjunto com as ações de entrada da plataforma e não as substitui. Ele não oferece suporte à definição de valores em campos indiretos, por exemplo, entradas **sys_journal_field**.

Por padrão, os eventos de e-mail são excluídos após 30 dias.

Vários registros

Sistemas de detecção externos (detectores de malware, vulnerabilidade e assim por diante) podem enviar e-mails que relatam vários itens de uma só vez. O analisador de e-mail oferece suporte a separadores no e-mail.

Por exemplo, um detector de malware pode enviar a você um relatório de e-mail sobre todos os sistemas em sua rede infectados por um malware específico com informações sobre o malware primeiro, seguidos por uma lista dos sistemas afetados.

Exemplo de e-mail malicioso

```
Subject: EvilChocolateBunny detected on multiple systems
Malware Hash: 20380285098260923490723
Malware Name: Evil Chocolate Bunny
Type: Keylogger
============================
System: WIN-GHARRISON
IP: 123.45.67.888
Status: File present, not infected
============================
System: WIN-ATUTER
IP: 123.45.67.889
Status: Infected
============================
System: WIN-BANGLIN
IP: 123.45.67.899
Status: File present, not infected
```

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Neste exemplo, quando o **Separador de registros** é definido na **Transformação de e-mail**como **==========**, ele divide o e-mail em quatro seções que são avaliadas separadamente. Isso cria um incidente de segurança para cada um dos três sistemas afetados.

Nota:
A seção de cabeçalho é detectada, mas não tem nenhum sistema afetado, portanto, ela é usada em todos os três registros e não cria um quarto registro.

As transformações de campo extraem dados de cada seção. Se algo no cabeçalho ou rodapé do e-mail se aplicar a todos os registros, como Hash de Malware, Nome de Malware e Tipo neste exemplo, a transformação de campo para eles deverá definir **o valor de Pesquisar para** um valor que pesquisa no corpo do e-mail **Em o início de uma linha no corpo do e-mail** ou **em qualquer lugar no corpo do e-mail**.

As transformações de campodevem ser definidas para pesquisar **no início de uma linha na seção de registro ou na seçãode** dados definidos em cada seção, como sistema, endereço IP ou status. As opções de seção de registro estão disponíveis somente quando há um separador de registro definido na transformação de e-mail.

Ao analisar um e-mail com um separador definido, os registros são criados somente para seções com pelo menos uma parte dos dados específicos da seção.

Neste exemplo, três registros são criados, embora haja quatro seções definidas. A primeira seção é um cabeçalho e não tem nada específico para apenas um sistema. Se algum dos campos na primeira seção estiver preenchido (Sistema, IP ou Status), um registro também será criado para essa seção.

Tópicos relacionados

Criar analisadores de e-mail no Security Operations

Security Operations mapeamento de dados de aprimoramento

Security Operations mapeamento de campo

Criar analisadores de e-mail no Security Operations

Análise de E-mails cria Security Operations registros de seu e-mail para segurança, vulnerabilidade e observáveis para agilizar a resposta e a correção de ameaças.

Antes de Iniciar

- Configure ferramentas de detecção externas para enviar e-mails para um endereço de e-mail central.
- Defina o endereço de e-mail em Propriedades do Security Operations. Para obter mais informações, consulte Criar Security Operations propriedades de e-mail.
- Atribua uma conta de usuário a este endereço de e-mail e forneça a esse usuário controles de acesso de segurança para criar e atualizar os registros de evento de e-mail.
- Tenha uma cópia do e-mail relevante da sua ferramenta de detecção externa à sua frente.
- Decida que tipo de registro você deseja criar, um incidente de segurança, registro de vulnerabilidade, tarefa e assim por diante. Esta opção determina a tabela selecionada.

Função necessária: sn_sec_cmn.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Análise de E-mails**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

> **Nota:**
> Se mais de um campo for especificado, todos os campos deverão corresponder ao e-mail para criar um registro.

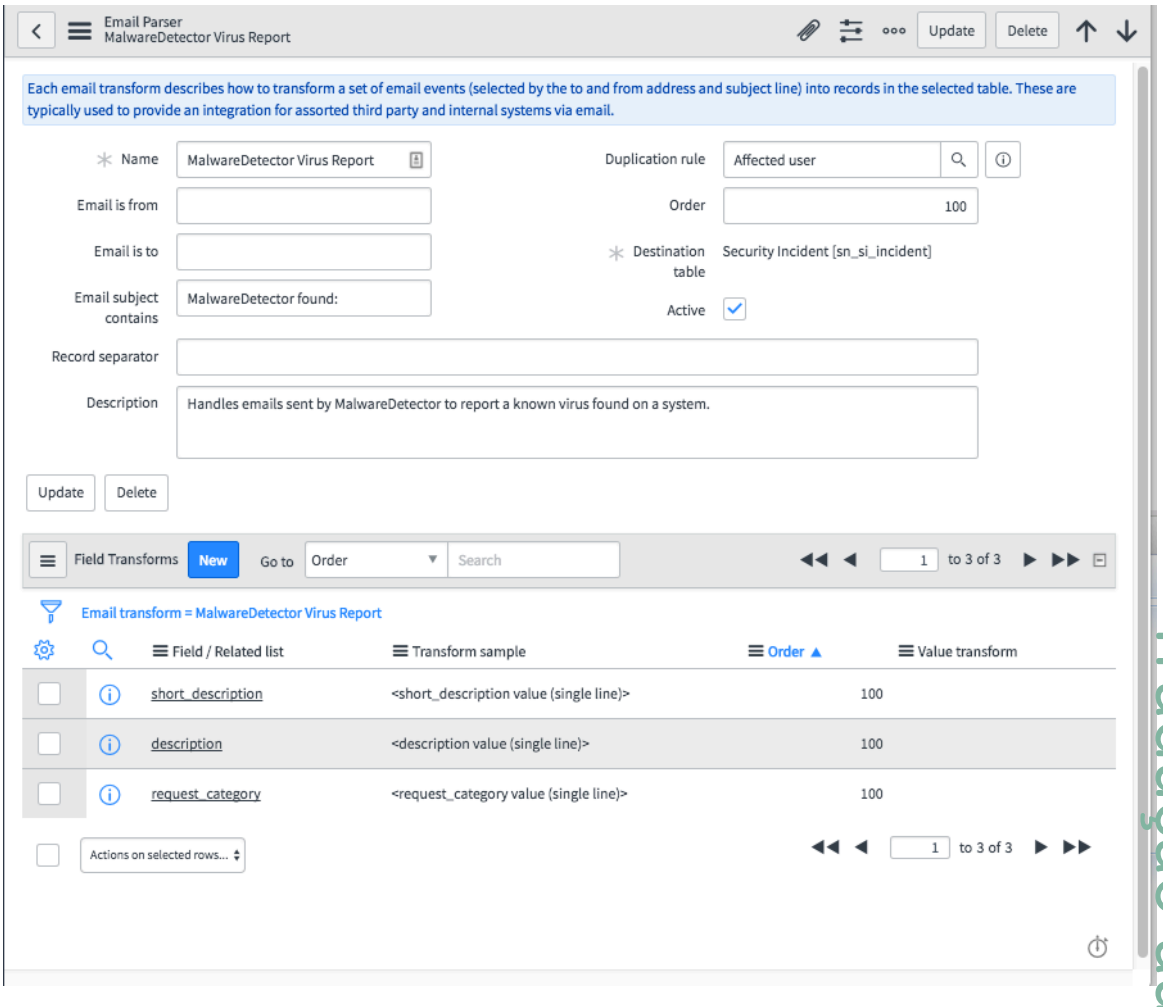
Analisador de e-mail

Campo	Descrição
Nome	O nome do analisador de e-mail.
O e-mail é de	Se preenchido, somente os e-mails deste endereço serão transformados por este analisador de e-mail.
O e-mail é para	Se preenchido, somente os e-mails deste endereço serão transformados por este analisador de e-mail.
O assunto do e-mail contém	Se preenchido, somente os e-mails em que o assunto contém esta frase serão transformados por este analisador de e-mail.
Regra de duplicação	Controla como lidar com e-mails duplicados para qualquer e-mail que esta transformação processa. Para obter mais informações, consulte Transformação de dados compartilhados.
Ordem	Em que ordem considerar as transformações. A primeira transformação de e-mail correspondente é usada. Normalmente, você deseja configurar os analisadores de e-mail mais específicos nos números mais baixos, com algum fallback. Forneça aos analisadores de e-mail catchall números de **ordem** mais altos para que eles sejam executados se nada mais corresponder. O padrão é 100. Quando tudo corresponde, o analisador de e-mail mais específico (corresponde **de**, **a**e **assunto**) é usado.
Tabela de destino	A tabela em que você deseja criar registros.
Ativo	Se esta transformação está ativa, em uso ou não. Se desmarcado, nenhum e-mail será transformado com este código.
Separador de registros	Quando os e-mails tratados por este analisador de e-mail criam vários registros, este campo contém o separador entre as informações desses registros. Para obter mais informações, consulte Security Operations análise de e-mail.
Descrição	Descrição deste analisador de e-mail, com qual ferramenta ele funciona, a finalidade e assim por diante.

4. Ao concluir suas entradas, clique com o botão direito do mouse no cabeçalho do formulário e selecione **Salvar**.
   Uma guia **Transformações de campo** é exibida. Esta guia mostra como os campos individuais na tabela de destino são definidos com base no conteúdo do e-mail.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Para adicionar **transformações de campo**, execute estas etapas.

   a. Na guia **Transformações de campo**, clique em **Novo**.

   b. Preencha os campos no formulário, conforme apropriado.

Opção	Descrição
Campo	**Descrição**
Armazenar valor em um campo ou uma lista relacionada	Selecione onde encontrar o valor. As opções incluem: ○ Armazene o valor em um campo no novo registro ○ Vincular a este valor a uma lista relacionada ○ Vincular a este valor, criando um novo registro se um registro correspondente não existir **Nota:** Se a tabela de destino não tiver listas relacionadas, este campo não será exibido.
Campo	Selecione o campo a ser preenchido com este valor.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Nota: Para campos de opção, as correspondências são feitas com as opções existentes usando o rótulo ou o valor de opção subjacente. Se nenhuma correspondência for encontrada, o campo será definido, mas nenhuma nova entrada será adicionada à lista de seleção. Para obter mais informações, consulte Listas de seleção. Para campos de referência, uma entrada é definida somente quando um valor correspondente ao nome de exibição do registro ou um `sys_id` válido é encontrado. Para obter mais informações, consulte Campos de referência.
Lista relacionada	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada** ou **Vincular a este valor, criando um novo registro se um registro correspondente não existir**, este campo especifica a lista relacionada à qual as informações serão adicionadas.
Campo de valor	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada** ou **Vincular a este valor, criando um novo registro se um registro correspondente não existir**, este campo especifica o campo na tabela exibida no relacionado lista. Ele é usado para pesquisar e localizar um registro existente. Por exemplo, se sua lista relacionada for **ICs afetados**, este campo poderá conter **Nome** ou Nome de **domínio totalmente qualificado**ou qualquer outro campo no registro de IC a ser usado para pesquisar o IC adicionado à lista de **ICs afetados**.
Dados de relacionamento	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada**, um registro será criado para vincular esse registro (como um incidente de segurança) ao valor (um IC, um Observável e assim por

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	diante.). Este campo especifica todas as informações adicionais (pares de campo e valor) que devem ser adicionadas ao registro de vinculação. Por exemplo, ao adicionar um Observável para um IP de origem, especifique que este IP é o IP de origem, em vez do IP de destino. Para vários valores, use um separador ^, por exemplo, type= Source IP^Active=true.
Novos dados de registro	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor, criando um novo registro se um registro correspondente não existir**, se nenhum registro relacionado correspondente ao valor analisado for encontrado, um registro será criado. Este campo especifica os dados estáticos a serem adicionados a esse registro. Para **ICs afetados**, se nenhum IC correspondente for encontrado, um registro de IC será criado). Quando isso acontece, o valor encontrado no e-mail é definido como o campo **Valor** no registro de IC. Você pode definir dados adicionais - uma anotação indicando por que o IC foi criado, algumas informações sobre com que tipo de ICs você está trabalhando e assim por diante. Um exemplo seria: description=Created by Malware Scanner email parser^type=autodetect.
Pesquisar valor	Selecione o local no e-mail para pesquisar. As opções incluem: ○ **No início de uma linha do corpo do e-mail** ○ **Em qualquer parte do corpo do e-mail** ○ **Na linha de assunto do e-mail** ○ **Sempre o valor estático** Quando você tiver definido um **Separador de registros**, mais opções (**Em qualquer lugar na seção de registro** e **No início de uma linha na seção de registro)** permitirão pesquisar somente na seção atual em vez de em todo o corpo do e-mail (consulte Security Operations análise de e-mail para obter mais informações informações. As informações que estão em um cabeçalho ou rodapé, aplicando-se a todos os registros, são pesquisadas em todo o corpo do e-mail. As informações que diferem en-

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	tre os registros são pesquisadas somente na seção.
Separador de valores	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada** ou **Vincular a este valor, criando um novo registro se um registro correspondente não existir**, este campo especifica o separador a ser usado para listas de itens. por exemplo, uma vírgula ou ponto e vírgula quando os dados do e-mail são uma lista de endereços IP.
Prefixo de valor	O texto que sempre precede o valor colocado neste campo para extrair.
Final do valor	Selecione o que indica o final do valor. As opções incluem: **Fim da linha**, **Fim do e-mail** (traz todo o texto restante no e-mail) ou **Até** (para quando encontra o texto especificado) ou **Até** (para quando encontra o texto especificado).
Sufixo de valor	Quando o **Fim do valor** é definido como **Até**, este campo especifica qual texto sempre segue o valor colocado neste campo. Por exemplo, procurar um valor que vem depois de "O computador afetado é" e antes de "". analisará "AB123" de "O vírus demente-coelho foi encontrado. O computador afetado é o AB123. A hora estimada da invasão foi 15h45" em um e-mail.
Transformação de valor	Escolha a entrada de transformação de campo a ser aplicada. Converte o valor encontrado no e-mail em um valor diferente, usado para preencher campos de opção, referência ocasional e outros campos.
Ordem	A ordem na qual o campo transforma a execução, da menor para a maior. Uma transformação de campo com uma entrada de ordem de 100 é tentada primeiro. Somente se essa transformação de campo não encontrar um valor, uma transformação de campo com uma ordem superior (200) no mesmo campo será executada.
Transformação de e-mail	A transformação à qual esta transformação de campo pertence.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Tabela de destino	Tabela de destino da transformação de e-mail. Ele contém dados informativos da transformação de e-mail.
Ativo	O padrão é marcado. Quando marcada, a transformação do campo é ativada. Desmarque esta caixa para desativar a transformação do campo.

a. Clique em **Enviar**.
O novo registro é usado para analisar as informações do e-mail em um novo registro.

Tópicos relacionados

Criar regras de duplicação no Security Operations

Criar transformações de valor de campo Security Operations

Definir Vulnerability Response notificações por e-mail

Editar registros de e-mail no Security Operations

Adicione ou crie transformações nos registros de evento de e-mail existentes.

Antes de Iniciar

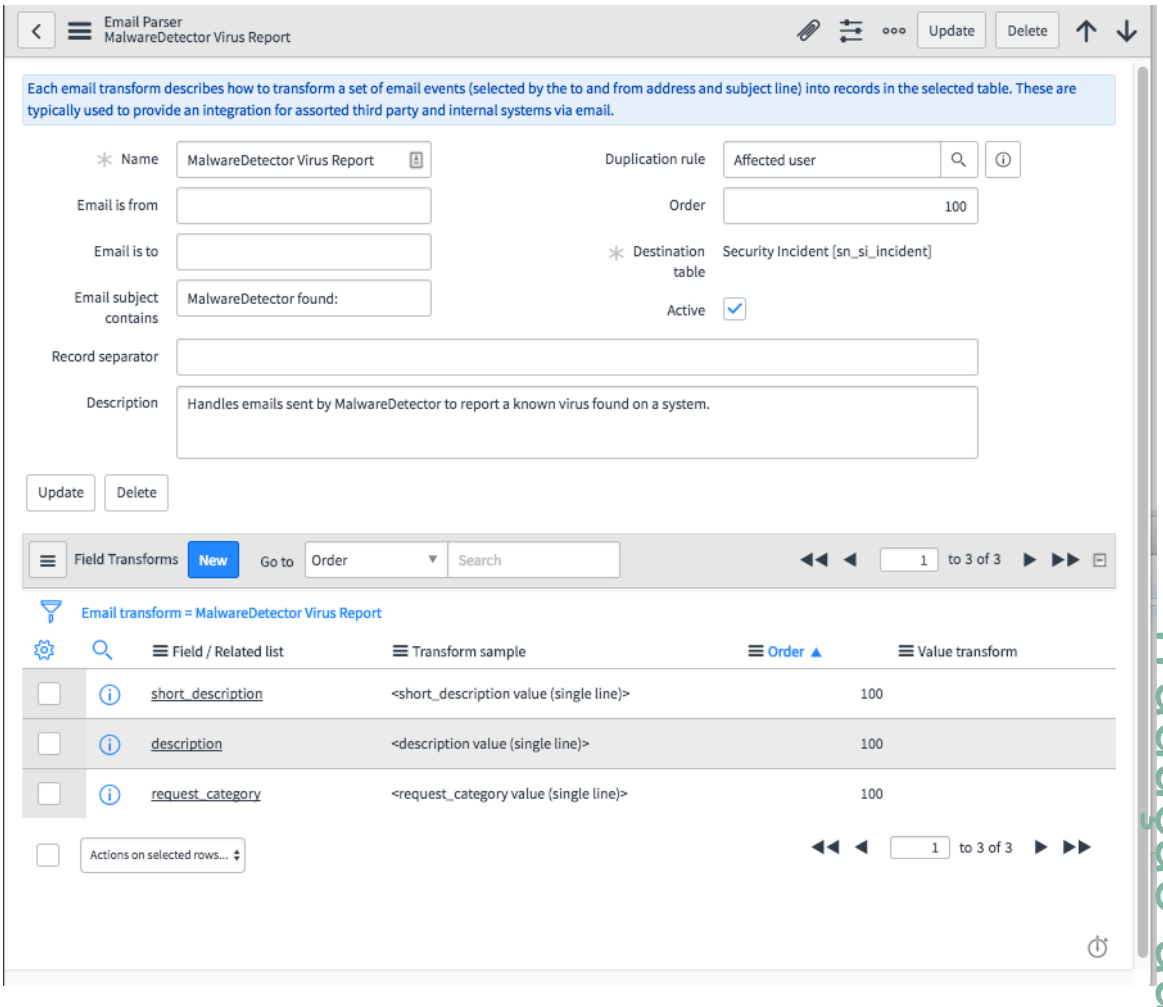
Função necessária: sn_sec_cmn.admin

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Análise de E-mails**.
2. Clique no analisador de e-mail para editar.
   Se o registro for somente leitura, clique no link aqui na mensagem de cabeçalho.
   Você será levado para o formulário editável da transformação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Edite os campos conforme apropriado.
4. Para editar **transformações de campo**, clique no campo e altere conforme apropriado.
5. Clique em **Atualizar.**

Eventos de e-mail Security Operations incompatíveis

Os eventos de e-mail que não correspondem a um analisador de e-mail têm o sinalizador "correspondido" não definido. Você pode exibir esses registros de evento de e-mail na lista E-mails Incompatíveis para revelar sistemas de detecção externos cujos e-mails ainda não foram analisados.

Ao criar analisadores de e-mail, você pode tentar reprocessar o evento de e-mail (a partir do formulário ou da lista) para validar um novo analisador de e-mail.

Exibir e reprocessar e-mails incompatíveis do Security Operations

Você pode revisar E-mails Incompatíveis para filtros descontinuados ou como candidatos a um novo filtro para manter ou melhorar a taxa na qual você detecta ameaças de e-mail.

Antes de Iniciar
Função necessária: sn_sec_cmn.read

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **E-mails Incompatíveis**.
   Se algum e-mail incompatível for encontrado, ele será listado.
2. Os campos do formulário são os seguintes:

Eventos de e-mail de segurança

Campo	Descrição
De	Endereço de e-mail do remetente.
Para	Endereço de e-mail dos destinatários.
Assunto	Linha de assunto no e-mail.
Corpo	Conteúdo do corpo do e-mail.
Correspondido	Indica se este evento de e-mail foi correspondido.

3. Para reprocessar este e-mail, crie um registro de e-mail ou edite um registro de e-mail existente para corresponder às informações deste e-mail.
   Consulte Criar analisadores de e-mail no Security Operations.
4. Navegar de volta para **Security Operations** > **E-mails Incompatíveis**.
5. Clique em **Reprocessar evento de e-mail** para tentar processar este e-mail.
   Ele retorna para a lista principal E-mails Incompatíveis. Se o novo registro de e-mail corresponder, o evento de e-mail não estará mais na lista. Uma mensagem indica se houve correspondência ou não.

Security Operations mapeamento de campo

TabelasSecurity Operations podem ser mapeadas de e para outras tabelas, vinculando um incidente de segurança a um caso de atendimento ao cliente ou um problema a outras partes do sistema Security Operations.

O mapeamento de campo define o mapeamento usado quando um registro da tabela de origem é usado para criar um novo registro na tabela de destino. Normalmente usados para criar um incidente de segurança a partir de outro registro, esses mapas definem quais campos em um incidente de segurança são inseridos em um novo problema ou quais campos de um incidente de cliente existente preenchem um novo incidente de segurança.

Mapear tabelas para tabelas com mapeamento de campo do Security Operations

Security Operations fornece granularidade de mapeamento de campo mais fina para que você possa mapear uma tabela Security Operations para qualquer outra tabela.

Antes de Iniciar

Função necessária: sec_cmn.write

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Utilitários** > **Mapeamento de Campos**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

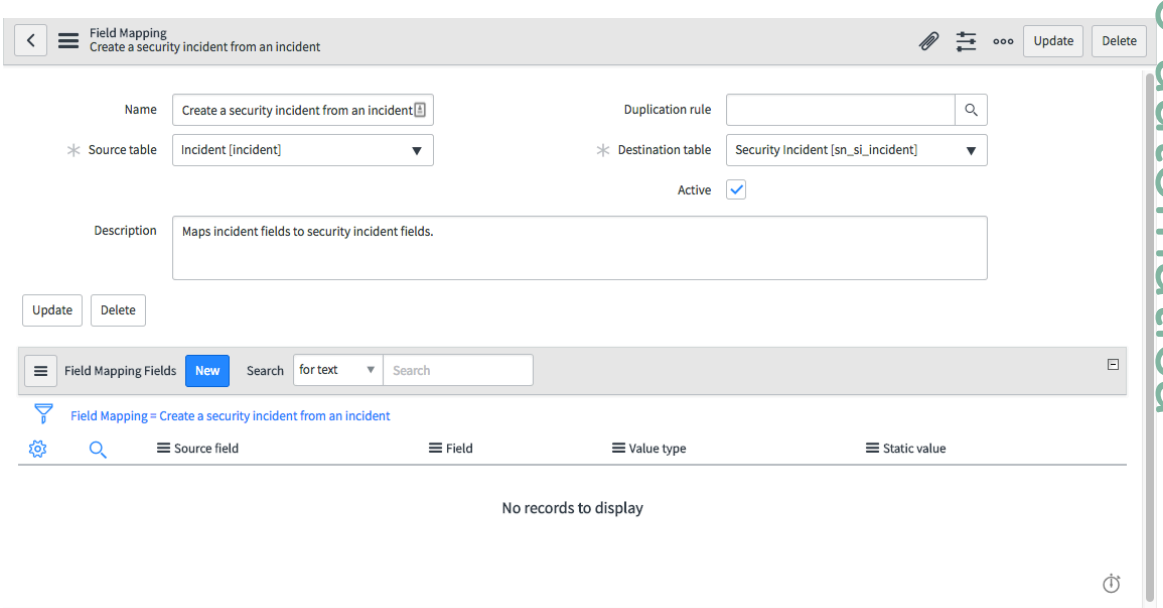
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de campo

Campo	Descrição
Nome	O nome do mapa de campo.
Tabela de origem	A tabela que fornece os dados a serem usados para criar um registro na tabela de destino.
Regra de duplicação	Controla como lidar com registros de origem que gerariam um registro duplicado. Para obter mais informações, consulte Transformação de dados compartilhados.
Tabela de destino	A tabela em que novos registros são criados.
Ativo	Marque esta caixa de seleção para ativar o mapeamento. **Nota:** Somente um mapeamento entre tabelas pode estar ativo de cada vez. Se dois mapas contiverem as mesmas tabelas, a versão mais antiga será desativada automaticamente.
Descrição	Descrição do mapa de campo.

4. Ao concluir suas entradas, clique com o botão direito do mouse no cabeçalho do formulário e selecione **Salvar**.
   A guia**Campos de mapeamento de campo** é exibida. Este registro define quais dados são colocados no campo de destino, em registros criados por esta transformação de campo.



5. Clique em **Nova**.
6. Preencha os campos no formulário, conforme apropriado.

Opção	Descrição
Campo	**Descrição**
Armazenar valor em um campo ou uma lista relacionada	Selecione onde encontrar o valor. As opções incluem:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	○ Adicionar novo valor a um campo no registro ○ Vincular a este valor a uma lista relacionada ○ Vincular a este valor, criando um registro se um registro correspondente não existir **Nota:** Se a tabela de destino não tiver listas relacionadas, este campo não será exibido.
Campo	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Adicionar novo valor em um campo no registro**, esse campo especificará o campo a ser preenchido. **Nota:** Para campos de opção, as correspondências são feitas com as opções existentes usando o rótulo ou o valor de opção subjacente. Se nenhuma correspondência for encontrada, o campo será definido, mas nenhuma nova entrada será adicionada à lista de seleção. Para obter mais informações, consulte Listas de seleção. Para campos de referência, uma entrada é definida somente quando um valor correspondente ao nome de exibição do registro ou um `sys_id` válido é encontrado. Para obter mais informações, consulte Campos de referência.
Lista relacionada	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada** ou **Vincular a este valor, criando um novo registro se um registro correspondente não existir**, este campo especifica a lista relacionada à qual as informações serão adicionadas.
Campo de valor	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada** ou **Vincular a este valor, criando um novo registro se um registro correspondente não existir**, este campo especifica o campo na tabela exibida no relacionado lista, que é

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	usada para pesquisar e encontrar um registro existente. Por exemplo, se sua lista relacionada for **ICs afetados**, este campo poderá conter **Nome** ou Nome de **domínio totalmente qualificado**ou qualquer outro campo no registro de IC que deva ser usado para pesquisar o IC é adicionado à lista de **ICs afetados**.
Dados de relacionamento	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada**, um novo registro será criado para vincular esse registro (como um incidente de segurança) ao valor (um IC, um observável e assim por diante). Este campo especifica todas as informações adicionais (pares de campo e valor) que devem ser adicionadas a esse registro de vinculação. Por exemplo, ao adicionar um observável para um IP de origem, você pode especificar que este IP é o IP de origem, em vez de um IP de destino. Para vários valores, use um separador ^, por exemplo, type= Source IP^active=true.
Novos dados de registro	**Quando Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor, criando um novo registro se um registro correspondente não existir**, se um registro relacionado correspondente ao valor analisado não for encontrado, um novo registro será criado. Este campo especifica os dados estáticos a serem adicionados a esse registro. Por exemplo, para **ICs afetados**, se não pudermos encontrar o IC, essa configuração indica que um novo IC foi criado). O valor encontrado no registro de origem é definido como o campo **Valor** no registro de IC. Você pode definir dados adicionais - uma anotação indicando por que este IC foi criado, algumas informações sobre com que tipo de ICs você está trabalhando. Um exemplo seria: `description=Created by malware Incident report^type=autodetect`
Separador de valores	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Vincular a este valor em uma lista relacionada** ou **Vincular a este valor, criando um novo registro se um registro correspondente não existir**, este campo especifica o separador a ser usado para listas de itens, geralmente uma vírgula ou ponto e vírgula.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Tipo de valor	Quando **Armazenar valor em um campo ou lista relacionada** estiver definido como **Adicionar novo valor em um campo no registro**, este campo especifica o tipo de valor. As opções incluem: ○ **Registro do campo de origem** ○ **Anexar ao campo como uma nova linha** ○ **Valor estático** ○ **Valor estático mais o valor do campo de registro de origem**
Campo de origem	Escolha o campo de origem que contém o valor a ser colocado no campo de destino ou na lista relacionada selecionada.
Campo estático	Valor estático para o campo.
Transformação de valor	Escolha a entrada de transformação do valor do campo a ser aplicada. Ele é usado para mapear campos de opção entre registros, por exemplo, convertendo o conjunto de opções de **Categoria** para um incidente de segurança no campo **Tipo** apropriado para uma Solicitação de Mudança.
Tabela de destino	Preenchido automaticamente com a tabela de destino.
Mapeamento de Campos	Preenchido automaticamente com o mapa de campo primário.
Tabela de origem	Preenchido automaticamente com a tabela de origem.

7. Clique em **Enviar**.

Security Operations transformações de valor de campo

Transforma valores de campo exclusivos do cliente em valores de campo reconhecidos por análise de e-mail Security Operations, aprimoramento de dados ou tabelas usando mapas de campo. Oferece suporte a campos de escolha, faz referência e alinha dados externos na terminologia e no formato padrão do seu novo registro.

Você pode mapear dados de campos como Categoria, Estado ou Grupo de atribuição para os valores usados na tabela Security Operations. Por exemplo, mapeie "Em análise" para "Trabalho em andamento".

Criar transformações de valor de campo Security Operations

Transformações de valor de campo define uma transformação entre os dados de origem fornecidos e o valor de substituição a ser usado.

Antes de Iniciar

Função necessária: sn_sec_cmn.basic ou sn_si.basic

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Defina cada entrada de transformação a ser aplicada quando houver uma correspondência com o valor de pesquisa ou quando o valor de pesquisa estiver contido nos dados de origem fornecidos ou quando nenhuma correspondência for encontrada. Defina um valor padrão para quando nenhuma correspondência for encontrada. Se nenhum valor padrão for definido e nenhuma correspondência for encontrada, os dados de origem originais serão usados.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Utilitários** > **Transformações de Valores de campos**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Transformações de valor de campo

Campo	Descrição
Nome	O nome da transformação do valor do campo.
Descrição	Descrição do mapa de campo.
Entradas de Transformação de Valor de Campo	A lista de entradas da tabela. **a.** Em **Substituir dados**, clique duas vezes em "Inserir uma nova linha". **b.** Escolha uma das seguintes opções: Quando a data deste campo corresponde Quando os dados para este campo contêm Quando nenhuma outra entrada de transformação corresponde aos dados (padrão) **c.** Clique na marca de seleção verde. **d.** Clique duas vezes em **Valor de pesquisa**e adicione seu valor de pesquisa. **e.** Clique na marca de seleção verde. **f.** Clique duas vezes em Valor de **substituição para** adicionar o valor correspondente ServiceNow. **g.** Repita se necessário.
Ativo	Marque esta caixa de seleção para ativar a transformação.
Aplicação	Escopo da aplicação.

4. Clique em **Enviar**.

Security Operations mapeamento de dados de aprimoramento

Mapeamento de Dados de Aprimoramento transforma dados de arquivos XML, JSON ou Propriedades em registros ServiceNow. Security Operations fluxos de trabalho usam mapas de dados de aprimoramento e fornecem dados de saída para incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Security Operations inclui vários mapas de dados de aprimoramento, acionados por vários fluxos de trabalho, por exemplo, Security Operations Integrations - Obter fluxo de trabalho de estatísticas de rede e Fluxo de trabalho de integração de comandos do sistema de operações de segurança – Obter processos em execução. A saída do mapa de dados de aprimoramento de Security Operations fluxos de trabalho é exibida na guia **Dados** de aprimoramento no formulário de incidente de segurança.

Criar um mapa de dados de aprimoramento Security Operations

Transforme dados do formato de arquivo JSON, XML ou Propriedades em registros ServiceNow usando mapas de dados de aprimoramento.

Antes de Iniciar

Função necessária: sn_sec_cmn.write

Por Que e Quando Desempenhar Esta Tarefa

Os mapas de dados de aprimoramento existentes são usados por fluxos de trabalho fornecidos em Security Operations. Você pode exibir a lista em **Mapeamento de dados de aprimoramento**. Para usar um mapa, você precisa de um gatilho, seja uma regra de negócios ou um fluxo de trabalho.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Utilitários** > **Mapeamento de Dados de Aprimoramento**.
2. Clique em **Nova**.
3. Preencha os campos, se for o caso.

Como criar um mapa de dados de aprimoramento

Campo	Descrição
Nome	Nome deste mapa de dados de aprimoramento.
Formato de entrada	Escolha um formato na lista: JSON (padrão) XML Formato do arquivo de propriedades

Chave de prefixo	Use para limitar o conjunto de dados de entrada a uma chave especificada. A raiz do conjunto de dados de entrada é definida como esta chave. Neste exemplo, se você inserir file_info, os valores de entrada serão limitados aos valores em file_info.
	`<?xml version="1.0" encoding="UTF-8"?>`
	`<malware>`
	`<version>2.0</version>`
	`<file_info>`
	`<malware>yes</malware>`
	`<sha1>24c051142583e10451a53893fed3aa5d80bfb1f6</sha1>`
	`<filetype>PE</filetype>`
	`<sha256>be9bd96808173e2d967feef8c8c5`

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	b8c4d73b621584fb11eb68434da1e6a0a930</sha256> <md5>ee8c91751b3010e38c479cf9ab09827a</md5> <size>546304</size> </file_info> </malware>
Aplicação	Escopo da aplicação.
Regra de duplicação	Regra que define quando um registro é considerado uma duplicata e quais ações tomar com registros duplicados.
Tabela de destino	Escolha uma tabela na lista.
Ativo	Marque esta caixa de seleção para ativar o mapa.
Descrição	Insira uma descrição do mapa de dados de aprimoramento.

4. Clique em **Enviar**.
   A guia Campos de mapeamento de dados de aprimoramento é exibida.
5. Clique em **Nova**.
6. Preencha os campos no formulário, conforme apropriado.

Campos de mapeamento de dados de aprimoramento

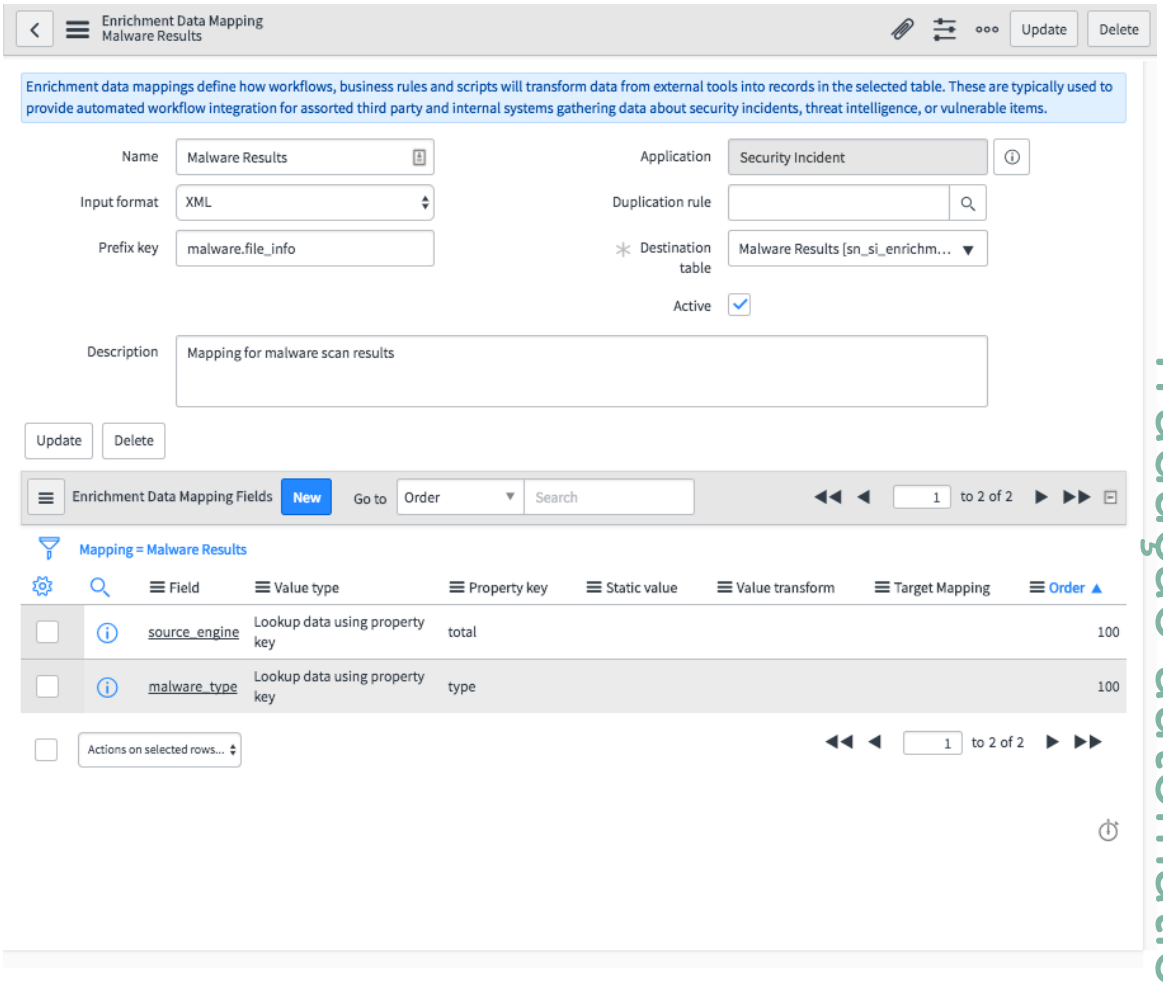
Campo	Descrição
Campo	Nome do mapa de dados de aprimoramento.
Tipo de valor	Escolha na lista: Pesquisar dados usando a chave de propriedade Valor estático Valor estático e dados da chave de propriedade O campo é uma matriz ou objeto (aninhamento de dados brutos) Cada opção tem entradas diferentes. Valores de campo e matrizes ou objetos exigem uma chave de propriedade.
Chave de propriedade	Determina a chave para a pesquisa de dados de entrada e o valor gravado no campo de destino.
Transformação de valor	A transformação do valor do campo que mapeia um valor para outro.
Aplicação	Escopo da aplicação.
Ordem	Em que ordem considerar o mapeamento. A primeira correspondência é usada. O padrão é 100.
Mapeamento	Nome do mapa de dados de aprimoramento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Tabela de destino	A tabela para a qual os campos a serem mapeados estão indo.

7. Clique em **Enviar**.
   Veja a seguir um exemplo de um mapa de dados de aprimoramento.



Tradução automática

Security Operations escalação definida pelo usuário

Você pode criar um caminho de escalação para incidentes de segurança em caso de problemas que exigem mais atenção ou experiência. Quando um grupo de escalação existe, um botão aparece em qualquer incidente de segurança nesse grupo.

Criar um grupo de escalação definido pelo usuário Security Operations

Escale um incidente de segurança para qualquer grupo associado ao incidente usando Escalações.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Grupos** > **Escalações**.
2. Clique em **Novo**.

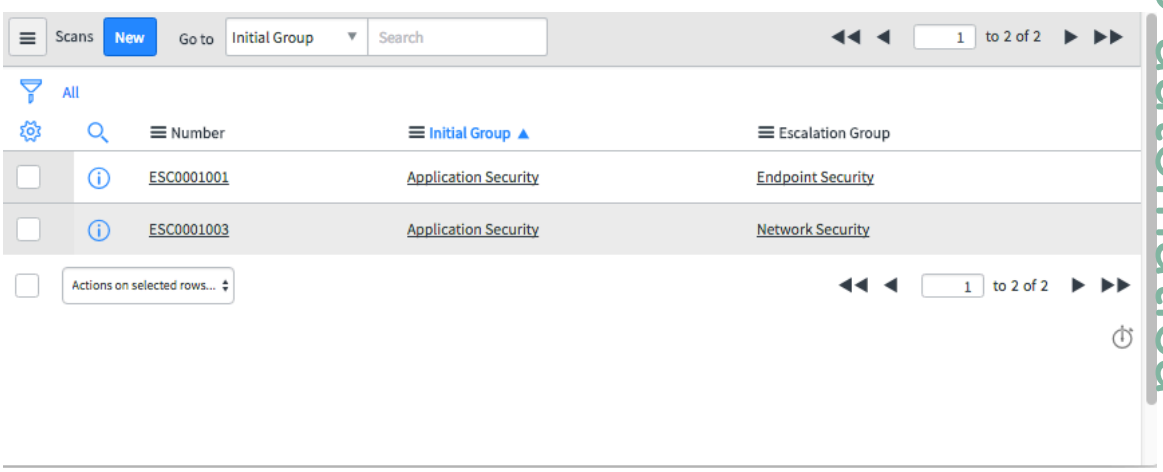
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Preencha os campos no formulário, conforme apropriado.

Escalações

Campo	Descrição
Número	Número do incidente de escalação (o campo é gerado automaticamente).
Grupo inicial	Selecione o grupo ao qual este incidente de segurança pertence.
Grupo de escalação	Selecione o grupo para o qual escalonar o incidente de segurança.

4. Clique em **Enviar**.
Um grupo de escalação está disponível para todos os incidentes de segurança no grupo inicial. Você pode criar vários grupos.



Tradução automática

Criar substituições de propriedade separadas por domínio

Ao usar a separação de domínio, você pode criar substituições para as propriedades existentes do Security Operations que permitem personalizar as funções das aplicações em cada um dos domínios.

Antes de Iniciar

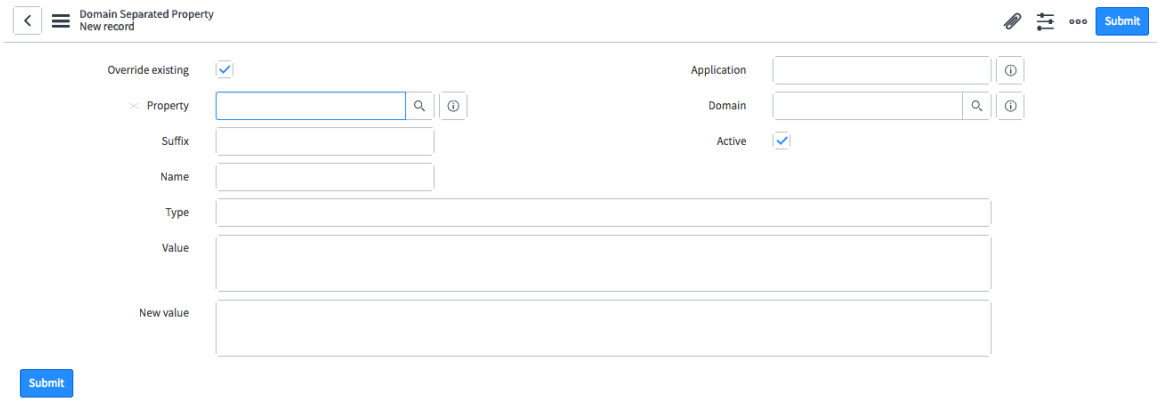
Requer que o Suporte de domínio - Extensões de domínio esteja ativado. Você também pode aprender sobre o Visualizador de substituição de domínio .

Função necessária: administrador

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Utilitários** > **Propriedades Separadas de Domínio**.
2. Clique em **Nova**.



3. No formulário, preencha os campos.

Formulário de propriedade do Domain Separation

Campo	Descrição
Substituir existente	Marque esta caixa de seleção para criar um valor específico de domínio para uma propriedade existente.
Aplicação	Selecione a aplicação que contém a propriedade que você deseja substituir.
Propriedade	Selecione a propriedade da aplicação selecionada para a qual você deseja criar uma substituição específica do domínio.
Domínio	Selecione o domínio para o qual você está criando esta substituição de propriedade.
Ativo	Ative ou desative a substituição.
Sufixo	Exibe o sufixo da propriedade.
Nome	Exibe o nome da propriedade.
Tipo	Exibe o tipo de propriedade.
Valor	Exibe o valor atual definido para a propriedade.
Novo valor	Insira um novo valor para a propriedade a ser aplicada a este domínio.

4. Clique em **Enviar**.
   A substituição da propriedade é aplicada à propriedade selecionada no domínio especificado. Quando a lógica desta propriedade é acionada, o sistema verifica se há substituições de propriedade separadas por domínio. Se uma substituição para o domínio for encontrada, o novo valor será usado. Caso contrário, o valor do domínio padrão será usado.

Tópicos relacionados

Noções básicas sobre o Domain Separation

Criar um grupo de sistemas operacionais

Grupos de sistemas operacionais são usados para mapear um sistema operacional para tipos de processo específicos e scripts em Security Incident Response fluxos de trabalho. Os

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

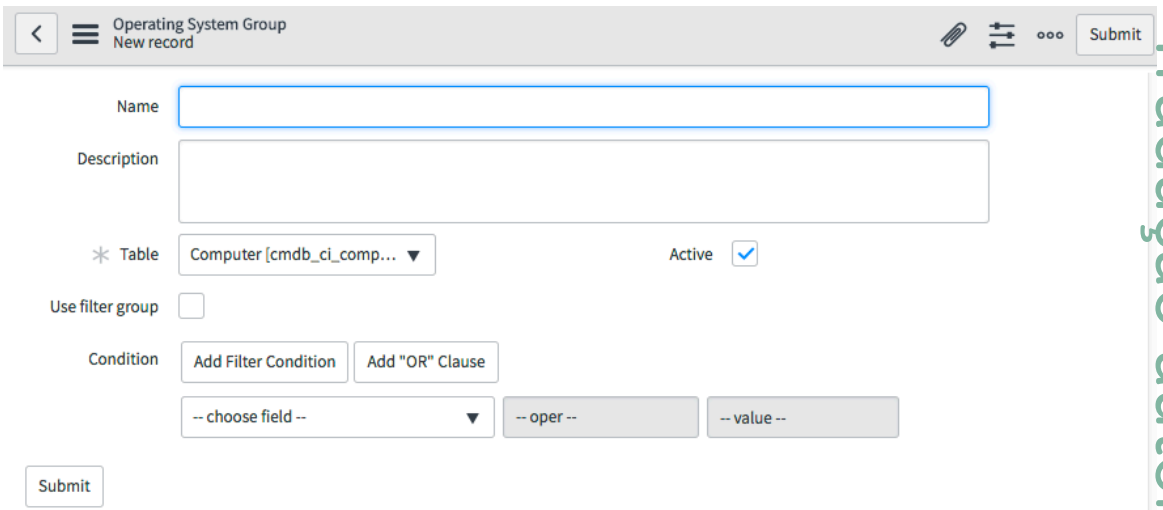
scripts definem como os processos em execução para os grupos de sistemas operacionais definidos são recuperados. Novos sistemas operacionais podem ser adicionados conforme necessário.

Antes de Iniciar

Função necessária: sn_sec_cmn.admin

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Utilitários** > **Grupos de Sistemas Operacionais**.
   O sistema básico inclui scripts para três sistemas operacionais:
   - SO baseado em BSD
   - SO baseado em POSIX
   - Sistema operacional Windows
2. Clique em **Nova**.



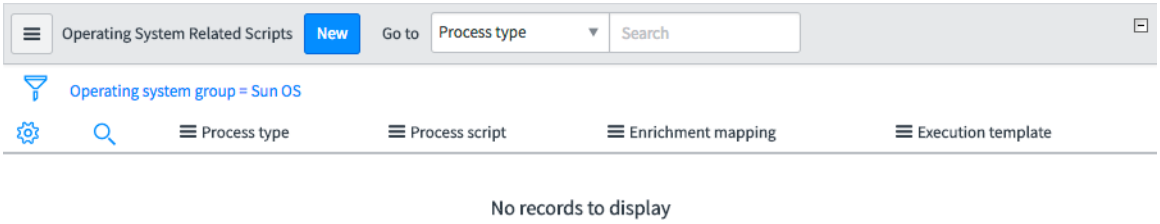
3. Preencha os campos, conforme necessário.

Campo	Descrição
Nome	O nome do grupo de sistemas operacionais.
Descrição	Uma descrição para o grupo de sistemas operacionais.
Tabela	A tabela afetada.
Ativo	Marque esta caixa de seleção para ativar o grupo de sistemas operacionais.
Usar grupo de filtros	Marque esta caixa de seleção para usar um grupo de filtros para localizar registros correspondentes na tabela selecionada.
Grupo de filtros	Selecione o grupo de filtros para localizar registros correspondentes na tabela selecionada. Este campo será exibido somente se você tiver marcado a caixa de seleção **Usar grupo de filtros**.
Condição	O Os campos doconstrutor de condição serão exibidos somente se você não marcar a caixa de seleção **Usar grupo de filtros**.

4. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
   A lista relacionada Scripts relacionados ao sistema operacional é aberta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Nova**.
6. Selecione scripts que correspondam aos fluxos de trabalho que você está usando para obter processos em execução, serviços e/ou estatísticas de rede.
7. Clique em **Enviar**.

Tópicos relacionados

Anexar um arquivo de script a um MID Server sincronizado

Configurar grupos de marcadores de segurança e marcadores

Você pode atribuir marcadores a incidentes de segurança, tarefas de resposta, itens vulneráveis, observáveis, IoCs e casos de segurança para criar metadados no registro de resposta e definir quem deve ter acesso a tipos específicos de conteúdo de segurança. Os marcadores podem ser adicionados a grupos de segurança para organizá-los.

Antes de Iniciar

Função necessária: sn_si.admin

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Marcadores de Segurança** > **Grupos**.
   Três grupos de classificação padrão estão incluídos no sistema de base.
   - **Lista de permissões/lista de proibições de aprimoramento**: este grupo define se um registro deve ser tratado como um registro da lista de permissões ou da lista de proibições. Os registros da lista de permissões geralmente são menos significativos, portanto, podem ser ignorados. Os registros da lista de proibições geralmente são de maior interesse.
   - **Metatag**: este grupo é fornecido como dados de demonstração. Você pode usá-lo para criar marcadores de classificação personalizados que são usados por aplicações de operações de segurança.
   - **Protocolo de semáforo**: este grupo é usado para garantir que informações confidenciais sejam compartilhadas com o público correto. Ele emprega quatro cores (branco, verde, âmbar e vermelho) para indicar diferentes graus de sensibilidade. Para cada cor, você pode atribuir as funções de acesso de leitura/gravação apropriadas. Ao compartilhar observáveis com um círculo de segurança confiável, o marcador atribuído ao perfil do círculo de segurança confiável determina quais observáveis marcados com TLP podem ser compartilhados com o círculo, da seguinte forma:
     - **TLP: WHITE:** somente observáveis com TLP: WHITE podem ser compartilhados com um perfil TLP: WHITE.
     - **TLP: VERDE:** observáveis com TLP: VERDE e TLP: BRANCO podem ser compartilhados com um perfil TLP: VERDE.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **TLP: ÂMBAR:** observáveis com TLP: ÂMBAR, TLP: VERDE e TLP: BRANCO podem ser compartilhados com um perfil TLP: ÂMBAR.
- **TLP: RED:**todos os observáveis, independentemente do marcador TLP, podem ser compartilhados com um perfil TLP: RED, já que TLP: RED é o marcador TLP com classificação mais alta.

Nota:
Você pode adicionar outras cores TLP, mas qualquer uma além das quatro cores incluídas é considerada inválida pelo Fórum de equipes de segurança e resposta a incidentes (FIRST).

2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Nome	Insira o nome do grupo de segurança.
Permitir várias seleções	Marque esta caixa se quiser atribuir vários marcadores de segurança a um registro que compartilha um grupo.
Ativo	Ative ou desative o grupo.
Descrição	Insira uma descrição deste grupo.

4. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
A lista relacionada Marcadores de segurança é exibida.
5. Na lista relacionada Marcadores de segurança, clique em **Novo**.
6. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Nome	O nome do marcador de classificação.
Grupo de marcadores de segurança	Se o marcador foi criado usando o botão **Novo** na lista relacionada do grupo, este campo será padronizado para o grupo atual. Se necessário, você pode adicionar o marcador a um grupo diferente, mas isso é opcional.
Ordem	Especifique a ordem em que o marcador aparece em formulários ou em uma lista.
Cor	Selecione a cor deste marcador.
Impor acesso restrito	Marque esta caixa de seleção para atribuir funções de leitura e/ou gravação necessárias para que os usuários leiam ou gravem em registros que tenham este marcador de segurança.
Ativo	Ative ou desative o marcador.
Descrição	Uma descrição deste marcador.
Função (acesso de leitura)	Para atribuir acesso de leitura a um marcador de segurança, clique no ícone de cadeado, selecione as funções de acesso apropriadas e clique no ícone de cadeado novamente. Este campo aparecerá somente se você marcar a caixa de seleção **Impor acesso restrito**.
Funções (acesso de gravação)	Para atribuir acesso de gravação a um marcador de segurança, clique no ícone de cadeado, selecione as funções de acesso apropriadas e clique no ícone de cadeado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	novamente. Este campo aparecerá somente se você marcar a caixa de seleção **Impor acesso restrito**.

7. Repita conforme necessário para criar mais marcadores de segurança.
8. Clique em **Atualizar**.

> **Nota:**
> Você também pode criar novos marcadores navegando até **Security Operations** > **Marcadores de Segurança** > **Marcadores**. O procedimento é o mesmo.

Criar regras de marcador de segurança

As regras de marcador de segurança fornecem filtragem para acesso ao marcador de segurança.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Marcadores de Segurança** > **Marcadores**.
2. Escolha ou crie um marcador de segurança.
3. Na guia relacionada **Regras de marcador de segurança**, clique em **Novo**.
4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Nome	O nome da regra de marcador de segurança.
Marcador de segurança	O marcador de segurança a ser anexado à regra.
Ativo	Ative ou desative o marcador de segurança.
Descrição	Uma descrição desta regra.

5. Determine **a filtragem de registro.**
6. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Usar grupo de filtros	Associa o grupo de filtros à regra.
Tabela	A tabela que contém a regra.
Condição	Adicione uma ou mais condições de filtro.

7. Clique em **Enviar**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Importar regras de marcador de segurança

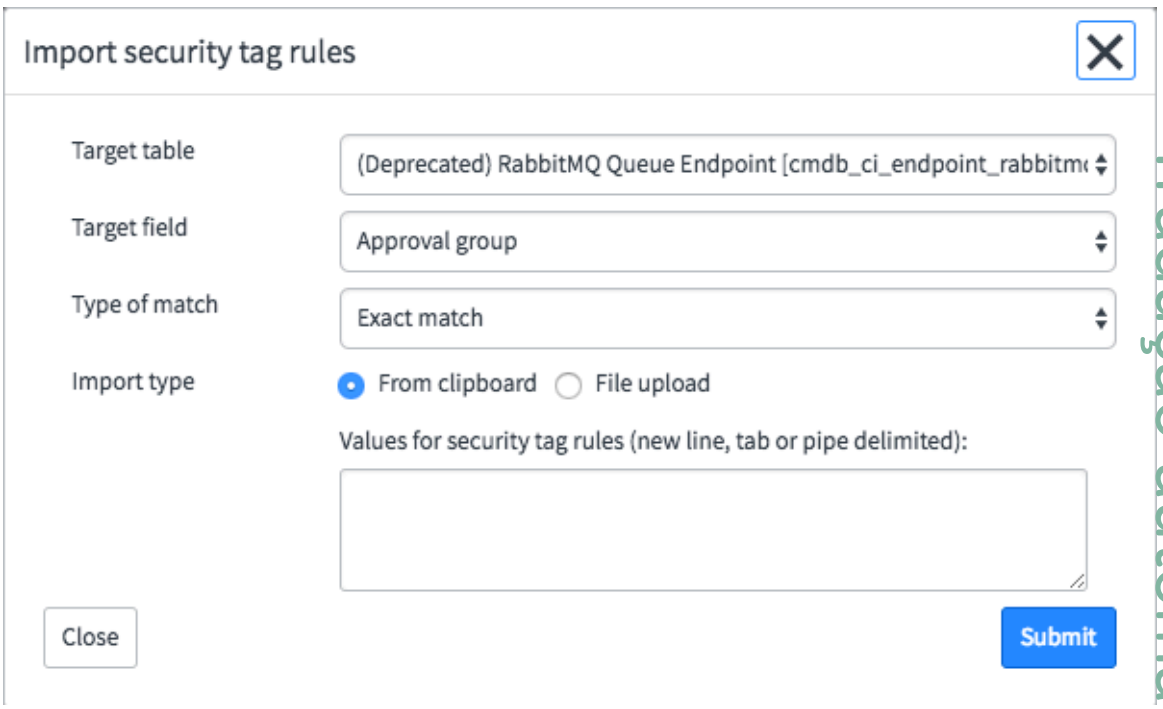
Você pode importar regras de marcador de segurança de outras tabelas em sua implantação.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Marcadores de Segurança** > **Marcadores**.
2. Escolha ou crie um marcador de segurança.
3. Clique no link relacionado **Importar regras de marcador de segurança**.



4. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Tabela de destino	Escolha a tabela a ser usada para importar regras.
Campo de destino	Escolha o campo a ser usado para importar regras.
Tipo de correspondência	Escolha como corresponder as regras importadas aos marcadores de **segurança** de: Correspondência exata (padrão) Contém Começa com Termina com Expressão regular
Tipo de importação	Escolher: **Da área de transferência**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Copie uma lista de valores delimitados para a área de texto. Os valores são analisados em marcadores de segurança. **Do carregamento do arquivo** Carregue um arquivo com valores delimitados. Os valores são analisados em marcadores de segurança. Adicione valores para as regras de marcador de segurança usando nova linha ou delimitadores de pipe.

5. Clique em **Enviar**

Anotações de segurança

Uma anotação de segurança é uma nota de explicação ou comentários adicionados a um item de configuração, observável ou uso em um incidente de segurança.

Várias anotações de segurança estão disponíveis para usuários e observáveis (requer o plug-in Inteligência contra ameaças). Relatórios sobre anotações de segurança também estão disponíveis.

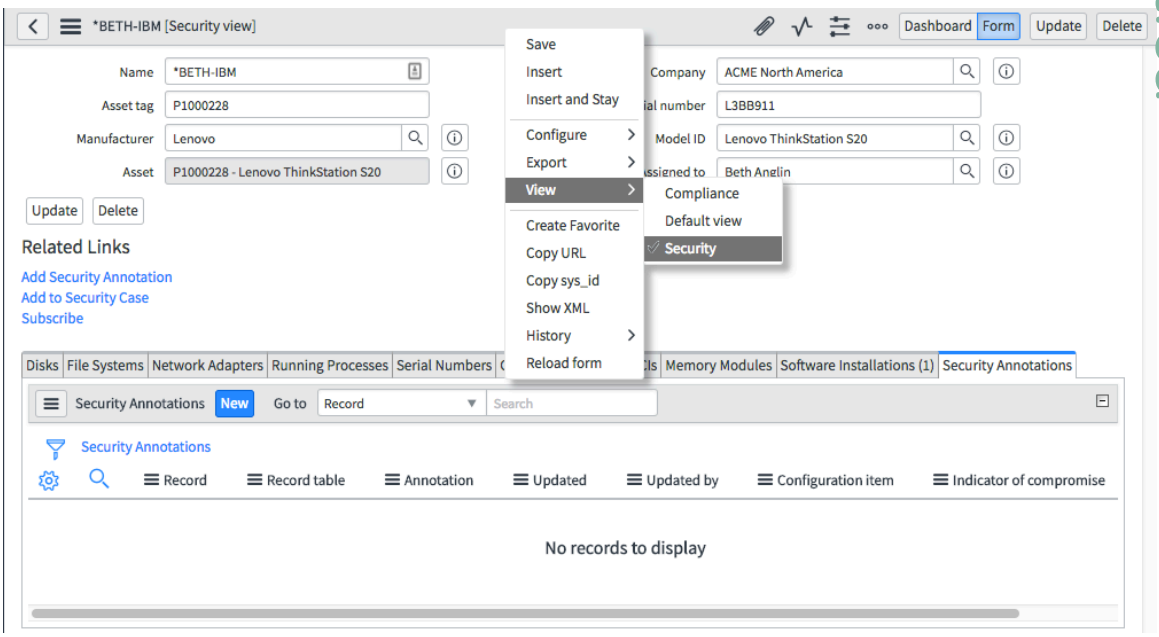
Criar anotações de segurança para ICs

As anotações em ICs permitem que você rastreie a atividade entre incidentes. Você pode adicionar anotações a um único ou vários ICs.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Em um incidente de segurança ou na tabela Item de configuração, abra um IC.
2. Clique com o botão direito do mouse no cabeçalho e escolha **Exibição** > **Segurança**.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Na guia da lista relacionada **Anotações de segurança**, clique em **Novo**.
4. Insira uma anotação.
   As anotações podem estar em qualquer formato de texto.
5. Clique em **Enviar**.

> **Nota:**
> Você pode adicionar a mesma anotação a vários ICs selecionando ICs na lista, escolhendo **Adicionar anotação de segurança**, inserindo uma anotação em qualquer formato de texto e clicando em **Enviar**.

Criar anotações de segurança para observáveis

Você pode selecionar um ou vários observáveis e aplicar anotações de segurança a eles usando o menu de opção **Ações nas linhas selecionadas**.

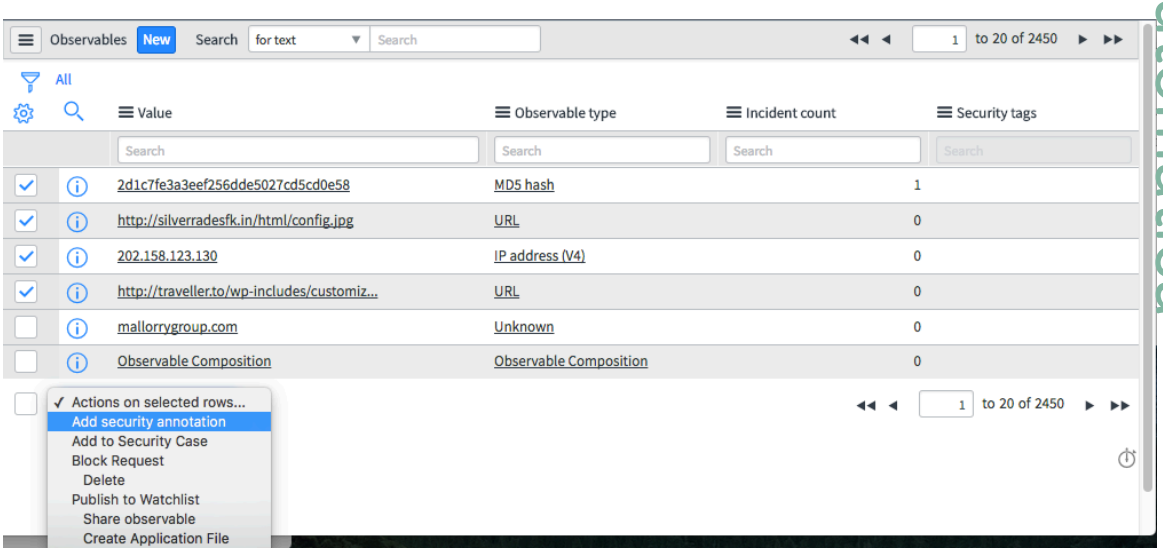
Antes de Iniciar

- Requer o plug-in Inteligência contra ameaças e a ativação. O plug-in Inteligência contra ameaças está disponível como uma assinatura separada.

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Inteligência contra ameaças** > **Observáveis**
2. Selecione um ou mais observáveis na lista.
3. No menu suspenso **Ações em linhas selecionadas**, escolha **Adicionar anotação de segurança**.



4. Insira uma anotação.
   As anotações podem estar em qualquer formato de texto.
5. Clique em **Enviar**.

Criar anotações de segurança para usuários

Você pode selecionar um ou vários usuários e aplicar anotações de segurança a eles usando o menu de opção **Ações nas linhas selecionadas**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Requer o plug-in Inteligência contra ameaças e a ativação. O plug-in Inteligência contra ameaças está disponível como uma assinatura separada.

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Administração de usuários** > **Usuários**
2. Selecione um ou mais usuários na lista.
3. No menu suspenso **Ações em linhas selecionadas**, escolha **Adicionar anotação de segurança**.
4. Insira uma anotação.
   As anotações podem estar em qualquer formato de texto.
5. Clique em **Enviar**.

Exibir relatórios de anotações de segurança

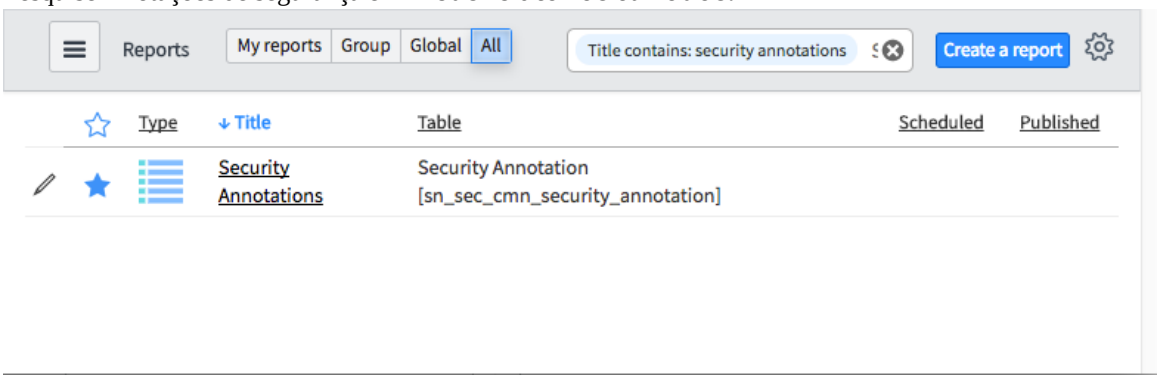
O relatório Anotações de segurança apresenta detalhes armazenados na tabela Anotações de segurança [sn_sec_cmn_security_annotations]. Você pode personalizar as colunas no relatório e agrupar os dados da maneira que desejar.

Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Relatórios** > **Exibir/Executar**.
2. Pesquise Anotações de segurança em **Meus relatórios** ou **Todos.**



Tópicos relacionados

Exibir a lista de Relatórios

Componentes instalados com Security Support Common

Vários tipos de componentes são instalados com Security Support Common. Eles fornecem funcionalidade comum para uso em várias aplicações de segurança, como Security Incident Response.

Localizando e exibindo componentes instalados

Consulte Exibir componentes instalados com Security Support Common mais informações sobre como localizar e exibir componentes instalados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Exibir componentes instalados com Security Support Common

Vários tipos de componentes são instalados quando você ativa o plug-in Security Support Common, incluindo, entre outros, tabelas, funções de usuário e módulos.

Localizando componentes

Nota:
A tabela Arquivos da Aplicação lista os componentes que são instalados com esta aplicação. Para obter instruções sobre como acessar esta tabela, consulte Encontrar componentes instalados com uma aplicação .

Se você quiser limitar a lista de componentes instalados a funções, trabalhos programados e tabelas para a aplicação Security Support Common, siga estas etapas:

Exibir listas filtradas de componentes instalados com uma aplicação

Filtre a tabela Arquivos de aplicações para que somente as funções, os trabalhos programados e as tabelas que são instaladas com uma aplicação sejam exibidos. A aplicação para a qual você deseja exibir esses componentes deve ser instalada para que seus arquivos sejam carregados na instância e na tabela de metadados. Siga estas etapas para exibir listas filtradas da tabela Arquivos de aplicações.

1. No navegador de filtros, insira **sys_metadata.list** para navegar até a tabela de metadados.
2. Selecione o construtor de condição (ícone de filtro) e selecione, **Aplicação** > **é** seguido pelo nome da sua aplicação.
3. No construtor de condição, para adicionar um segundo filtro, clique em **E**e selecione, **Classe** > **é um** e escolha uma das seguintes classes na lista: **Função**, **Trabalho programado**ou **Tabela**.
4. Selecione **Executar**.

Os resultados da classe selecionada são exibidos em uma lista filtrada.

[store-future: BEGIN review]

Acesso ao módulo por função para aplicações Security Operations

Para cada aplicação, consulte os itens de menu que podem ser acessados por uma função específica.

[End]
[store-future: BEGIN review]

Acesso ao módulo por função do Configuration Compliance

Para o Configuration Compliance, consulte os itens de menu que podem ser acessados por uma função específica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

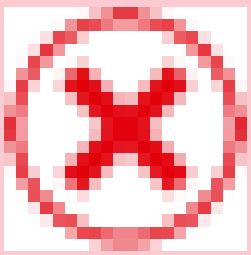
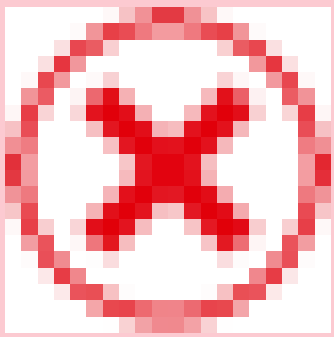
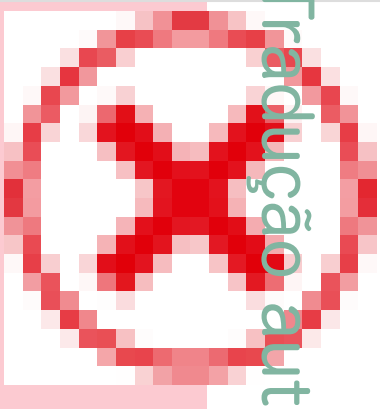
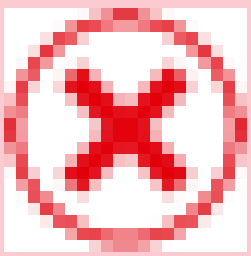
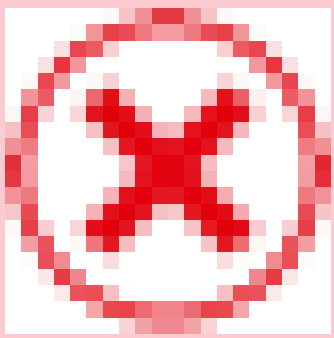
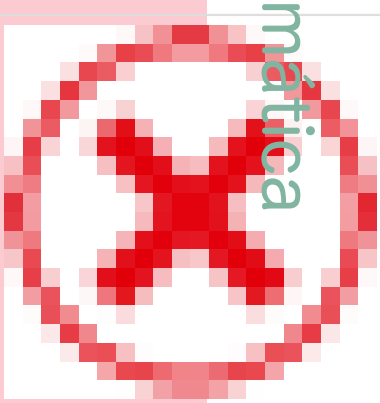
Acesso ao módulo para: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Acesso ao módulo para: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informações para outras funções:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

Módulo	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	s
(Grupo de apps principal)					
Visão geral					
Políticas					

Tradução automática

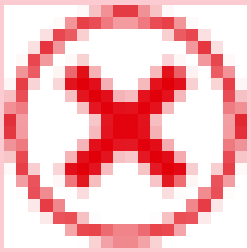
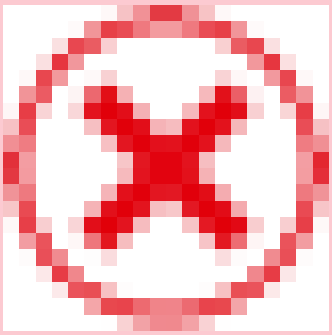
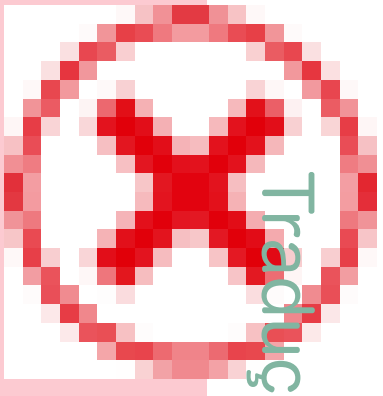
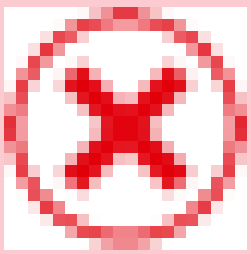
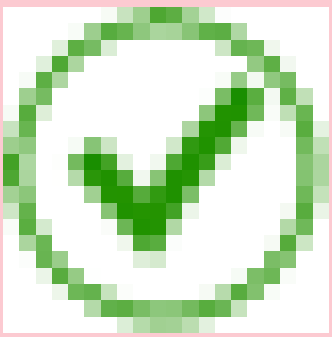
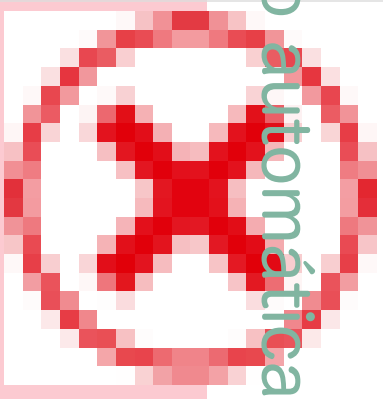
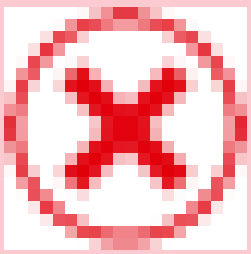
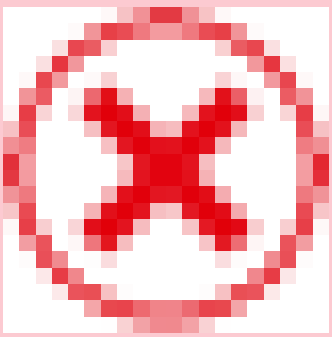
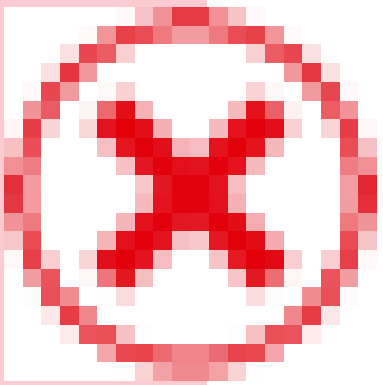
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informações para outras funções:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

Módulo	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules
Testes				
Minhas aprovações				
Resultados de testes				
Resultados de testes sem Triagem				

Tradução automática

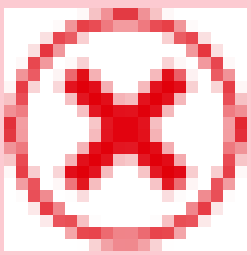
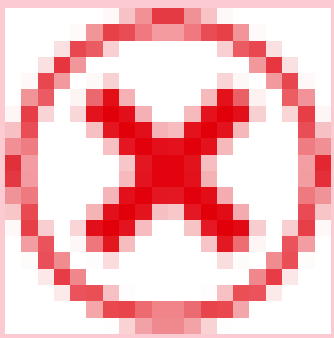
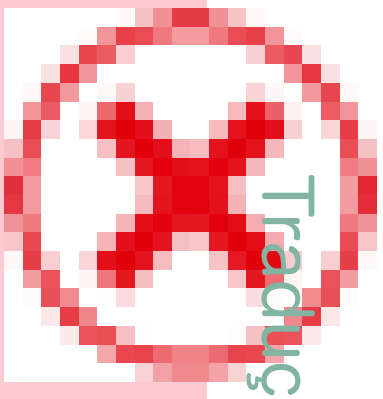
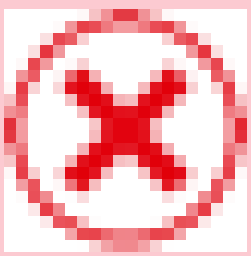
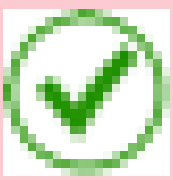
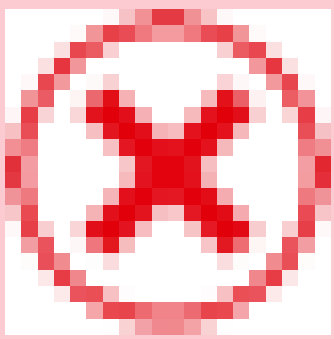
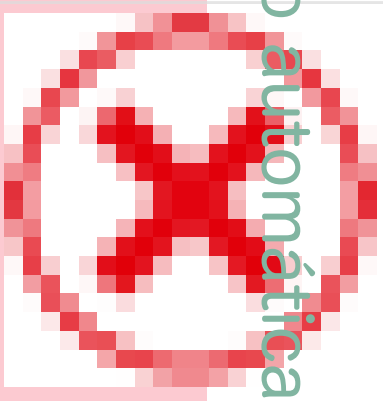
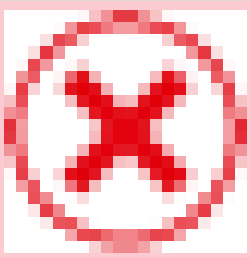
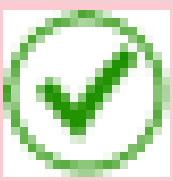
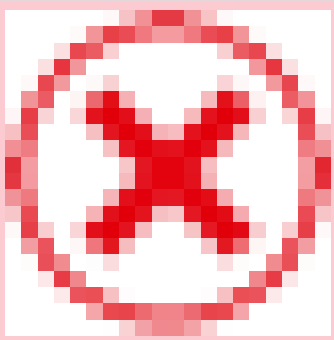
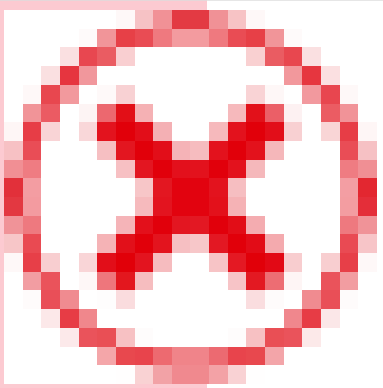
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informações para outras funções:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

Módulo	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules
Meus Resultados de testes em Aberto				
Resultados de testes em Aberto				
Perto da meta				

Tradução automática

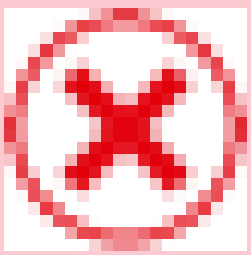
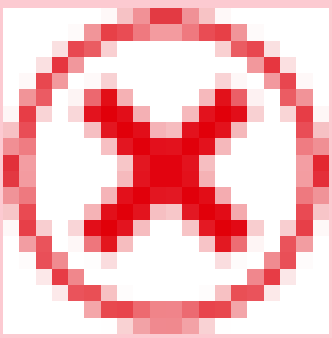
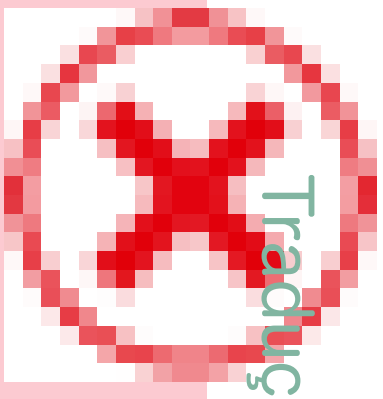
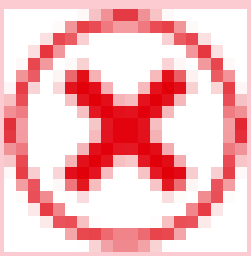
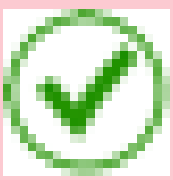
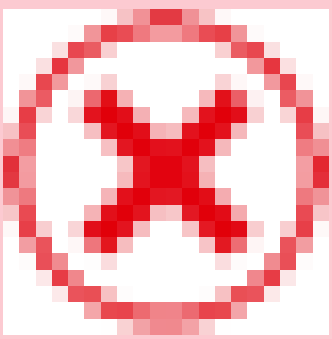
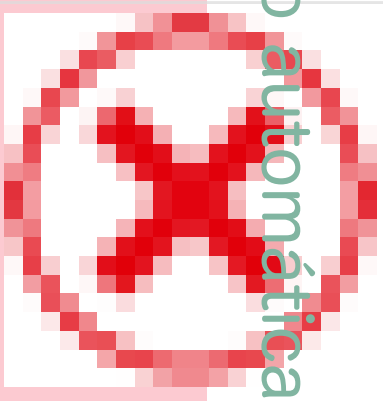
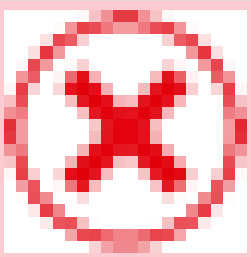
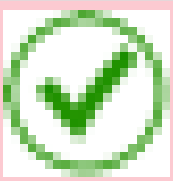
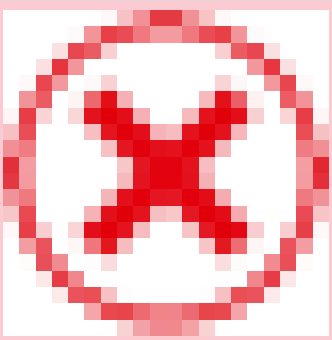
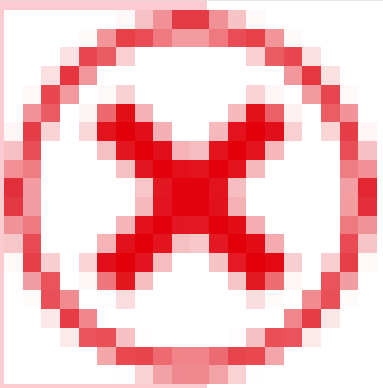
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informações para outras funções:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

Módulo	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules	s
Meta não atingida					
Não designado					
Vários adiamentos					

Tradução automática

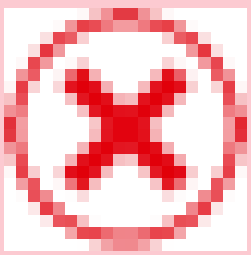
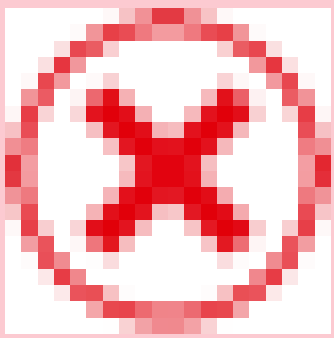
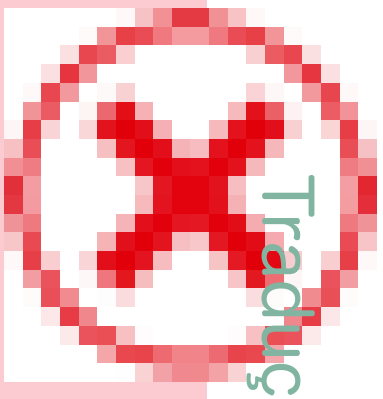
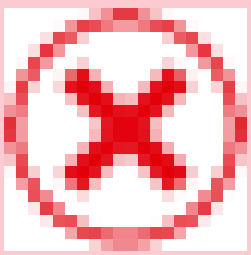
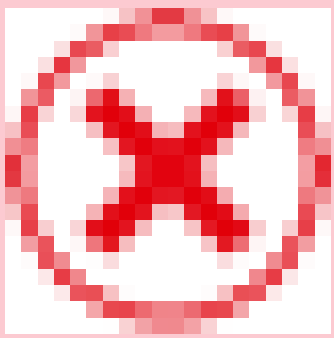
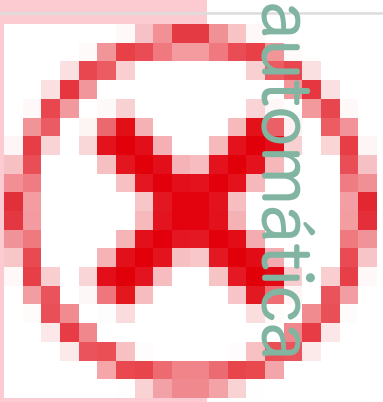
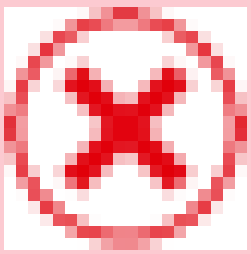
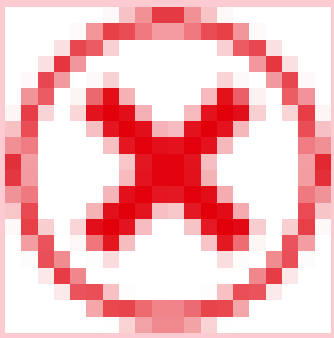
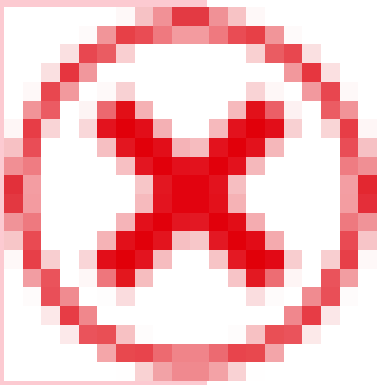
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informações para outras funções:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

Módulo	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules
Todos				
Grupos de resultados de testes				
Meus Grupos Abertos				
Todos os Grupos Abertos				

Tradução automática

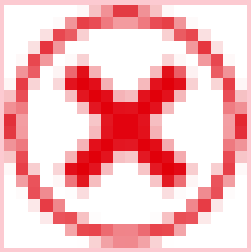
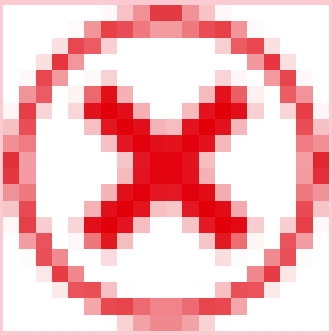
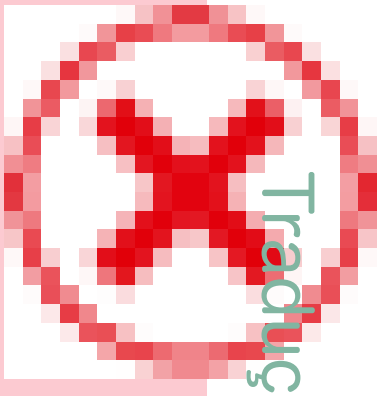
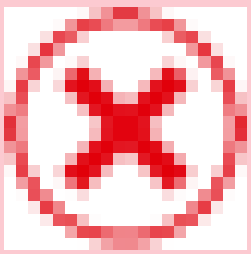
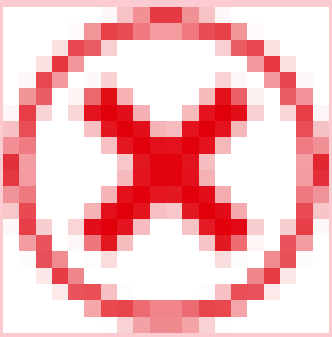
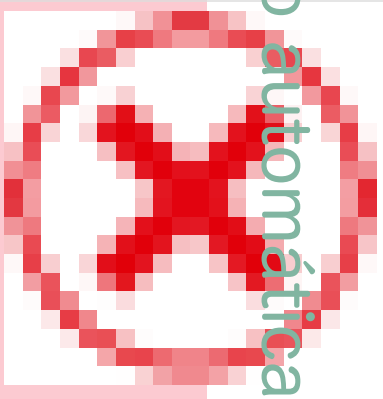
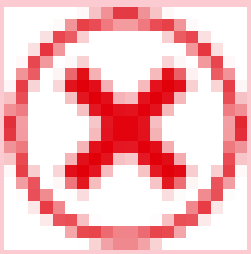
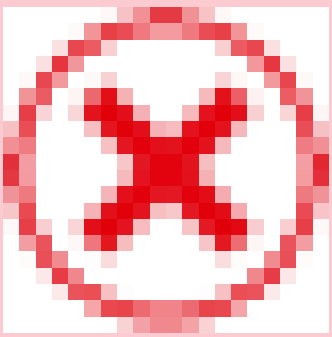
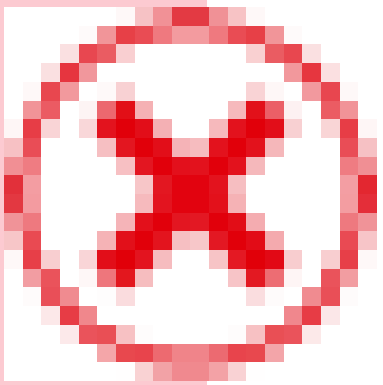
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informações para outras funções:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

Módulo	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules
Vários adiamentos				
Todos os Grupos				
Dados de suporte				
Fontes Autorizadas				

Tradução automática

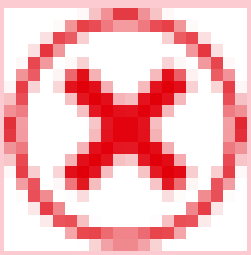
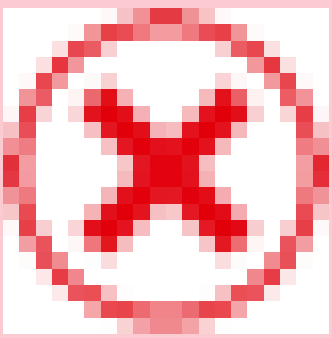
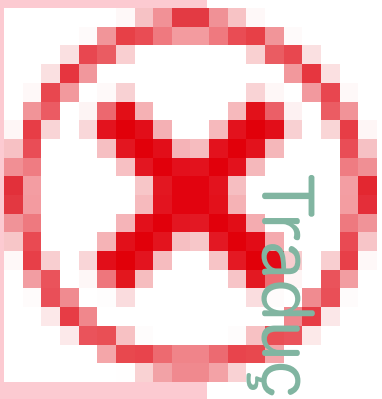
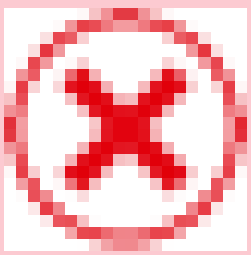
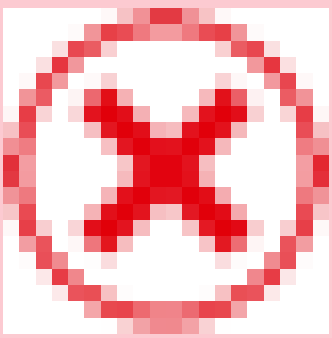
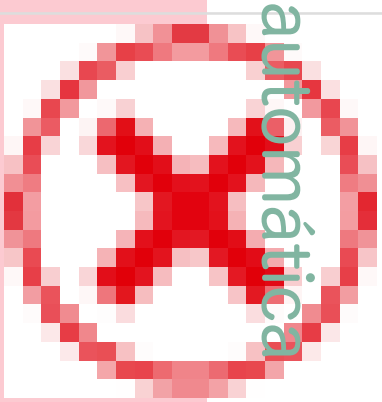
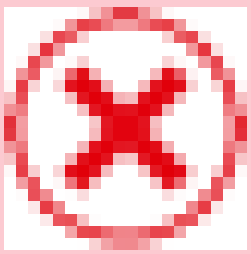
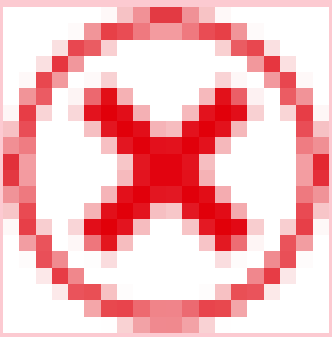
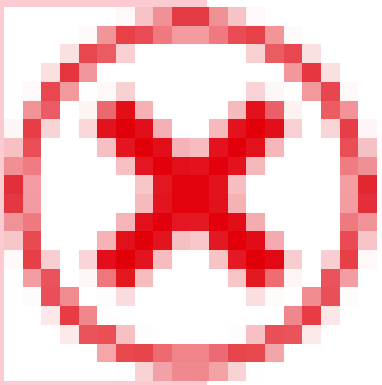
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informações para outras funções:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

Módulo	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules
Tecnologias				
Administração				
Regras de atribuição				
Fechar automaticamente resultados de testes obsoletos				

Tradução automática

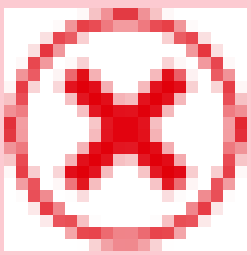
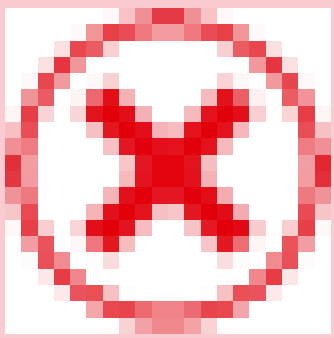
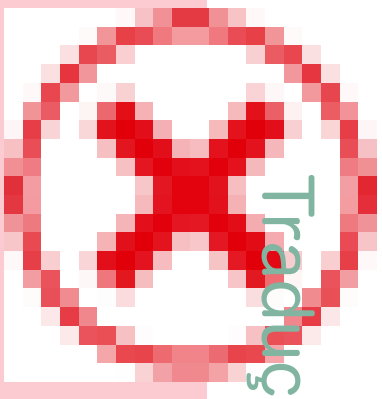
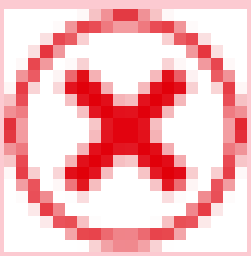
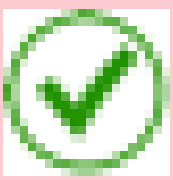
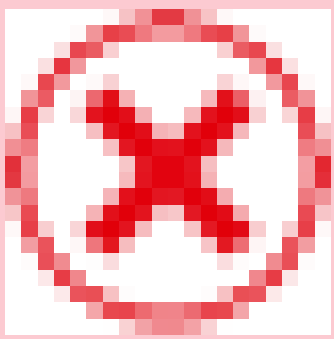
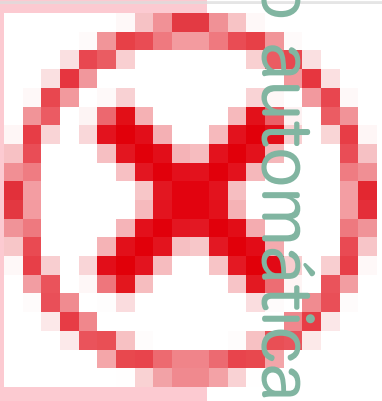
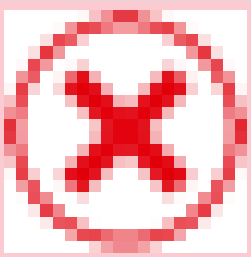
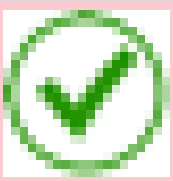
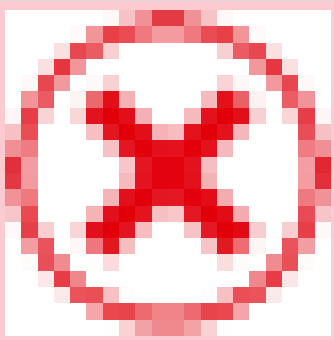
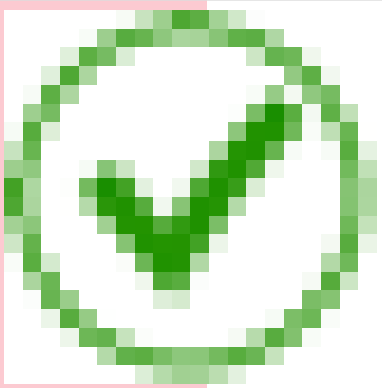
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informações para outras funções:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

Módulo	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules
Regras de Grupo				
Regra de exceção automática				
Regras de aprovação				

Tradução automática

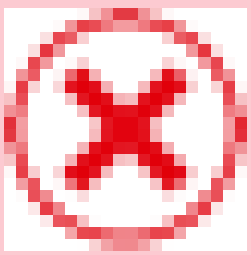
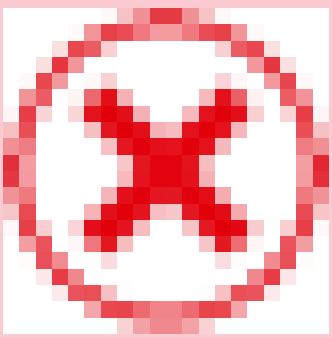
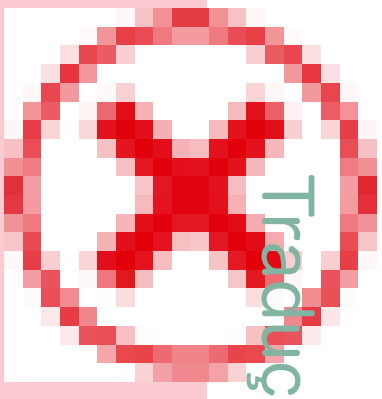
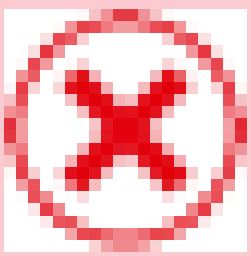
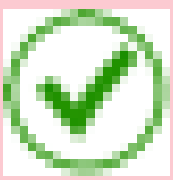
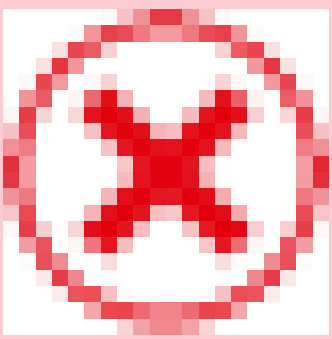
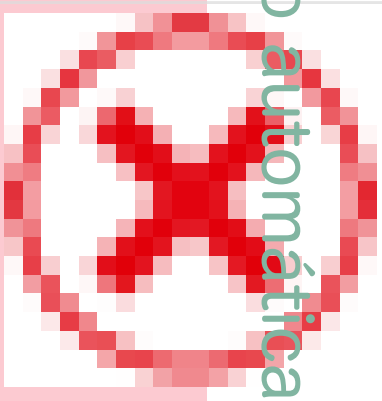
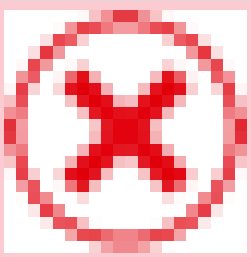
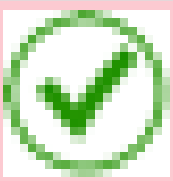
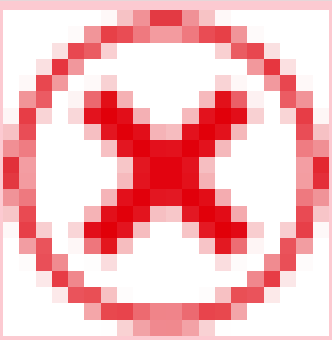
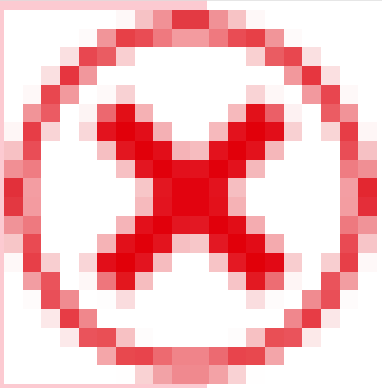
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informações para outras funções:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

Módulo	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules
Calculadoras de Risco				
Calculadoras de acúmulo de pontuação de risco				
Regras de destino de correção				

Tradução automática

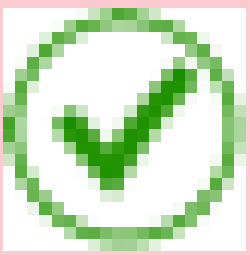
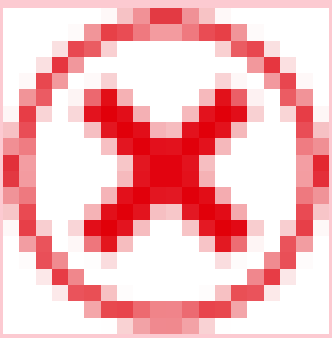
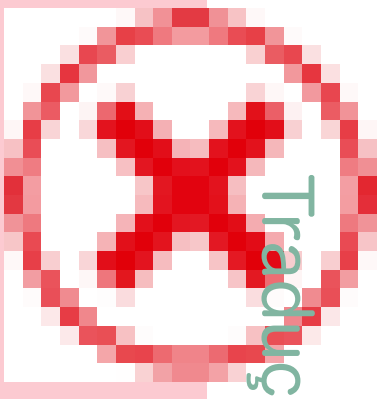
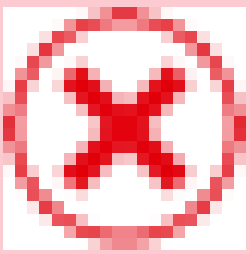
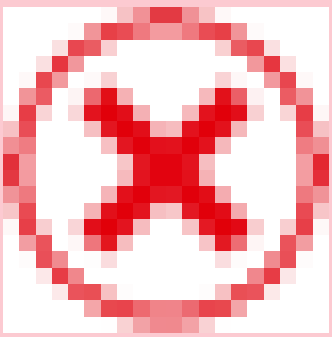
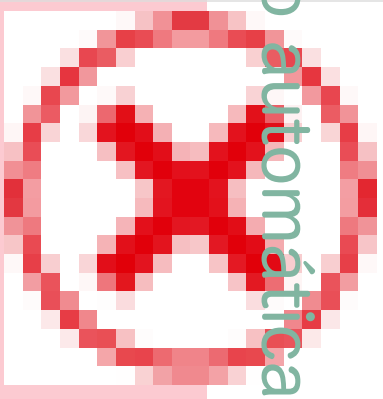
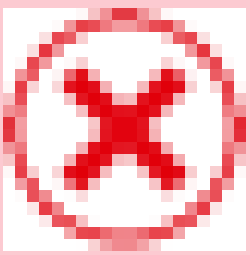
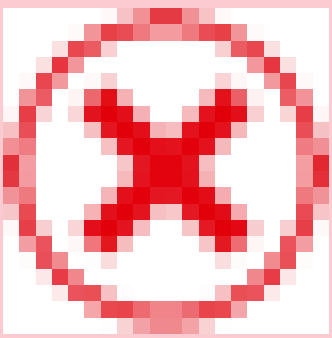
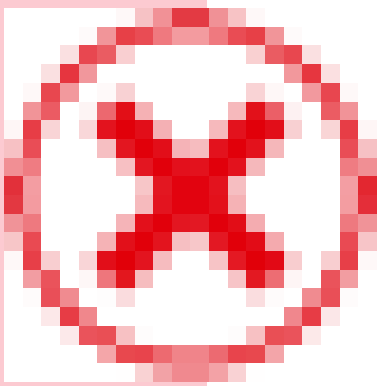
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

Informações para outras funções:

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

sn_vulc.remediation_owner

Módulo	sn_vul_qualys.admin	sn_vulc.admin	sn_vulc.exception_approver	sn_vulc.manage_approval_rules
Mapeamento de Criticalidade				
Notificações				
Gestão de exceção				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
(Grupo de apps principal)				
Visão geral	✗	✗	✓	
Políticas	✗	✗	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
Testes	✗	✗	✓	✗
Minhas aprovações	✗	✗	✗	✗

Resultados de testes

Tradução automática

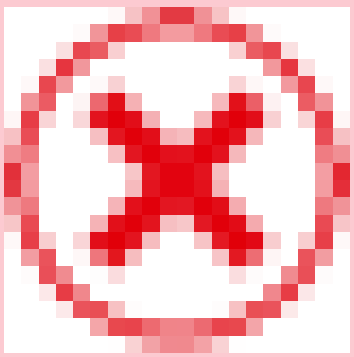
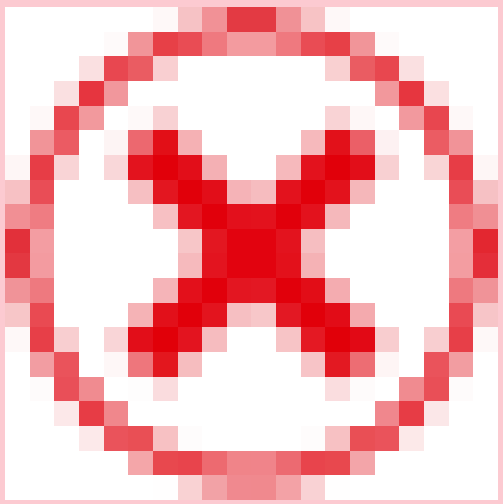
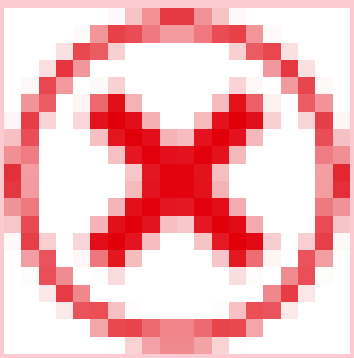
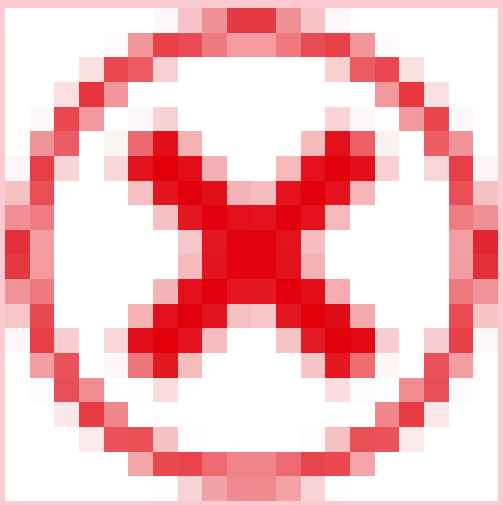
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
Resultados de testes sem Triagem				
Meus Resultados de testes em Aberto				

Tradução automática

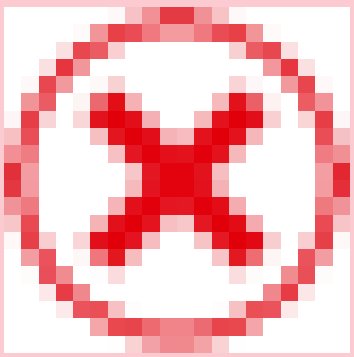
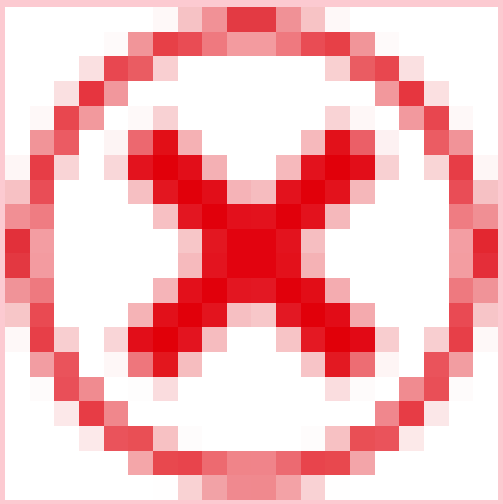
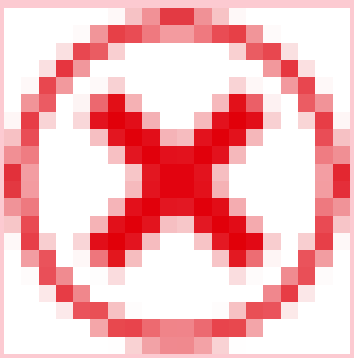
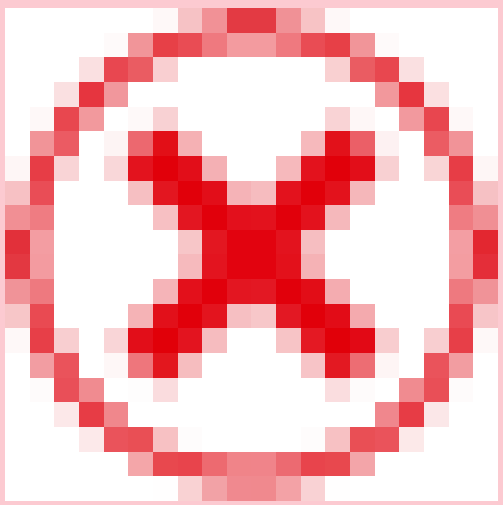
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
Resultados de testes em Aberto				
Perto da meta				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
Meta não atingida	✗	✗	✓	✗
Não designado	✗	✗	✓	✗

Tradução automática

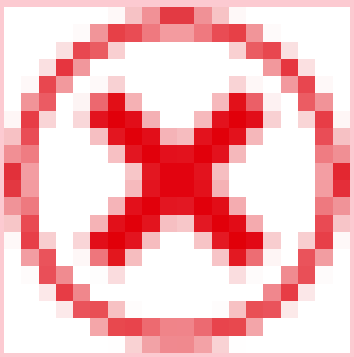
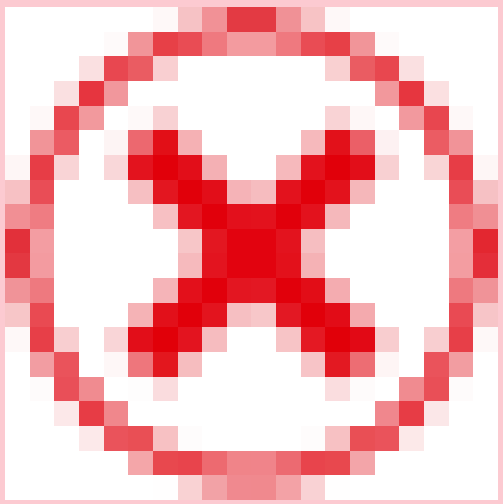
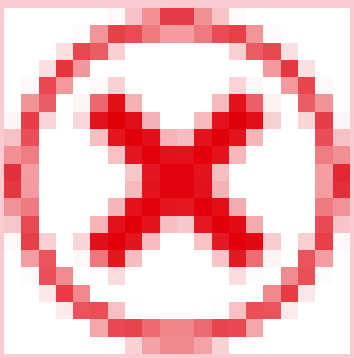
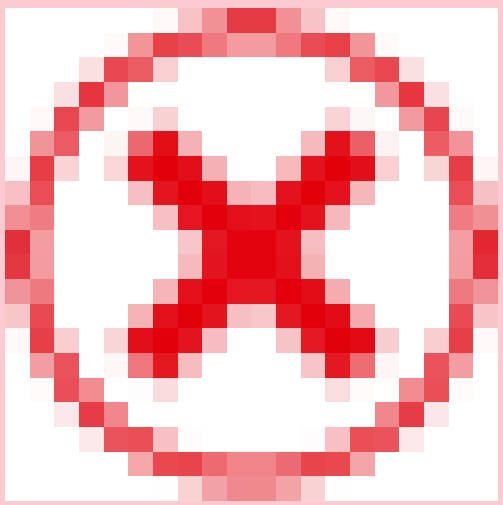
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
Vários adiamentos				
Todos				

Grupos de resultados de testes

Tradução automática

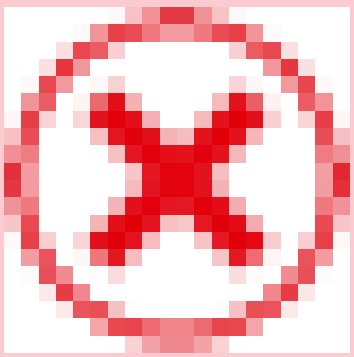
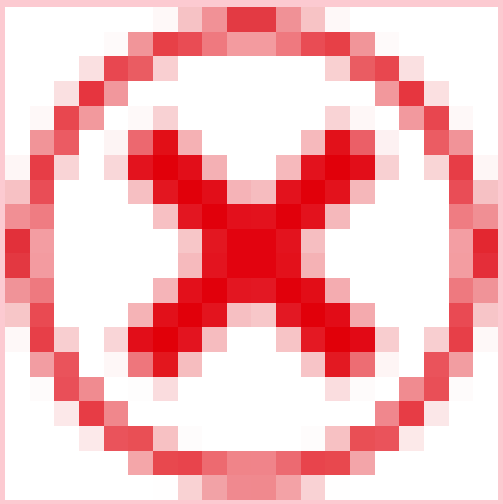
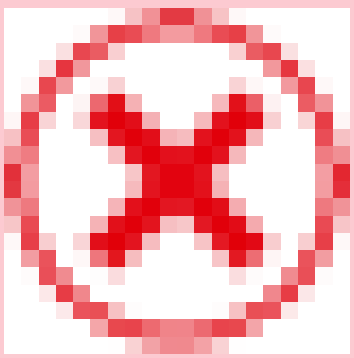
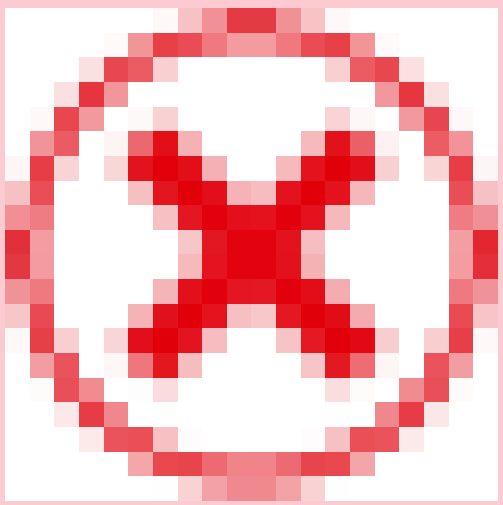
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
Meus Grupos Abertos				
Todos os Grupos Abertos				

Tradução automática

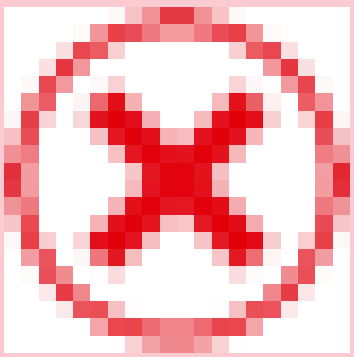
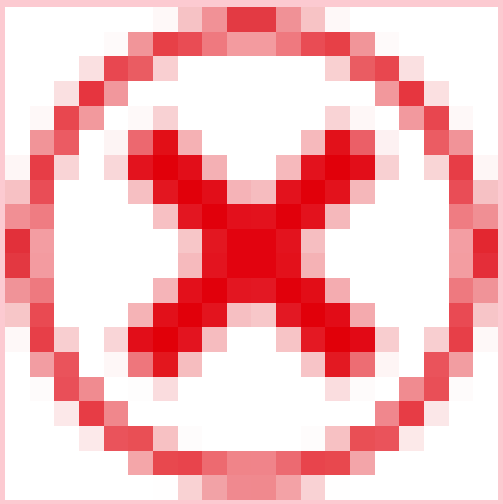
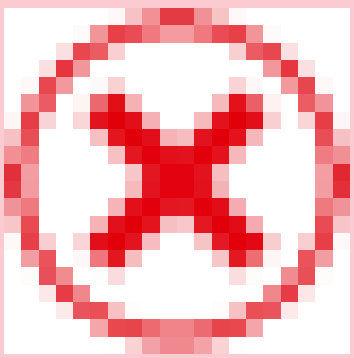
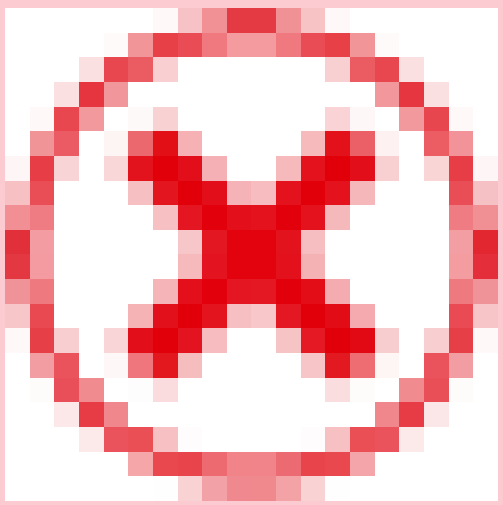
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
Vários adiamentos				
Todos os Grupos				
Dados de suporte				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
Fontes Autorizadas	✗	✗	✓	
Tecnologias	✗	✗	✓	
Administração				

Tradução automática

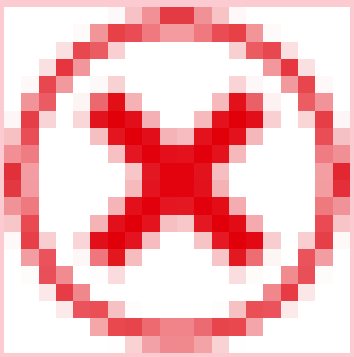
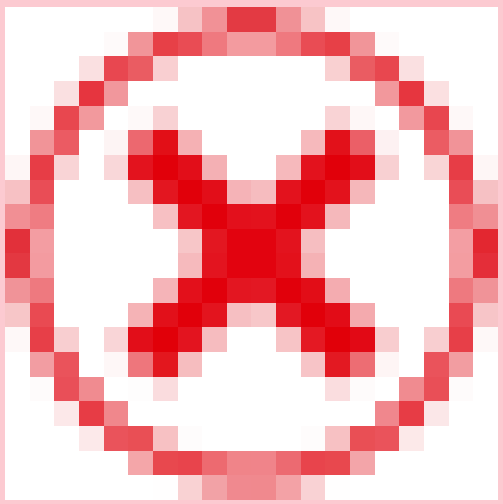
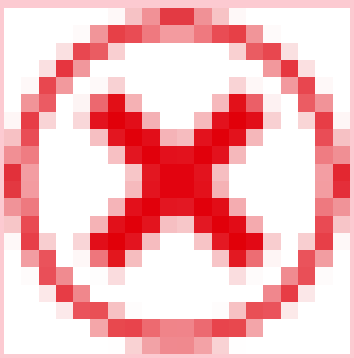
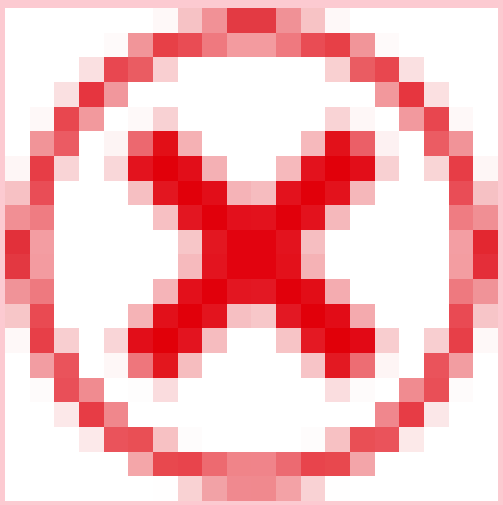
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
Regras de atribuição				
Fechar automaticamente resultados de testes obsoletos				

Tradução automática

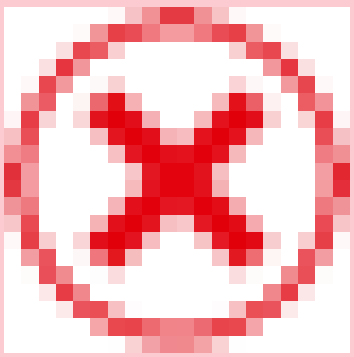
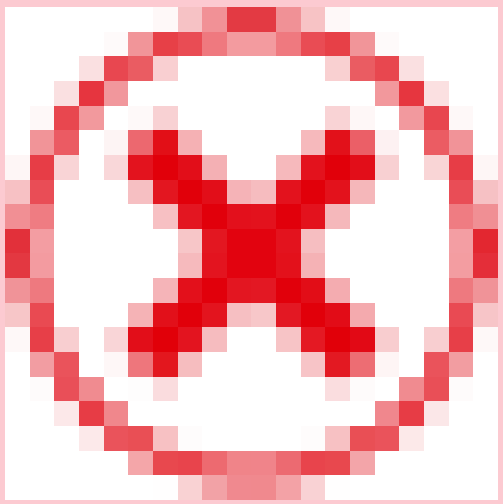
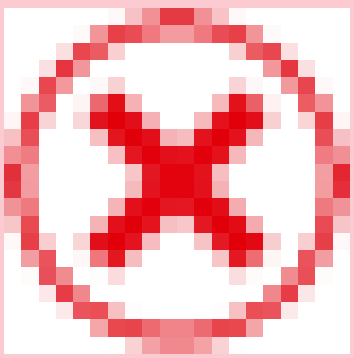
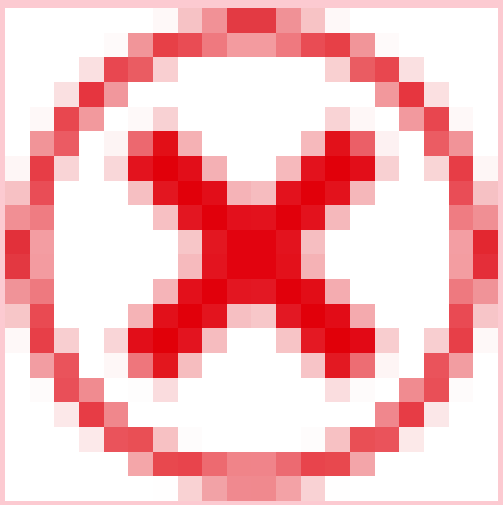
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
Regras de Grupo				
Regra de exceção automática				

Tradução automática

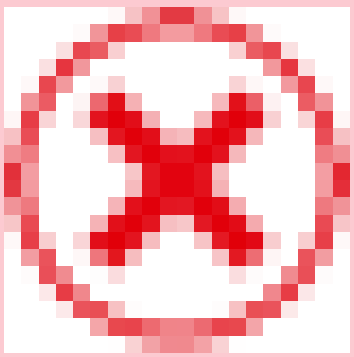
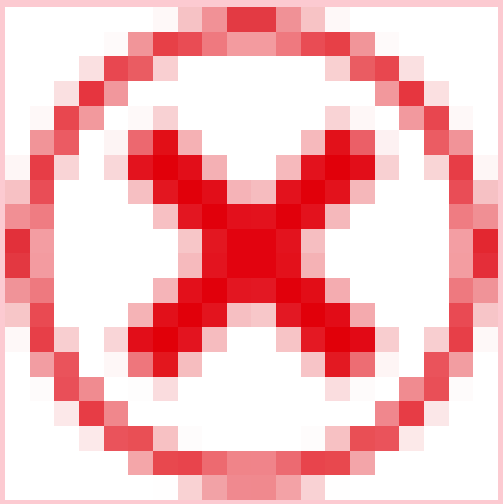
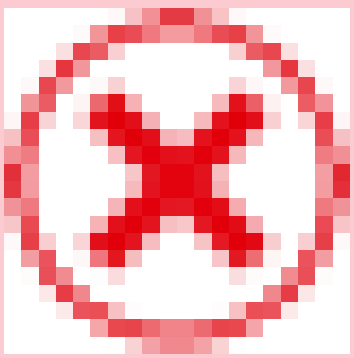
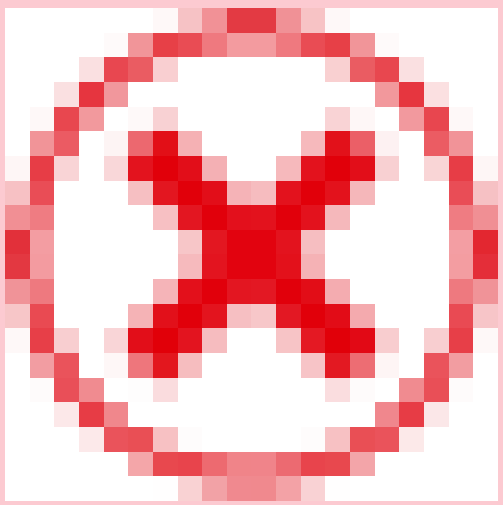
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
Regras de aprovação				
Calculadoras de Risco				

Tradução automática

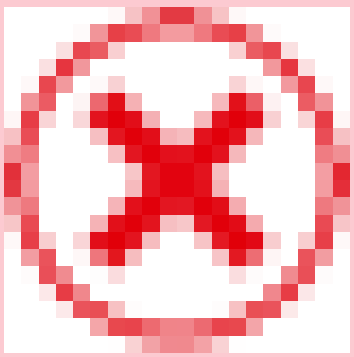
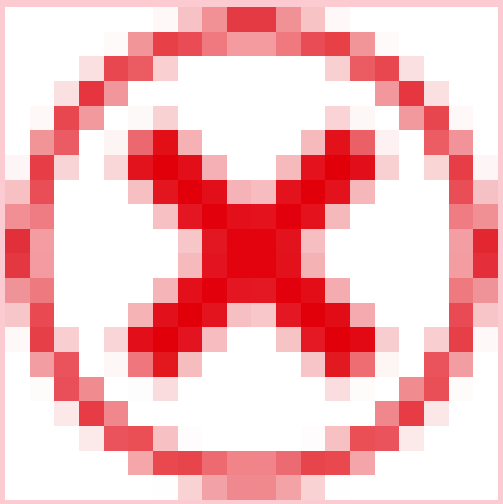
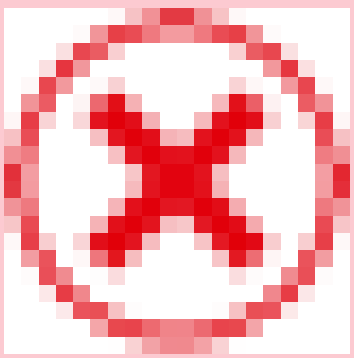
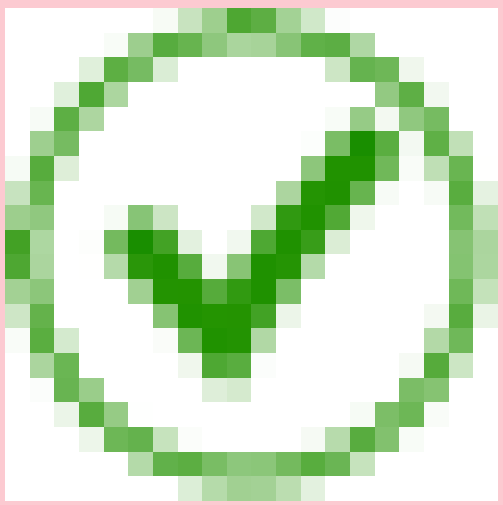
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
Calculadoras de acúmulo de pontuação de risco				
Regras de destino de correção				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
Mapeamento de Criticalidade	✗	✗	✗	✗
Notificações	✓	✗	✗	✗

Tradução automática

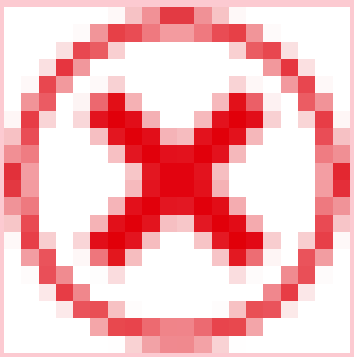
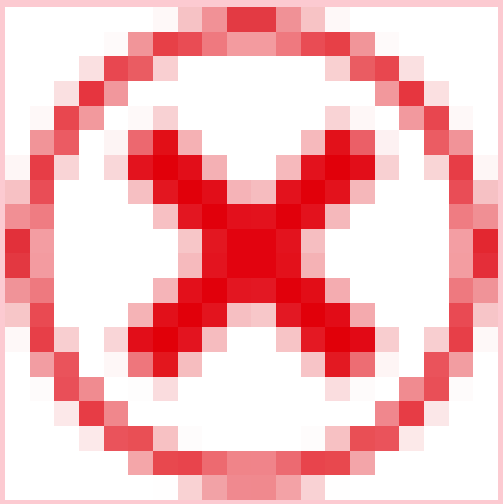
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.remediation_owner

Módulo	sn_vulc.manage_notifications	sn_vulc.manage_remediation_target_rules	sn_vulc.read	sn_vulc.read
Gestão de exceção				

Tradução automática

Acesso ao módulo para: sn_vulc.remediation_owner

Acesso ao módulo para: sn_vulc.remediation_owner

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Módulo	sn_vulc.remediation_owner
(Grupo de apps principal)	

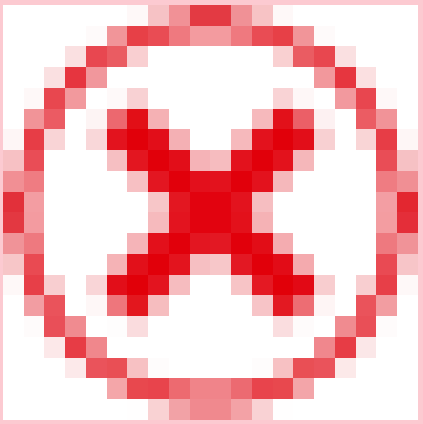
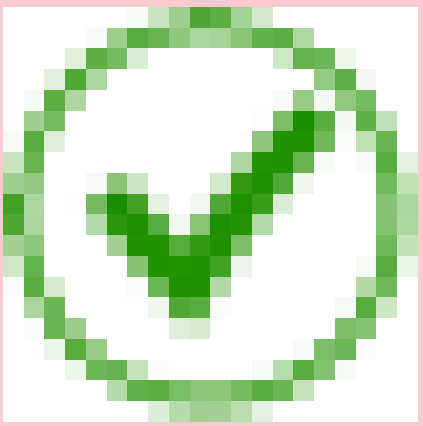
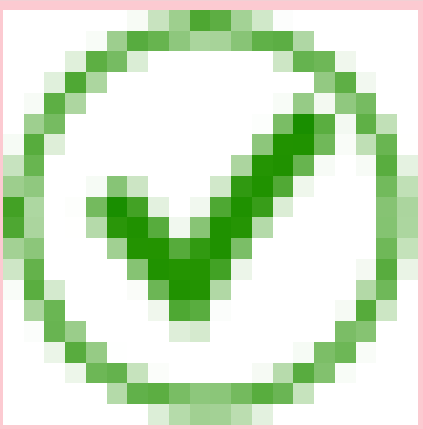
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.remediation_owner

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Módulo	sn_vulc.remediation_owner
Visão geral	
Políticas	
Testes	

Tradução automática

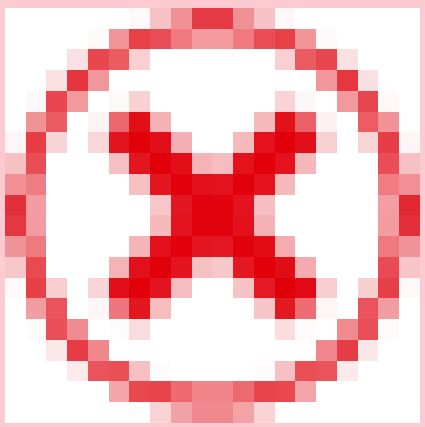
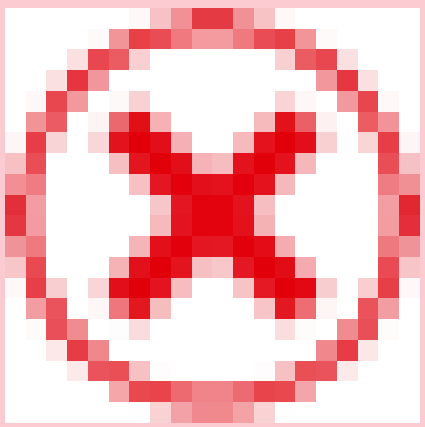
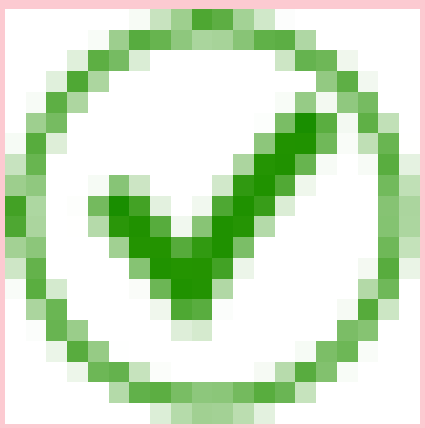
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.remediation_owner

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Módulo	sn_vulc.remediation_owner
Minhas aprovações	
Resultados de testes	
Resultados de testes sem Triagem	
Meus Resultados de testes em Aberto	

Tradução automática

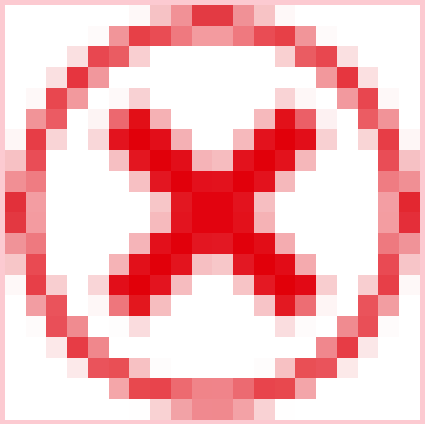
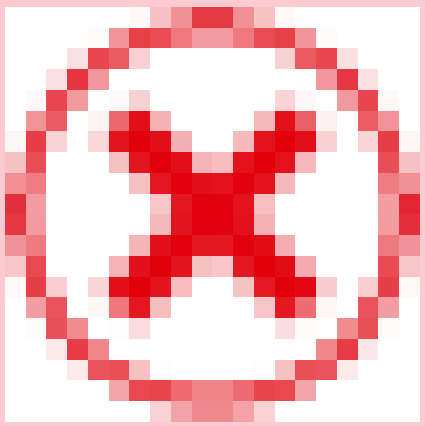
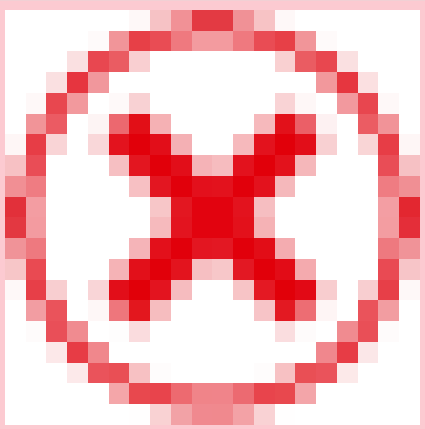
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.remediation_owner

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Módulo	sn_vulc.remediation_owner
Resultados de testes em Aberto	
Perto da meta	
Meta não atingida	

Tradução automática

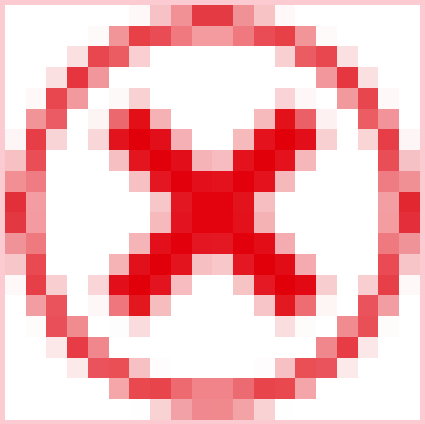
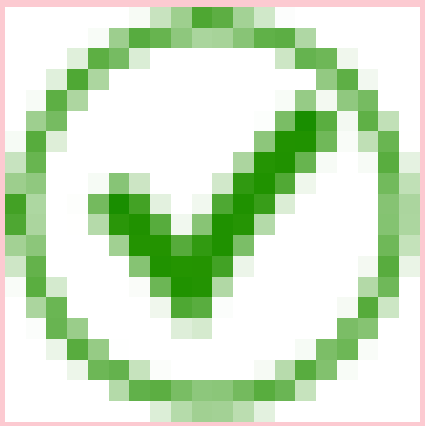
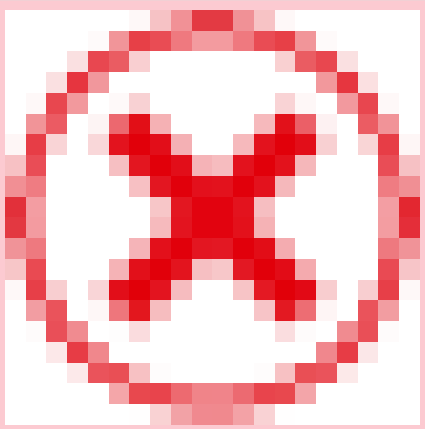
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.remediation_owner

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Módulo	sn_vulc.remediation_owner
Não designado	
Vários adiamentos	
Todos	
Grupos de resultados de testes	

Tradução automática

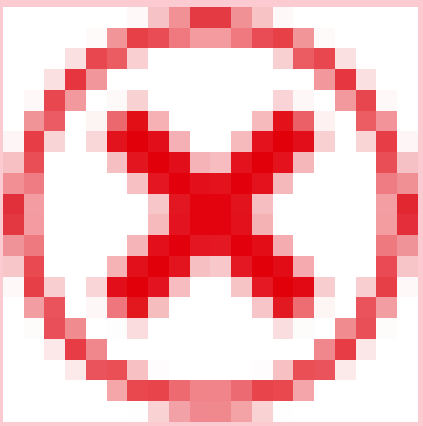
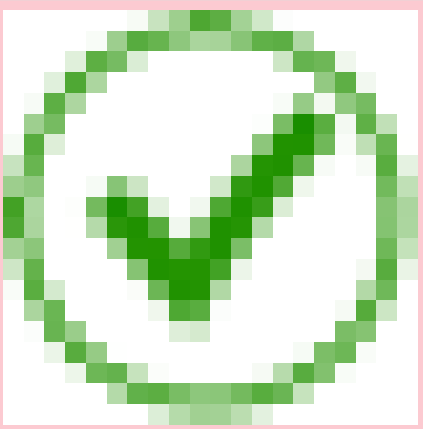
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.remediation_owner

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Módulo	sn_vulc.remediation_owner
Meus Grupos Abertos	
Todos os Grupos Abertos	
Vários adiamentos	

Tradução automática

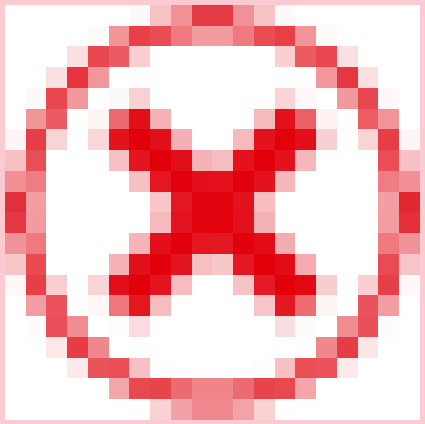
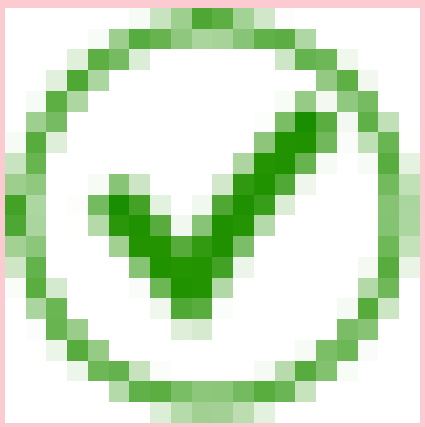
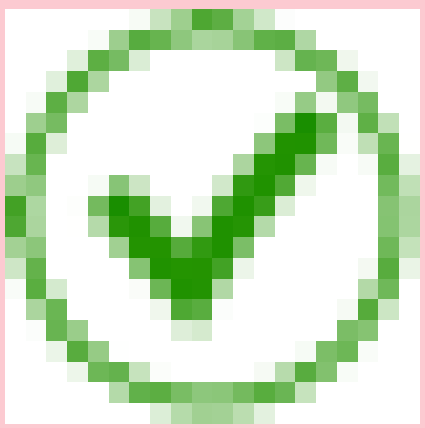
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.remediation_owner

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Módulo	sn_vulc.remediation_owner
Todos os Grupos	
Dados de suporte	
Fontes Autorizadas	
Tecnologias	
Administração	

Tradução automática

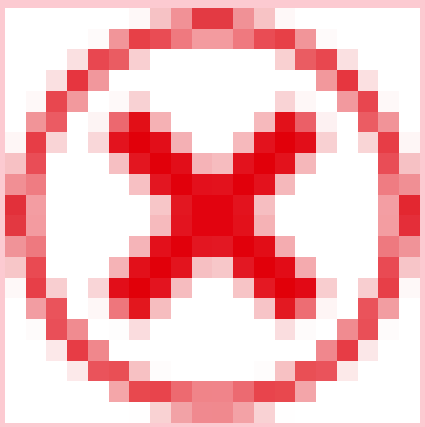
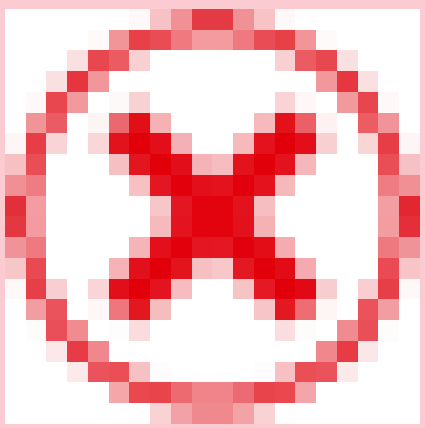
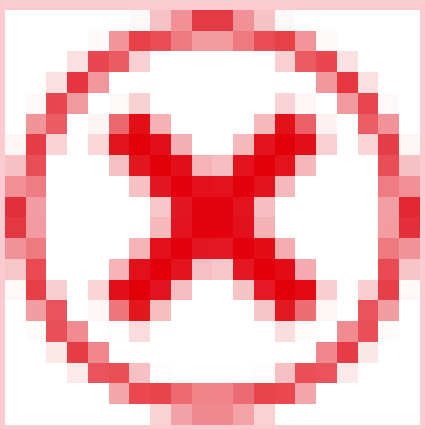
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.remediation_owner

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Módulo	sn_vulc.remediation_owner
Regras de atribuição	
Fechar automaticamente resultados de testes obsoletos	
Regras de Grupo	

Tradução automática

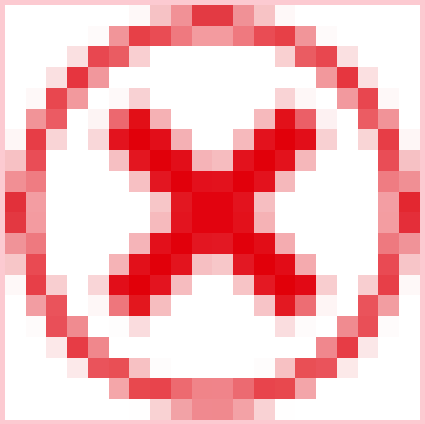
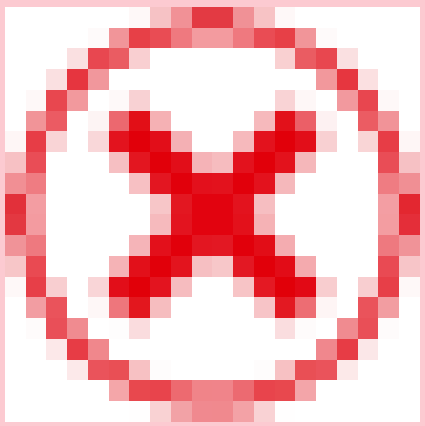
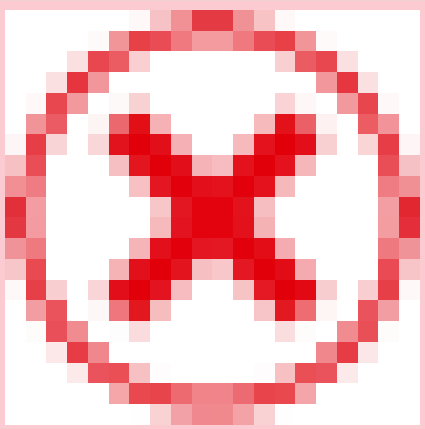
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.remediation_owner

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Módulo	sn_vulc.remediation_owner
Regra de exceção automática	
Regras de aprovação	
Calculadoras de Risco	

Tradução automática

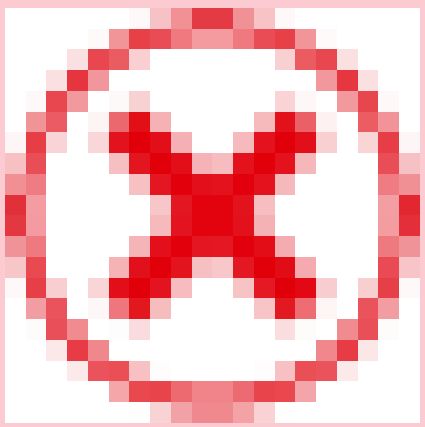
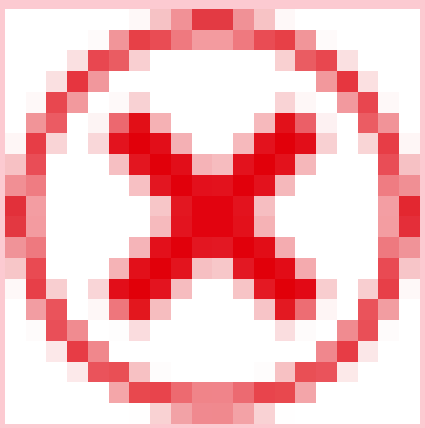
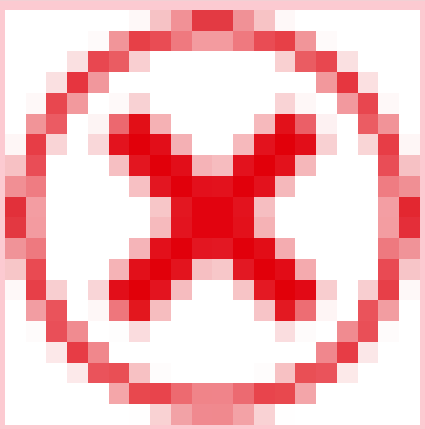
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.remediation_owner

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Módulo	sn_vulc.remediation_owner
Calculadoras de acúmulo de pontuação de risco	
Regras de destino de correção	
Mapeamento de Criticalidade	

Tradução automática

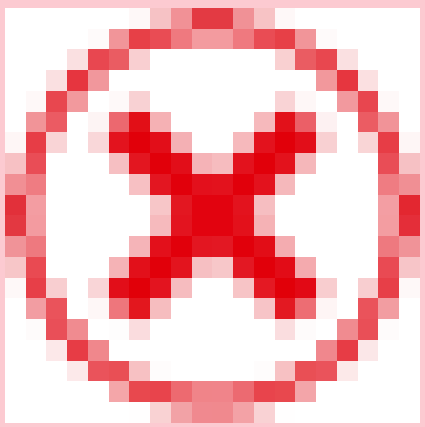
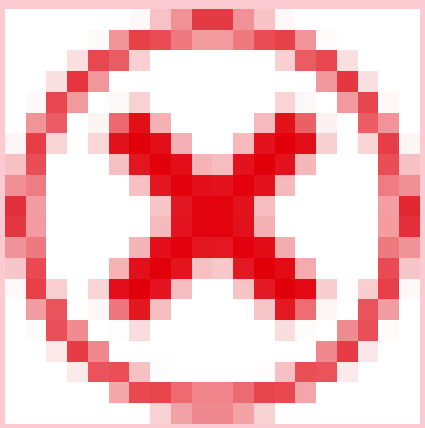
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vulc.remediation_owner

Informações para outras funções:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.exception_approver, sn_vulc.manage_approval_rules, sn_vulc.manage_auto_exception_rule

sn_vulc.manage_notifications, sn_vulc.manage_remediation_target_rules, sn_vulc.read, sn_vulc.read_remediation_target_rules

Módulo	sn_vulc.remediation_owner
Notificações	
Gestão de exceção	

[End]

[store-future: BEGIN review]

Acesso ao módulo por função do Vulnerability Response do contêiner

Para o Vulnerability Response do contêiner, consulte os itens de menu que podem ser acessados por uma função específica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

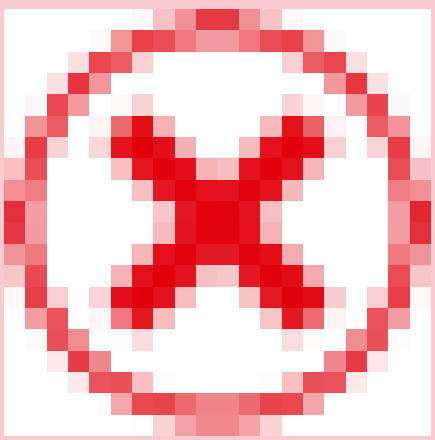
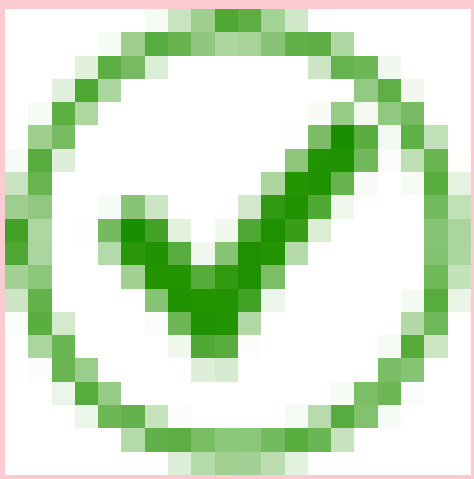
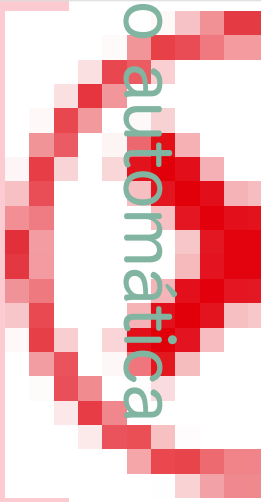
Informações para outras funções:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.conf
(Grupo de apps principal)			
Visão geral			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

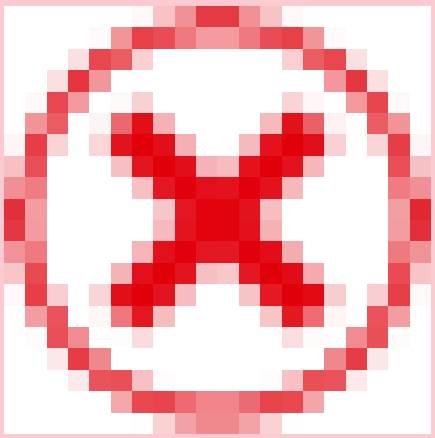
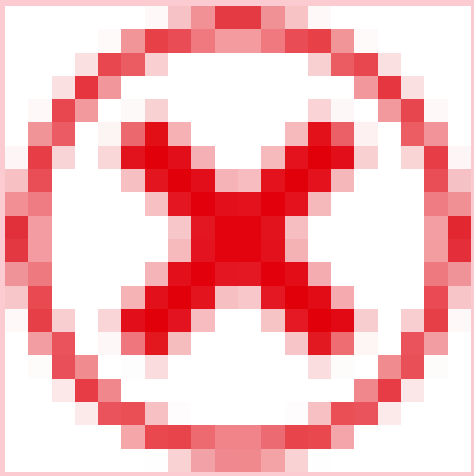
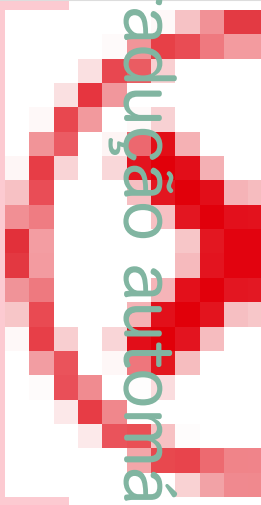
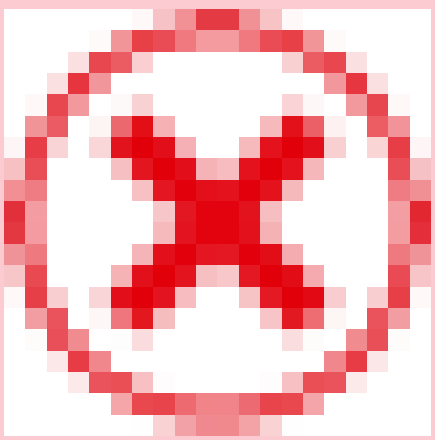
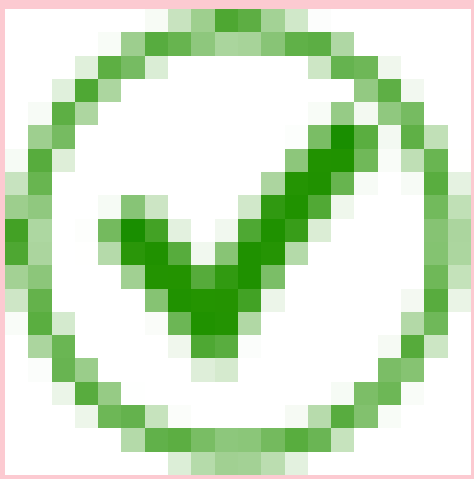
Informações para outras funções:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.conf
Minhas aprovações			
Itens vulneráveis de contêiner			
Atribuídos a Mim			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informações para outras funções:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.conf
Atribuído aos Meus grupos	✗	✓	✗
Risco crítico e alto	✗	✓	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

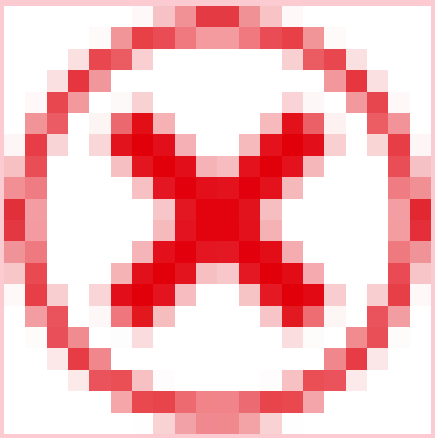
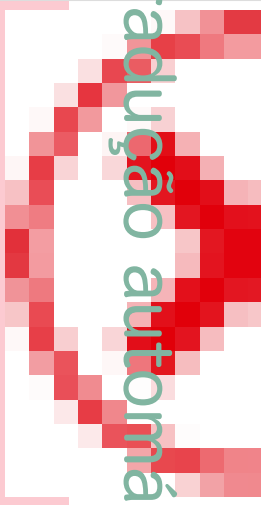
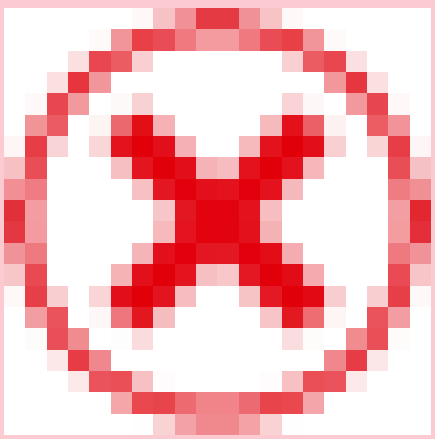
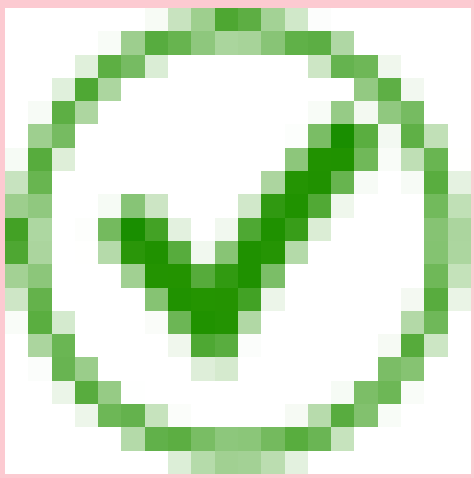
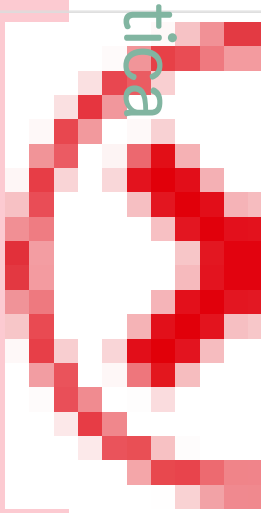
Informações para outras funções:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.conf
Explorável			
Perto da meta			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

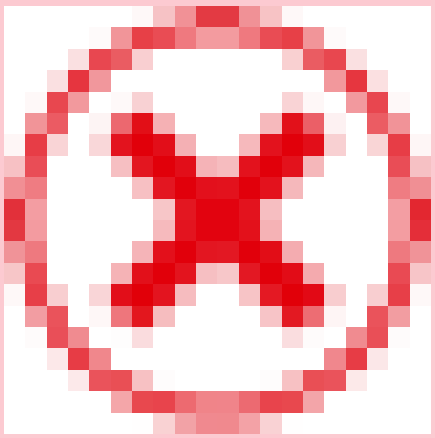
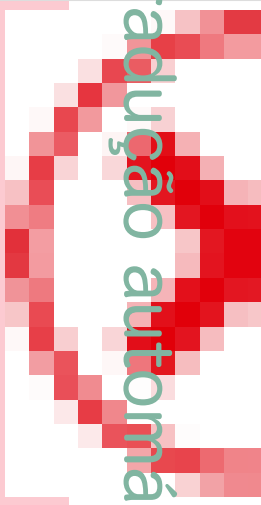
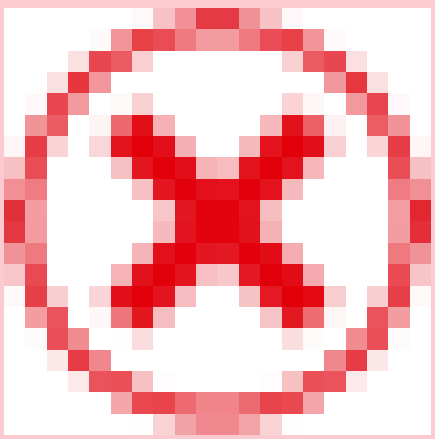
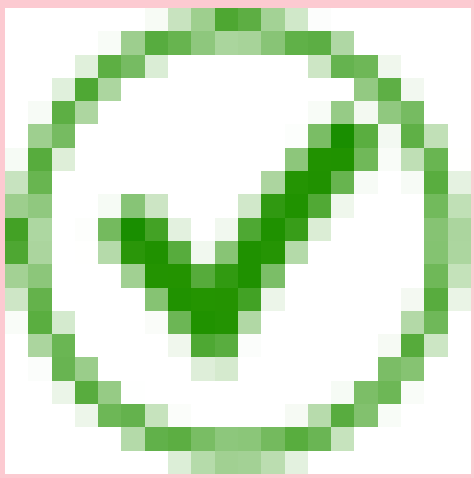
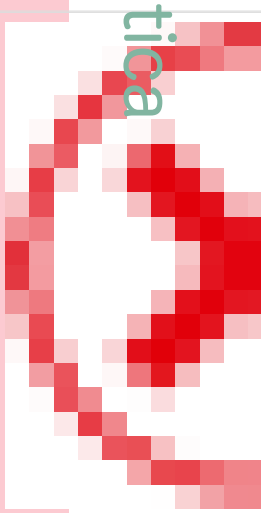
Informações para outras funções:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.conf
Meta não atingida			
Todos			
Bibliotecas			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

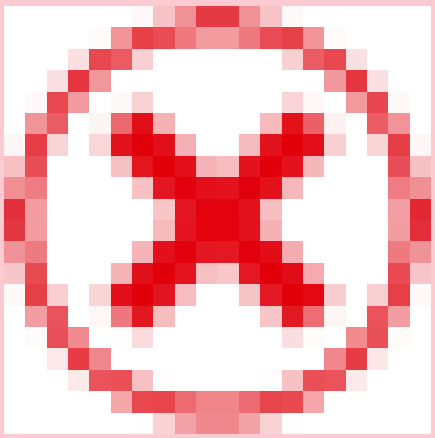
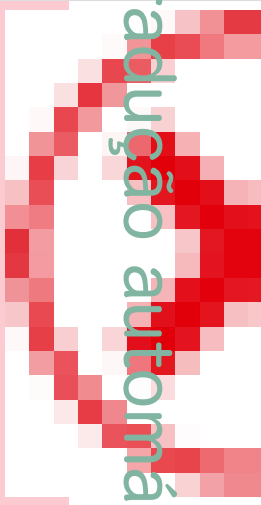
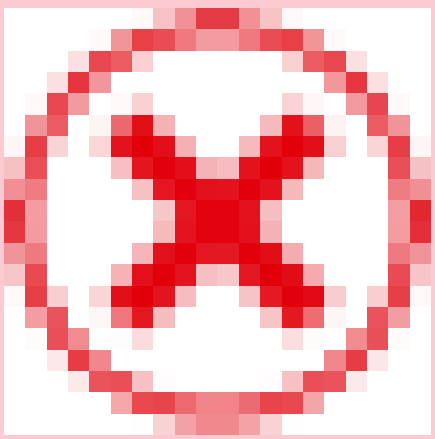
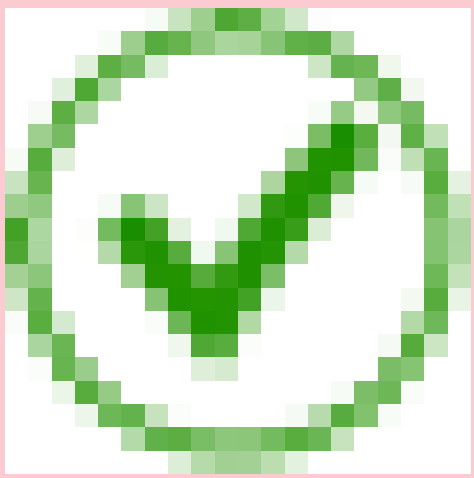
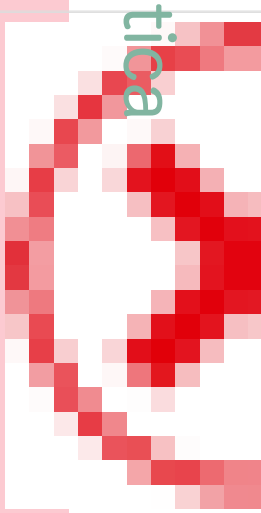
Informações para outras funções:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.conf
NVD			
Terceiros			
Administração			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informações para outras funções:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.conf
Regras de atribuição	✗	✗	✗
Calculadoras de vulnerabilidade	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informações para outras funções:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.conf
Regras de destino de correção	✗	✗	✗
Configurar granularidade de IV	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informações para outras funções:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.conf
Regras de exceção	✗	✗	✗
Regras de aprovação	✓	✓	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

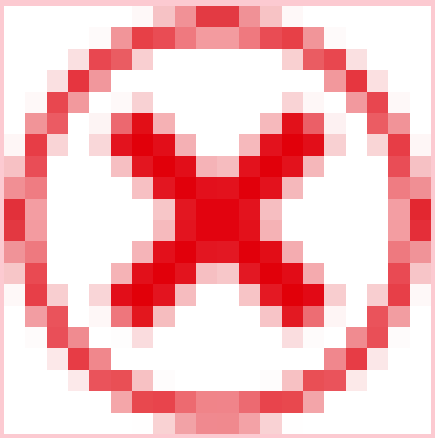
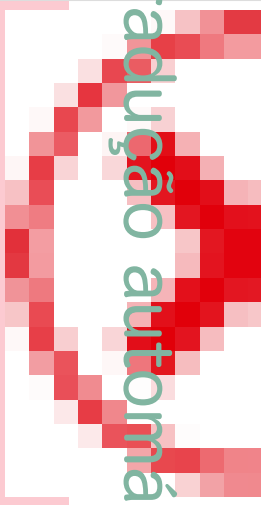
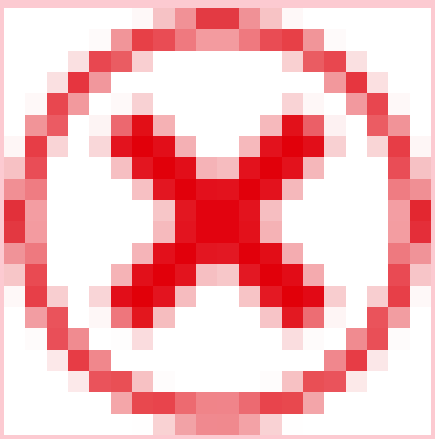
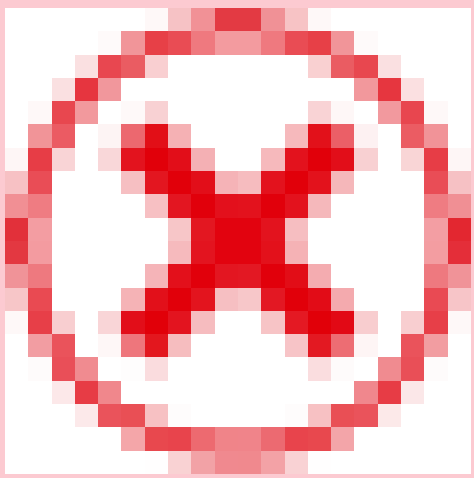
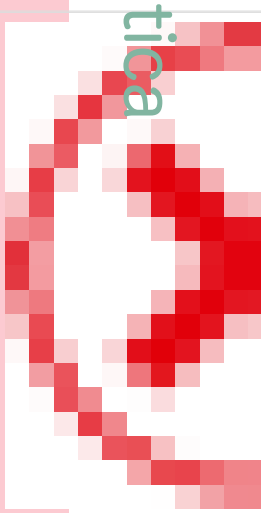
Informações para outras funções:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.conf
Integrações de segurança do contêiner			
Fechar automaticamente itens vulneráveis			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

Informações para outras funções:

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul_container.configure_integrations	sn_vul_container.conf
Mapas de Gravidade Normalizados	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

Acesso ao módulo para: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

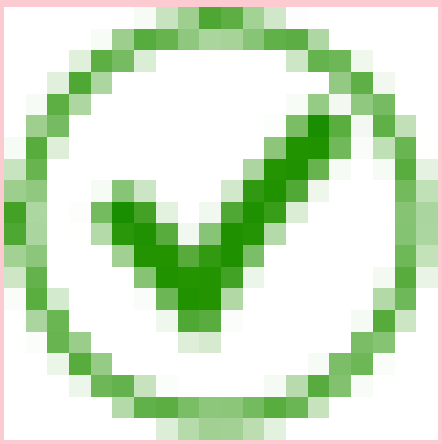
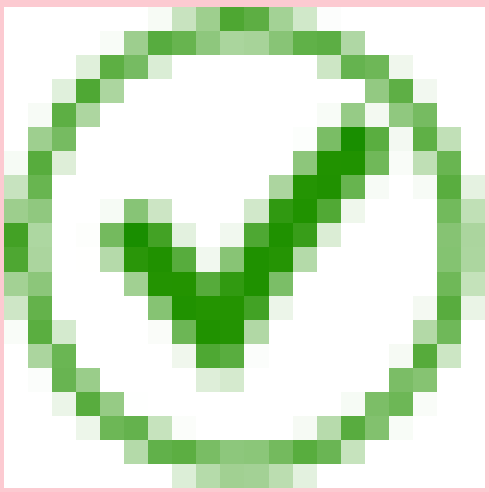
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.ma
(Grupo de apps principal)			
Visão geral			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

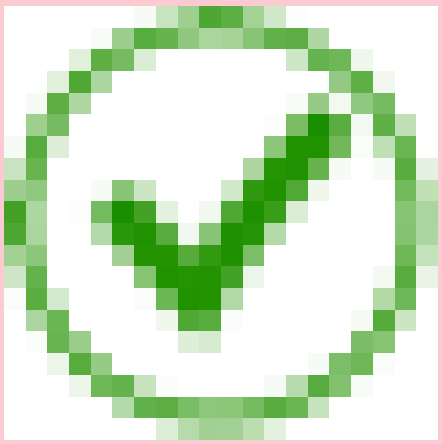
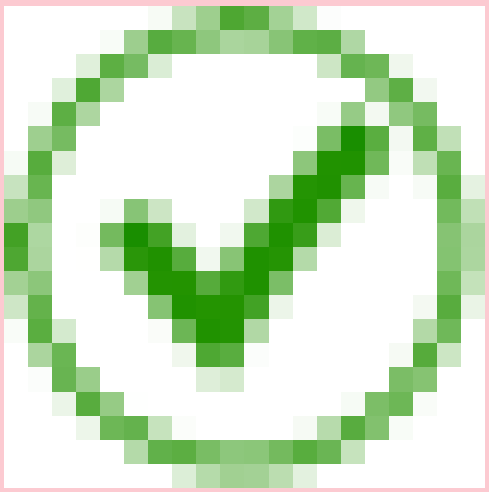
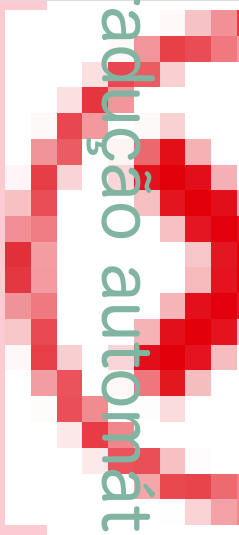
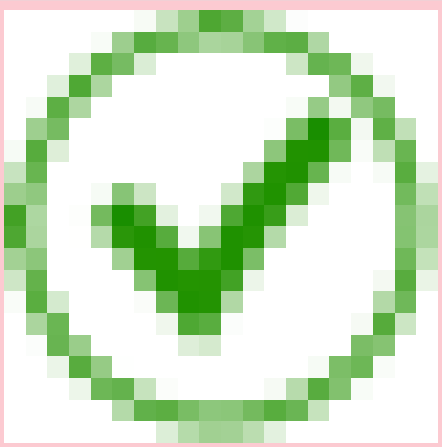
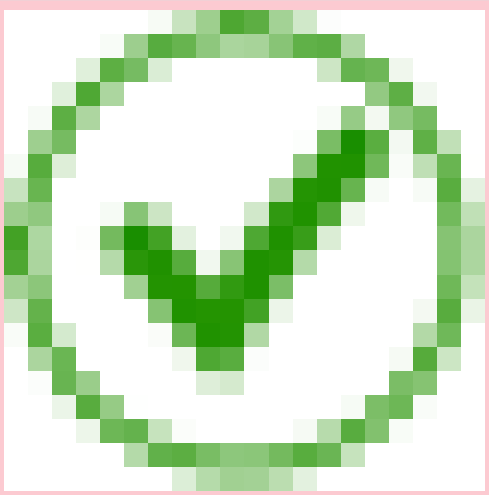
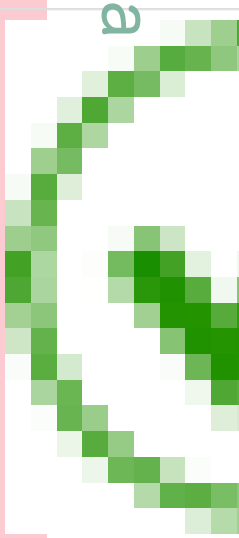
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.ma
Minhas aprovações			
Itens vulneráveis de contêiner			
Atribuídos a Mim			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

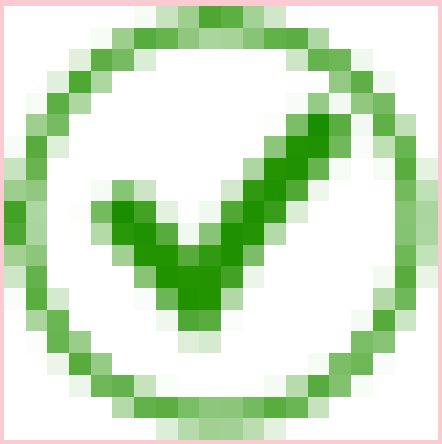
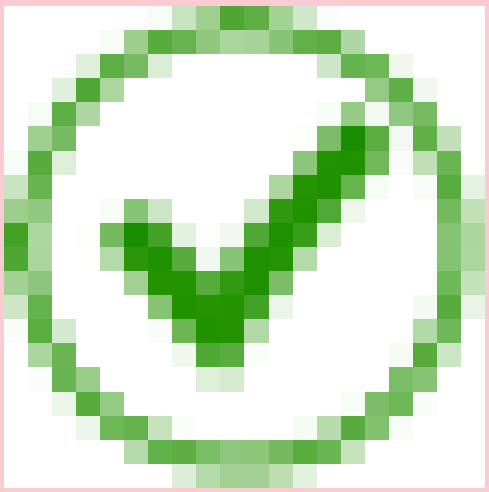
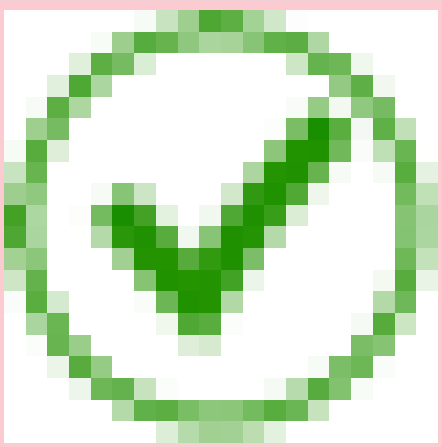
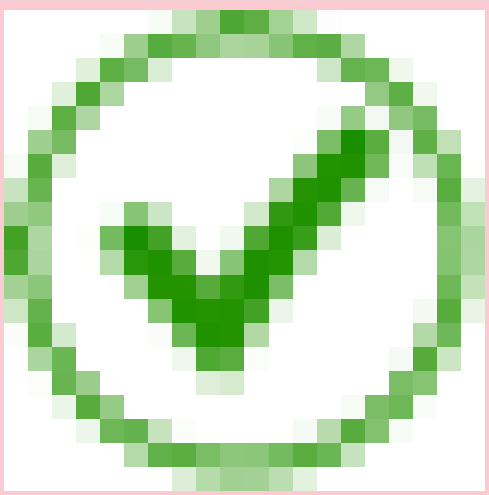
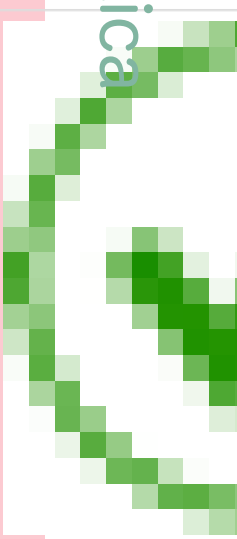
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.ma
Atribuído aos Meus grupos			
Risco crítico e alto			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

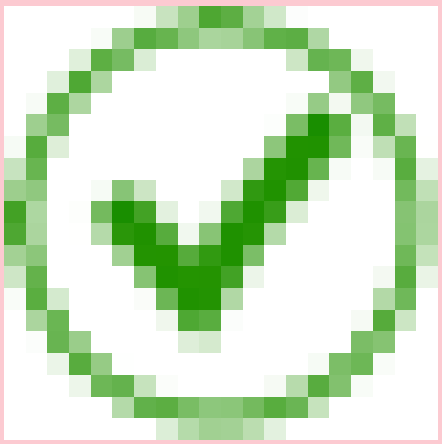
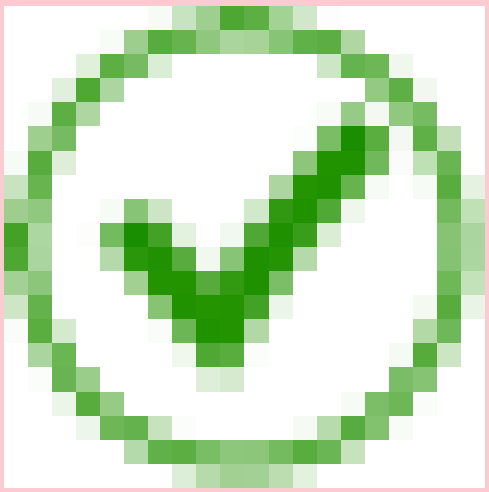
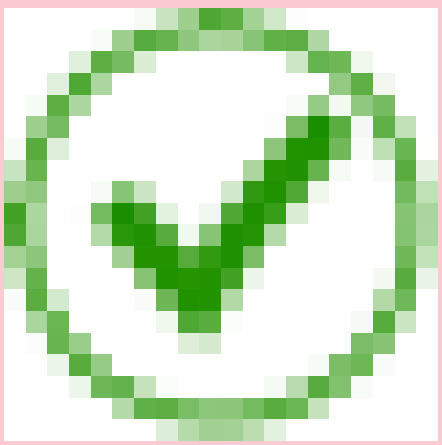
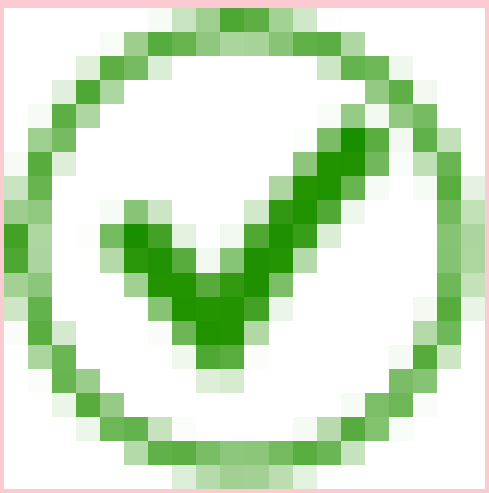
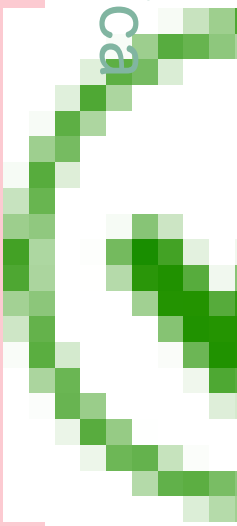
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.ma
Explorável			
Perto da meta			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

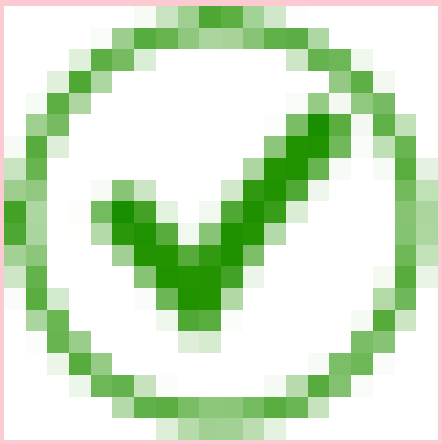
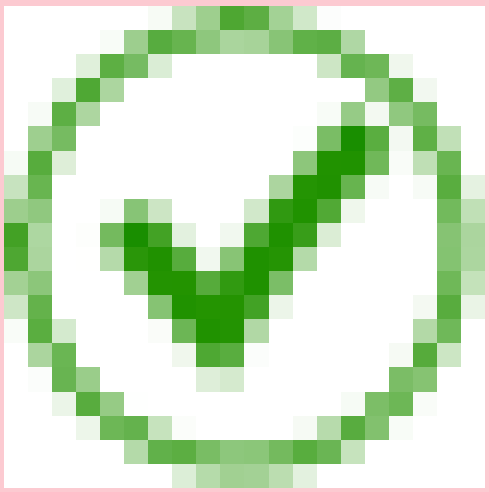
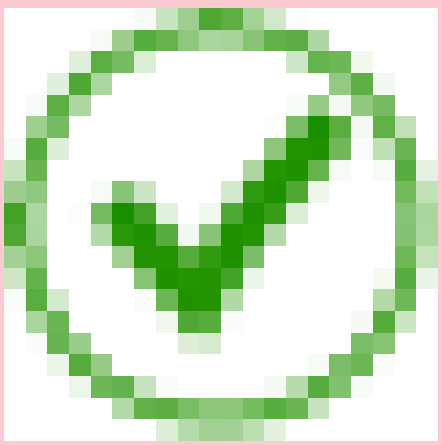
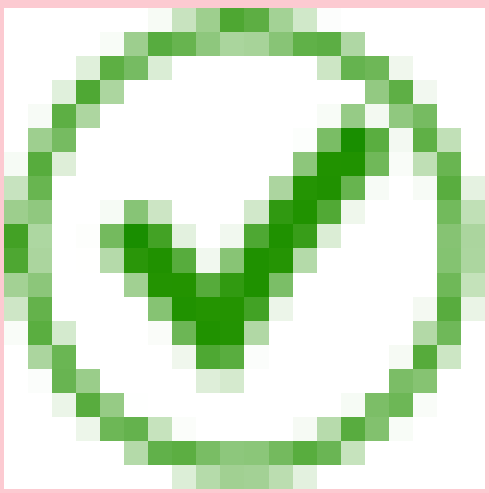
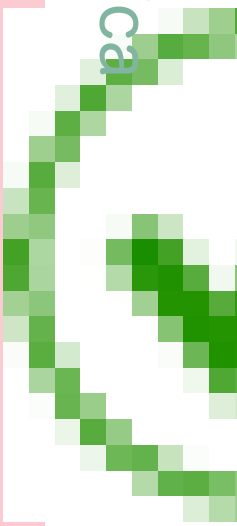
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.ma
Meta não atingida			
Todos			
Bibliotecas			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

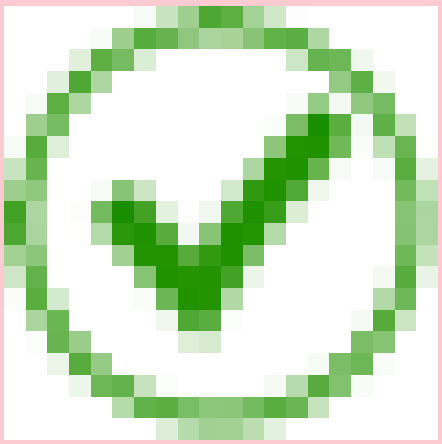
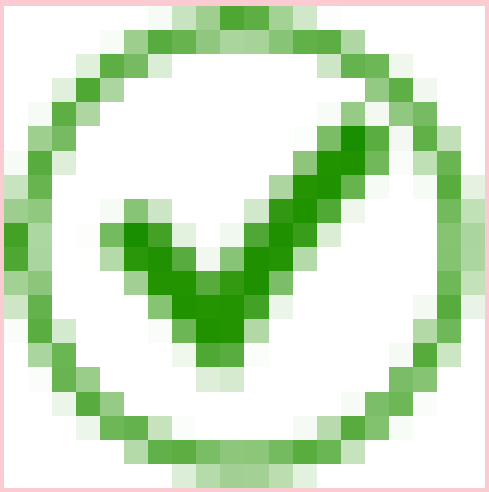
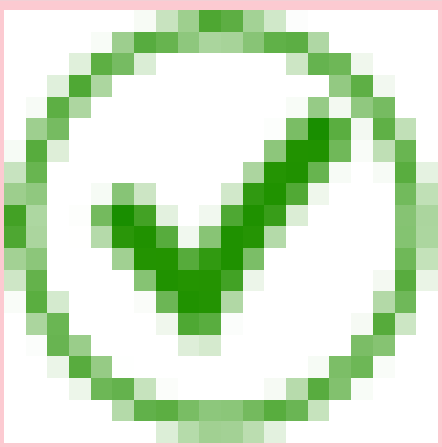
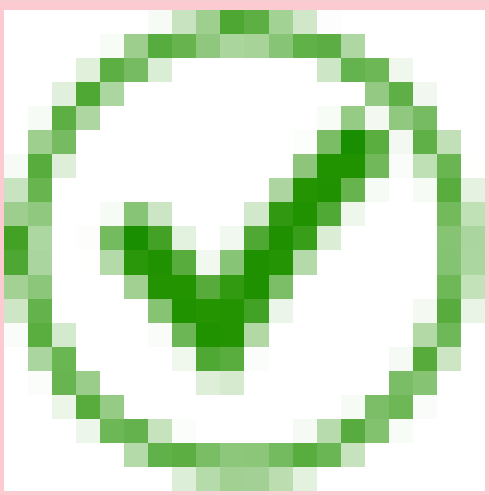
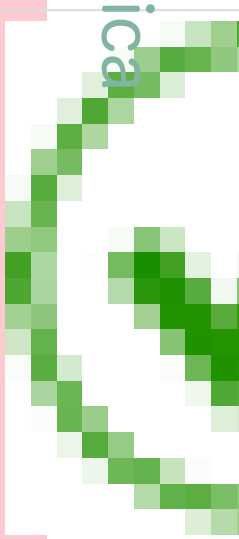
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.ma
NVD			
Terceiros			
Administração			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

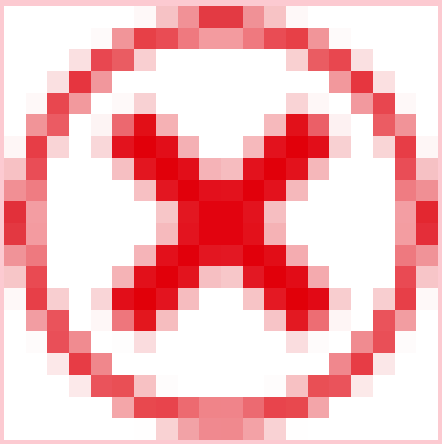
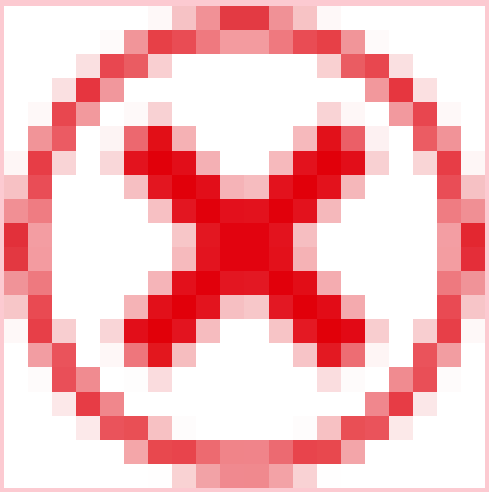
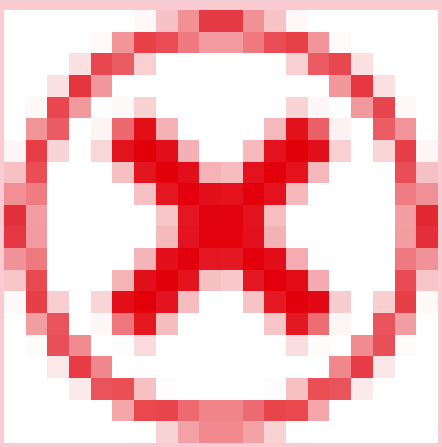
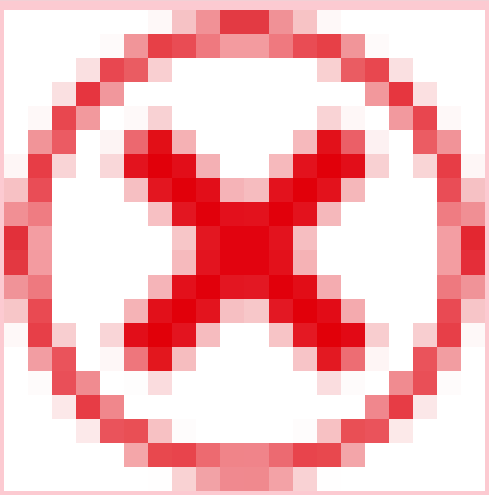
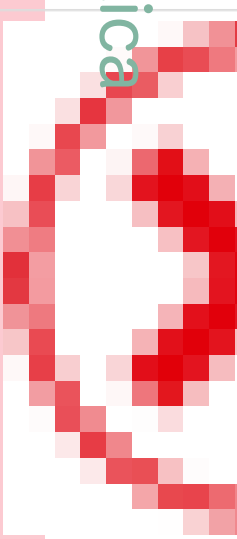
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.ma
Regras de atribuição			
Calculadoras de vulnerabilidade			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

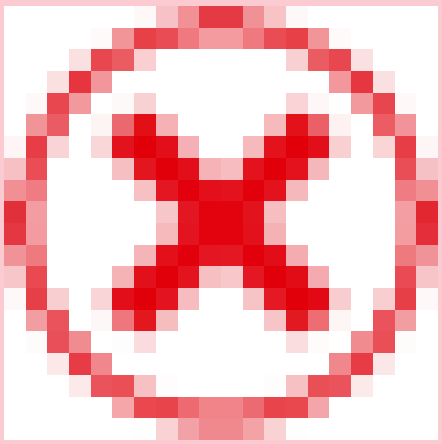
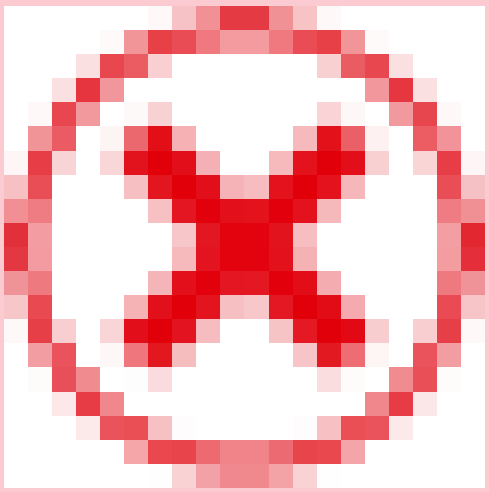
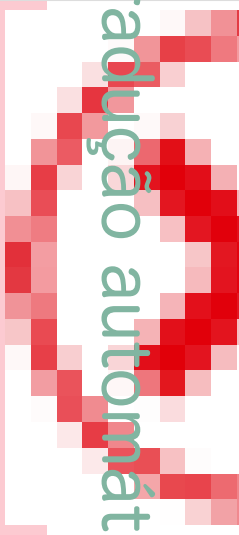
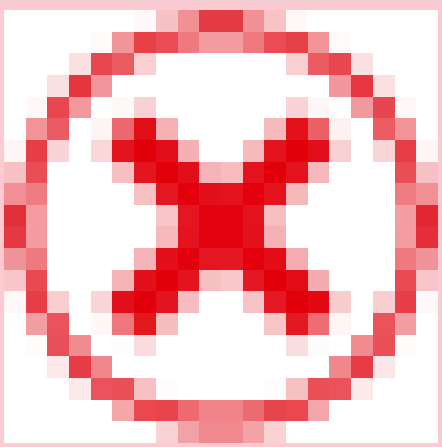
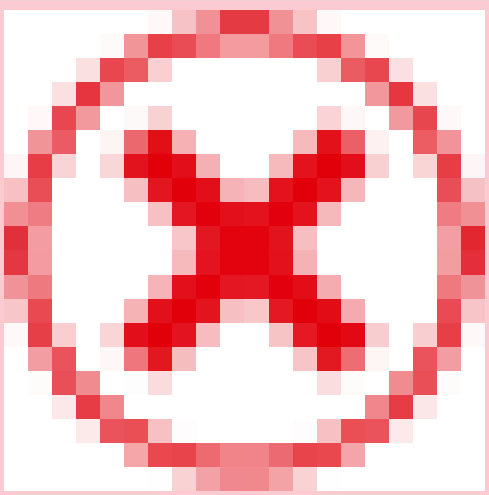
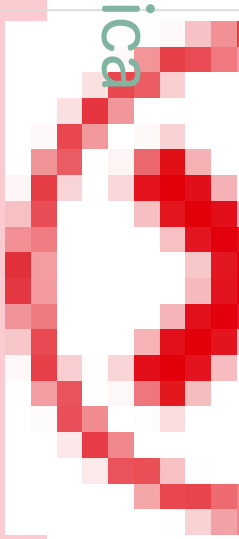
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.ma
Regras de destino de correção			
Configurar granularidade de IV			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

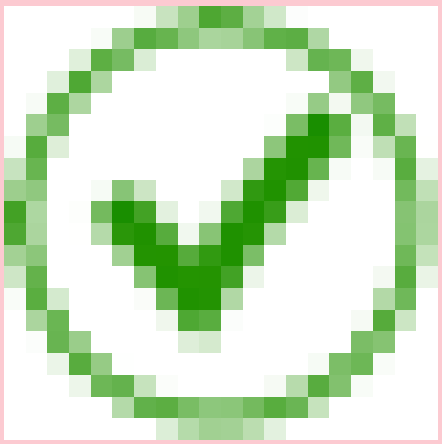
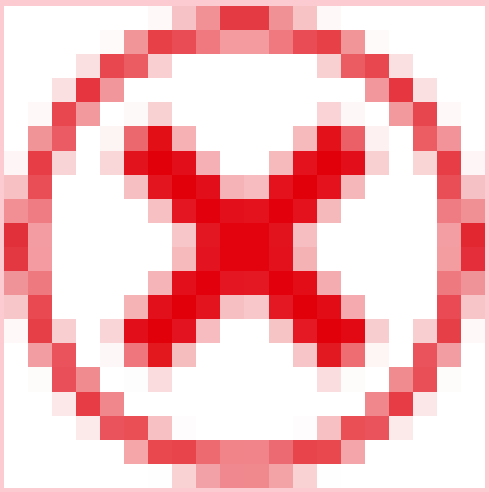
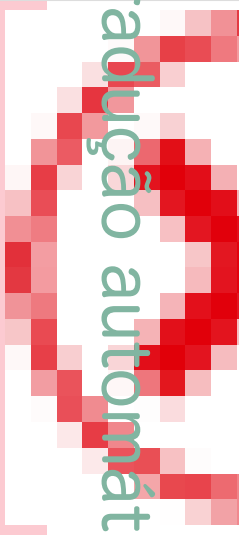
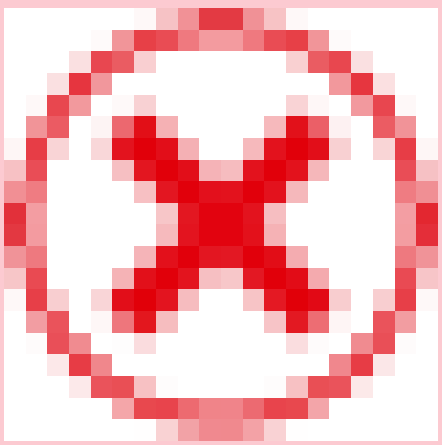
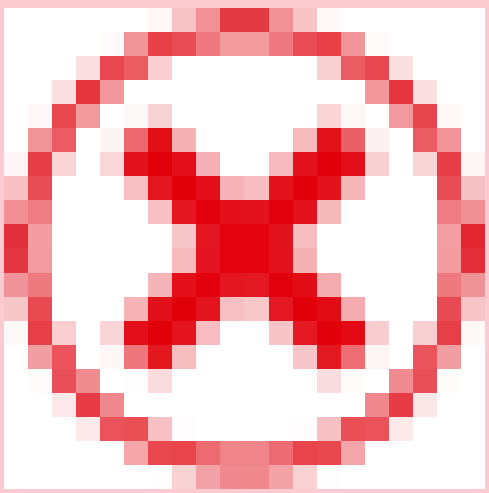
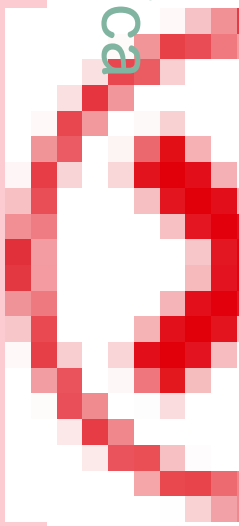
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.ma
Regras de exceção			
Regras de aprovação			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

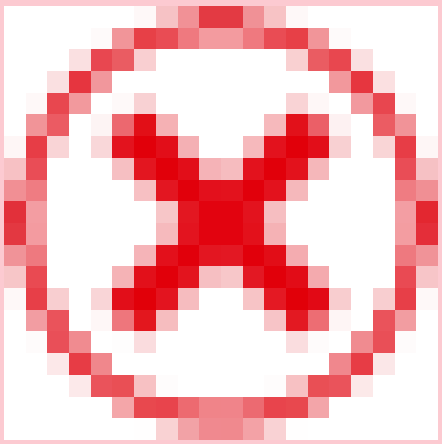
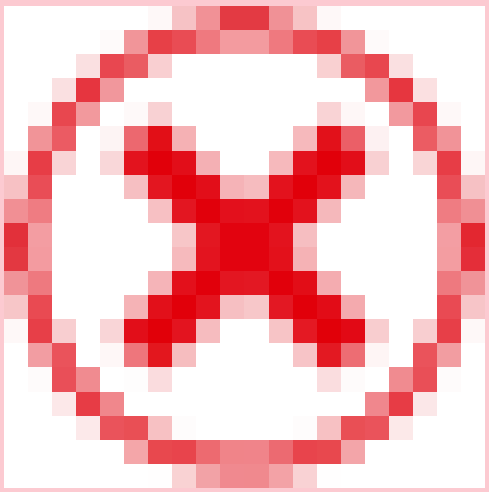
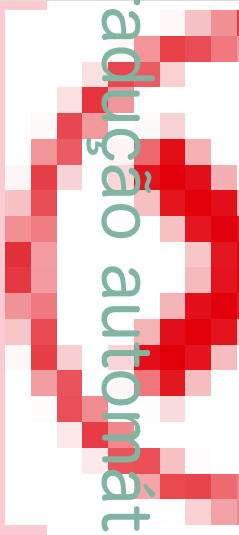
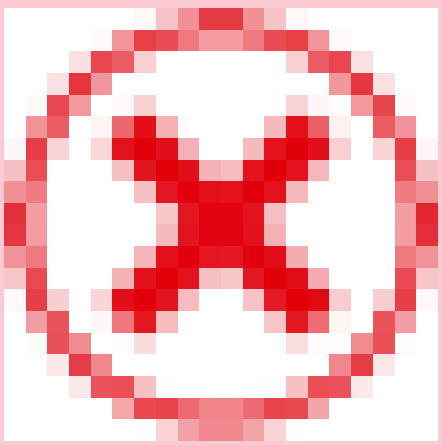
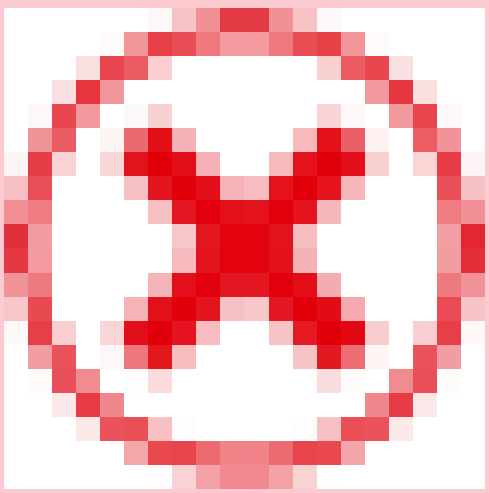
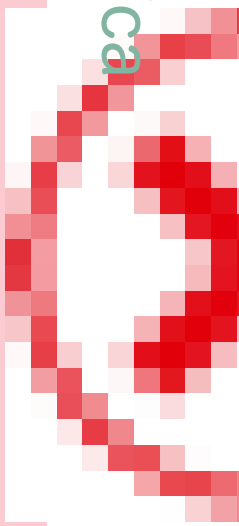
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.ma
Integrações de segurança do contêiner			
Fechar automaticamente itens vulneráveis			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

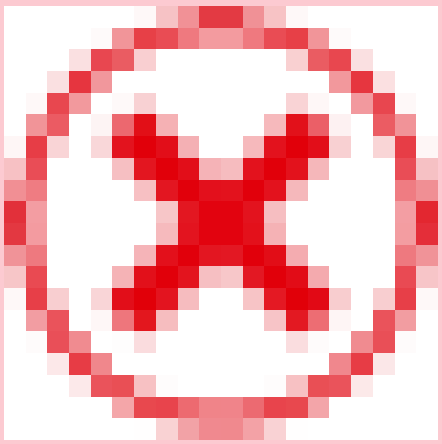
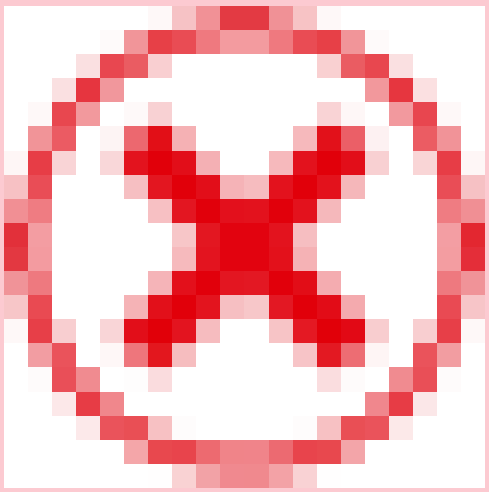
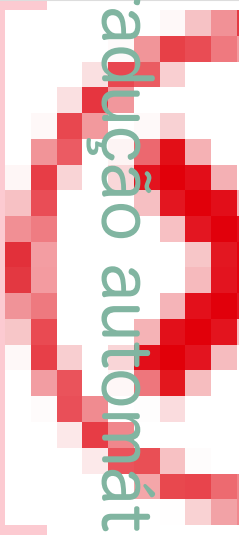
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.exception_approver	sn_vul_container.false_positive_approver	sn_vul_container.ma
Mapas de Gravidade Normalizados			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

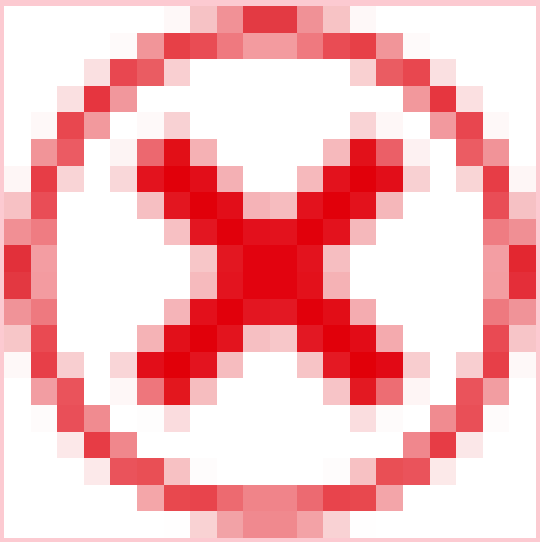
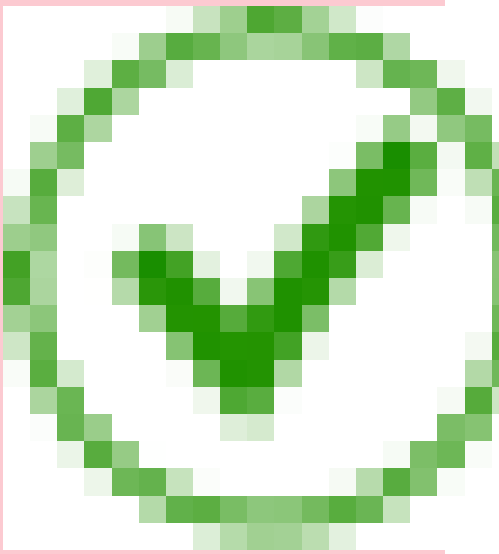
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_container.manage
(Grupo de apps principal)			
Visão geral			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

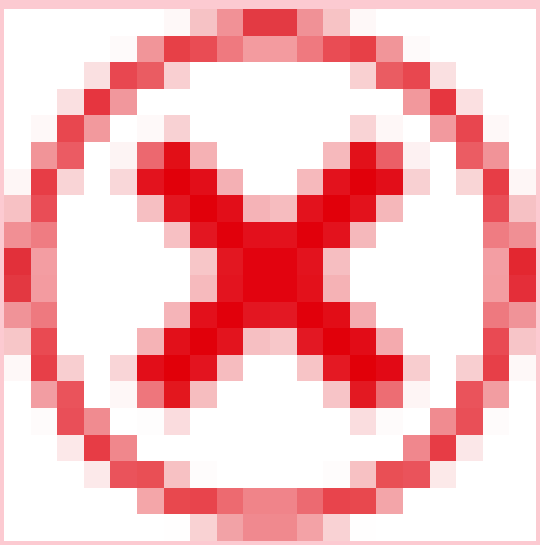
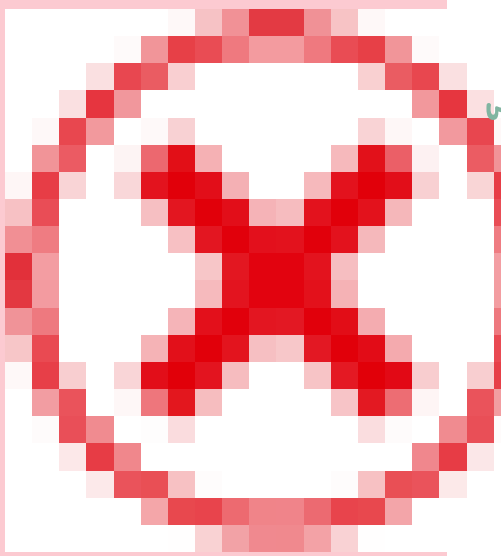
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Minhas aprovações			
Itens vulneráveis de contêiner			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

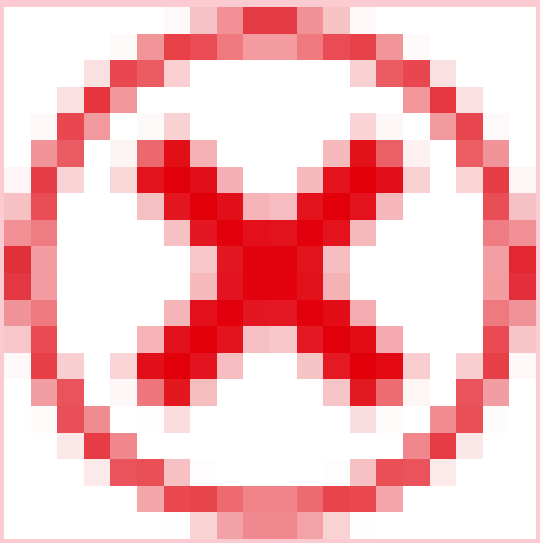
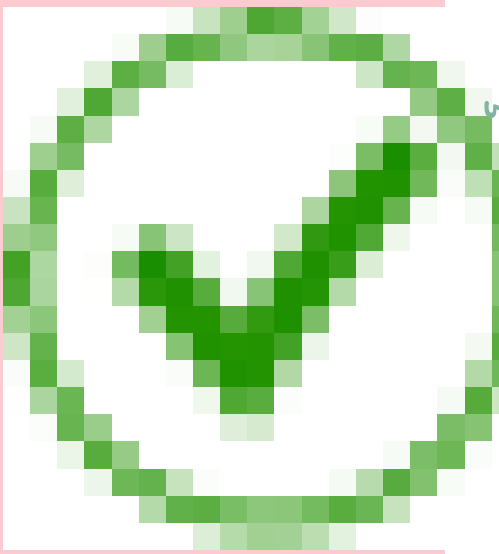
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Atribuídos a Mim			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

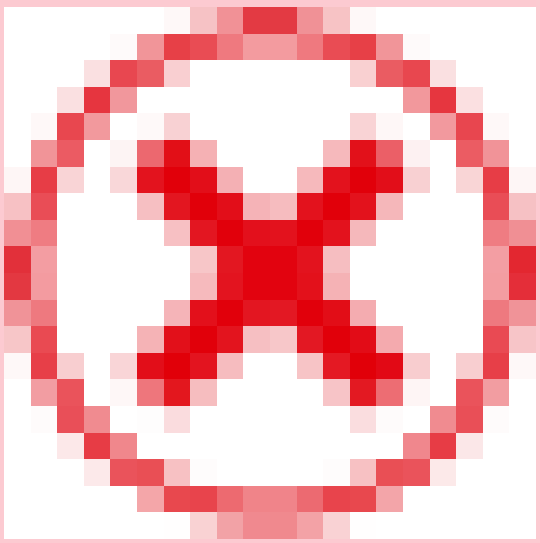
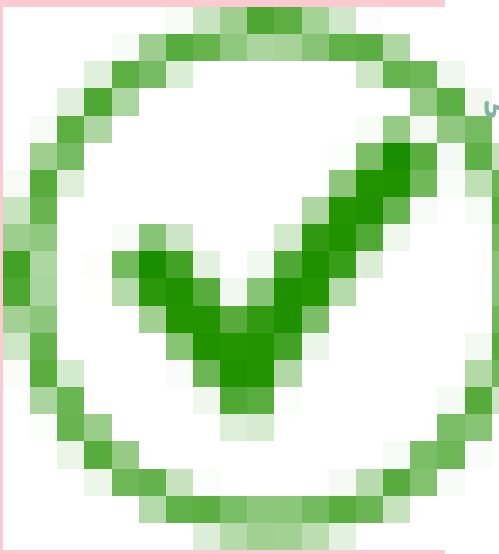
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Atribuído aos Meus grupos			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

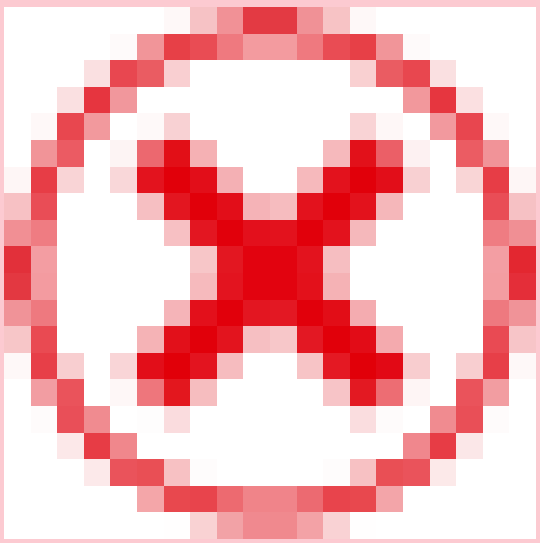
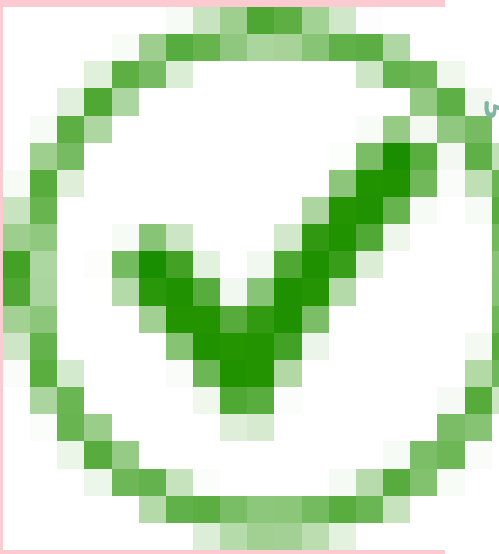
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Risco crítico e alto			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

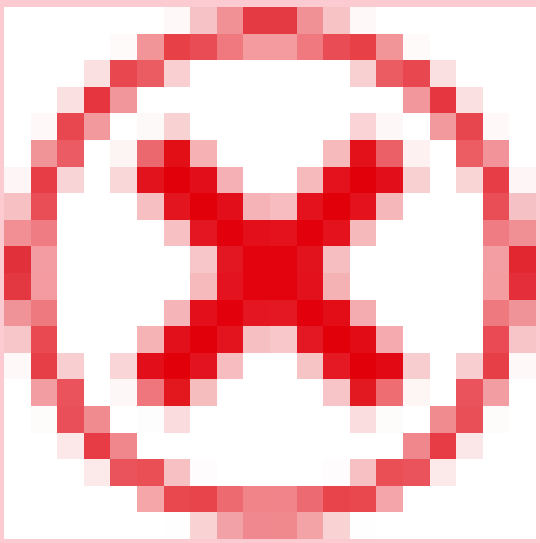
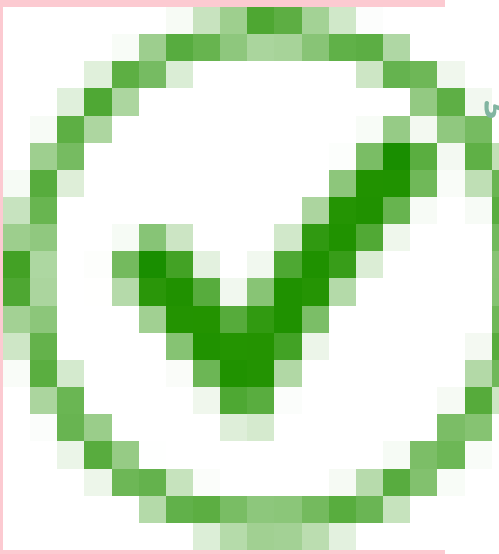
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Explorável			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

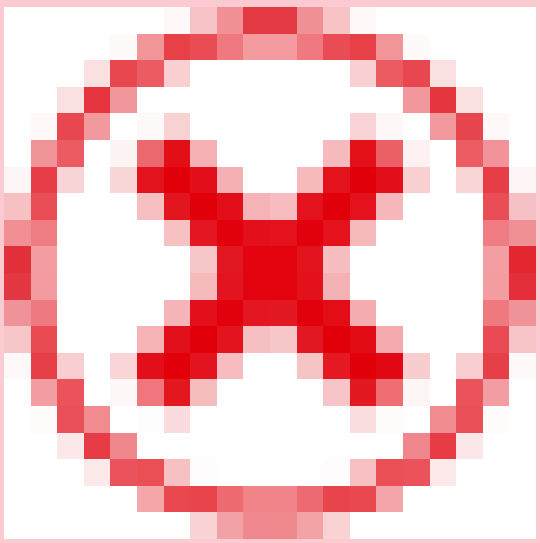
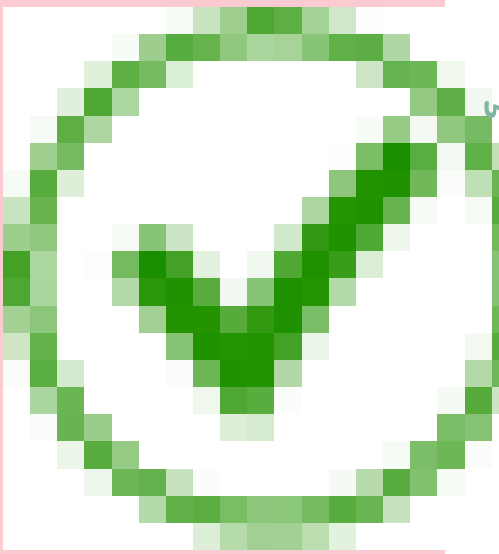
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Perto da meta			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

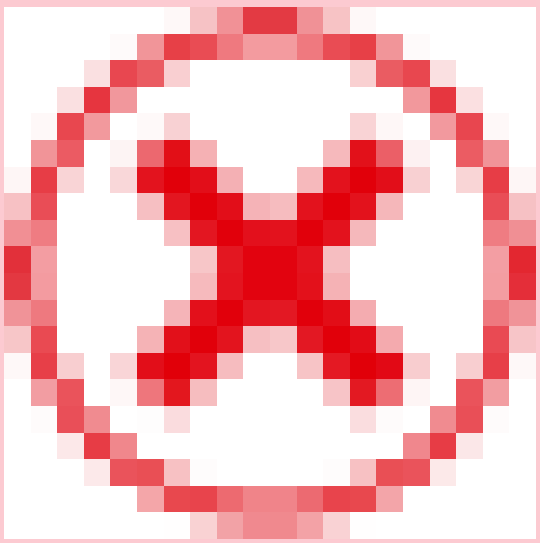
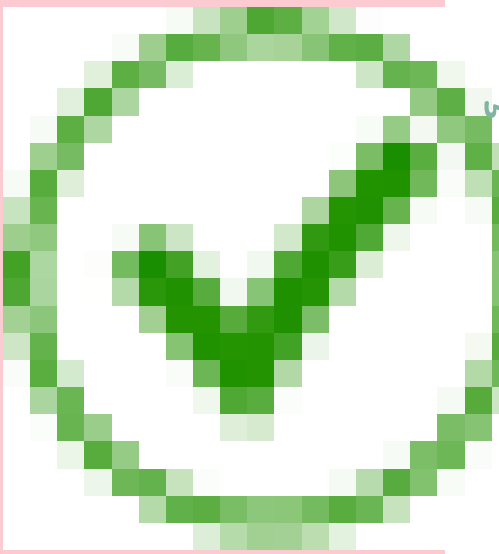
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Meta não atingida			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

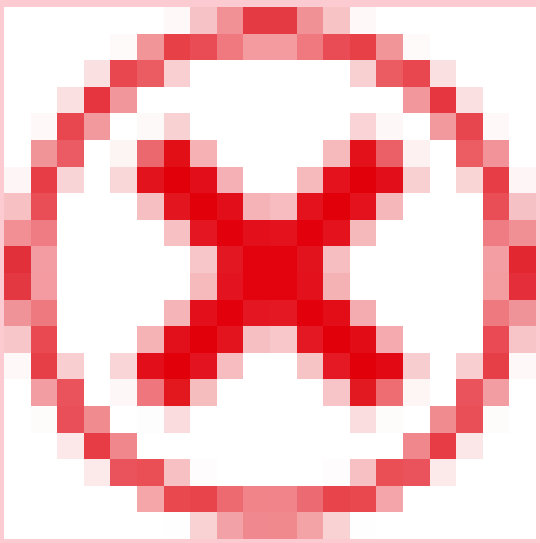
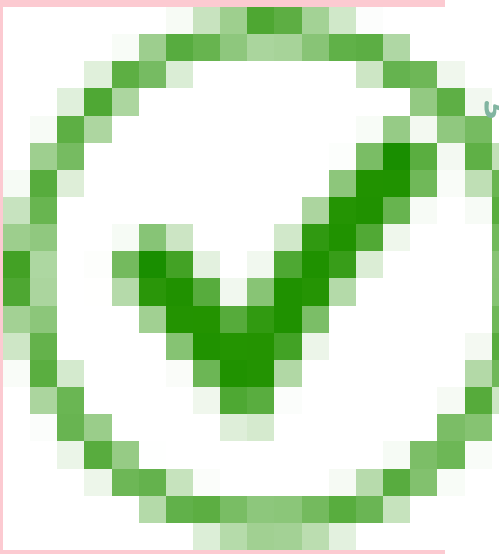
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Todos			
Bibliotecas			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

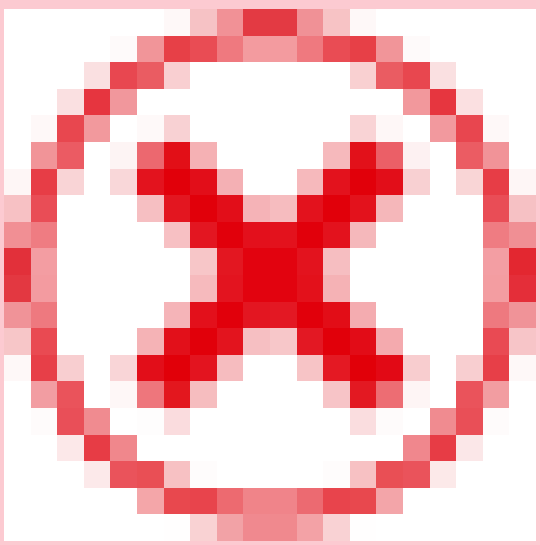
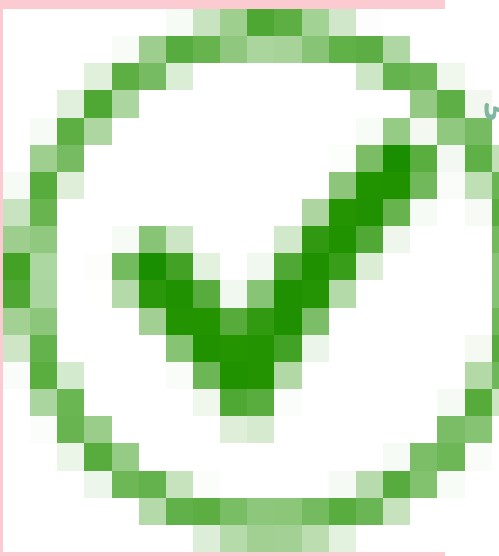
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
NVD			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

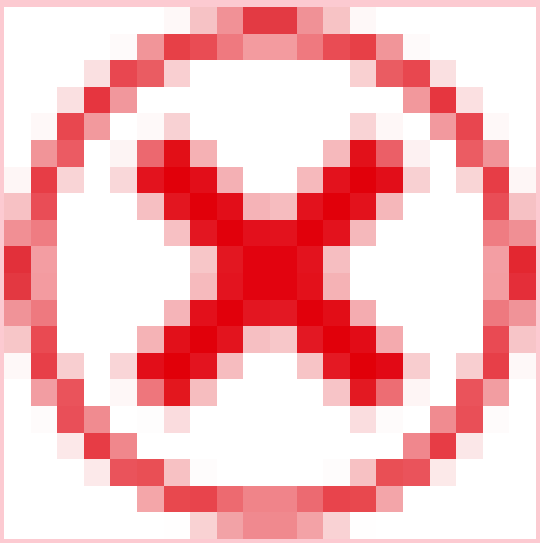
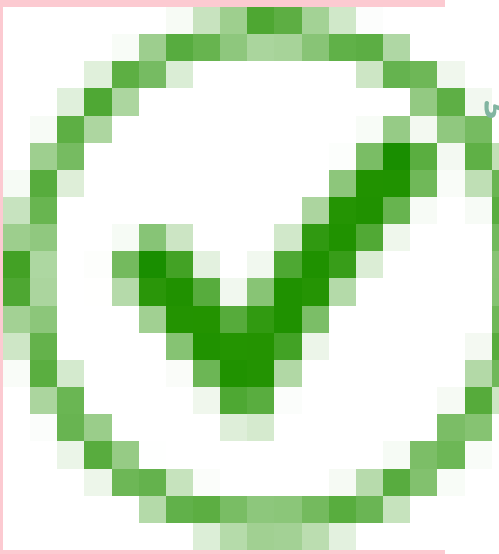
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Terceiros			
Administração			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

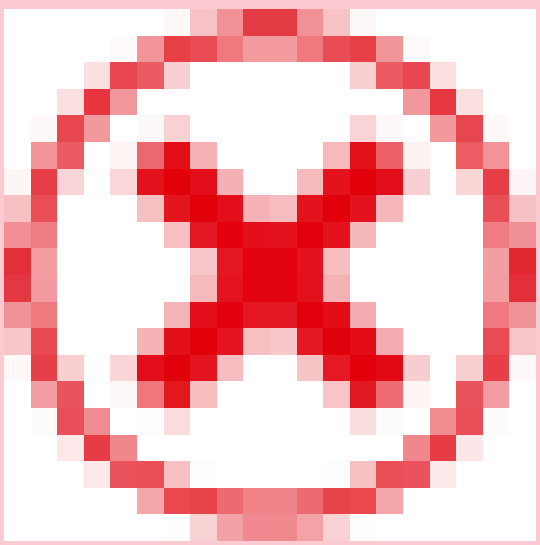
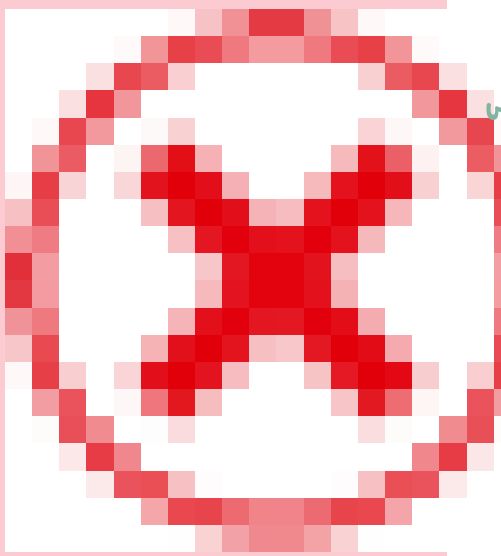
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Regras de atribuição			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

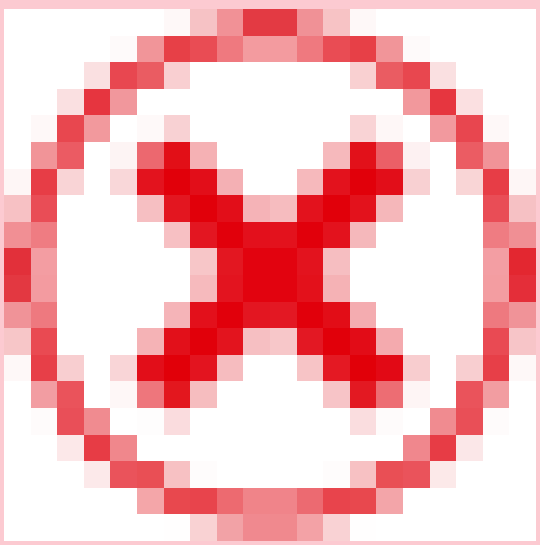
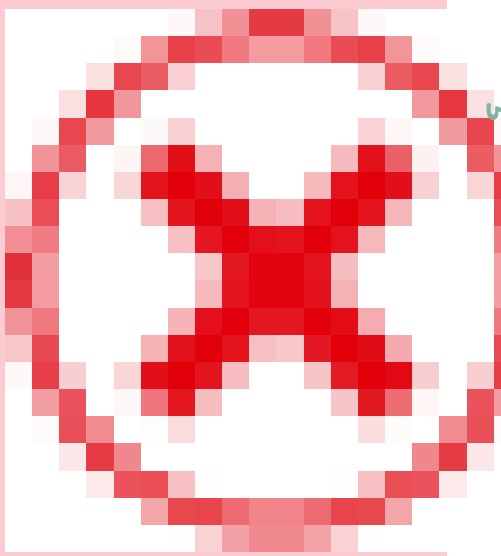
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Calculadoras de vulnerabilidade			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

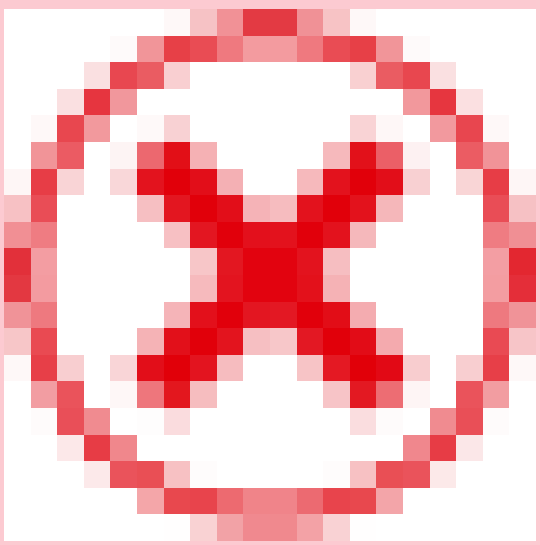
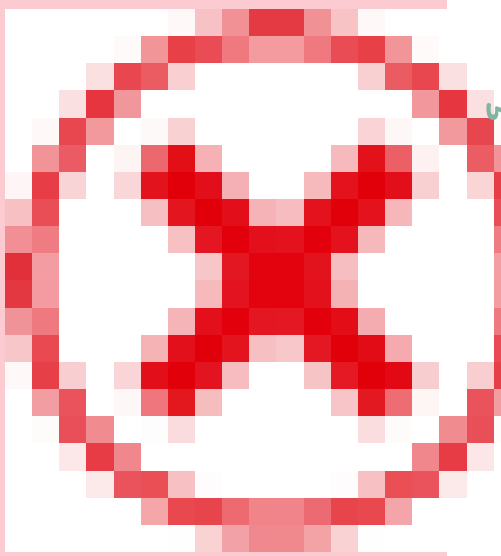
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Regras de destino de correção			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

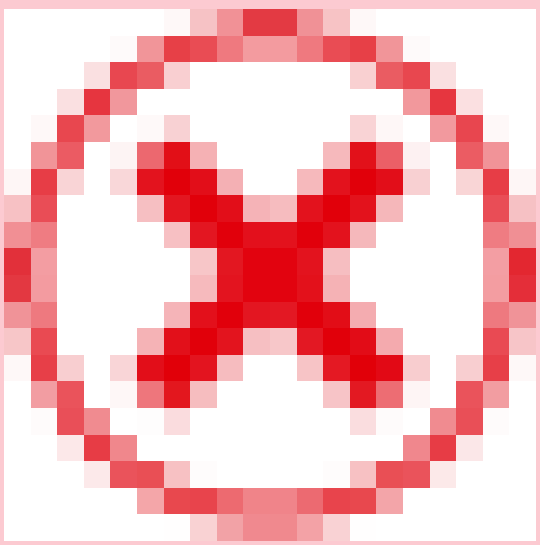
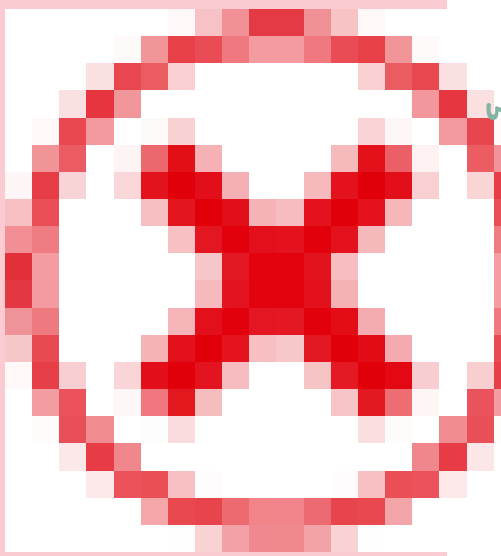
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Configurar granularidade de IV			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

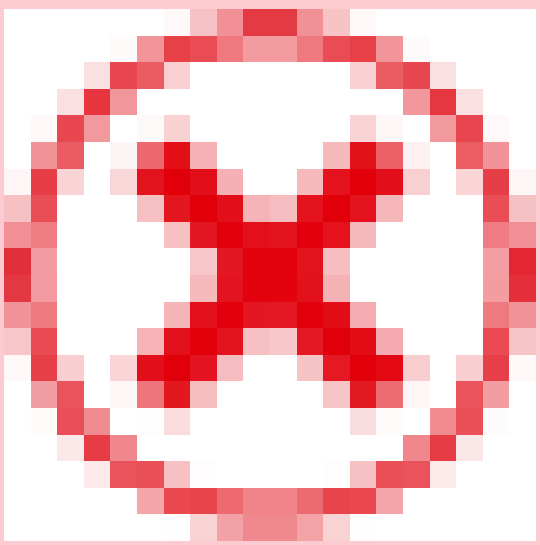
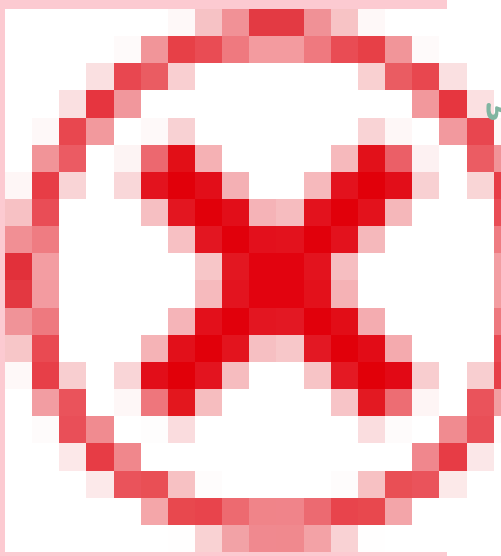
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Regras de exceção			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

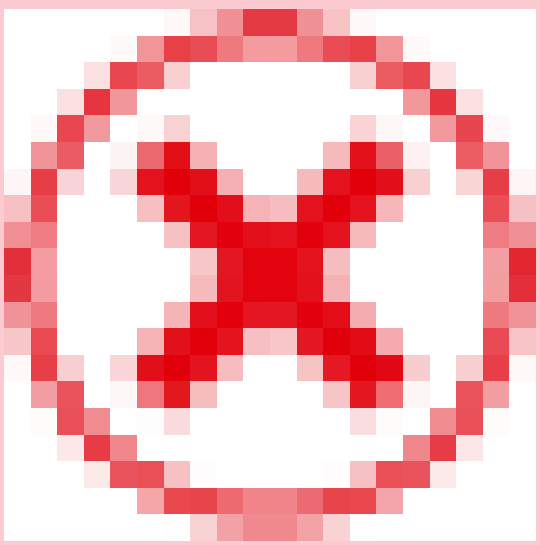
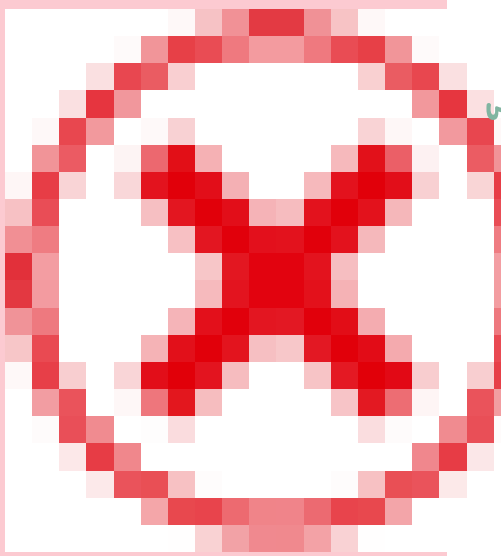
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Regras de aprovação			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

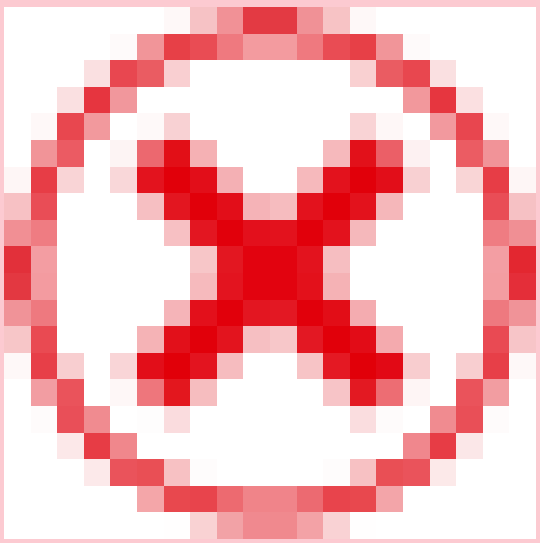
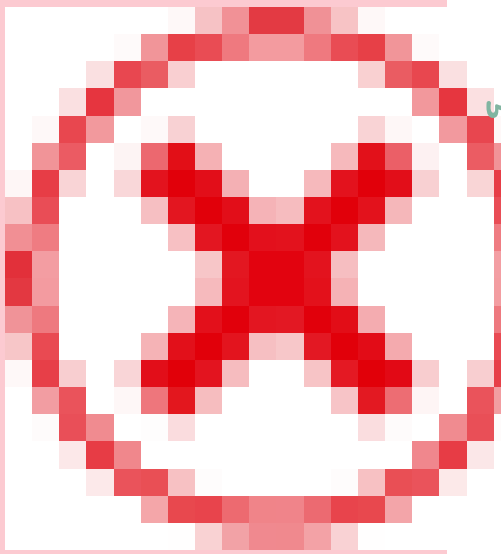
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Integrações de segurança do contêiner			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

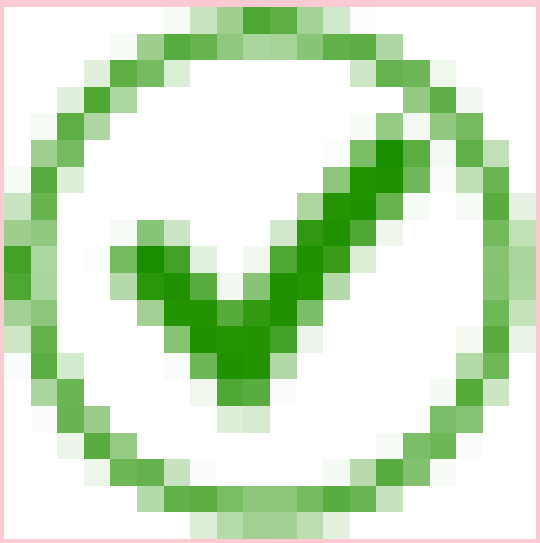
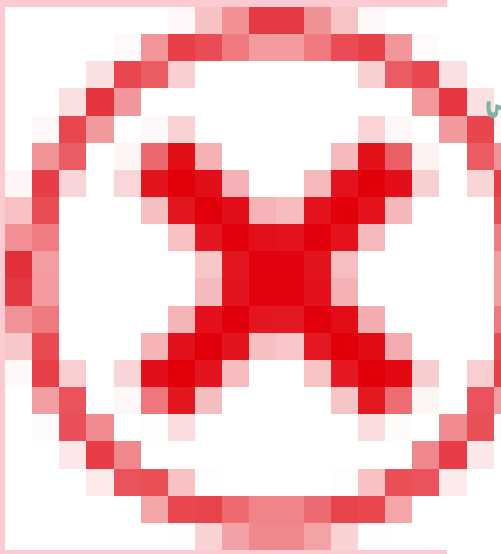
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul_container.manage_remediation_target_rules
Fechar automaticamente itens vulneráveis			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

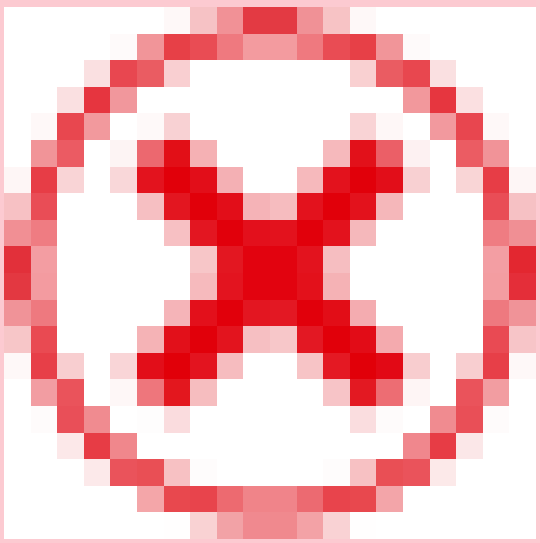
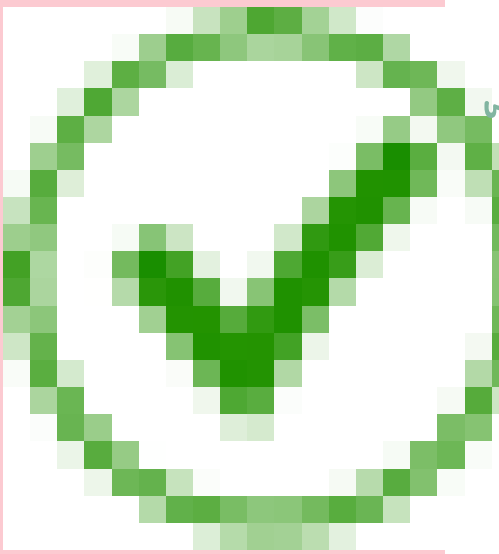
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container.manage_auto_close_stale_vi	sn_vul_container.manage_normalized_severity	sn_vul manag
Mapas de Gravidade Normalizados			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

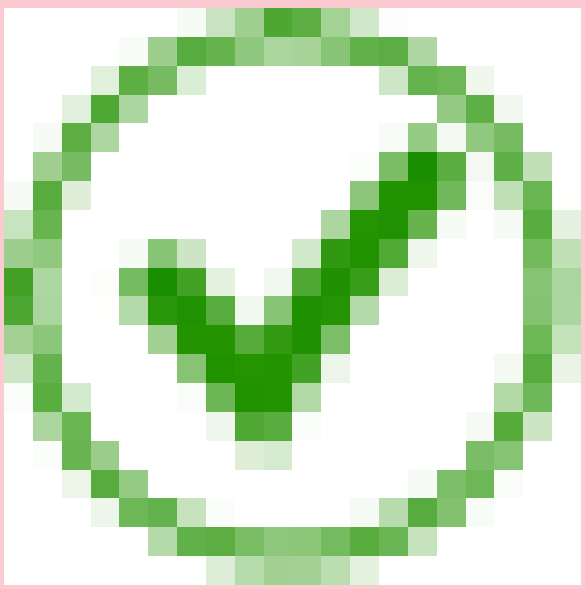
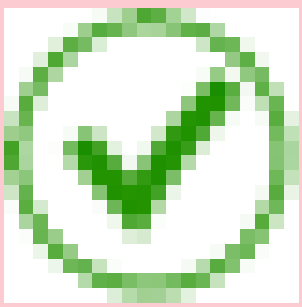
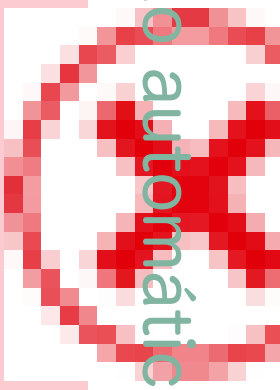
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
(Grupo de apps principal)			
Visão geral			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

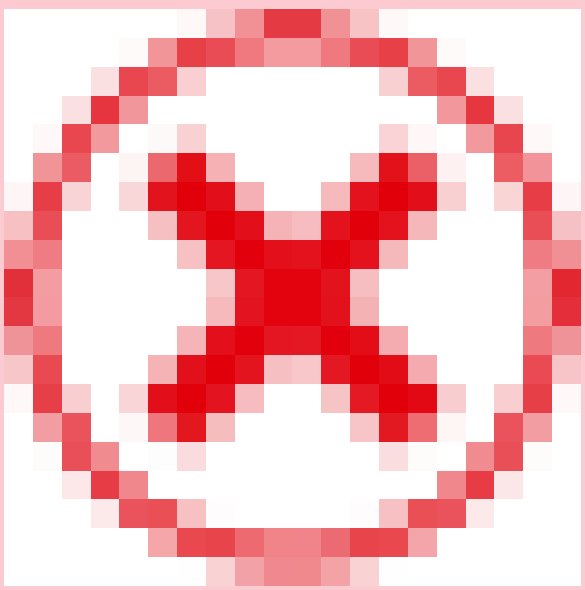
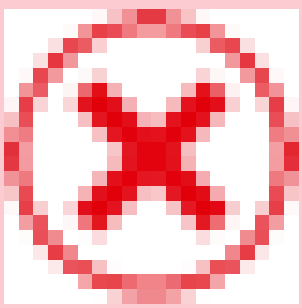
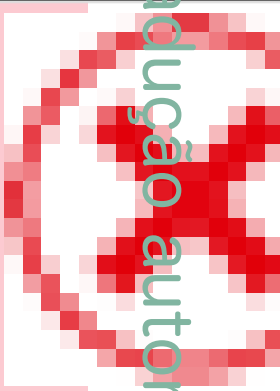
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Minhas aprovações			
Itens vulneráveis de contêiner			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

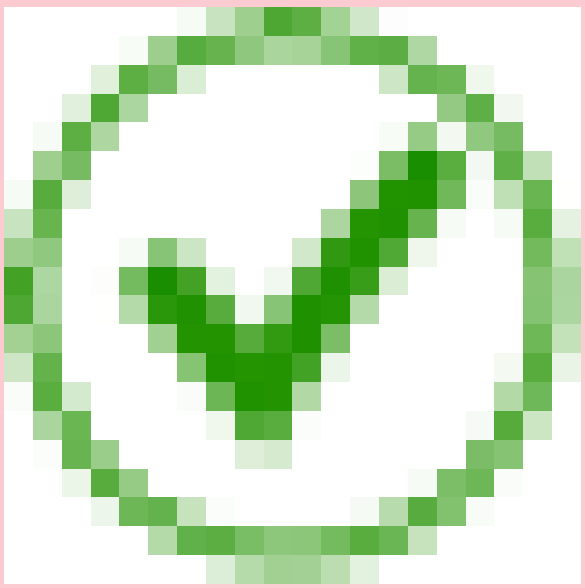
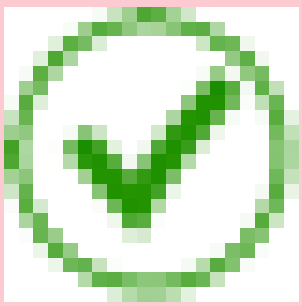
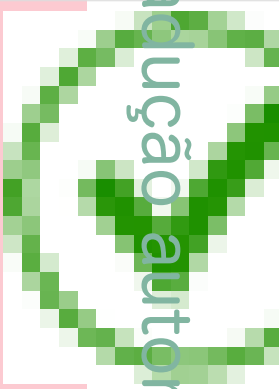
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Atribuídos a Mim			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

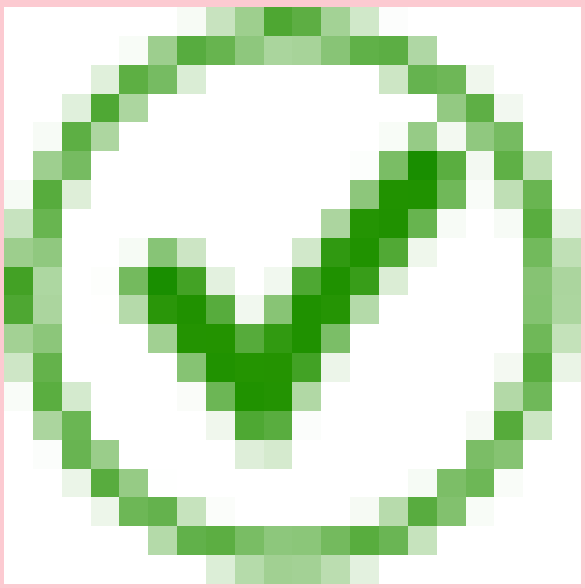
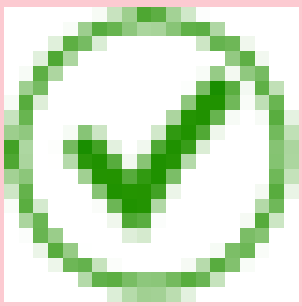
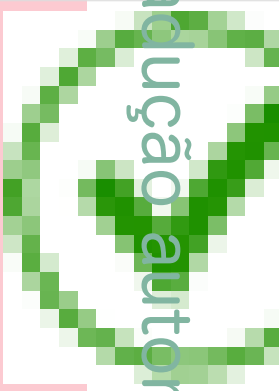
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Atribuído aos Meus grupos			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

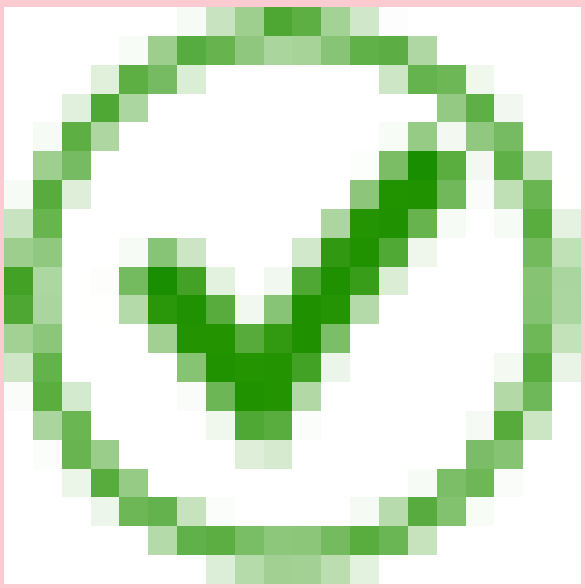
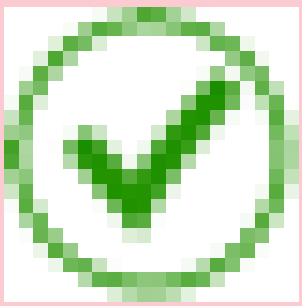
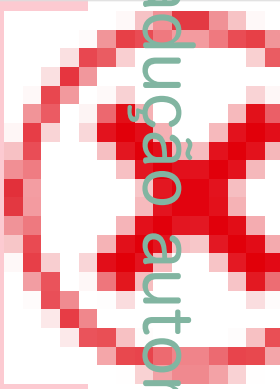
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Risco crítico e alto			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

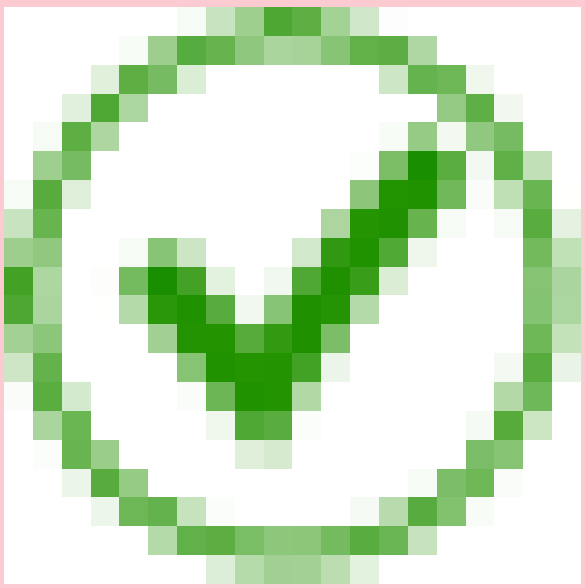
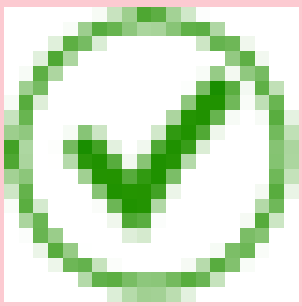
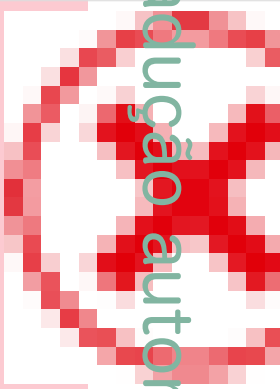
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Explorável			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

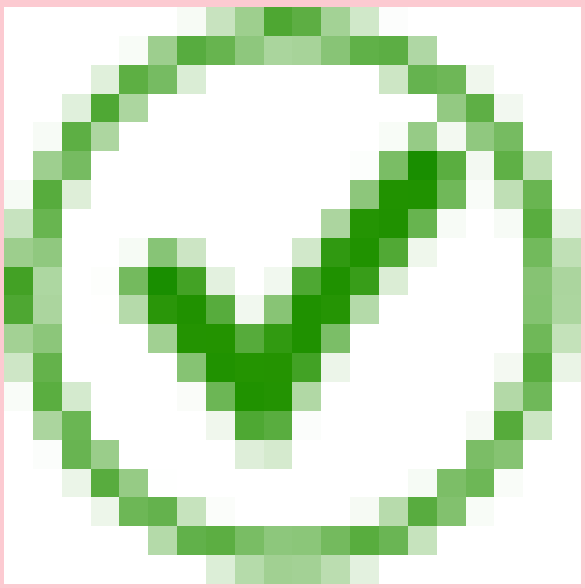
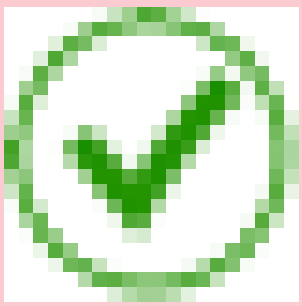
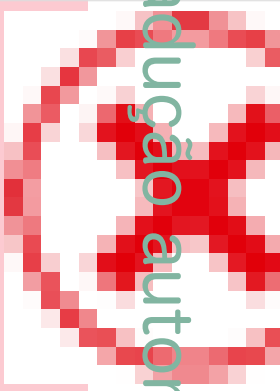
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Perto da meta			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

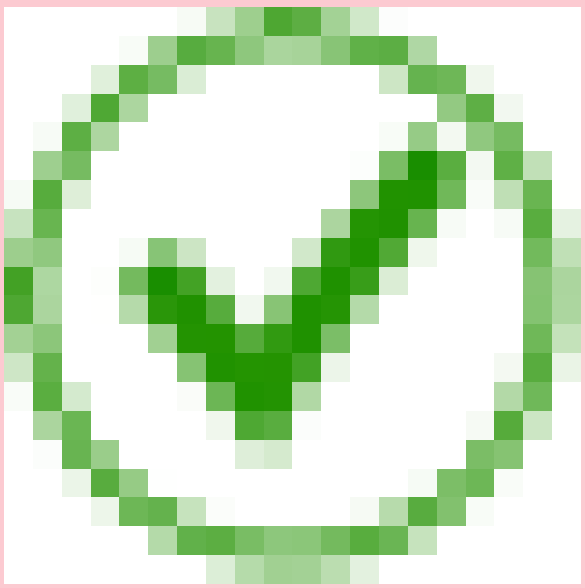
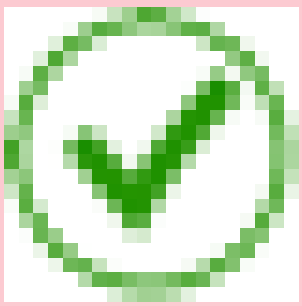
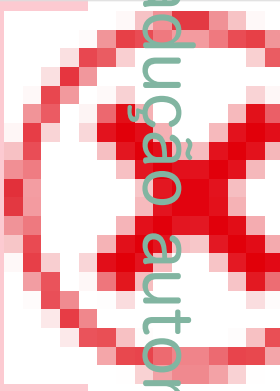
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Meta não atingida			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

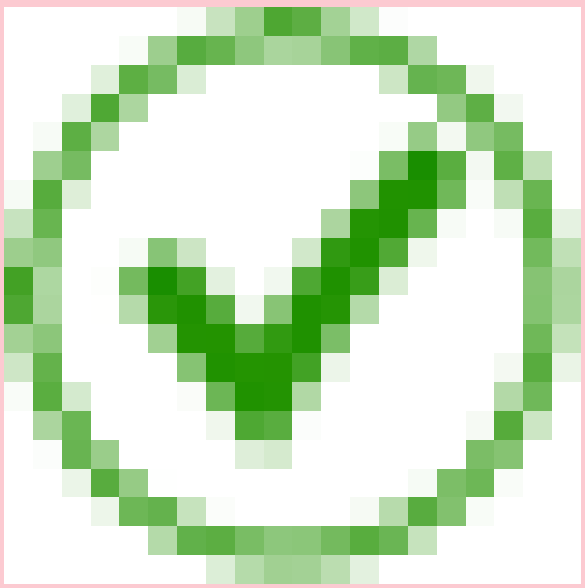
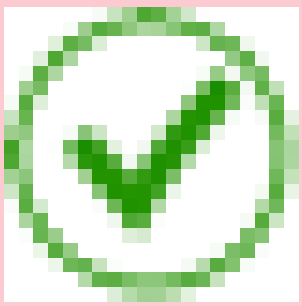
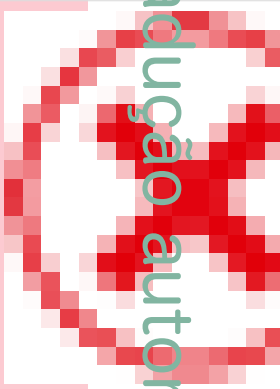
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Todos			
Bibliotecas			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

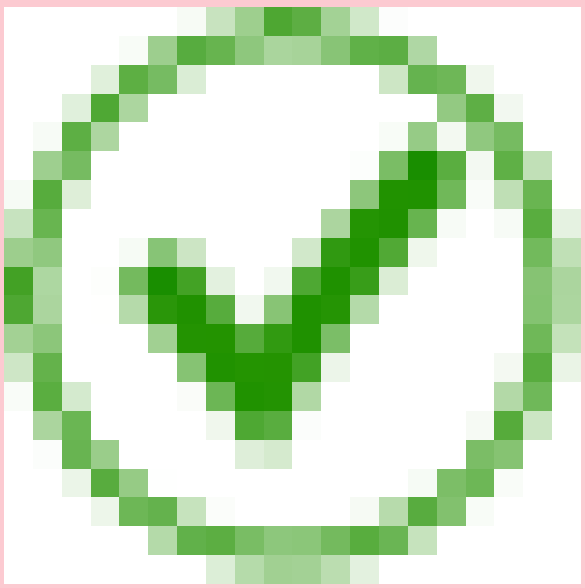
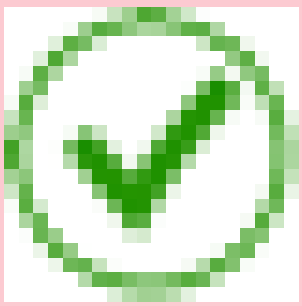
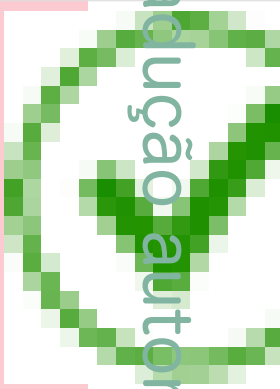
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
NVD			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

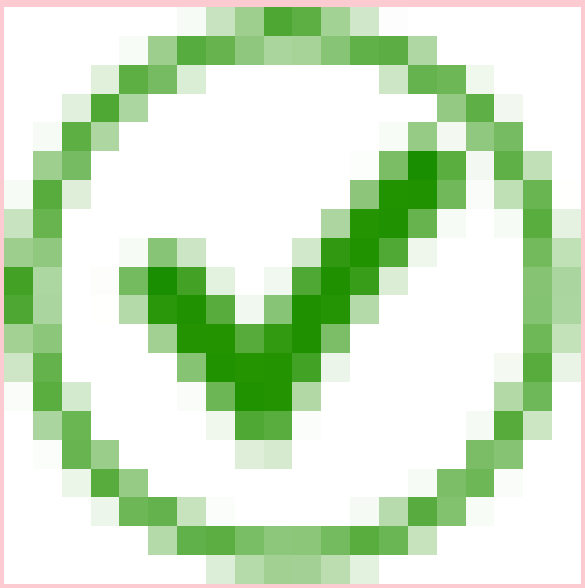
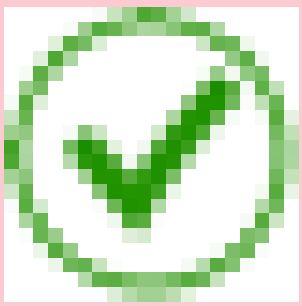
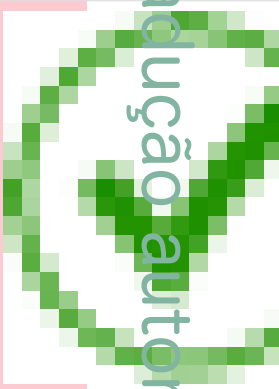
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Terceiros			
Administração			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

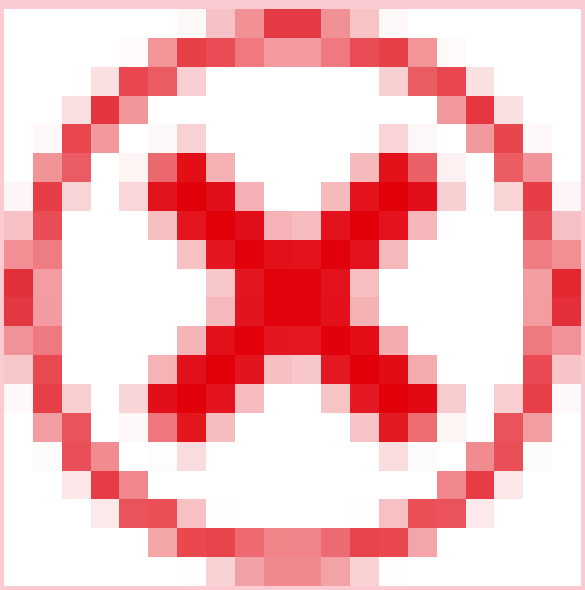
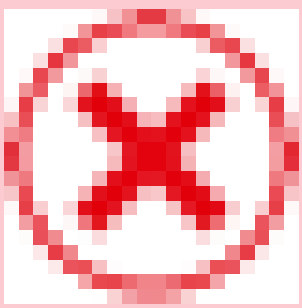
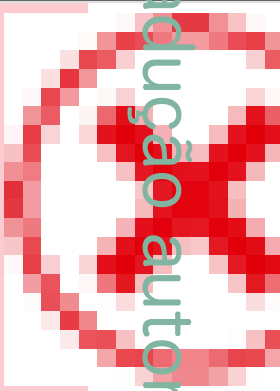
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Regras de atribuição			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

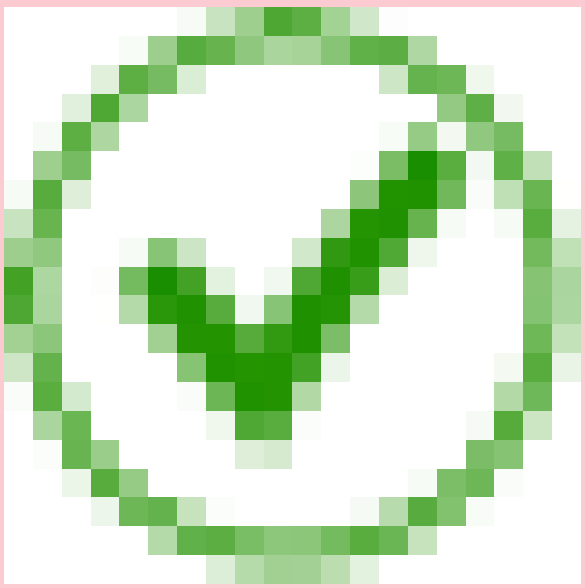
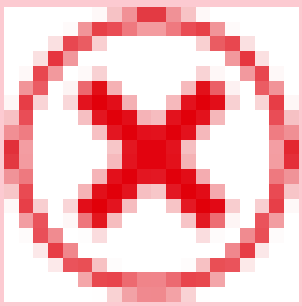
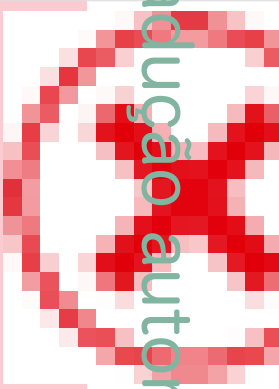
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Calculadoras de vulnerabilidade			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

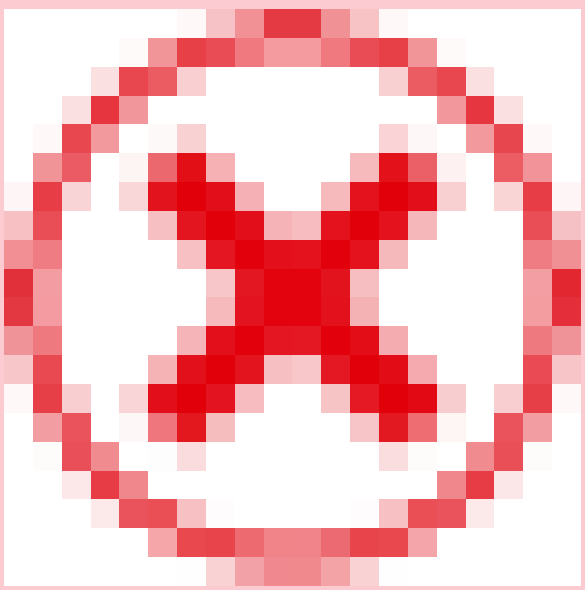
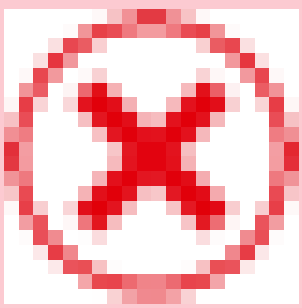
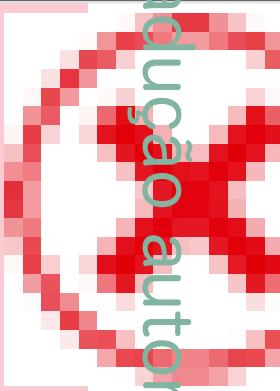
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Regras de destino de correção			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

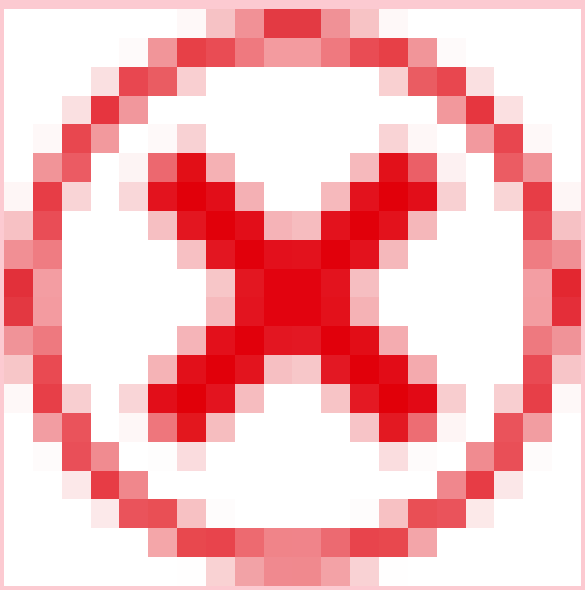
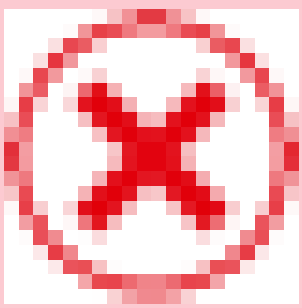
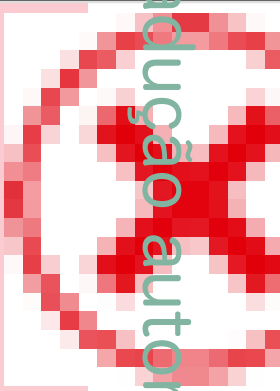
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Configurar granularidade de IV			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

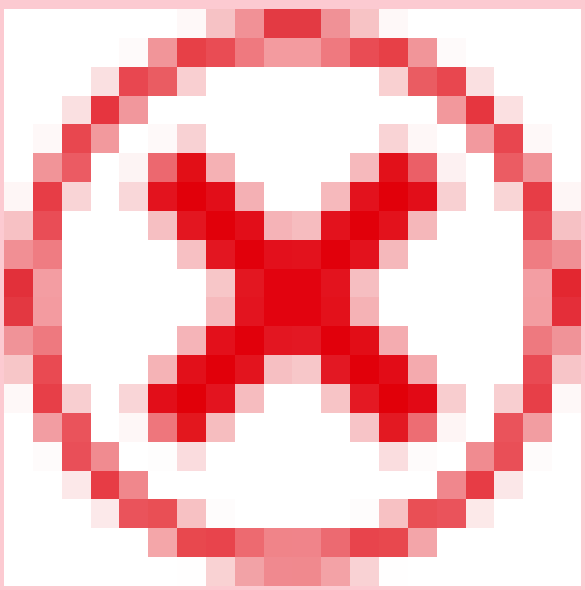
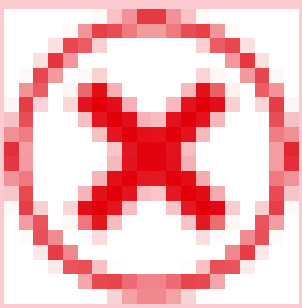
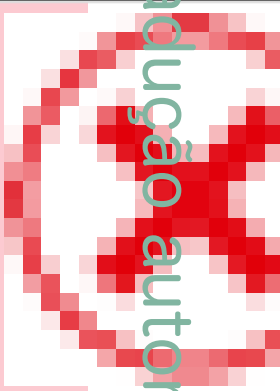
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Regras de exceção			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

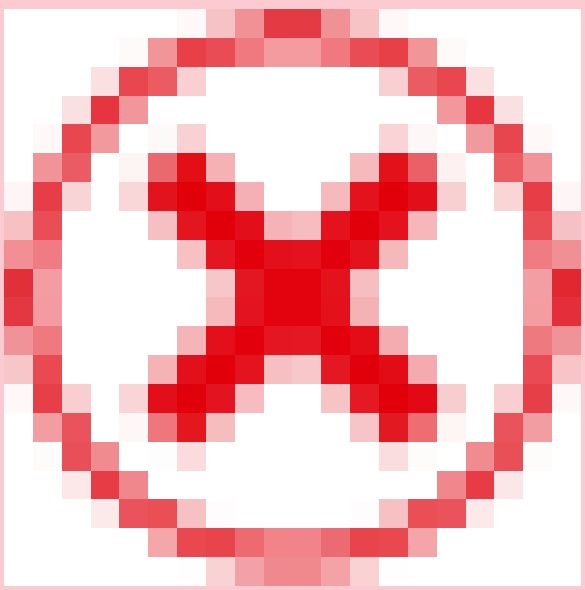
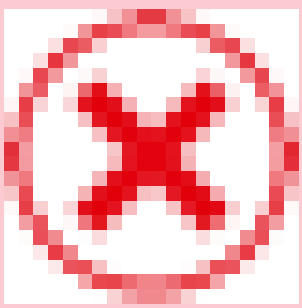
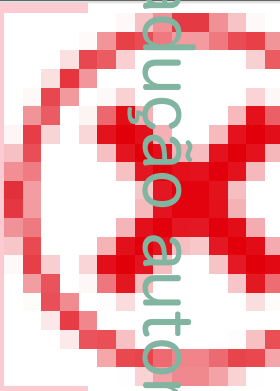
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Regras de aprovação			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

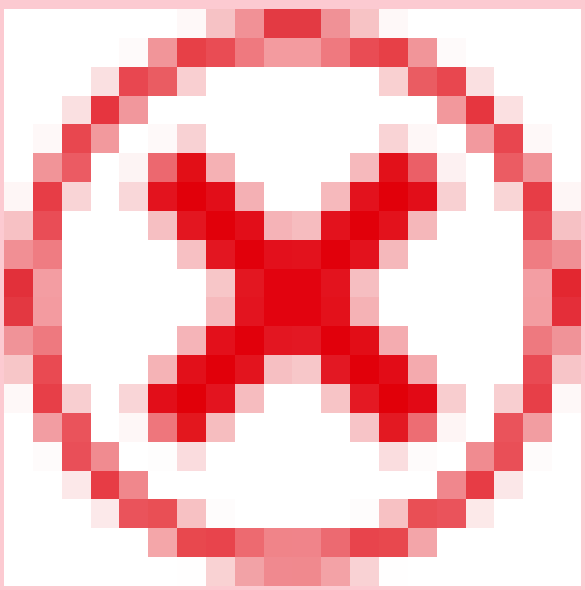
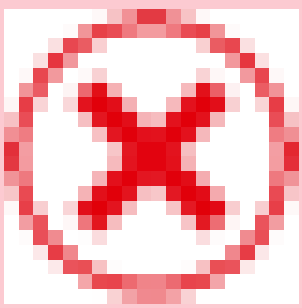
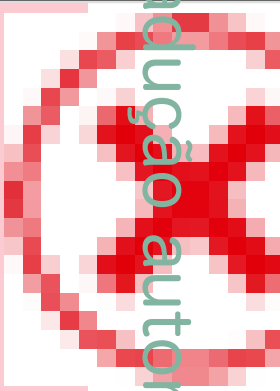
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Integrações de segurança do contêiner			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

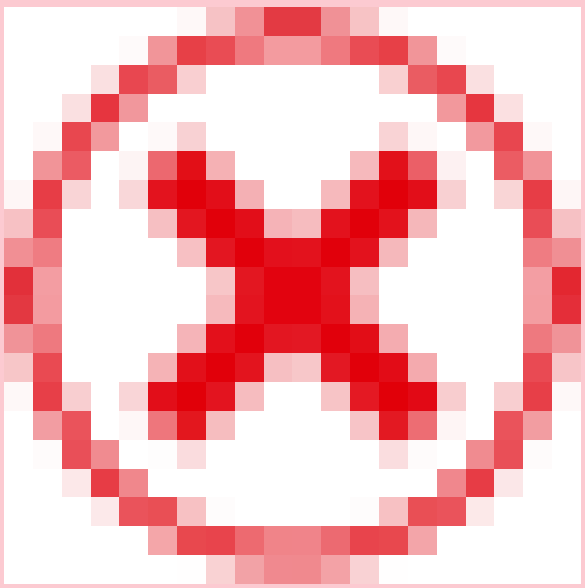
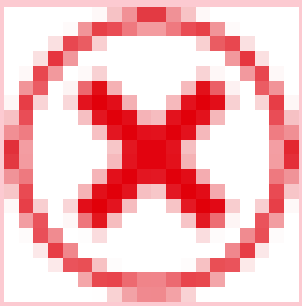
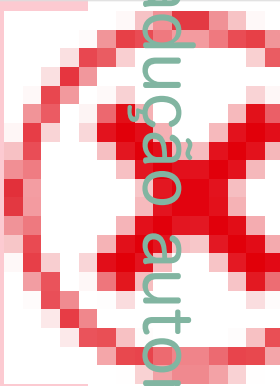
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Fechar automaticamente itens vulneráveis			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

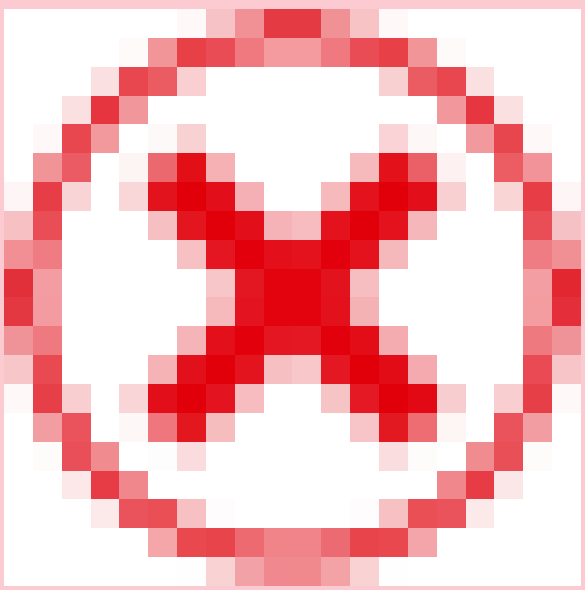
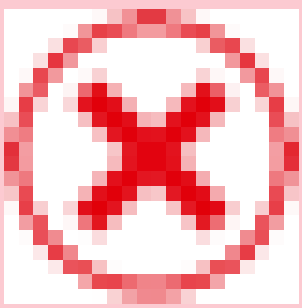
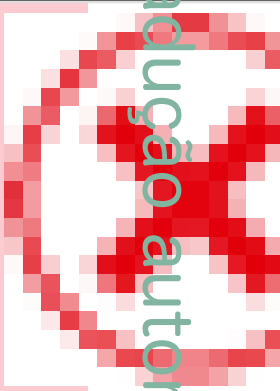
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.read_auto_exception_rule

Módulo	sn_vul_container. manage_risk_score_configuration	sn_vul_container.read_all	sn_vul_container.read_a
Mapas de Gravidade Normalizados			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

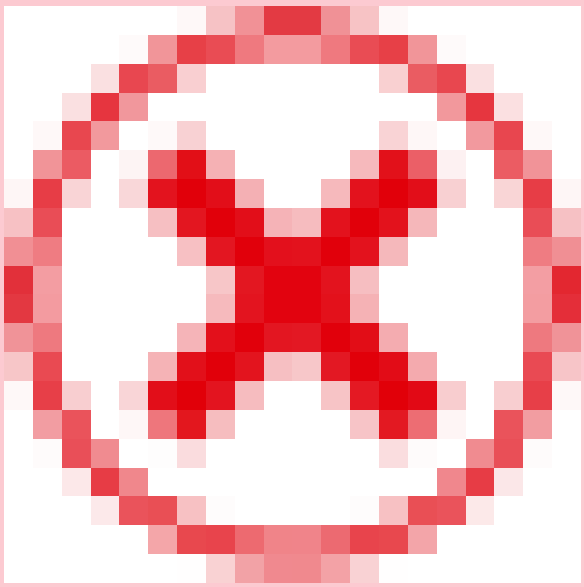
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
(Grupo de apps principal)	
Visão geral	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

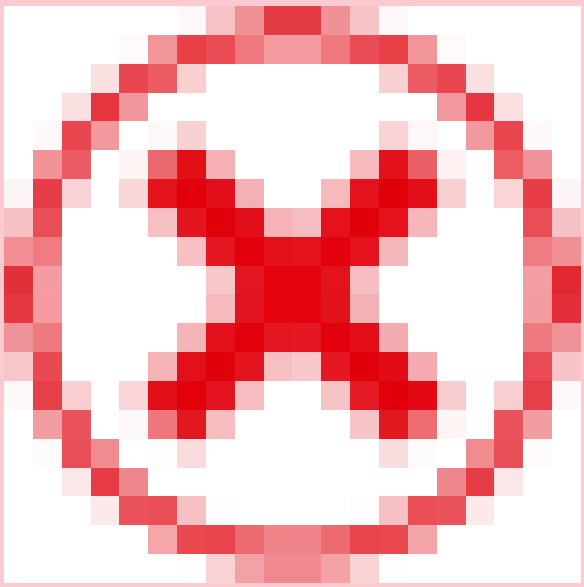
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Minhas aprovações	
Itens vulneráveis de contêiner	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

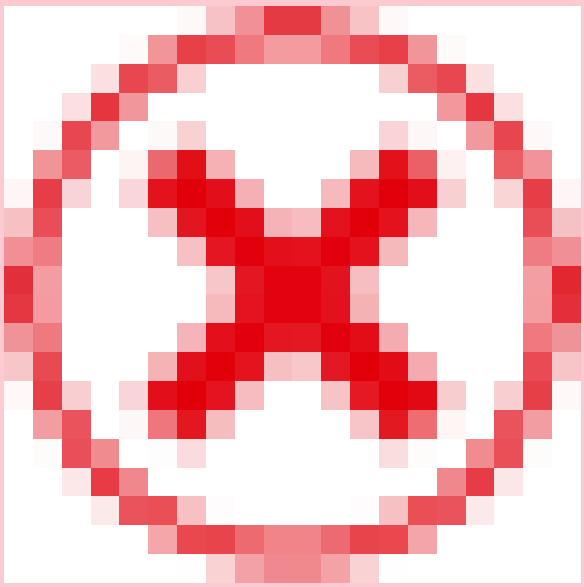
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Atribuídos a Mim	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

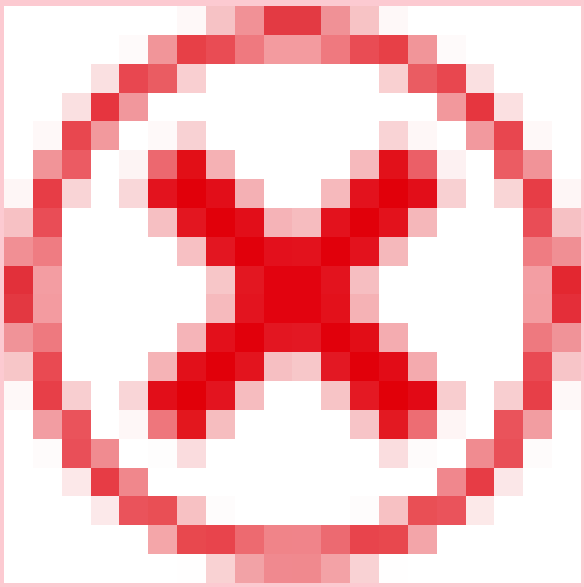
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Atribuído aos Meus grupos	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

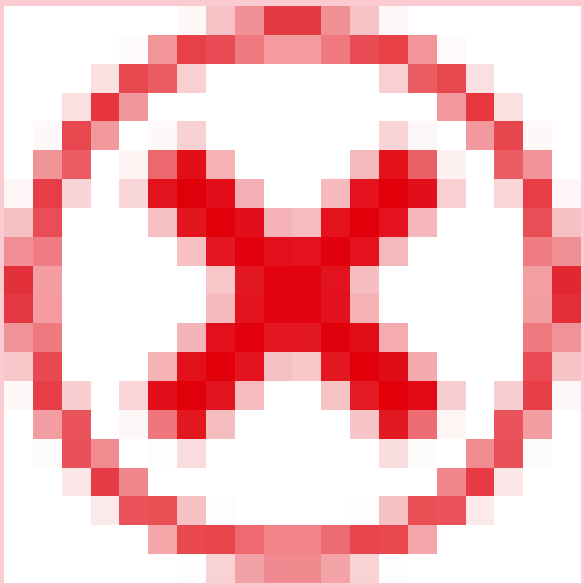
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Risco crítico e alto	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

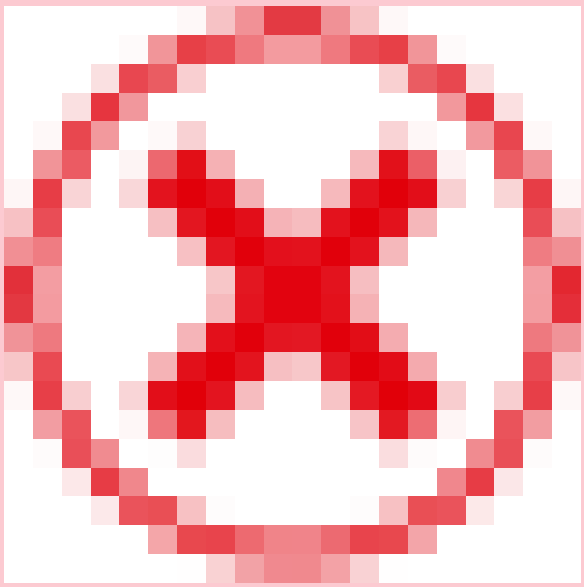
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Explorável	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

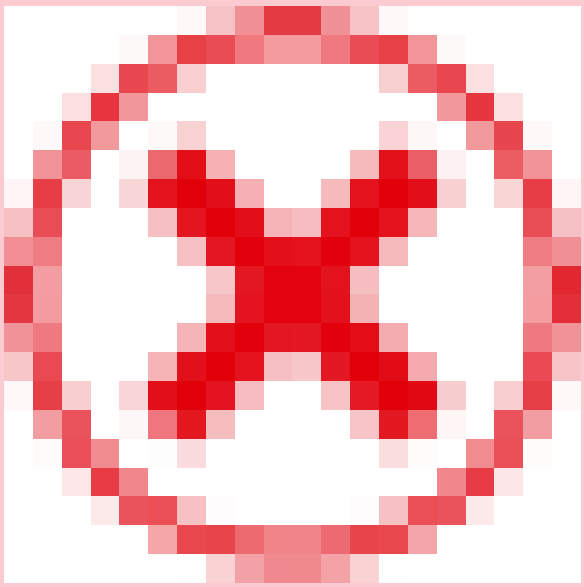
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Perto da meta	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

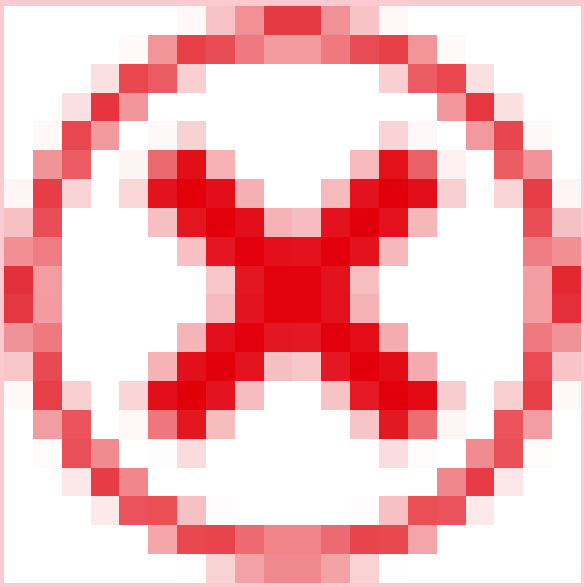
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Meta não atingida	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

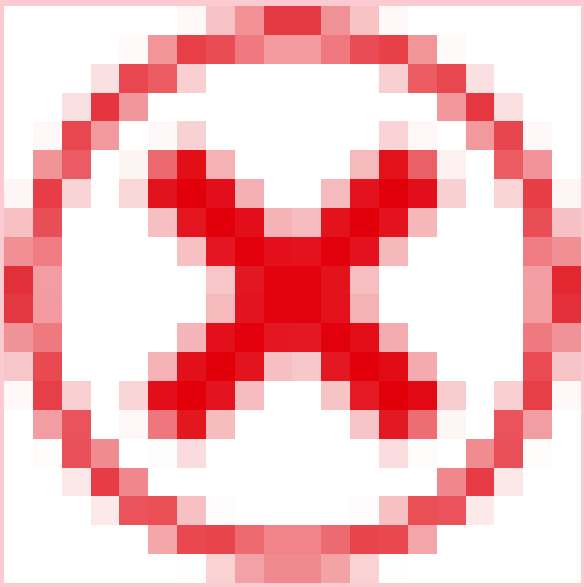
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Todos	
Bibliotecas	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

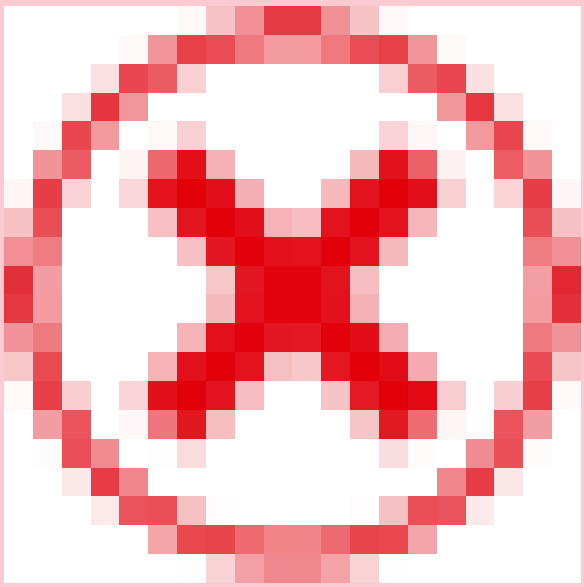
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
NVD	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

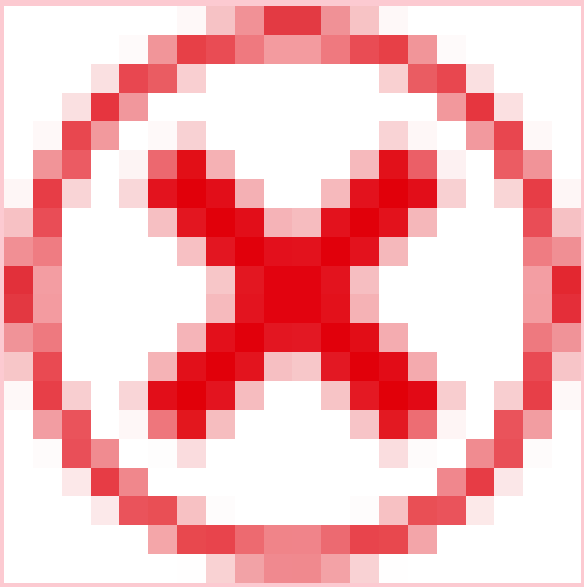
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Terceiros	
Administração	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

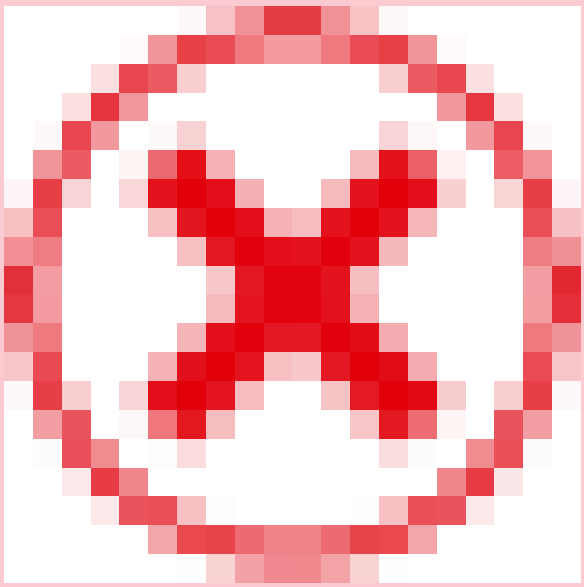
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Regras de atribuição	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

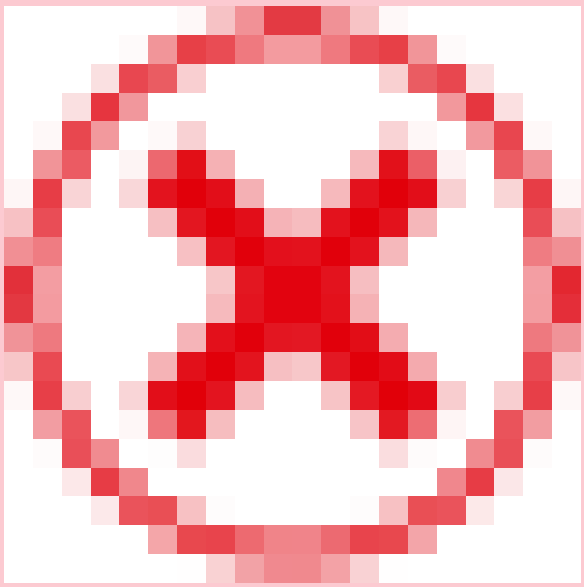
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Calculadoras de vulnerabilidade	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

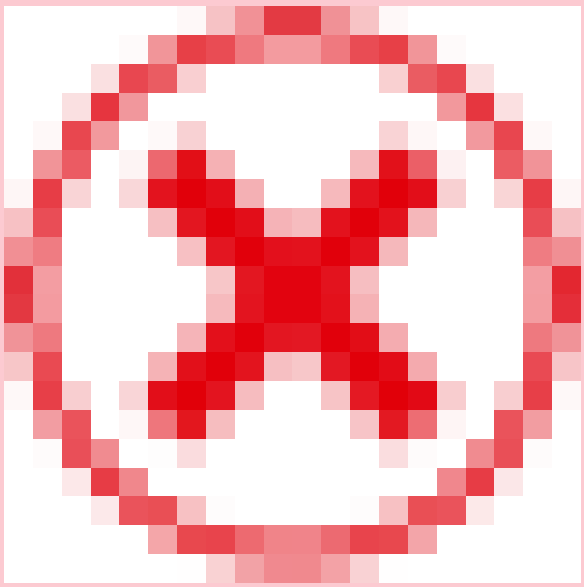
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Regras de destino de correção	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

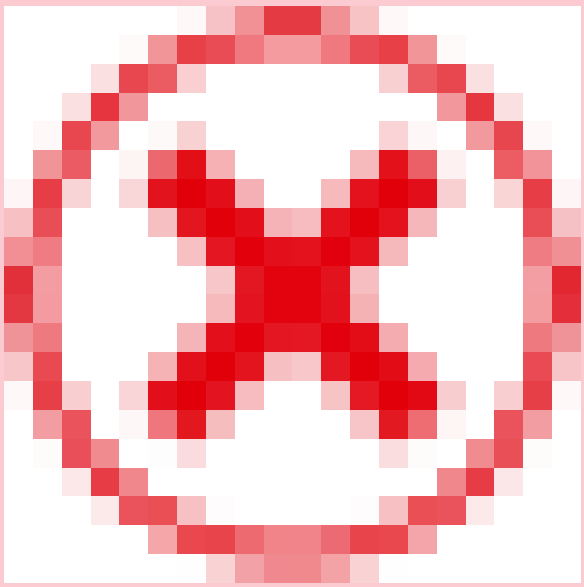
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Configurar granularidade de IV	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

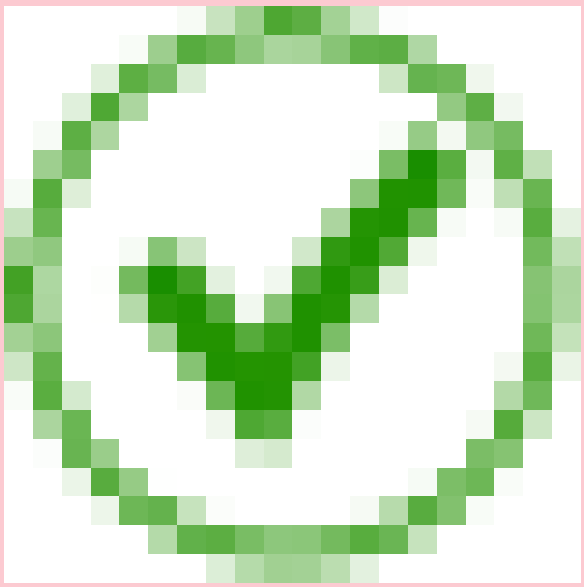
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Regras de exceção	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

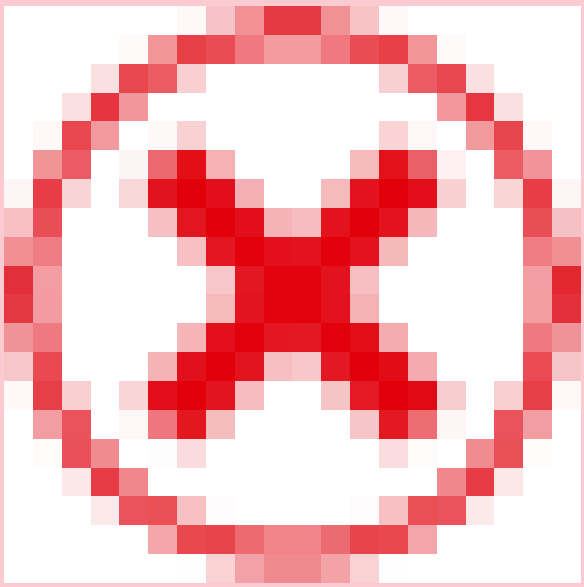
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Regras de aprovação	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

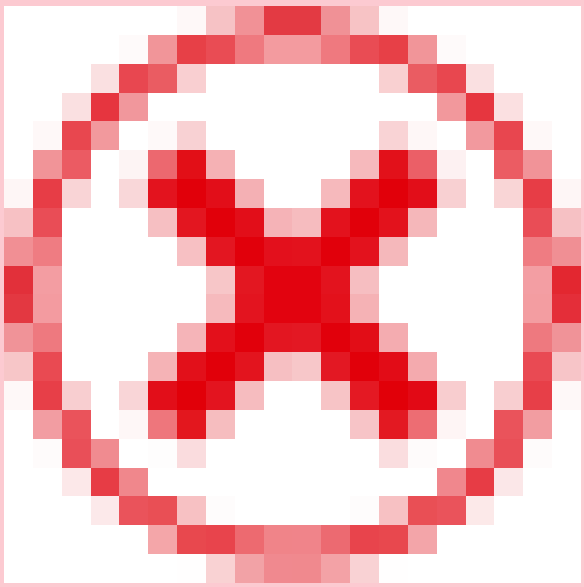
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Integrações de segurança do contêiner	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

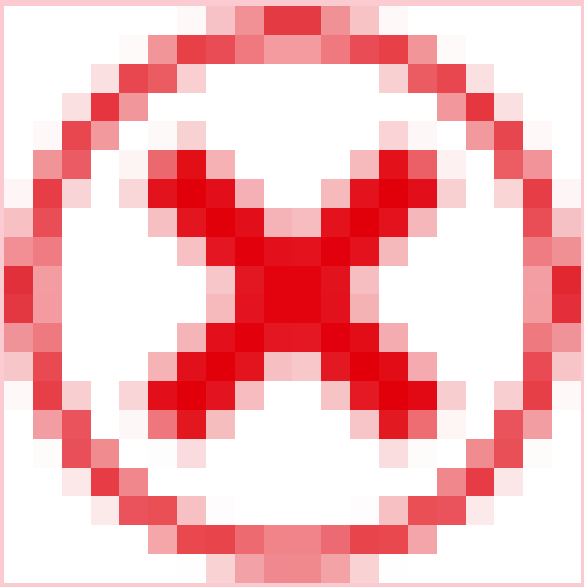
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Fechar automaticamente itens vulneráveis	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul_container.read_auto_exception_rule

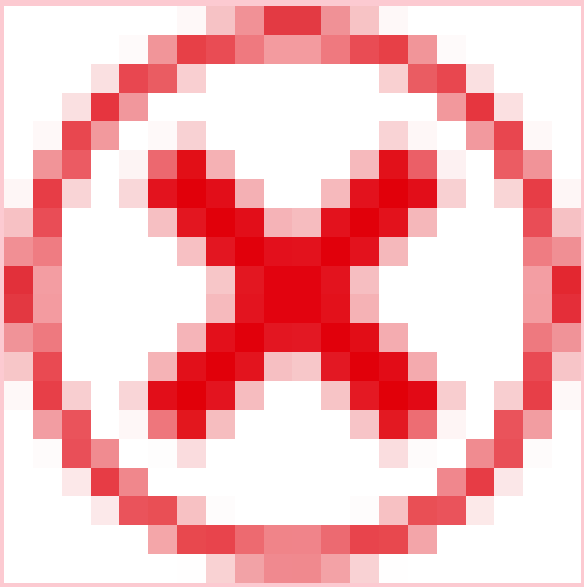
Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul_container.configure_integrations, sn_vul_container.configure_vi_granularity

sn_vul_container.exception_approver, sn_vul_container.false_positive_approver, sn_vul_container.manage_assignment_rules

sn_vul_container.manage_auto_close_stale_vi, sn_vul_container.manage_normalized_severity, sn_vul_container.manage_remediation_target_rules

sn_vul_container.manage_risk_score_configuration, sn_vul_container.read_all, sn_vul_container.read_assigned

Módulo	sn_vul_container.read_auto_exception_rule
Mapas de Gravidade Normalizados	

[End]

[store-future: BEGIN review]

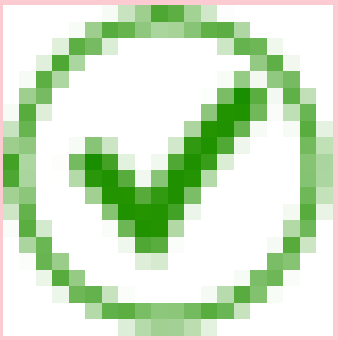
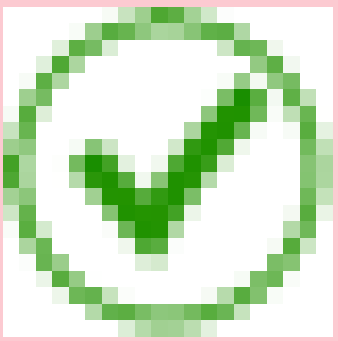
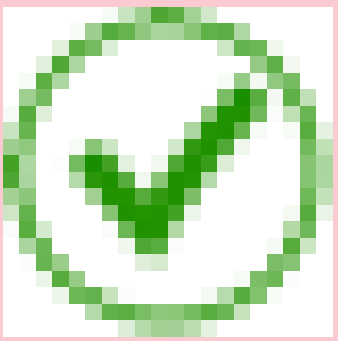
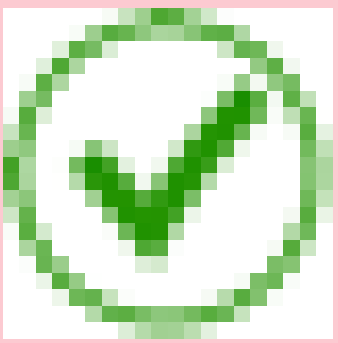
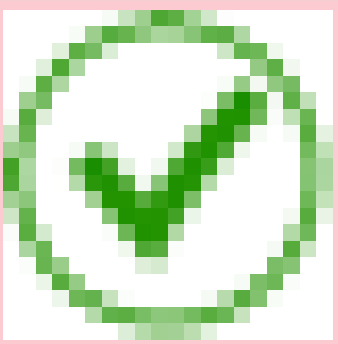
Acesso ao módulo por função para Administração do DLP

Para Administração do DLP, consulte os itens de menu que podem ser acessados por uma função específica.

Módulo	sn_dlir.analista
(Grupo de apps principal)	

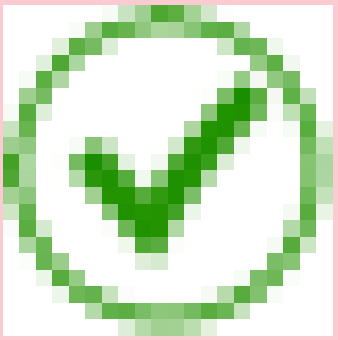
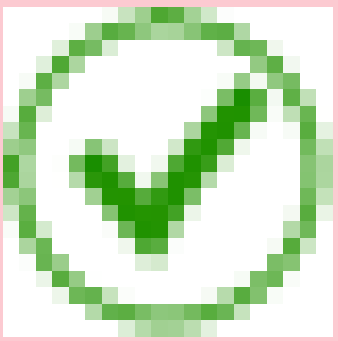
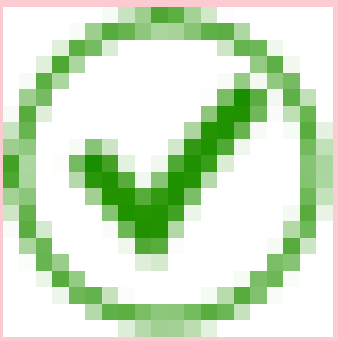
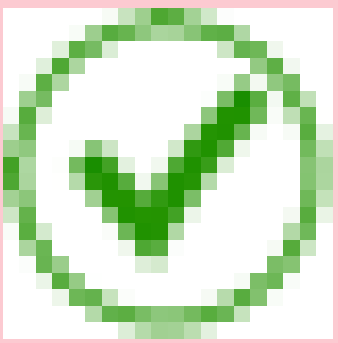
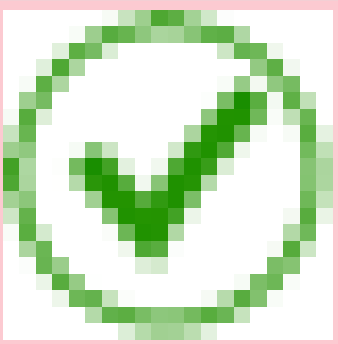
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_dlir.analista
Configuração padrão	
Regras de atribuição	
Regras do prazo da resposta	
Modelos de e-mail	
Avaliações	

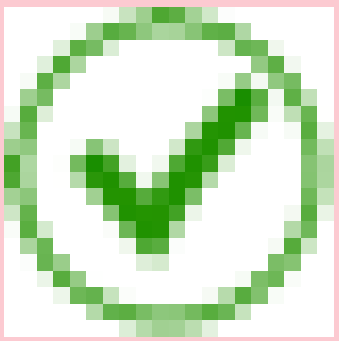
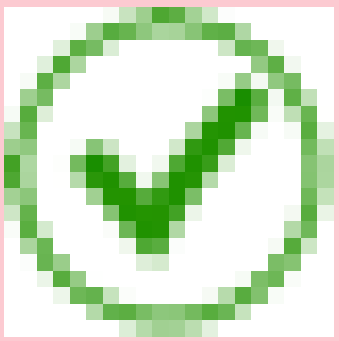
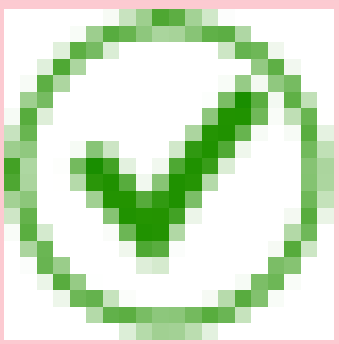
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_dlir.analista
Opções de resposta do incidente	
Configuração da Tabela de Idade	
Delegar configuração	
Estados personalizados	
Repetir regras de identificação de infração	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_dlir.analista
Campos personalizados	
Configurações Avançadas	
Restrições de acesso a incidentes	
Restrições de nível de registro	
Restrições de nível de campo	

[End]

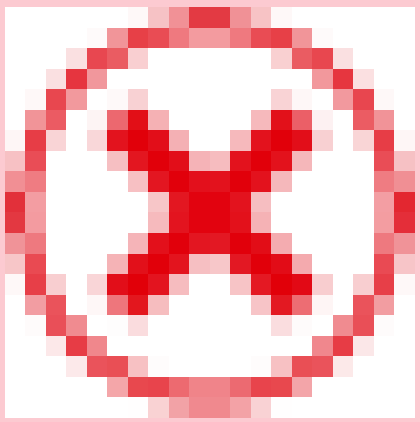
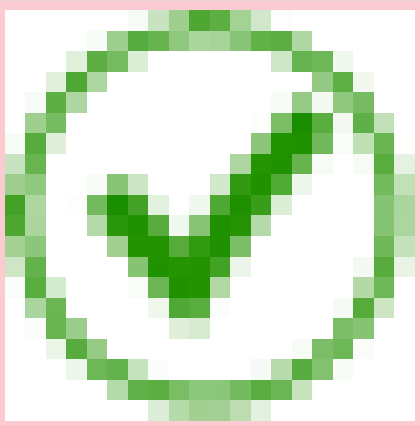
[store-future: BEGIN review]

Acesso ao módulo por função da Gestão de incidentes do DLP

Para o DLP Incident Management, consulte os itens de menu que podem ser acessados por uma função específica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_dlir.analista
(Grupo de apps principal)	
Portal de operações do DLP	
Portal do usuário final do DLP	
Painel do DLP	

[End]

[store-future: BEGIN review]

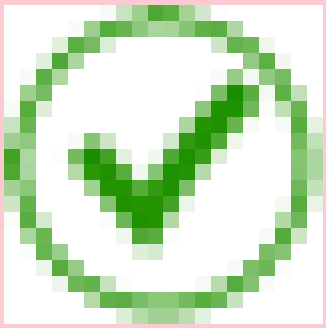
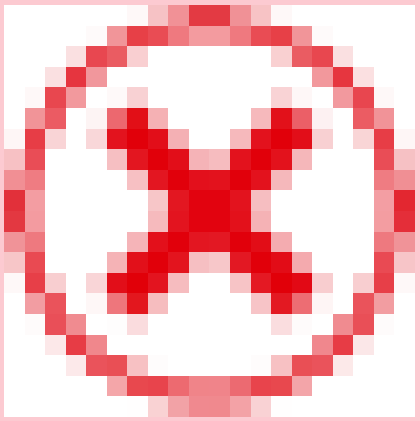
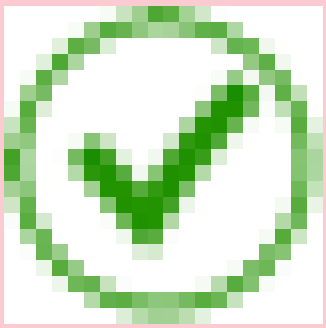
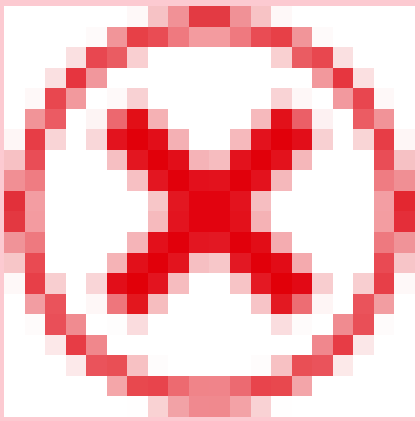
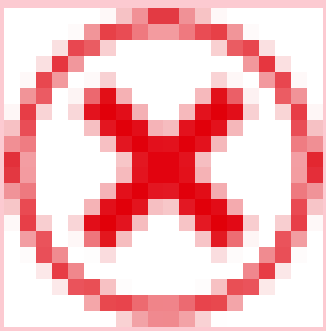
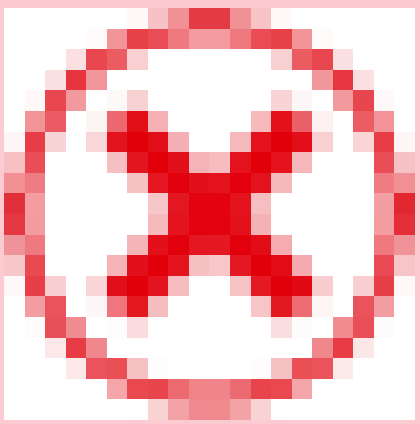
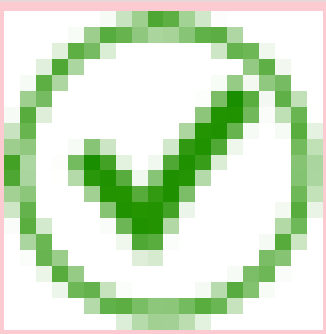
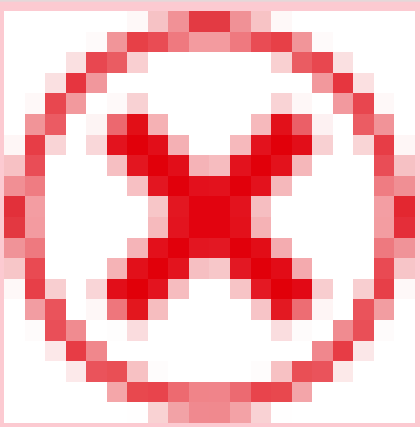
Acesso ao módulo por função para Data Certification

Para Data Certification, consulte os itens de menu que podem ser acessados por uma função específica.

Módulo	certification_admin	certification_filter_admin
(Grupo de apps principal)		

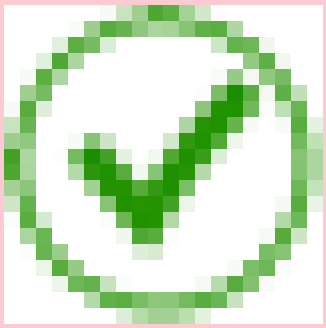
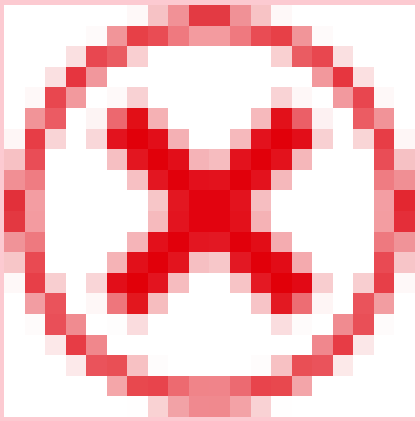
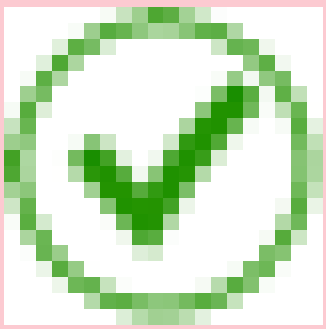
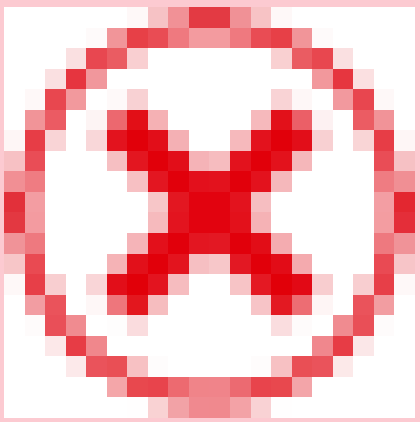
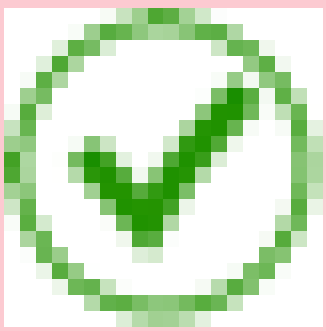
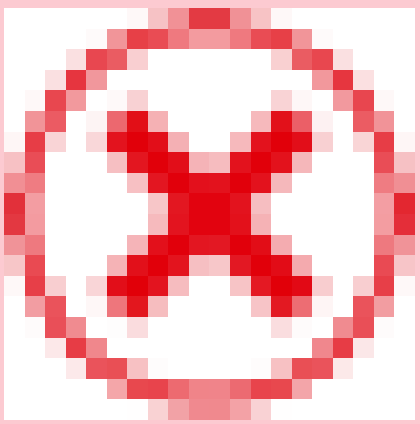
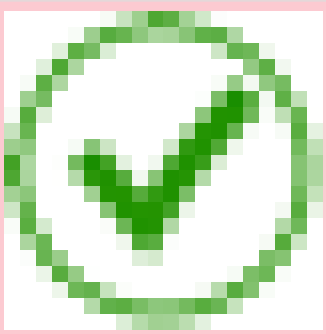
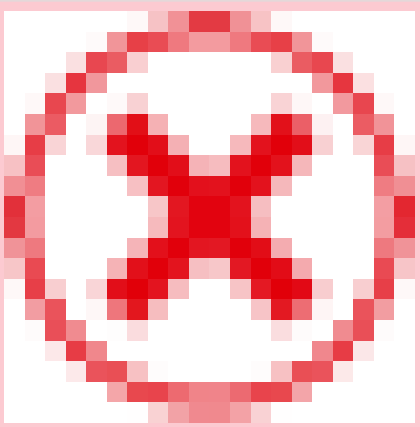
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	certification_admin	certification_filter_admin
Visão geral		
Introdução		
Tarefas		
Minhas Tarefas		
Abertos		

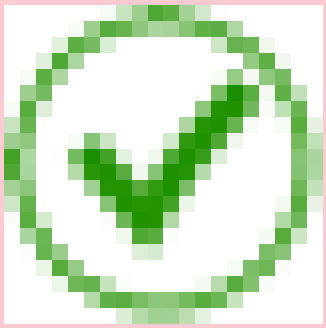
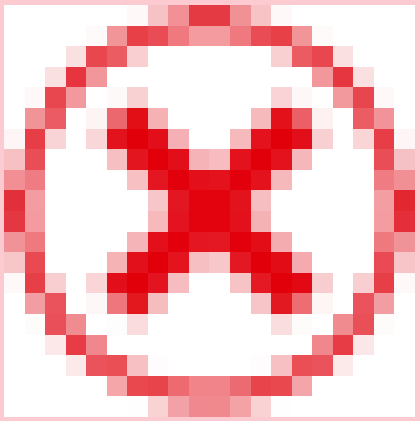
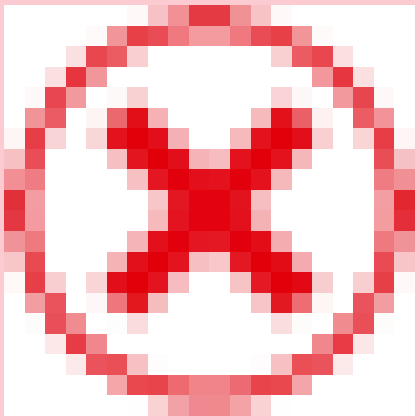
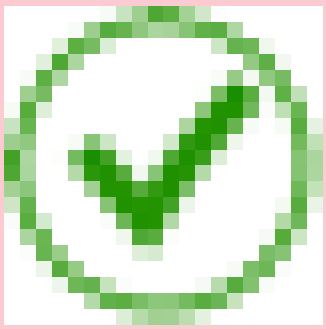
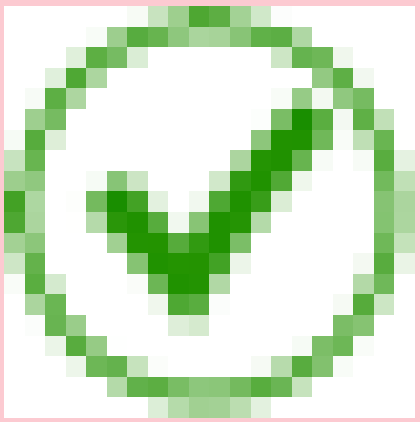
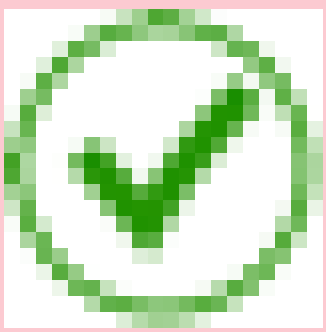
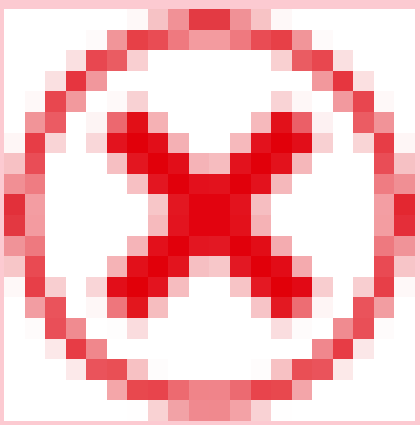
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	certification_admin	certification_filter_admin
Todas as tarefas		
Certificações		
Certificado		
Pendente		
Todos		

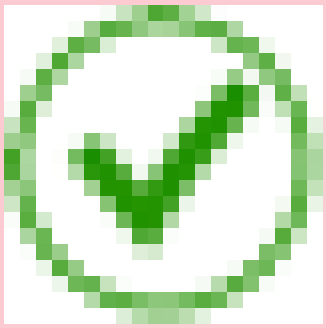
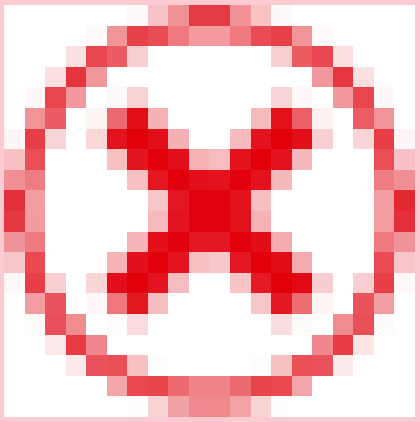
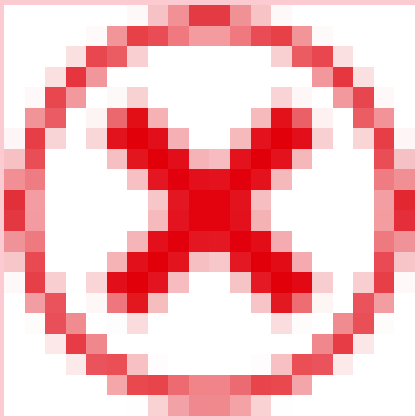
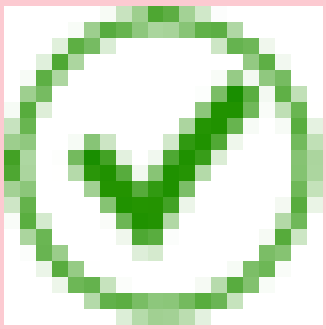
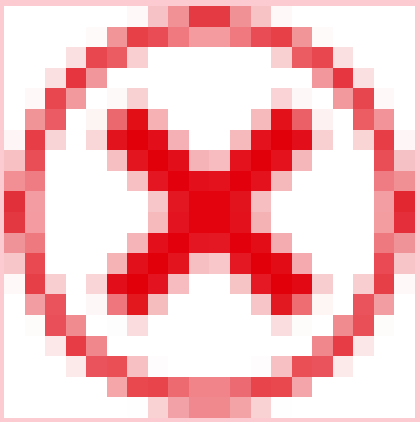
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	certification_admin	certification_filter_admin
Programações		
Criar novo		
Definições de Programação		
Filtros de certificação		
Instâncias		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	certification_admin	certification_filter_admin
Resultados de Auditoria		
Auditorias		
Definições de Auditoria		
Instâncias de Auditoria		

[End]

[store-future: BEGIN review]

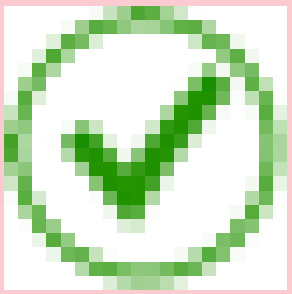
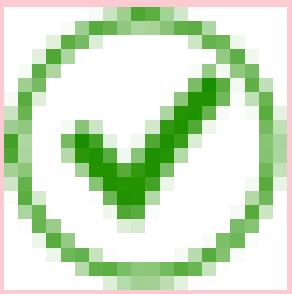
Acesso ao módulo por função para IBM QRadar Integration

Para o IBM QRadar Integration, consulte os itens de menu que podem ser acessados por uma função específica.

Módulo	sn_si.analyst
(Grupo de apps principal)	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_si.analyst
Perfil do IBM QRadar	
Importação de infração do IBM QRadar	
IBM QRadar de ataque a tarefa	
Tradução de campo do IBM QRadar	
Configurações de integração do IBM QRadar	

[End]

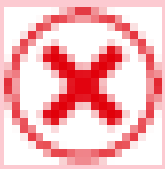
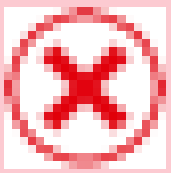
[store-future: BEGIN review]

Acesso ao módulo por função para integração de MISP

Para integração de MISP, consulte os itens de menu que podem ser acessados por uma função específica.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_si.admin	sn_si.analista	sn_ti.admin	sn_ti.read	sn_ti.escrever
(Grupo de apps principal)					
Configurações de integração					
Configuração de pesquisa de detecções					
Perfis automáticos de criação de evento					
Fila de criação de evento automático					
Dados do evento de MISP					
Eventos de MISP associados					
Informação do usuário de MISP					

[End]

[store-future: BEGIN review]

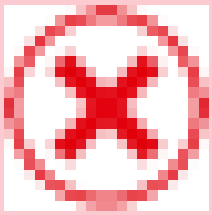
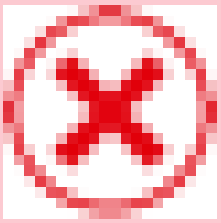
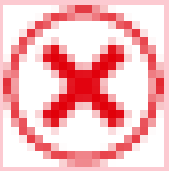
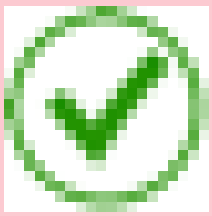
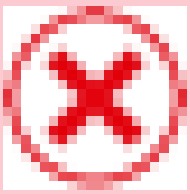
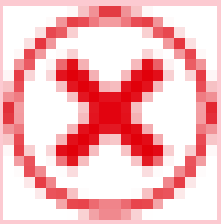
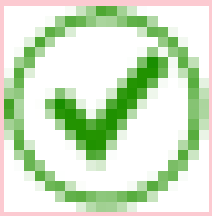
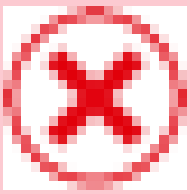
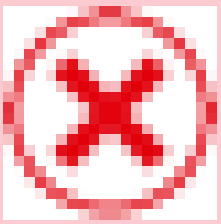
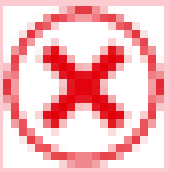
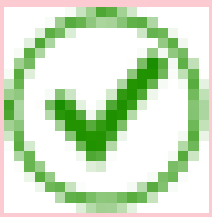
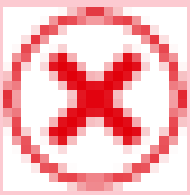
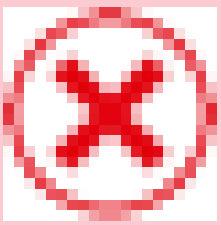
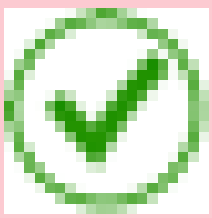
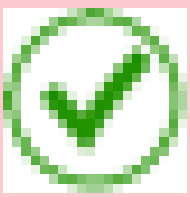
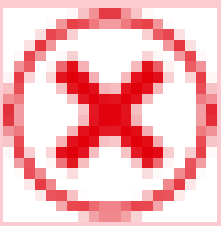
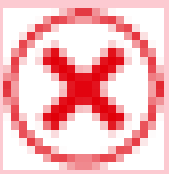
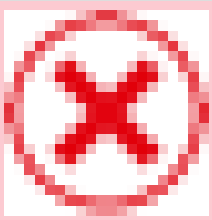
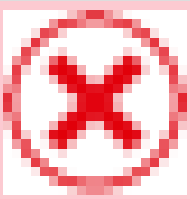
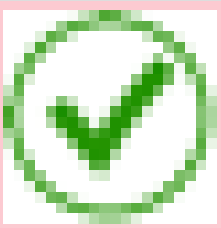
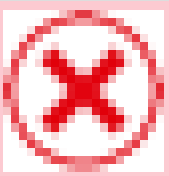
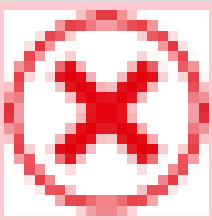
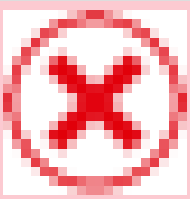
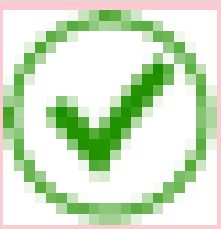
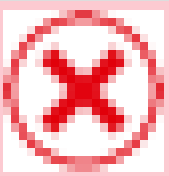
Acesso ao módulo por função do Microsoft Azure Defender para IoT

Para o Microsoft Azure Defender for IoT, consulte os itens de menu que podem ser acessados por uma função específica.

Módulo	cmdb_inst_admin	cmdb_ot_admin	connection_admin	import_admin
(Grupo de apps principal)				

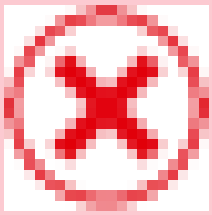
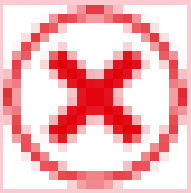
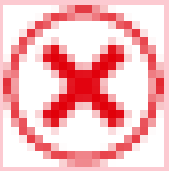
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	cmdb_inst_admin	cmdb_ot_admin	connection_admin	import_admin
Configuração				
Fontes de dados				
IntegrationHub ETL				
Programações de Importação				
Propriedades				
Conexões e Credenciais				
Aliases de credencial de conexão				
Credenciais				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

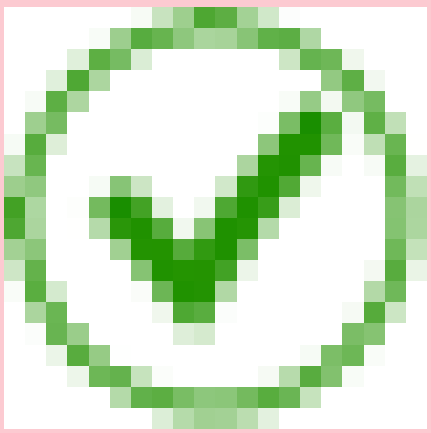
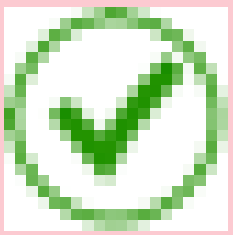
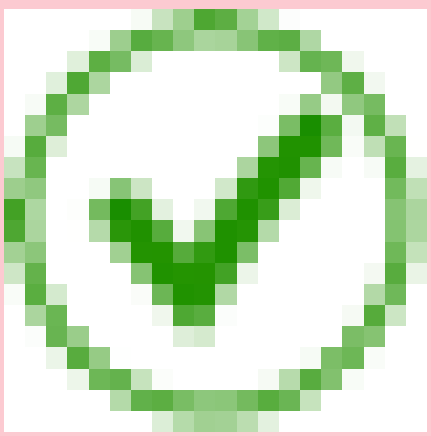
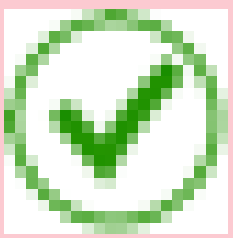
Módulo	cmdb_inst_admin	cmdb_ot_admin	connection_admin	import_admin
Conexões				

[End]

[store-future: BEGIN review]

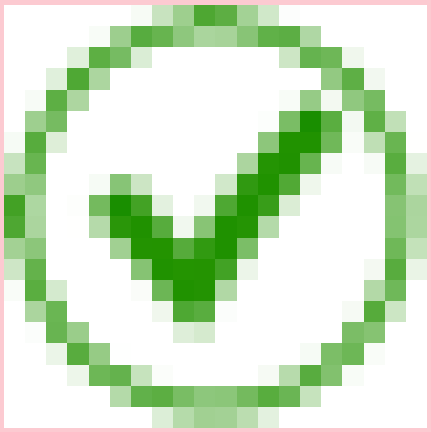
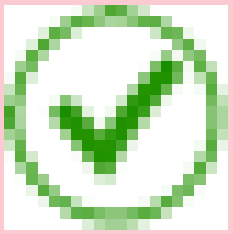
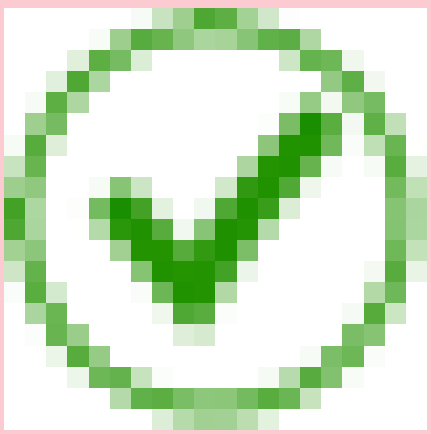
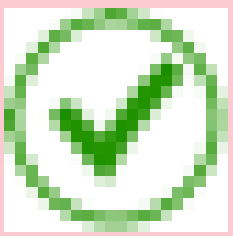
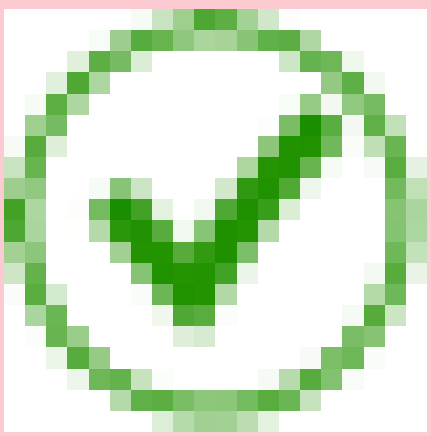
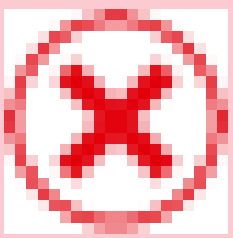
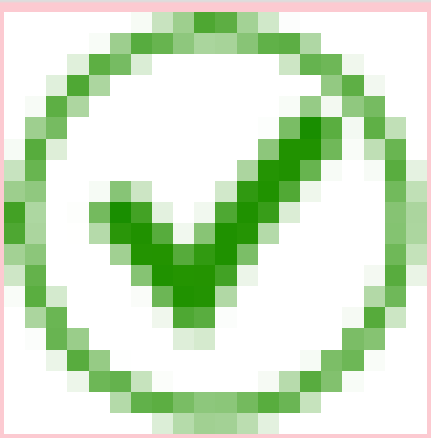
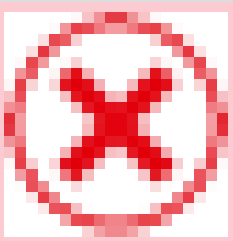
Acesso ao módulo por função para Qualys Vulnerability Integration

Para o Qualys Vulnerability Integration, consulte os itens de menu que podem ser acessados por uma função específica.

Módulo	sn_vul.configure_qualys_integration	sn_vul_qualys.read
(Grupo de apps principal)		
Visão geral		
Status da Execução da Integração		

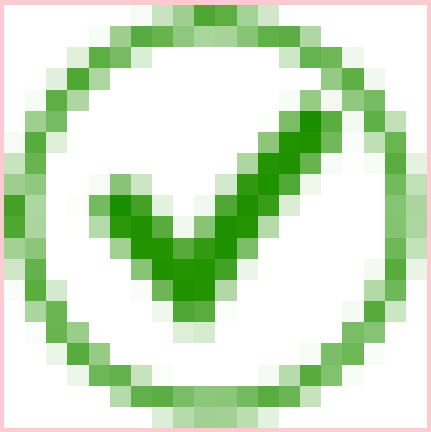
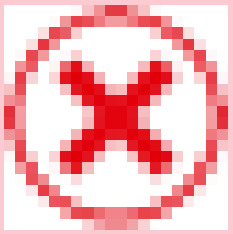
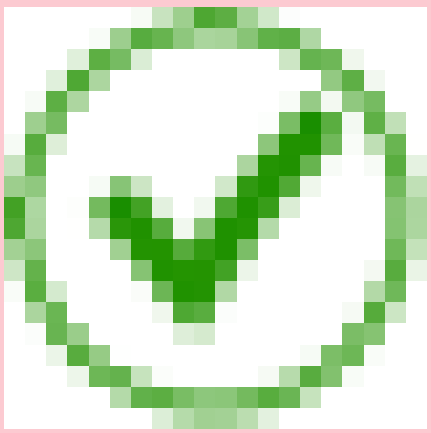
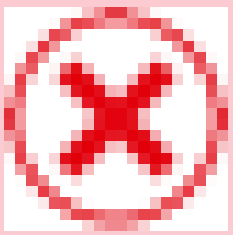
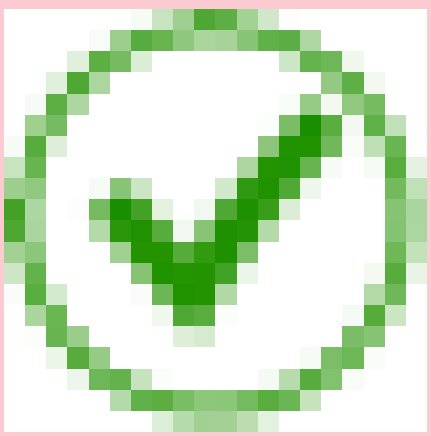
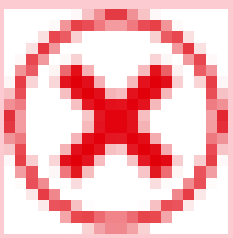
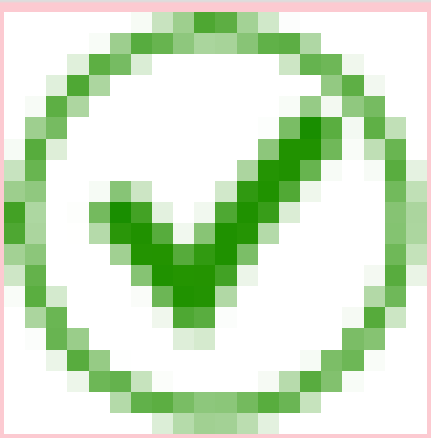
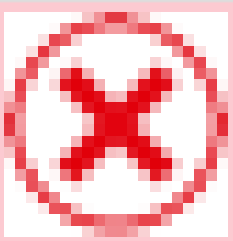
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_vul.configure_qualys_integration	sn_vul_qualys.read
Dispositivos de Scanner		
Listas de Pesquisa		
Administração		
Instâncias de Integração		
Integrações Primárias		

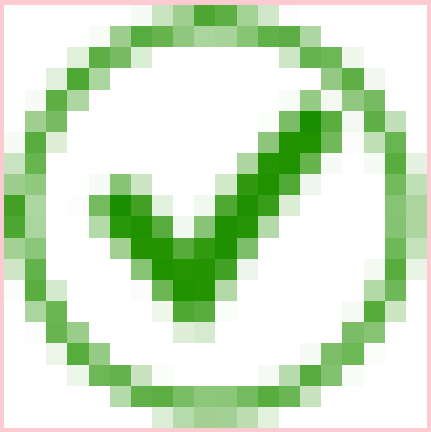
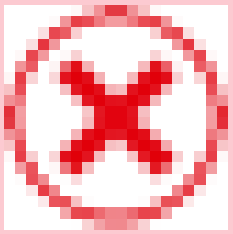
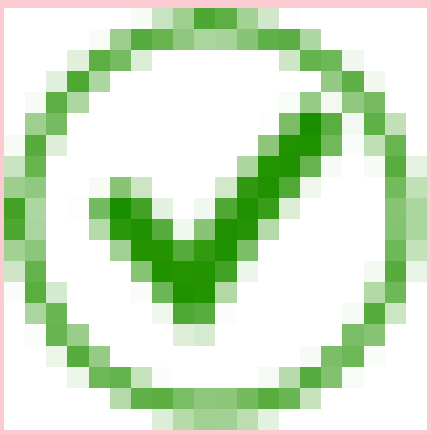
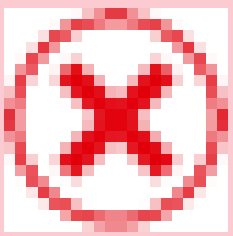
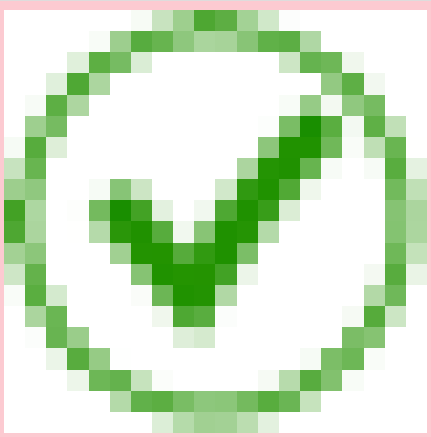
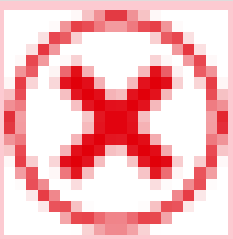
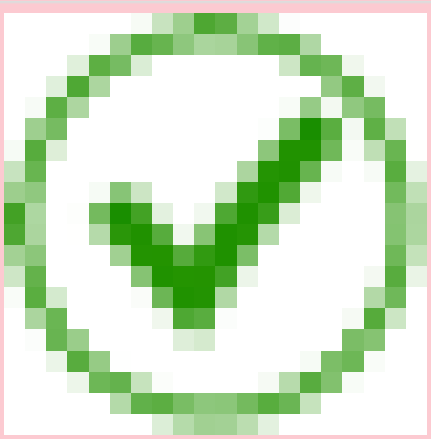
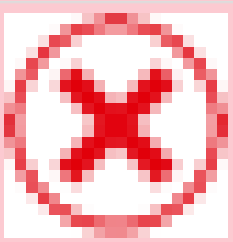
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_vul.configure_qualys_integration	sn_vul_qualys.read
Integrações de Suporte		
Tabelas do conjunto de importação		
Importação de host		
Importação da Lista de Detecção de Host		
Importação da Base de Conhecimento		

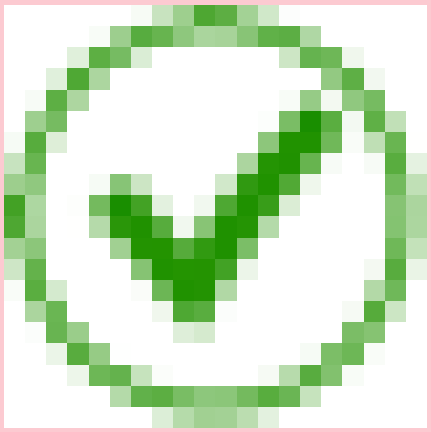
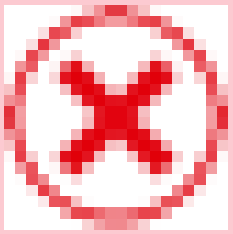
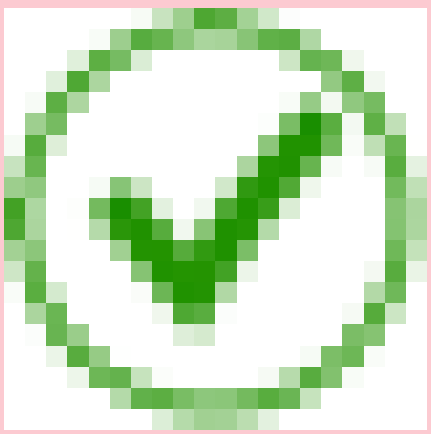
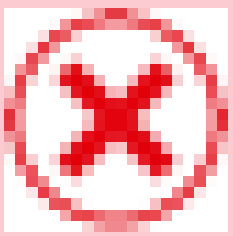
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_vul.configure_qualys_integration	sn_vul_qualys.read
Importação de Lista de Tíquetes		
Importação de Lista de Pesquisa Dinâmica		
Importação de Lista de Pesquisa Estática		
Importação de Grupo de Ativos		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

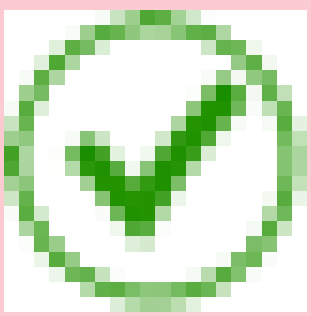
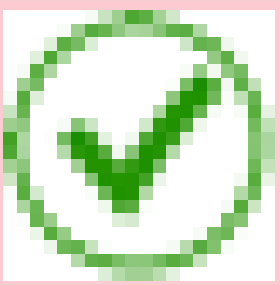
Módulo	sn_vul.configure_qualys_integration	sn_vul_qualys.read
Importação de Dispositivo		
Importação de Paginação de Detecção de Host		

[End]

[store-future: BEGIN review]

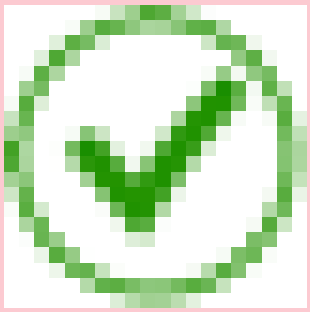
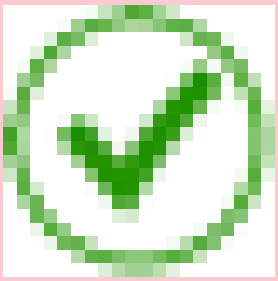
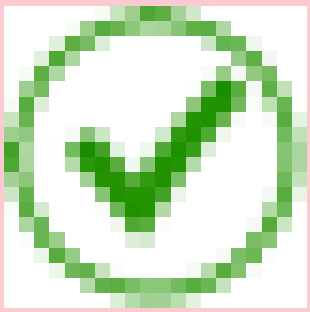
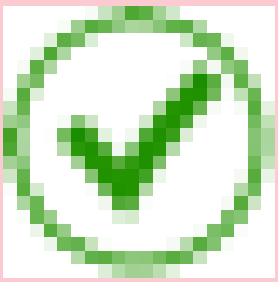
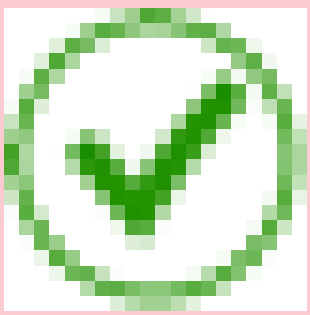
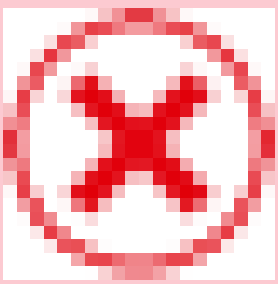
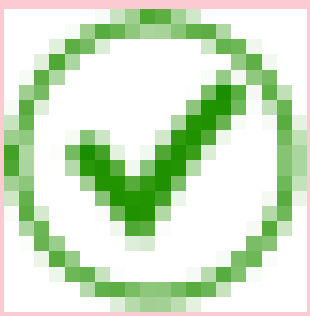
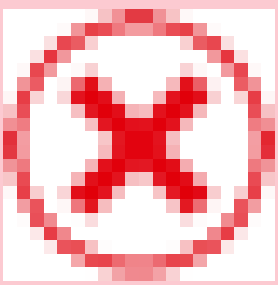
Acesso ao módulo por função para Rapid7 Vulnerability Integration

Para Rapid7 Vulnerability Integration, consulte os itens de menu que podem ser acessados por uma função específica.

Módulo	sn_vul_r7.admin	sn_vul_r7.read
(Grupo de apps principal)		
Status da Execução da Integração		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_vul_r7.admin	sn_vul_r7.read
Sites		
Soluções		
Administração		
Integrações		
Configuração		

[End]

[store-future: BEGIN review]

Acesso ao módulo por função para incidente de segurança

Para Incidente de segurança, consulte os itens de menu que podem ser acessados por uma função específica.

Tradução automática

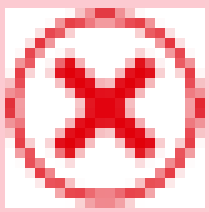
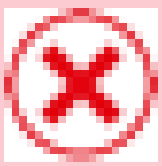
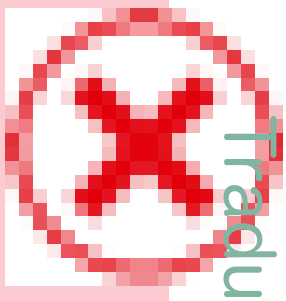
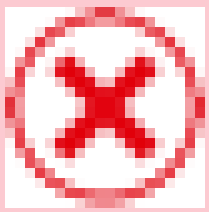
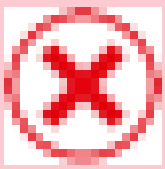
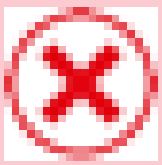
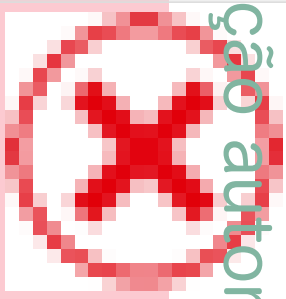
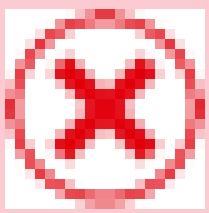
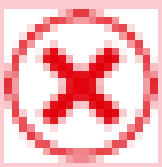
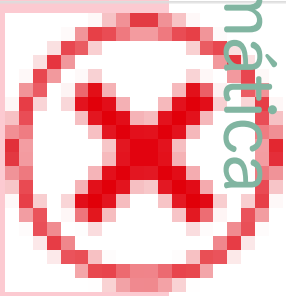
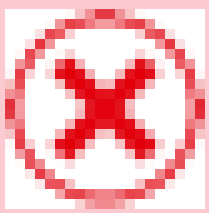
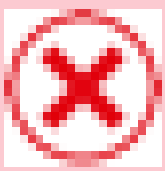
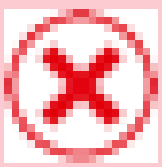
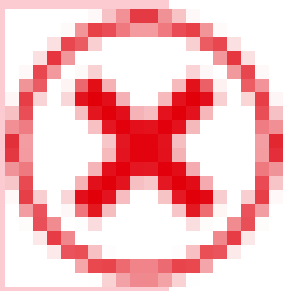
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informações para outras funções:

sn_si.special_access, sn_si_approver_user

Módulo	sn_sec_cmn.read	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.externo	sn_si.knowledge_admin	sn_si
(Grupo de apps principal)							
Nova IU de incidentes							
Impacto do Serviço							
Visão geral							
Tempo real							
Incidentes							

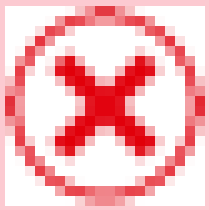
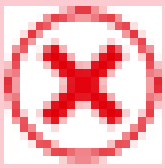
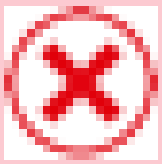
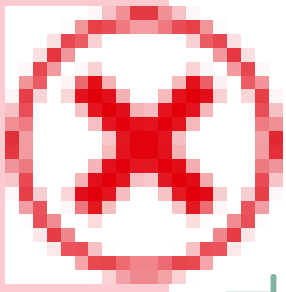
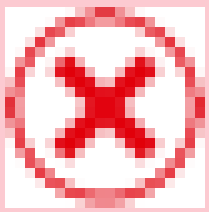
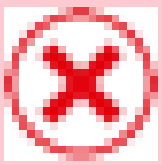
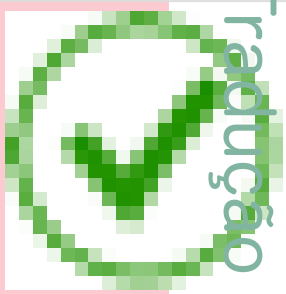
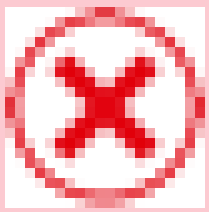
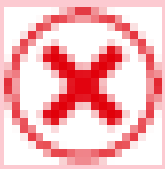
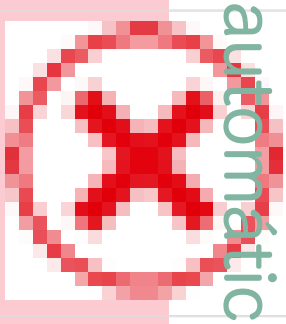
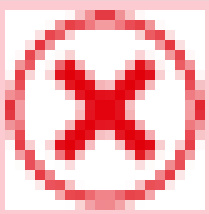
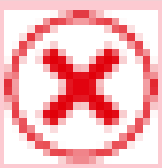
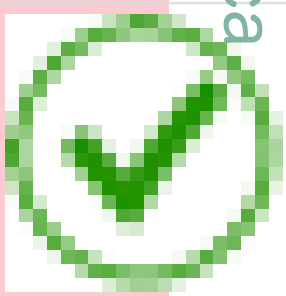
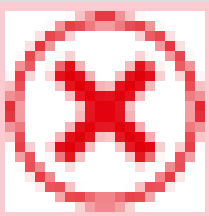
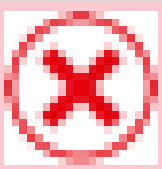
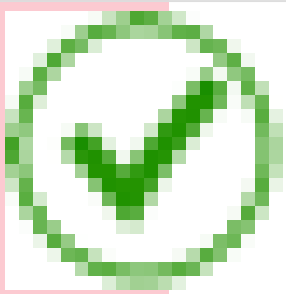
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informações para outras funções:

sn_si.special_access, sn_si_approver_user

Módulo	sn_sec_cmn.read	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.externo	sn_si.knowledge_admin	sn_si
Visível para Mim							
Atribuídos a Mim							
Meus Trabalhos							
Atribuído à Equipe							
Mostrar incidentes em aberto							

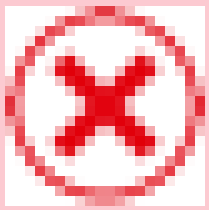
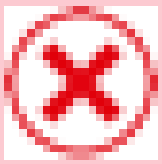
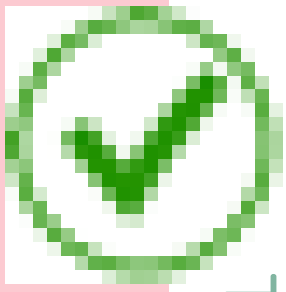
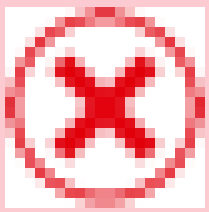
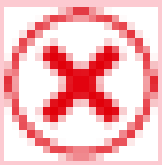
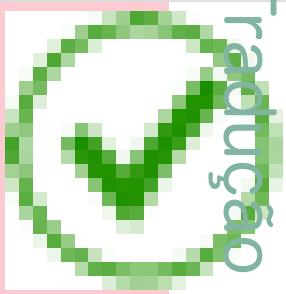
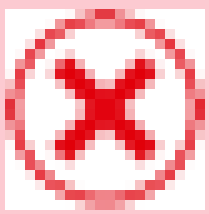
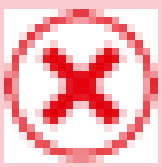
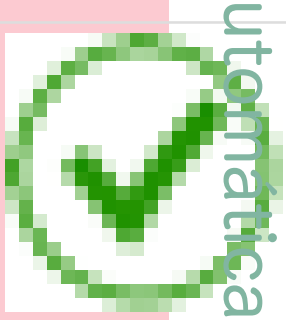
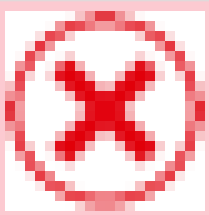
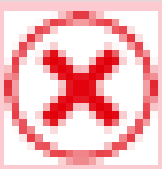
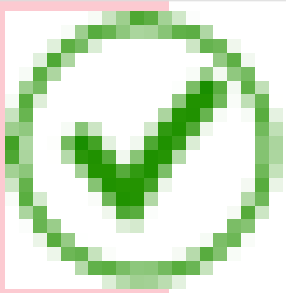
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informações para outras funções:

sn_si.special_access, sn_si_approver_user

Módulo	sn_sec_cmn.read	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.externo	sn_si.knowledge_admin	sn_si
Mostrar Todos os Incidentes							
Incidentes não atribuídos							
Tarefas de resposta							
Atribuídos a Mim							
Atribuído à Equipe							

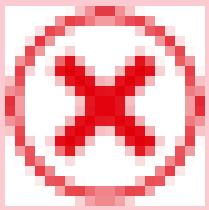
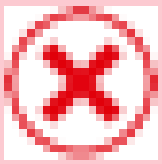
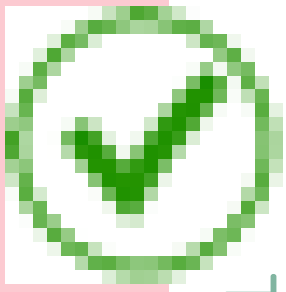
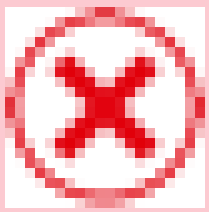
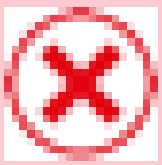
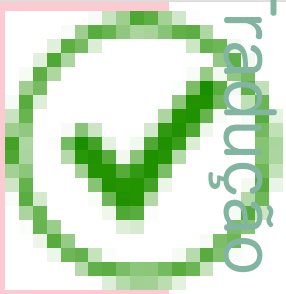
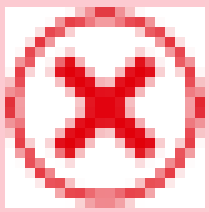
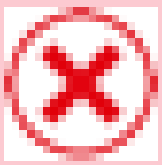
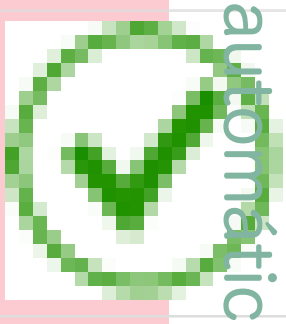
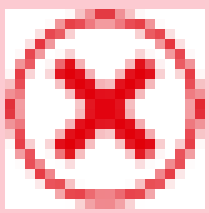
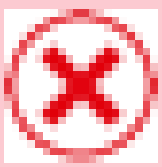
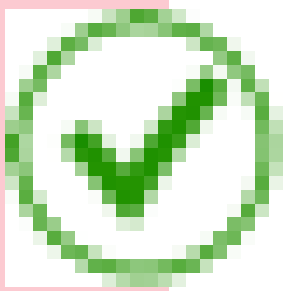
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informações para outras funções:

sn_si.special_access, sn_si_approver_user

Módulo	sn_sec_cmn.read	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.externo	sn_si.knowledge_admin	sn_si
Mostrar Tarefas Abertas							
Mostrar Todas as Tarefas							
Tarefas não atribuídas							
Solicitações de Entrada							
Atribuídos a Mim							

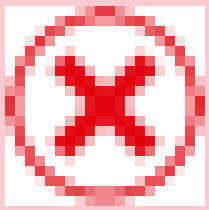
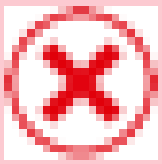
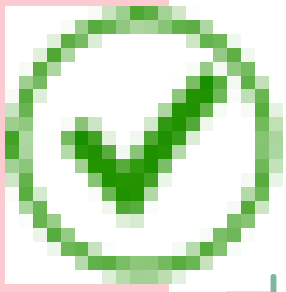
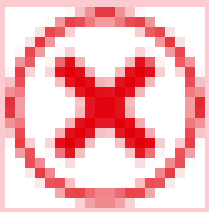
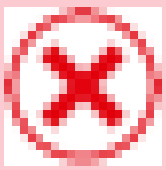
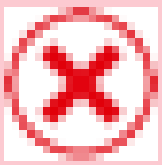
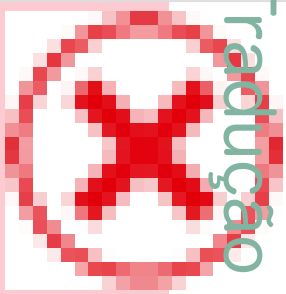
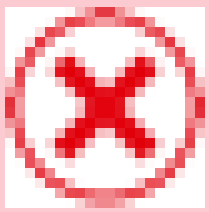
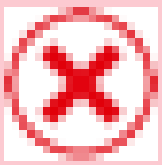
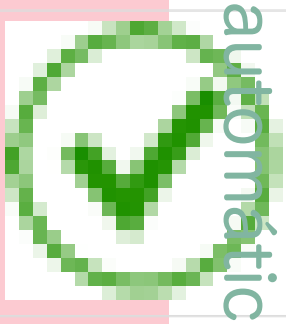
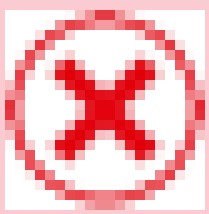
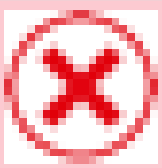
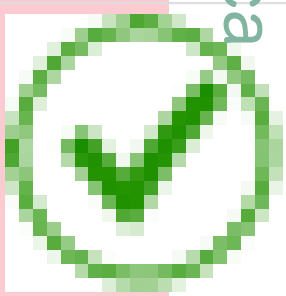
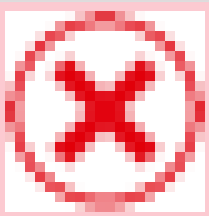
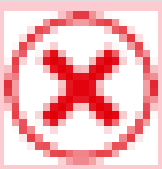
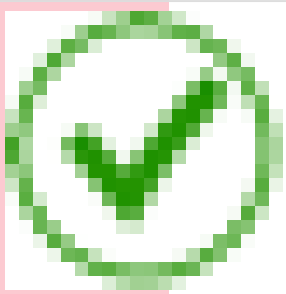
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informações para outras funções:

sn_si.special_access, sn_si_approver_user

Módulo	sn_sec_cmn.read	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.externo	sn_si.knowledge_admin	sn_si
Atribuído à Equipe							
Minhas aprovações							
Mostrar solicitações em aberto							
Mostrar Todas as Solicitações							
Solicitações Não Atribuídas							

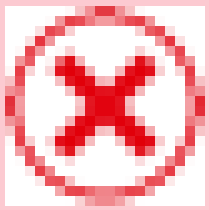
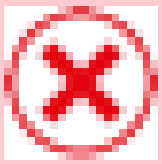
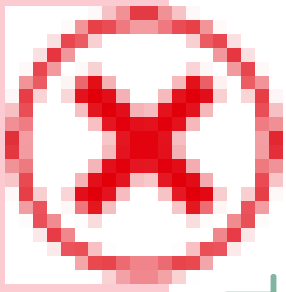
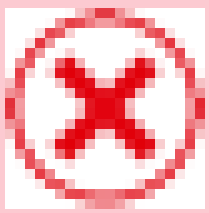
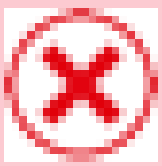
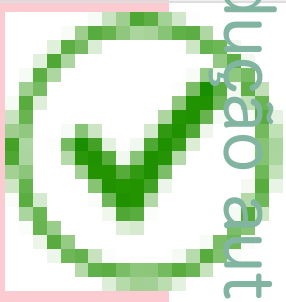
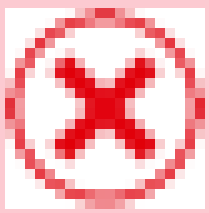
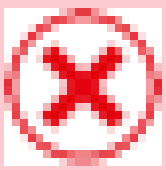
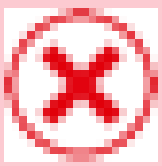
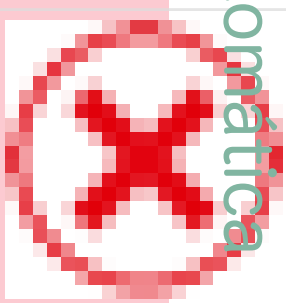
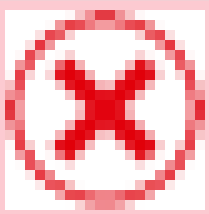
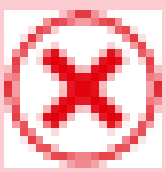
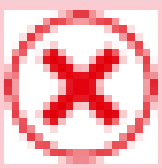
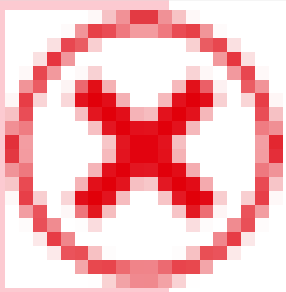
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informações para outras funções:

sn_si.special_access, sn_si_approver_user

Módulo	sn_sec_cmn.read	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.externo	sn_si.knowledge_admin	sn_si
Meu Mapa							
Alertas e eventos							
Análise pós-incidente							
Minhas Revisões Pendentes							
Revisões pendentes da equipe							
Todas as Revisões Incompletas							
Configuração							

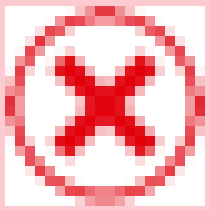
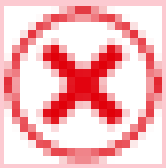
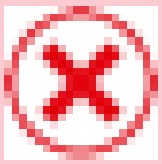
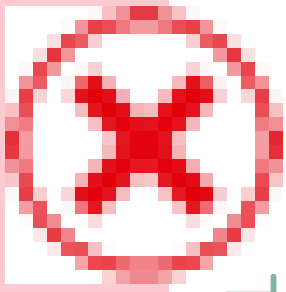
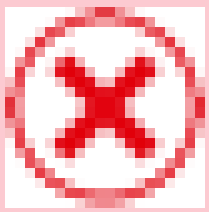
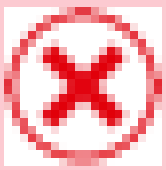
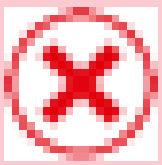
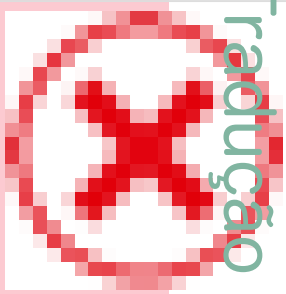
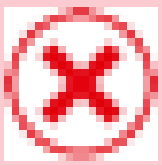
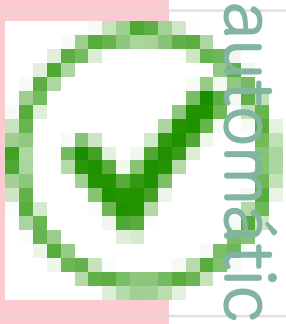
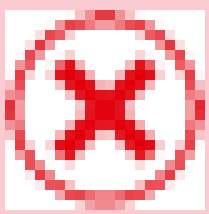
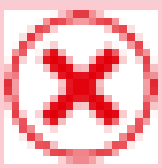
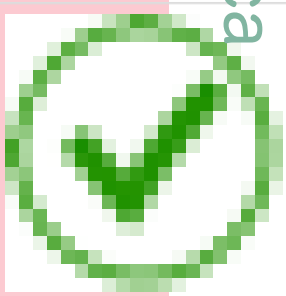
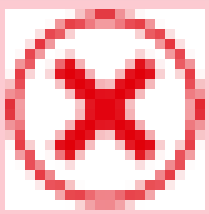
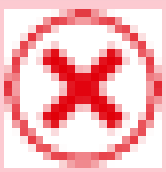
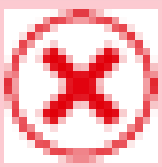
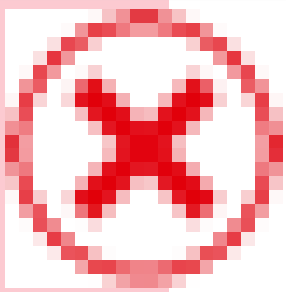
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informações para outras funções:

sn_si.special_access, sn_si_approver_user

Módulo	sn_sec_cmn.read	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.externo	sn_si.knowledge_admin	sn_si
Grupos de calculadoras de incidentes de segurança							
Calculadoras de Severidade							
Configuração de pontuação de risco							
Configuração do Feed de Notícias							
Grupos							

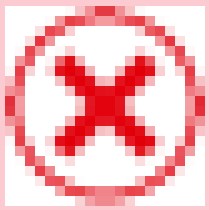
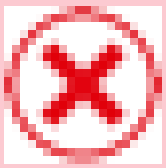
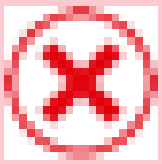
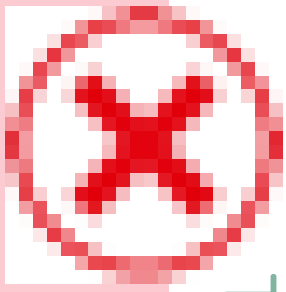
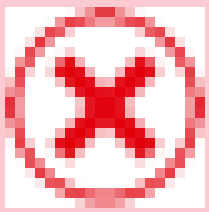
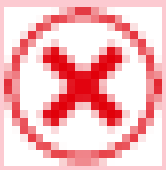
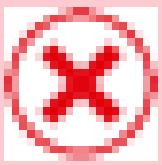
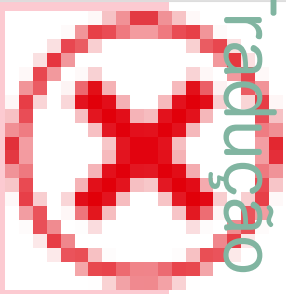
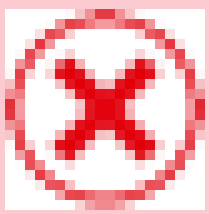
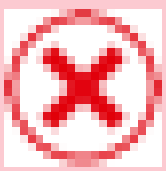
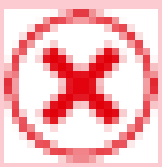
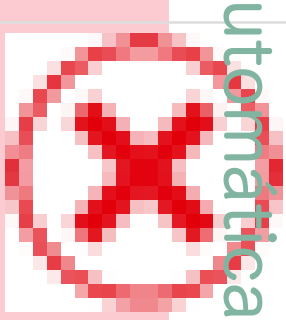
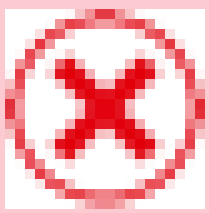
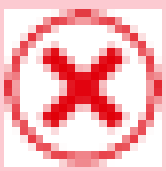
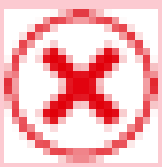
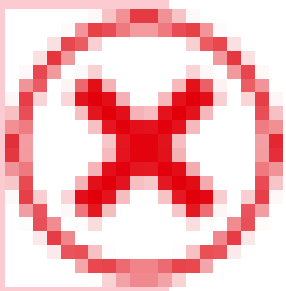
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informações para outras funções:

sn_si.special_access, sn_si_approver_user

Módulo	sn_sec_cmn.read	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.externo	sn_si.knowledge_admin	sn_si
Funções							
SLAs							
Configuração do espaço de analista (nova IU)							
Assistente de configuração							
Configuração de filtro da página principal							

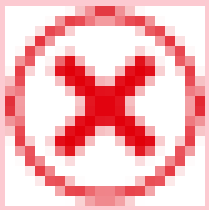
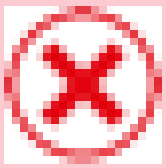
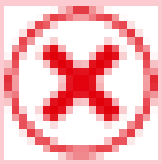
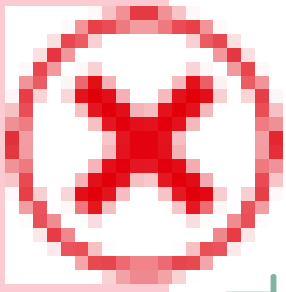
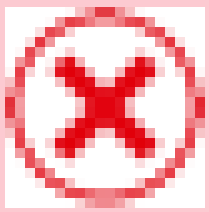
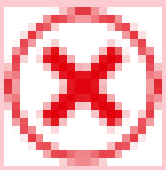
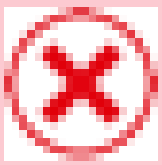
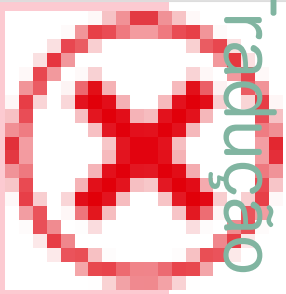
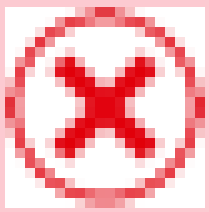
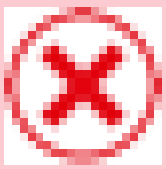
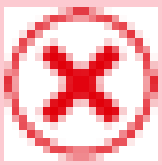
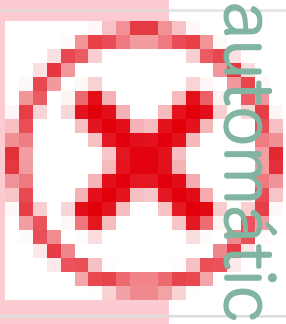
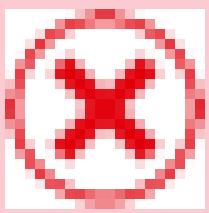
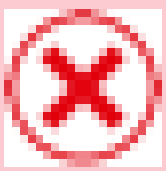
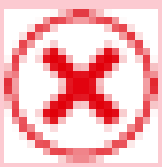
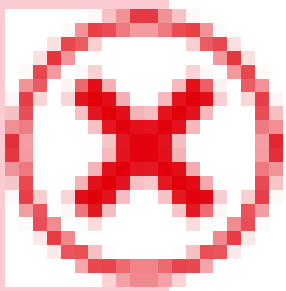
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informações para outras funções:

sn_si.special_access, sn_si_approver_user

Módulo	sn_sec_cmn.read	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.externo	sn_si.knowledge_admin	sn_si
Ações de IU de Formulário							
Configurações de Lista relacionada							
Propriedades do espaço do analista							
Catálogo e Conhecimento							
Modelos de Incidente de segurança							

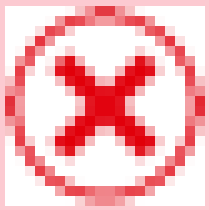
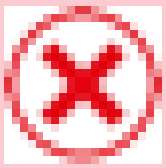
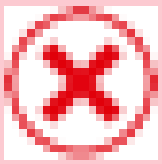
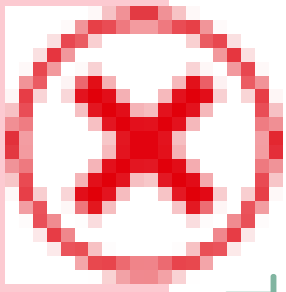
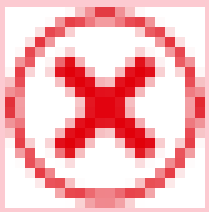
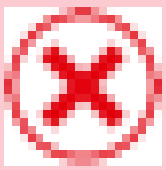
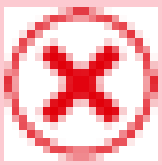
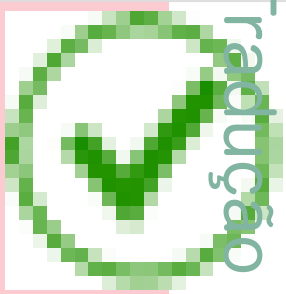
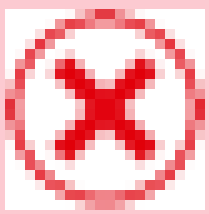
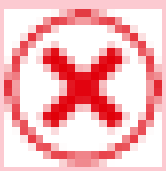
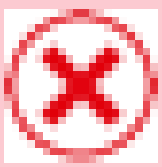
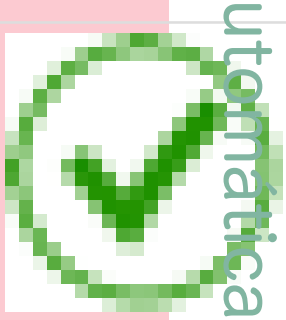
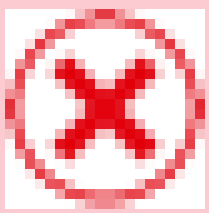
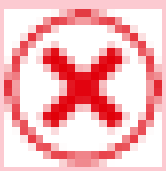
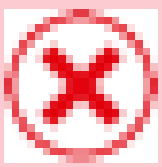
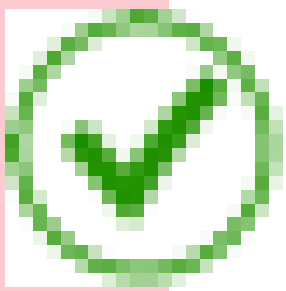
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informações para outras funções:

sn_si.special_access, sn_si_approver_user

Módulo	sn_sec_cmn.read	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.externo	sn_si.knowledge_admin	sn_si
Manter Itens do catálogo							
Conhecimento							
Runbook manual							
Criar Novo Runbook							
Exibir Documentos do Runbook							
Administração							

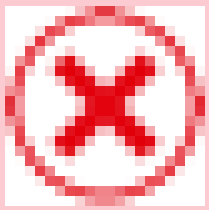
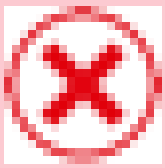
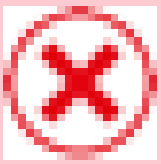
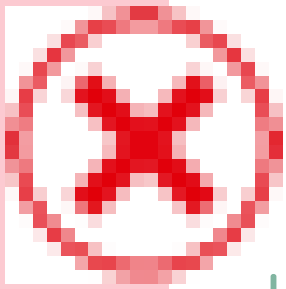
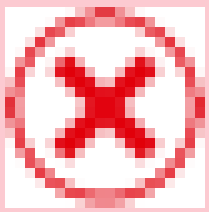
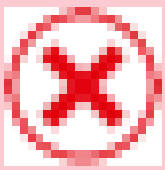
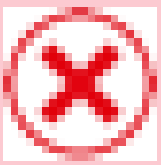
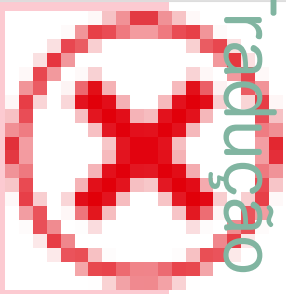
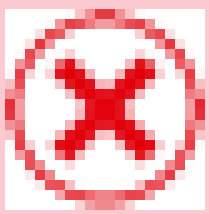
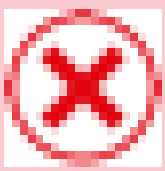
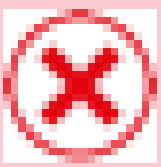
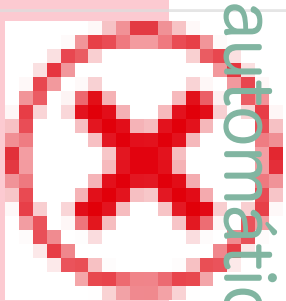
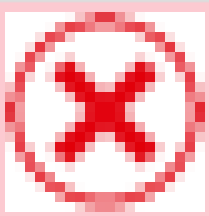
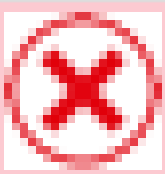
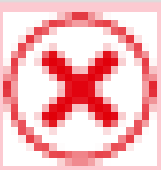
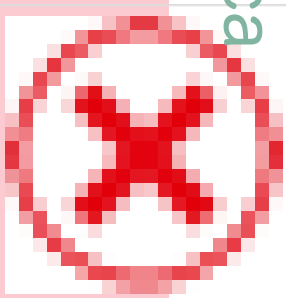
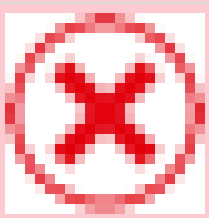
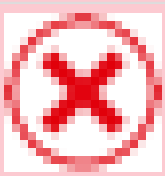
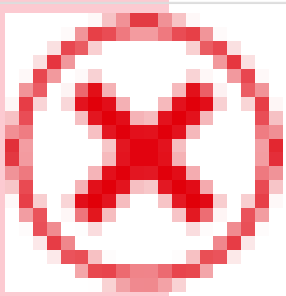
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informações para outras funções:

sn_si.special_access, sn_si_approver_user

Módulo	sn_sec_cmn.read	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.externo	sn_si.knowledge_admin	sn_si
Propriedades							
Configuração							
Notificações							
Definição de Relatório de Criticidade de Serviço							
Definição de Criticalidade de Serviço							

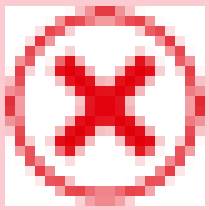
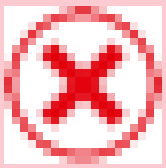
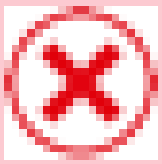
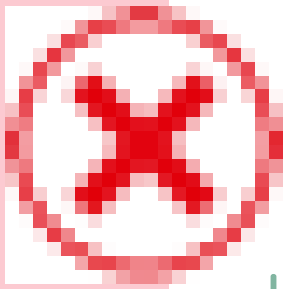
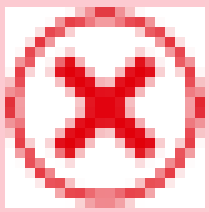
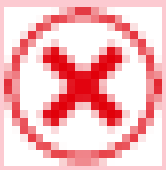
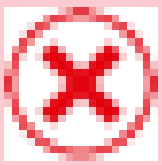
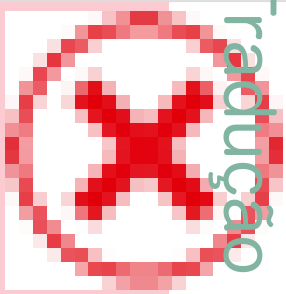
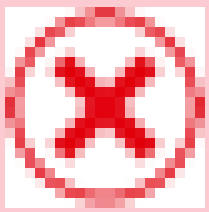
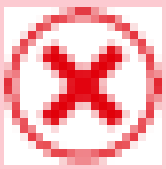
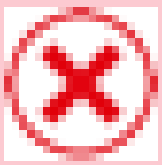
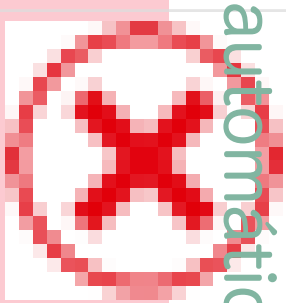
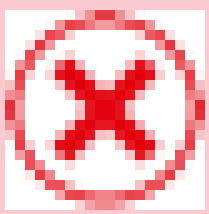
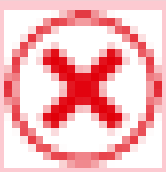
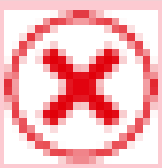
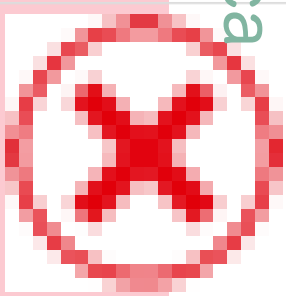
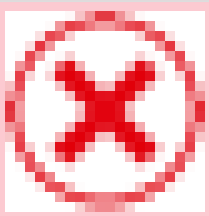
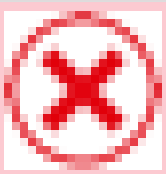
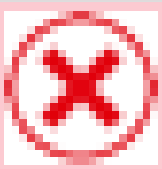
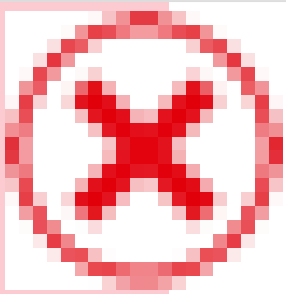
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informações para outras funções:

sn_si.special_access, sn_si_approver_user

Módulo	sn_sec_cmn.read	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.externo	sn_si.knowledge_admin	sn_si
Definição de Impacto de Serviço							
Configuração de avaliações de análise pós-incidente							
Configuração do relatório de análise pós-incidente							
Definição em tempo real							
Seleção de processo							

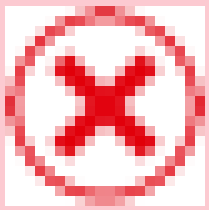
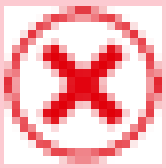
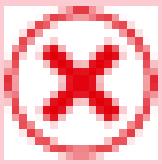
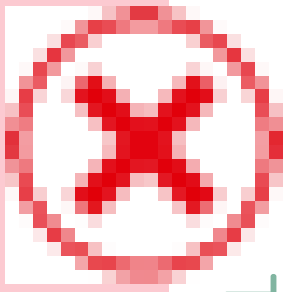
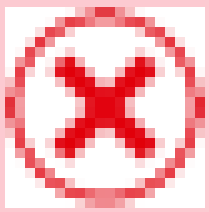
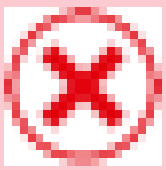
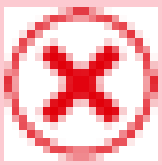
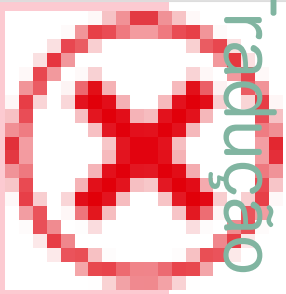
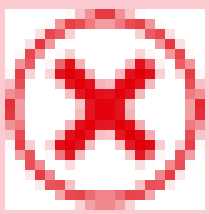
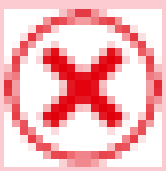
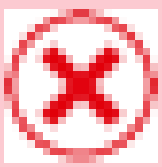
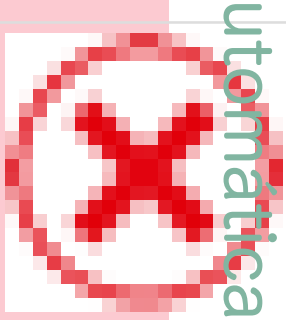
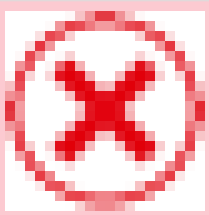
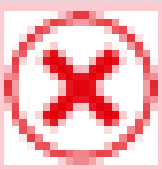
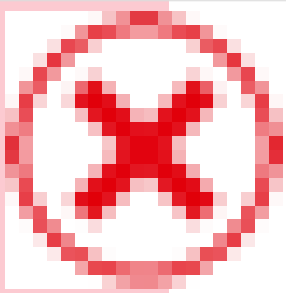
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informações para outras funções:

sn_si.special_access, sn_si_approver_user

Módulo	sn_sec_cmn.read	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.externo	sn_si.knowledge_admin	sn_si
Definições de Processo							
Avaliadores de Resultado de Fluxo de Trabalho de Modelo							
E-mails de Phishing							
Administração de licença							
Relatar E-mail de Phishing							

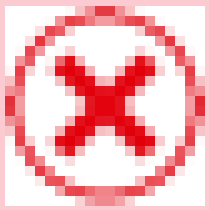
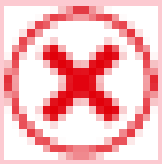
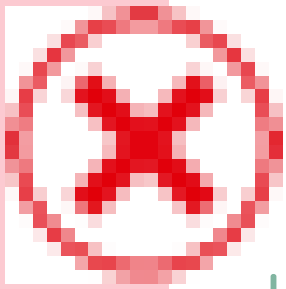
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Informações para outras funções:

sn_si.special_access, sn_si_approver_user

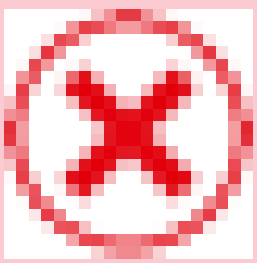
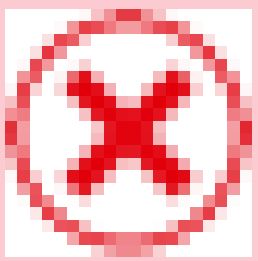
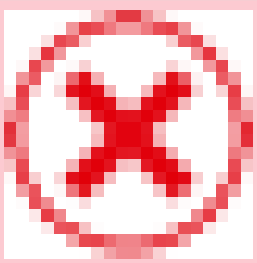
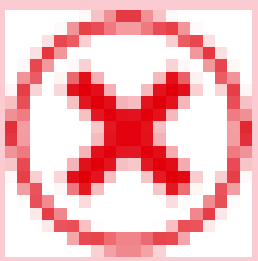
Módulo	sn_sec_cmn.read	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.externo	sn_si.knowledge_admin	sn_si
Mostrar todos os e-mails de phishing							

Acesso ao módulo para: sn_si.special_access, sn_si_approver_user

Acesso ao módulo para: sn_si.special_access, sn_si_approver_user

Informações para outras funções:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Módulo	sn_si.special_access	sn_si_approver_user
(Grupo de apps principal)		
Nova IU de incidentes		
Impacto do Serviço		

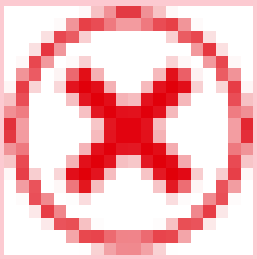
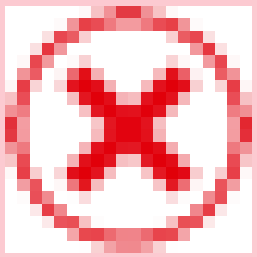
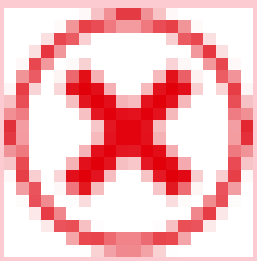
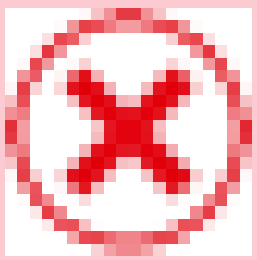
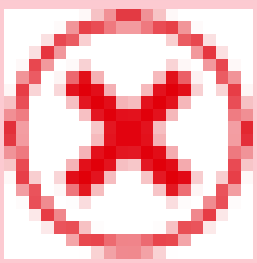
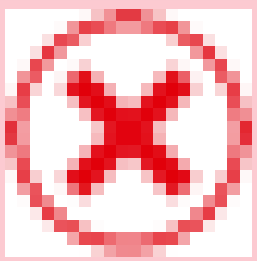
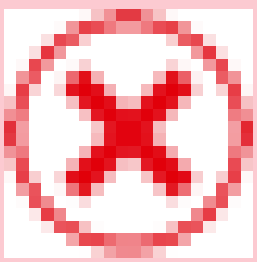
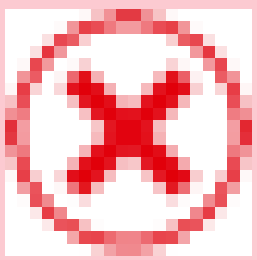
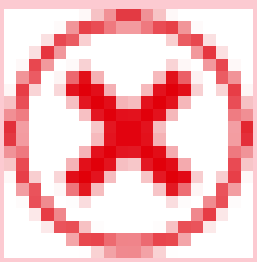
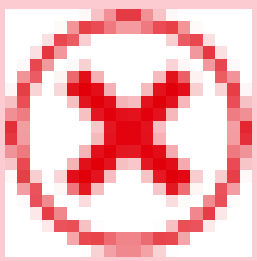
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_si.special_access, sn_si_approver_user

Informações para outras funções:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Módulo	sn_si.special_access	sn_si_approver_user
Visão geral		
Tempo real		
Incidentes		
Visível para Mim		
Atribuídos a Mim		
Meus Trabalhos		

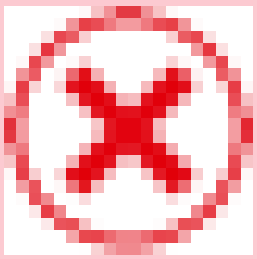
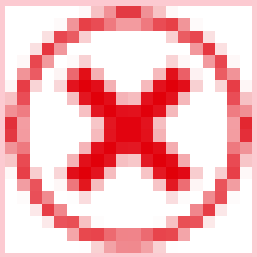
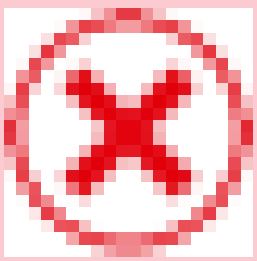
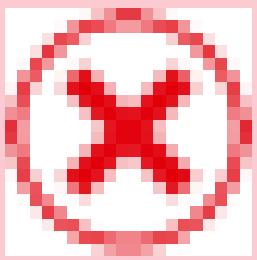
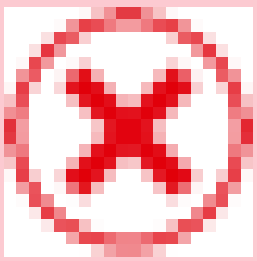
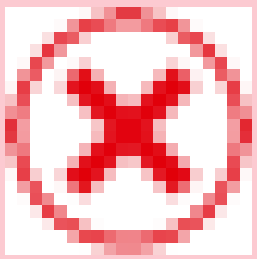
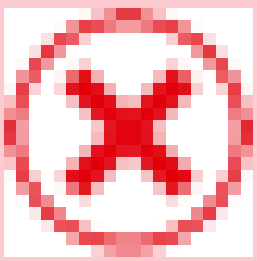
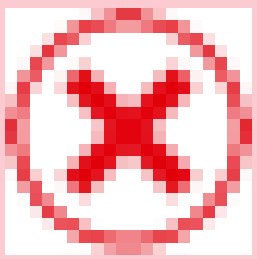
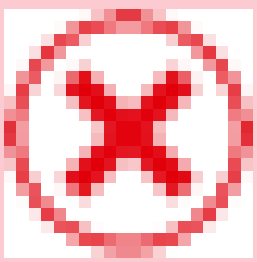
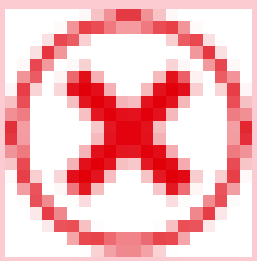
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_si.special_access, sn_si_approver_user

Informações para outras funções:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Módulo	sn_si.special_access	sn_si_approver_user
Atribuído à Equipe		
Mostrar incidentes em aberto		
Mostrar Todos os Incidentes		
Incidentes não atribuídos		
Tarefas de resposta		
Atribuídos a Mim		

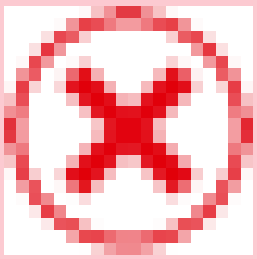
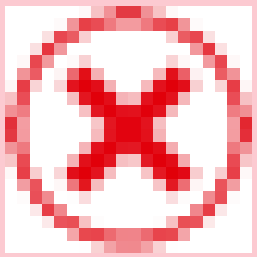
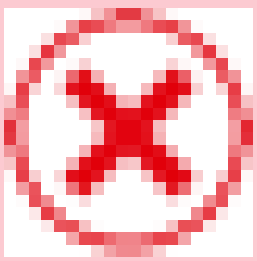
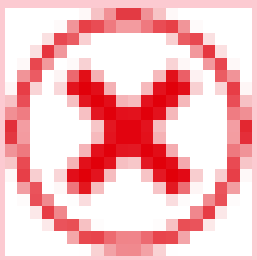
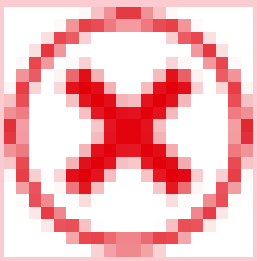
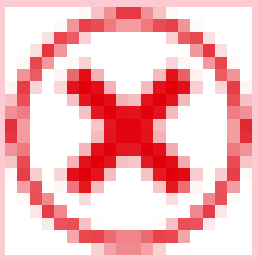
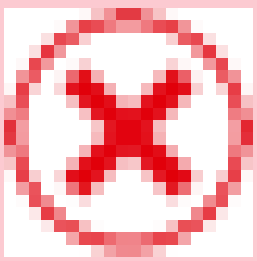
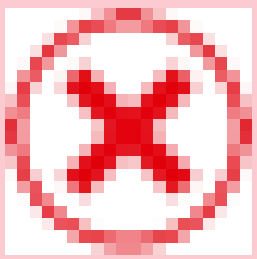
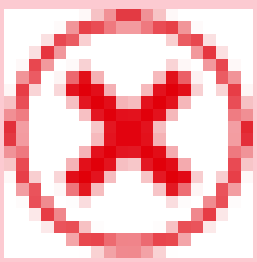
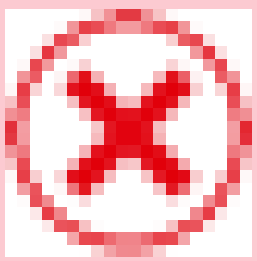
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_si.special_access, sn_si_approver_user

Informações para outras funções:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Módulo	sn_si.special_access	sn_si_approver_user
Atribuído à Equipe		
Mostrar Tarefas Abertas		
Mostrar Todas as Tarefas		
Tarefas não atribuídas		
Solicitações de Entrada		
Atribuídos a Mim		

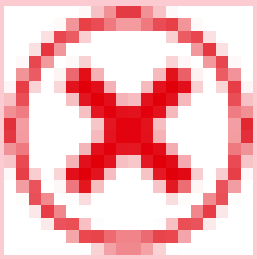
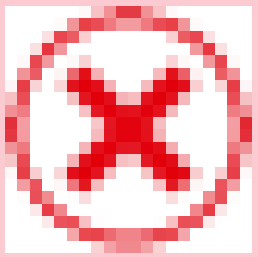
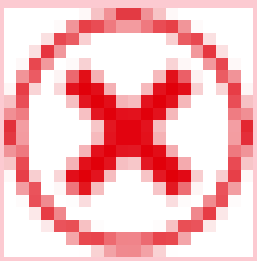
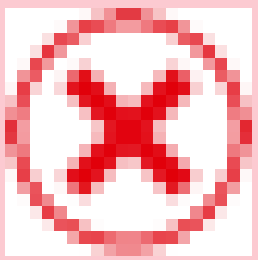
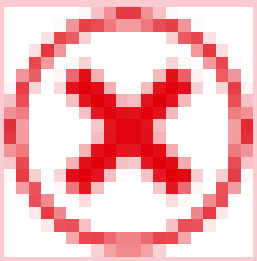
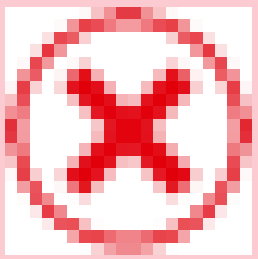
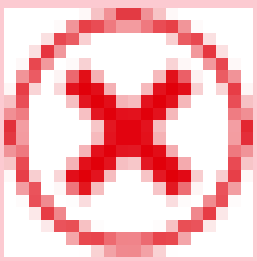
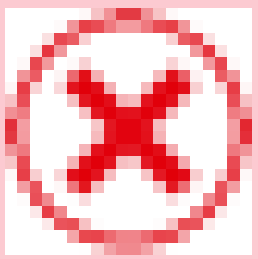
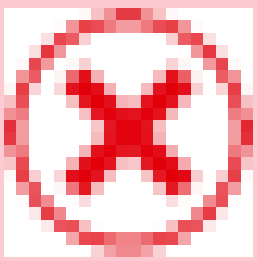
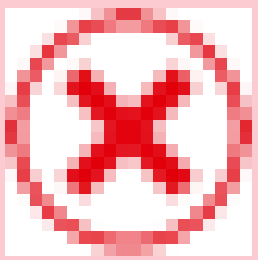
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_si.special_access, sn_si_approver_user

Informações para outras funções:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Módulo	sn_si.special_access	sn_si_approver_user
Atribuído à Equipe		
Minhas aprovações		
Mostrar solicitações em aberto		
Mostrar Todas as Solicitações		
Solicitações Não Atribuídas		

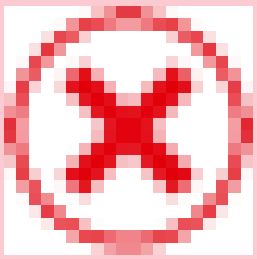
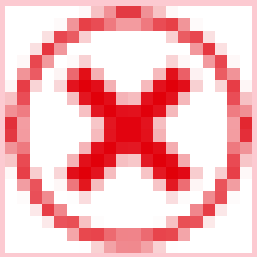
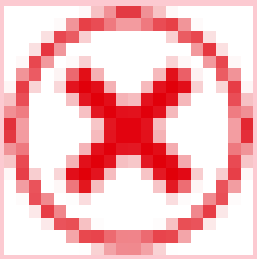
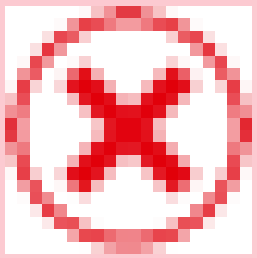
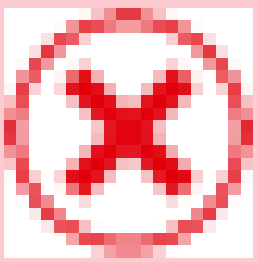
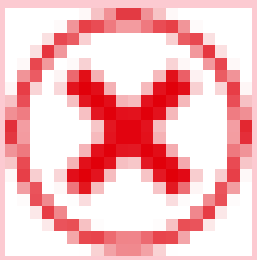
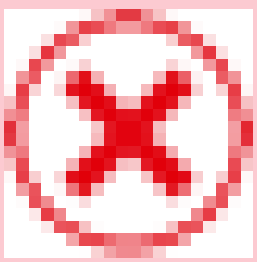
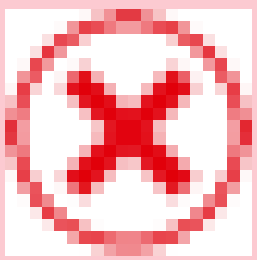
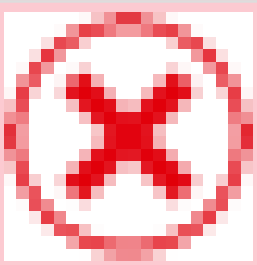
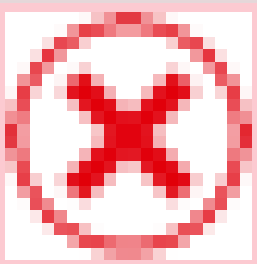
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_si.special_access, sn_si_approver_user

Informações para outras funções:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Módulo	sn_si.special_access	sn_si_approver_user
Meu Mapa		
Alertas e eventos		
Análise pós-incidente		
Minhas Revisões Pendentes		
Revisões pendentes da equipe		
Todas as Revisões Incompletas		
Configuração		
Grupos de calculadoras de incidentes de segurança		

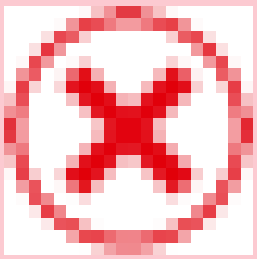
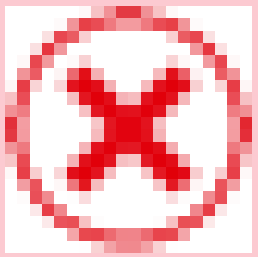
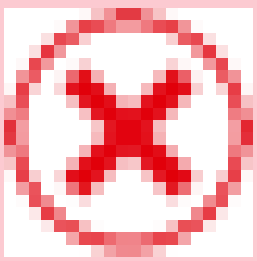
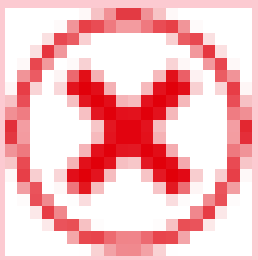
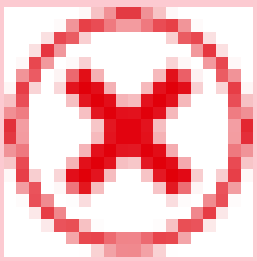
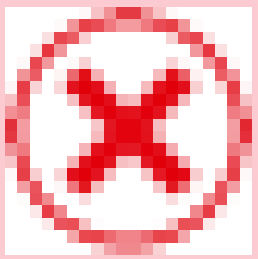
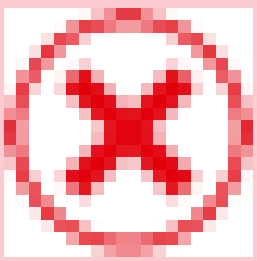
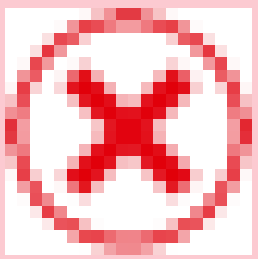
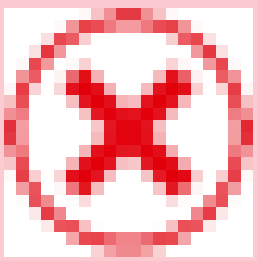
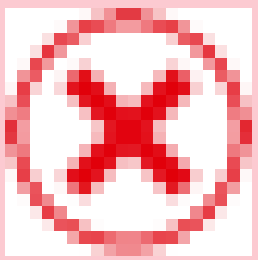
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_si.special_access, sn_si_approver_user

Informações para outras funções:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Módulo	sn_si.special_access	sn_si_approver_user
Calculadoras de Severidade		
Configuração de pontuação de risco		
Configuração do Feed de Notícias		
Grupos		
Funções		

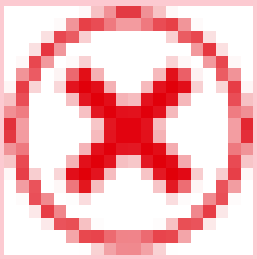
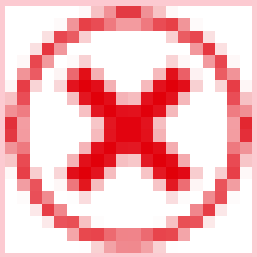
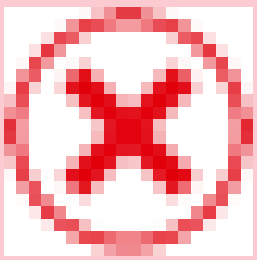
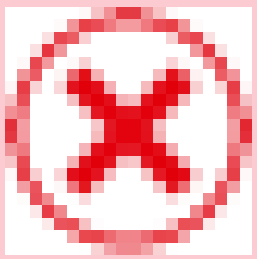
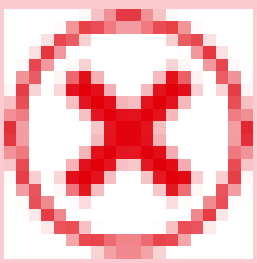
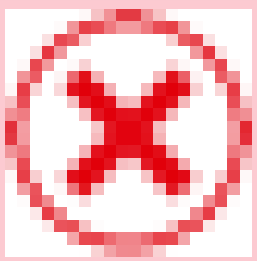
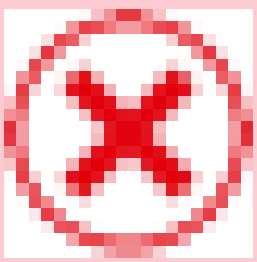
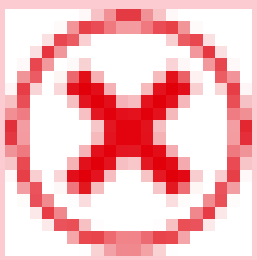
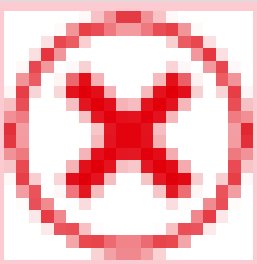
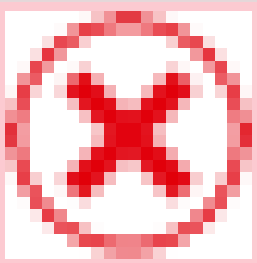
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_si.special_access, sn_si_approver_user

Informações para outras funções:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Módulo	sn_si.special_access	sn_si_approver_user
SLAs		
Configuração do espaço de analista (nova IU)		
Assistente de configuração		
Configuração de filtro da página principal		
Ações de IU de Formulário		
Configurações de Lista relacionada		

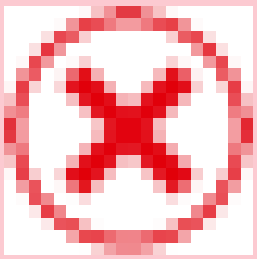
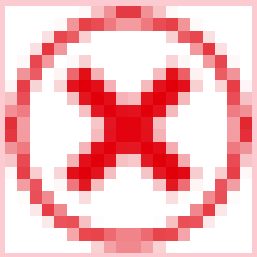
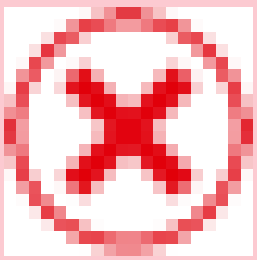
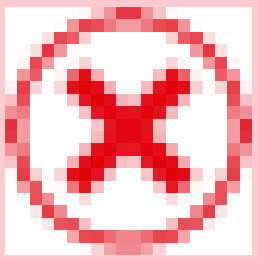
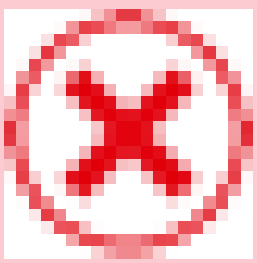
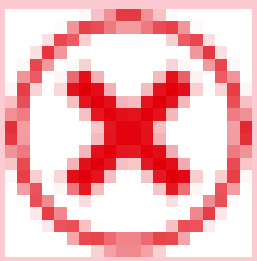
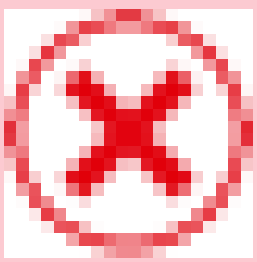
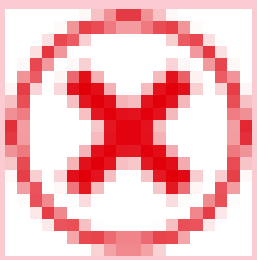
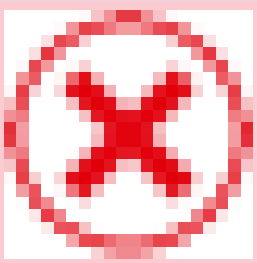
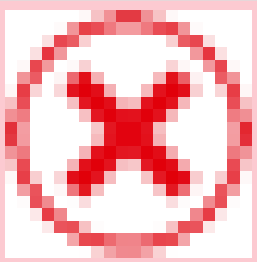
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_si.special_access, sn_si_approver_user

Informações para outras funções:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Módulo	sn_si.special_access	sn_si_approver_user
Propriedades do espaço do analista		
Catálogo e Conhecimento		
Modelos de Incidente de segurança		
Manter Itens do catálogo		
Conhecimento		
Runbook manual		
Criar Novo Runbook		

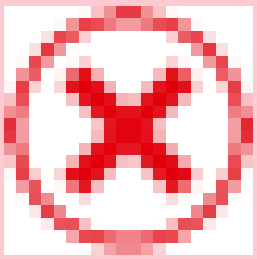
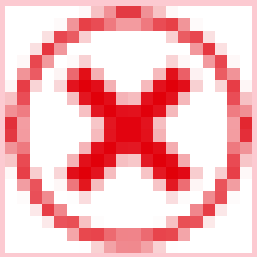
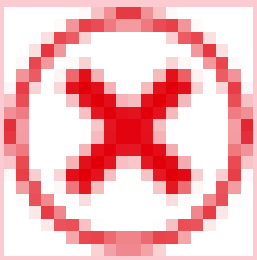
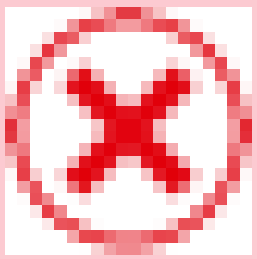
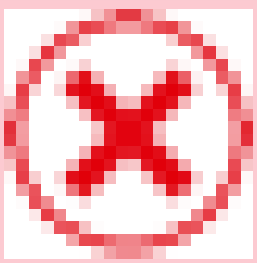
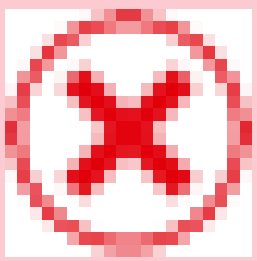
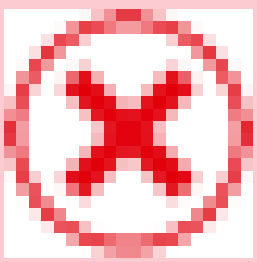
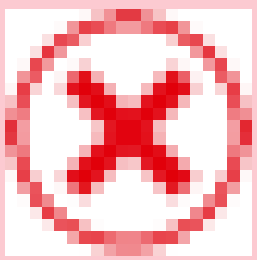
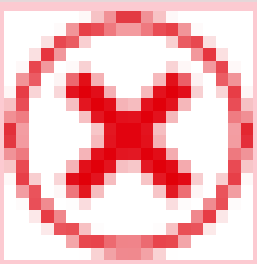
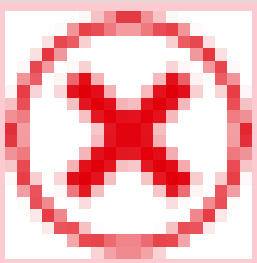
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_si.special_access, sn_si_approver_user

Informações para outras funções:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Módulo	sn_si.special_access	sn_si_approver_user
Exibir Documentos do Runbook		
Administração		
Propriedades		
Configuração		
Notificações		
Definição de Relatório de Criticidade de Serviço		

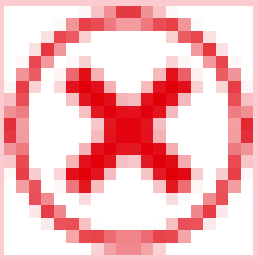
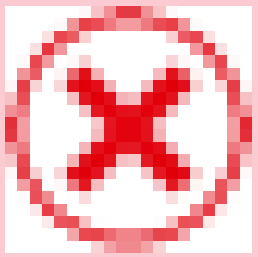
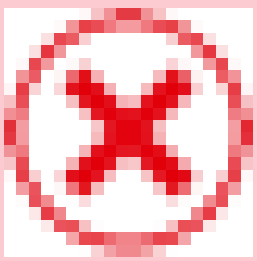
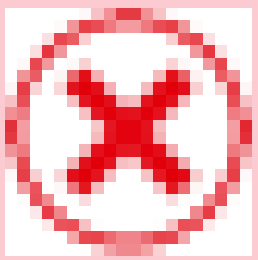
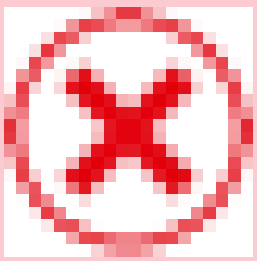
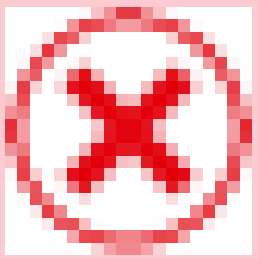
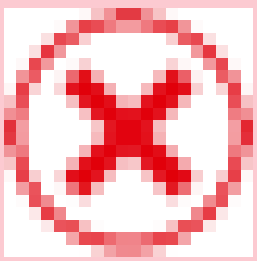
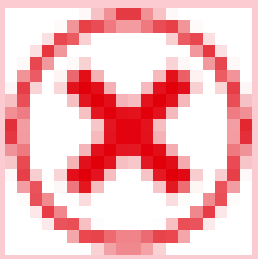
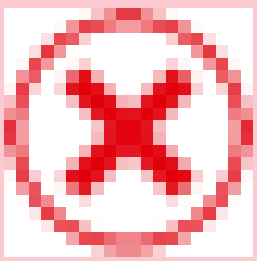
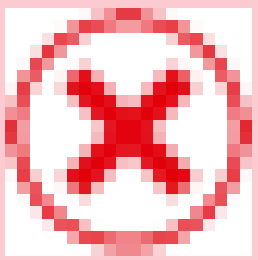
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_si.special_access, sn_si_approver_user

Informações para outras funções:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Módulo	sn_si.special_access	sn_si_approver_user
Definição de Criticalidade de Serviço		
Definição de Impacto de Serviço		
Configuração de avaliações de análise pós-incidente		
Configuração do relatório de análise pós-incidente		
Definição em tempo real		

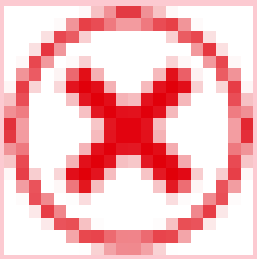
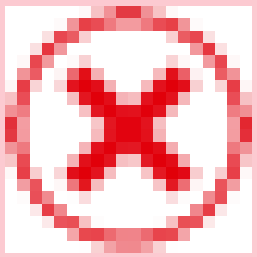
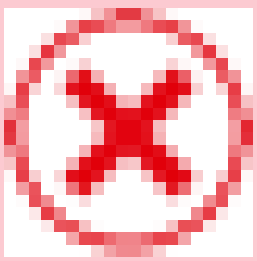
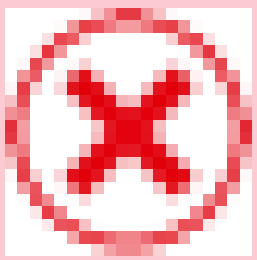
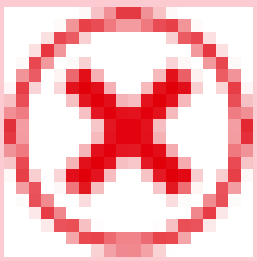
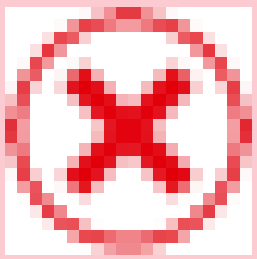
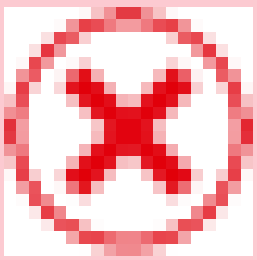
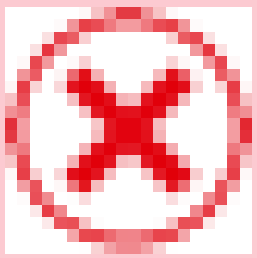
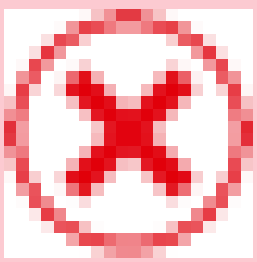
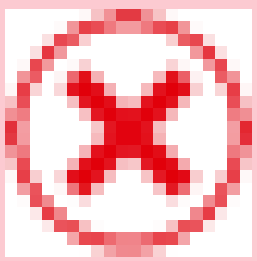
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_si.special_access, sn_si_approver_user

Informações para outras funções:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Módulo	sn_si.special_access	sn_si_approver_user
Seleção de processo		
Definições de Processo		
Avaliadores de Resultado de Fluxo de Trabalho de Modelo		
E-mails de Phishing		
Administração de licença		
Relatar E-mail de Phishing		

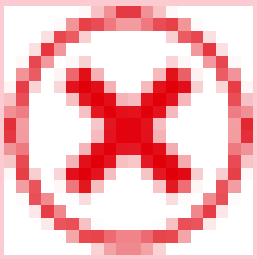
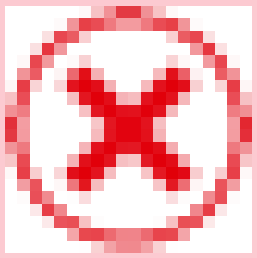
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_si.special_access, sn_si_approver_user

Informações para outras funções:

sn_sec_cmn.read, sn_si.admin, sn_si.analyst, sn_si.ciso, sn_si.external, sn_si.knowledge_admin, sn_si.manager, sn_si.read

Módulo	sn_si.special_access	sn_si_approver_user
Mostrar todos os e-mails de phishing		

[End]

[store-future: BEGIN review]

Acesso ao módulo por função do Security Operations

Para Security Operations, consulte os itens de menu que podem ser acessados por uma função específica.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
(Grupo de apps principal)					

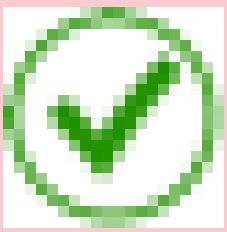
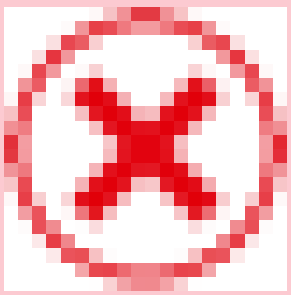
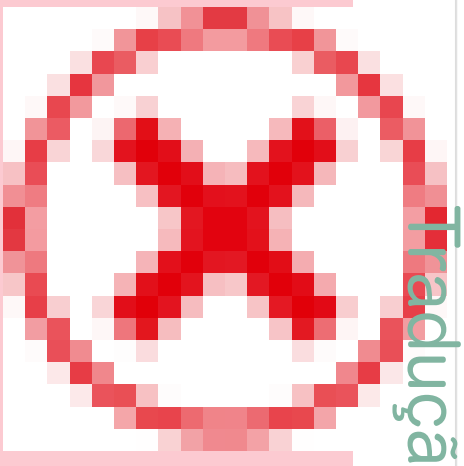
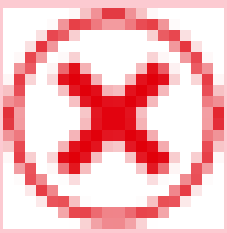
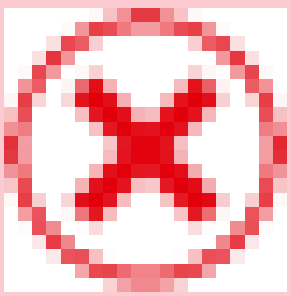
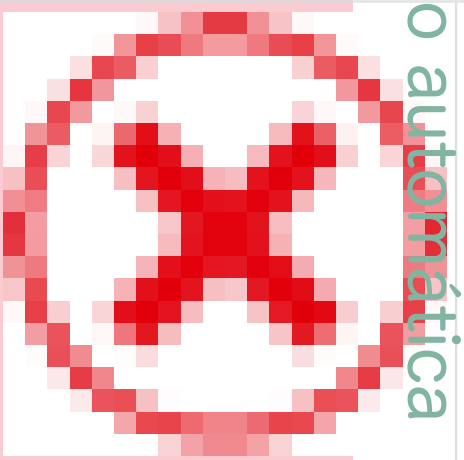
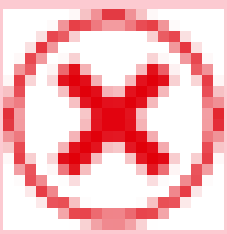
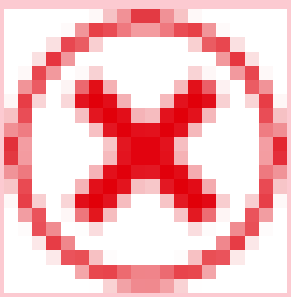
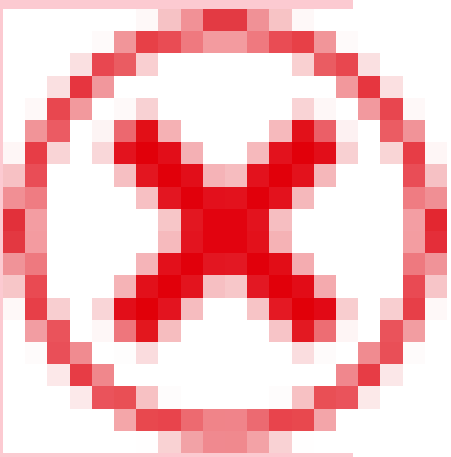
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
Integrações					
Fluxos de capacidades de integração					
Execuções de capacidade					

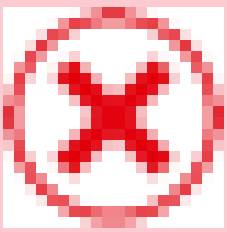
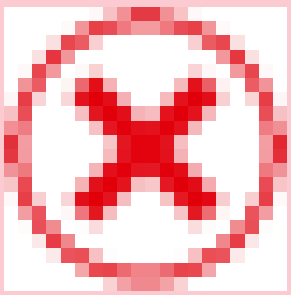
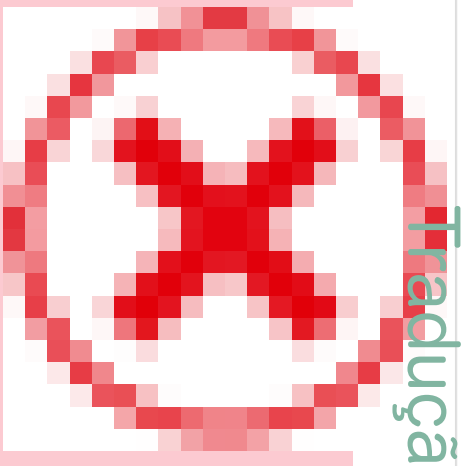
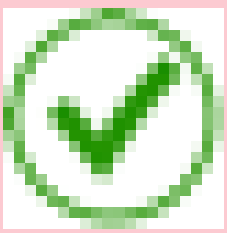
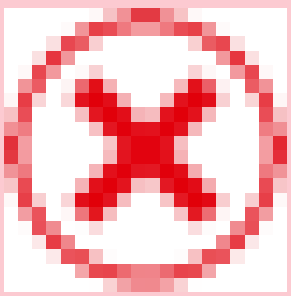
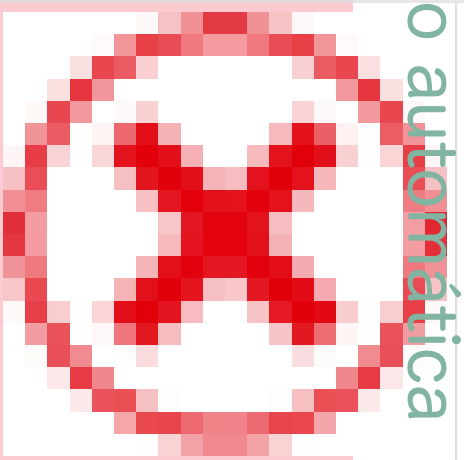
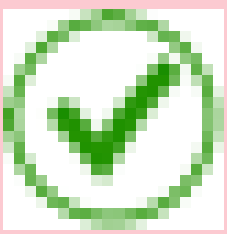
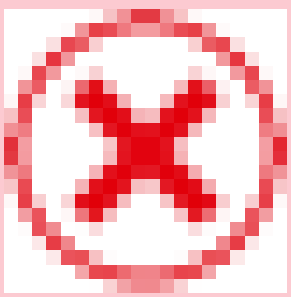
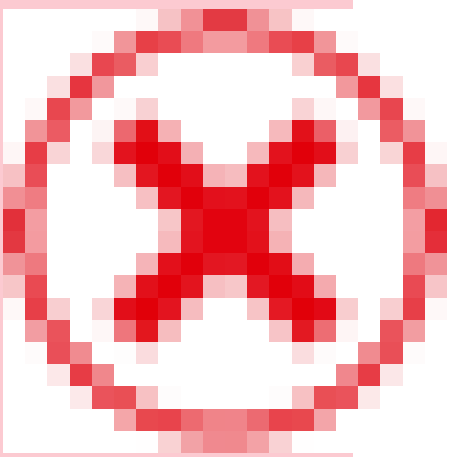
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
Limite de classificação da implementação da capacidade					
Configurações de Integração					
Configuração de Pesquisa de Vistas					

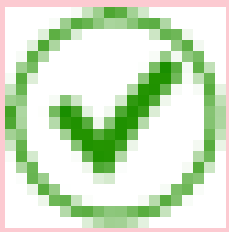
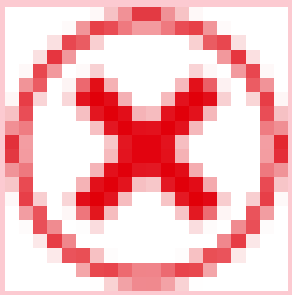
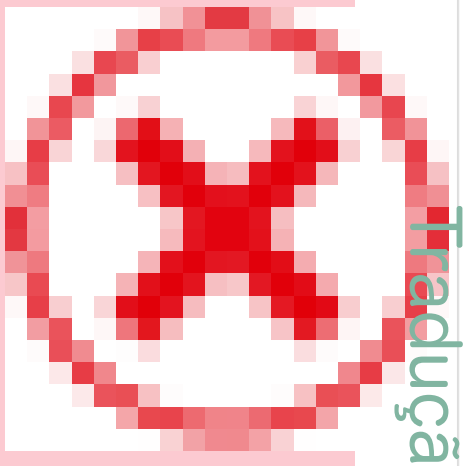
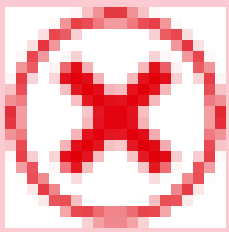
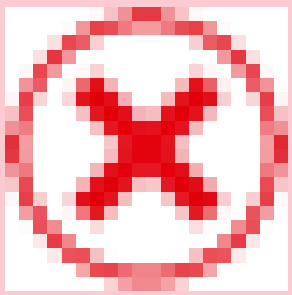
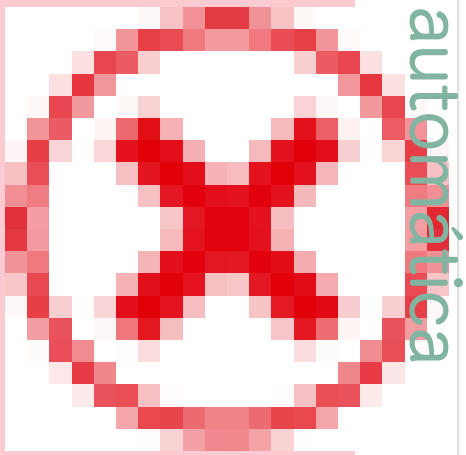
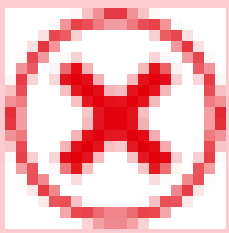
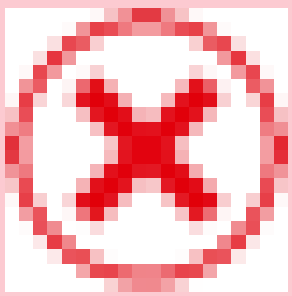
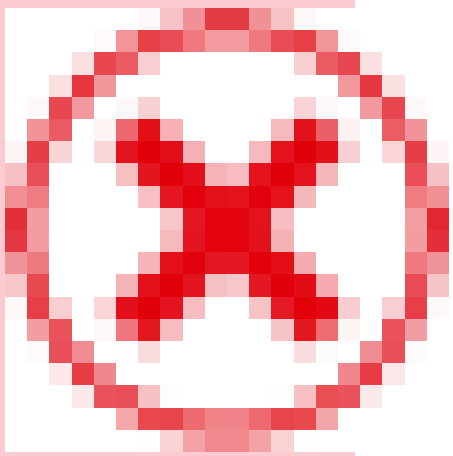
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
Capacidades de integração					
Integrações					
Fluxos de capacidades de integração					
Execuções de capacidade					

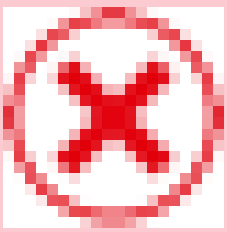
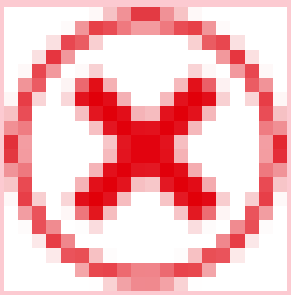
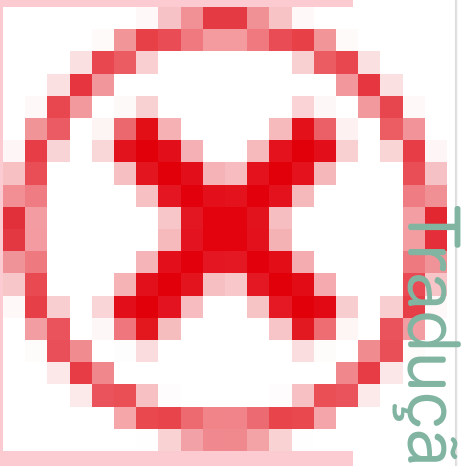
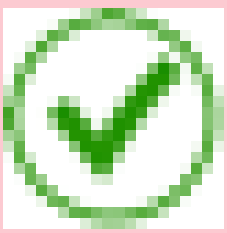
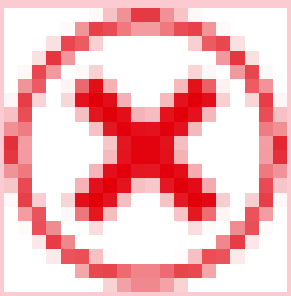
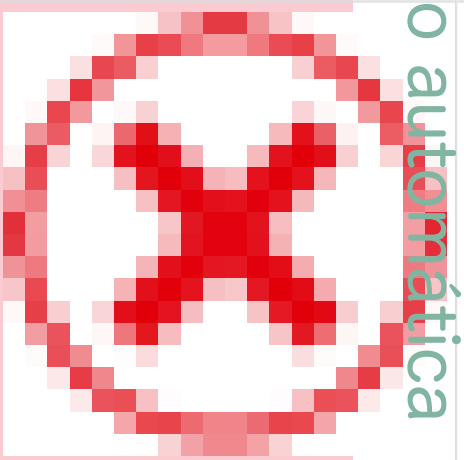
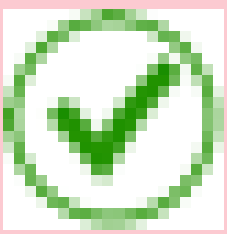
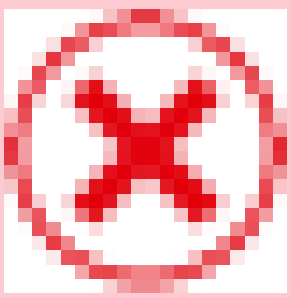
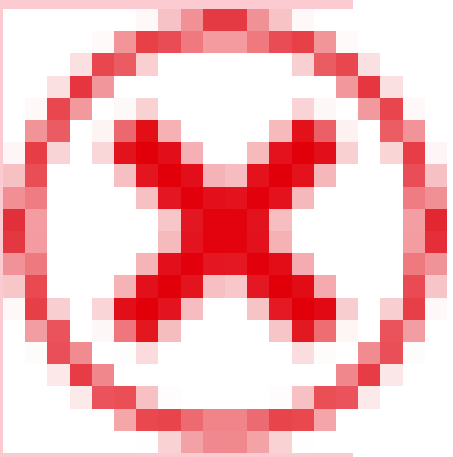
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
Limite de classificação da implementação da capacidade					
Configurações de Integração					
Configuração de Pesquisa de Vistas					

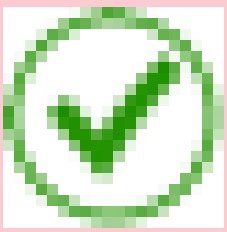
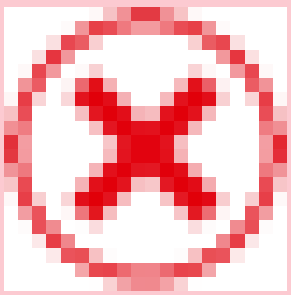
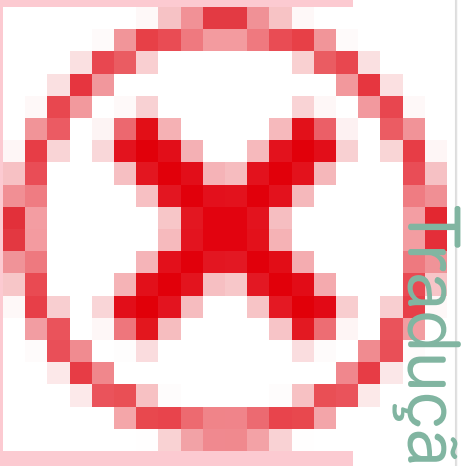
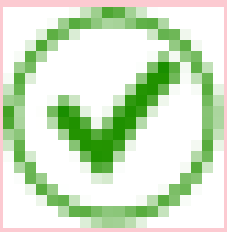
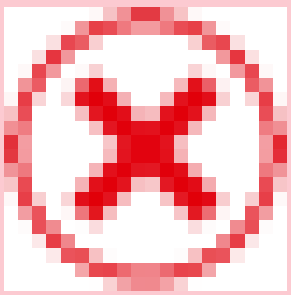
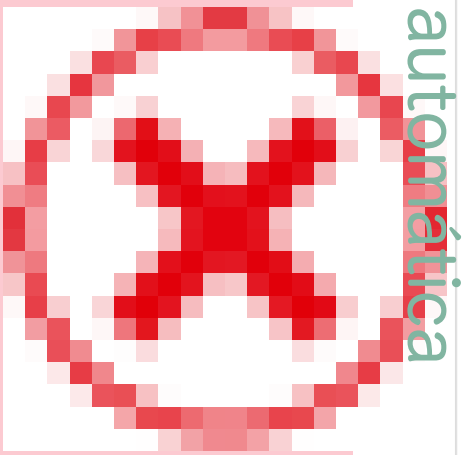
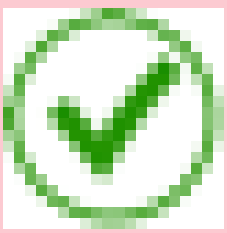
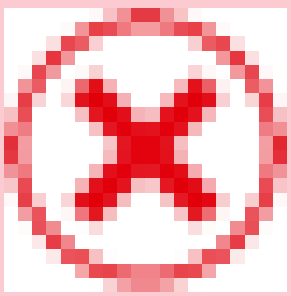
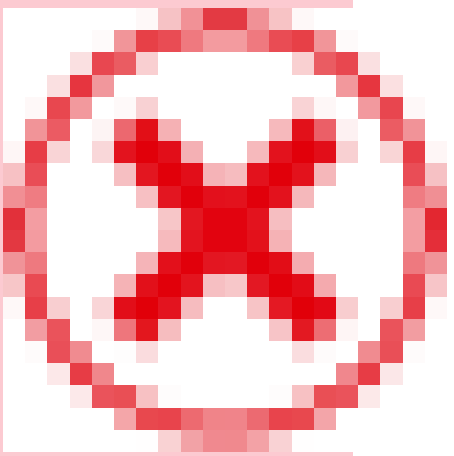
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
Capacidades de integração					
Processamento de E-mails					
Análise de E-mails					
Regras de Duplicação					

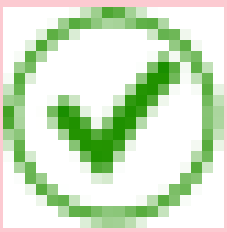
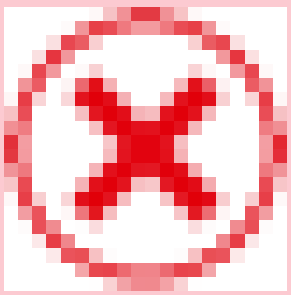
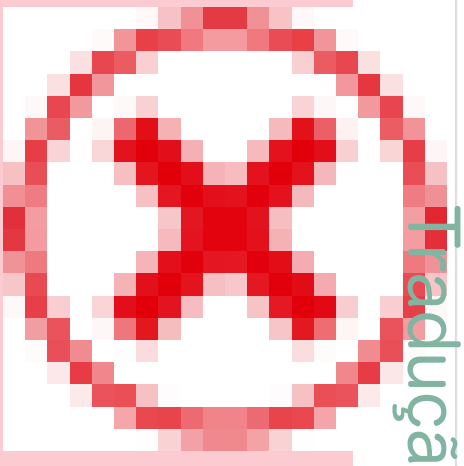
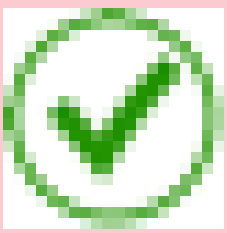
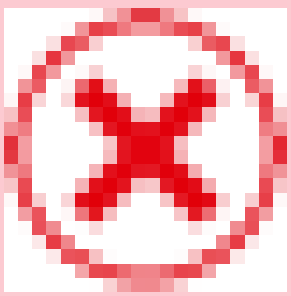
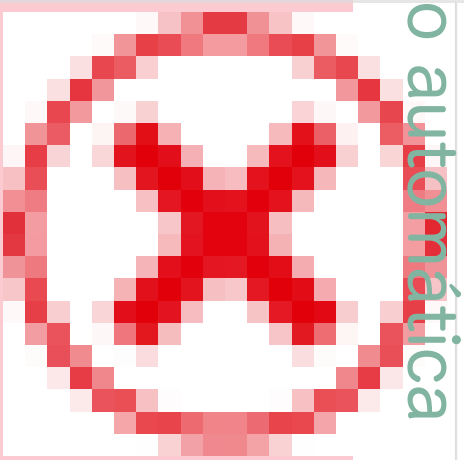
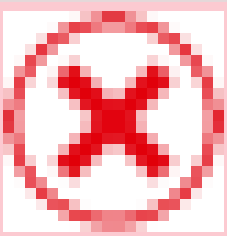
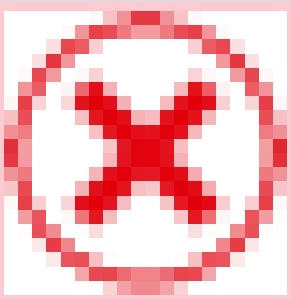
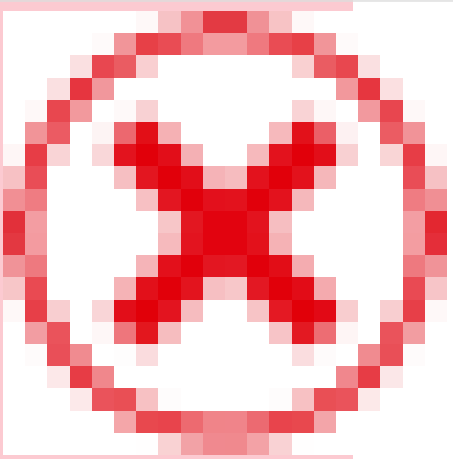
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
Propriedades					
E-mails Incompatíveis					
Phishing relatado pelo usuário de regras de ingestão					

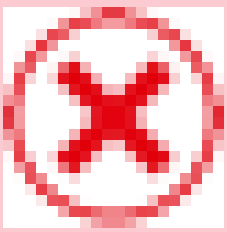
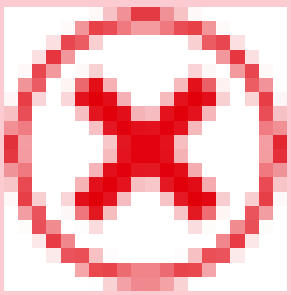
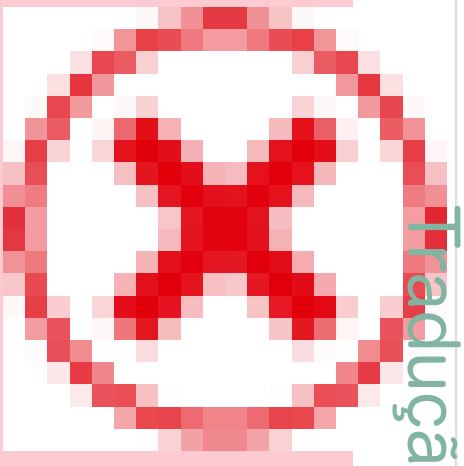
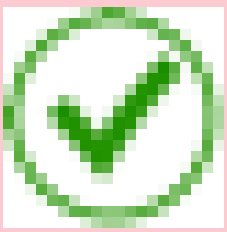
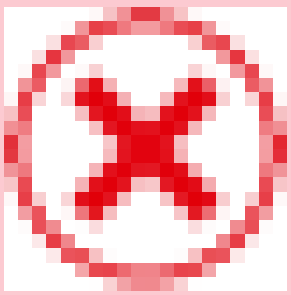
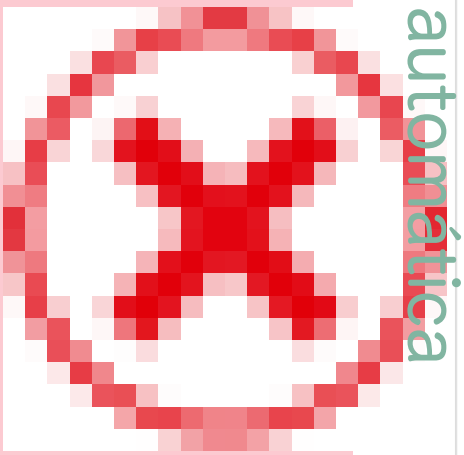
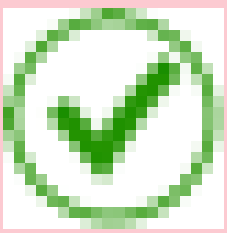
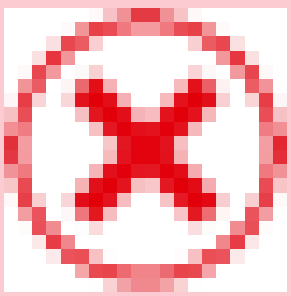
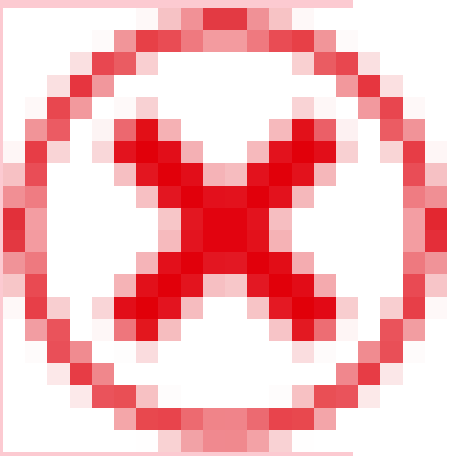
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
Propriedades do Phishing Reportado pelo Usuário					
Grupos					
Grupos de Filtros					
Escalações					

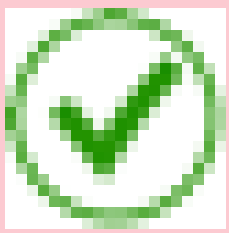
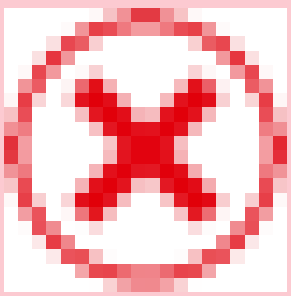
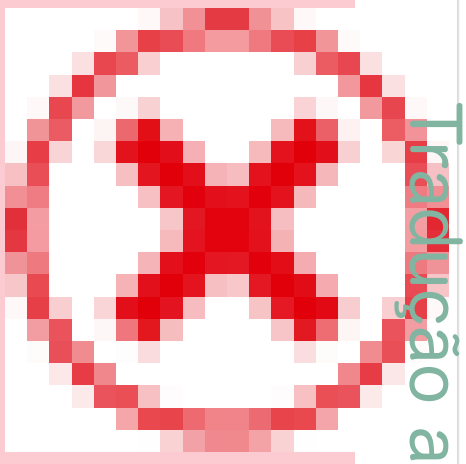
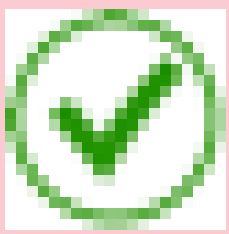
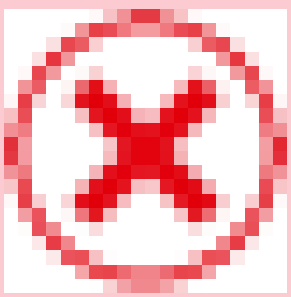
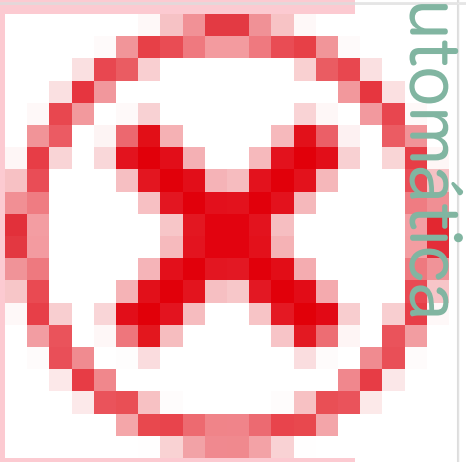
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
Enriquecimentos de Dados					
Marcadores de Segurança					
Grupos					
Marcadores					
Workflows					

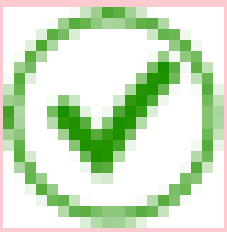
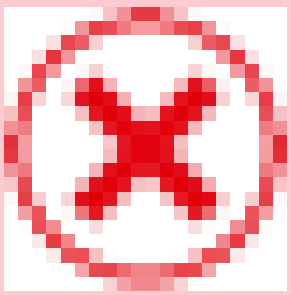
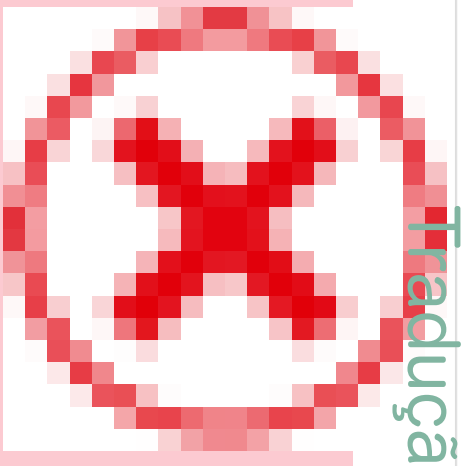
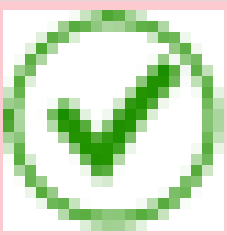
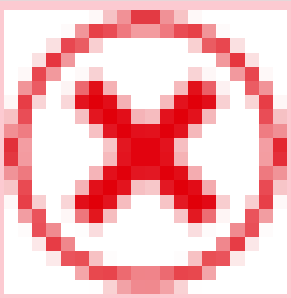
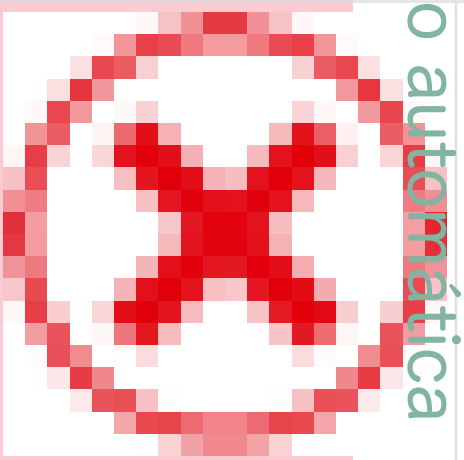
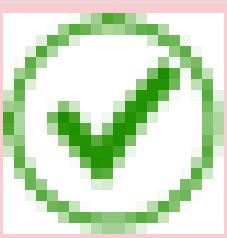
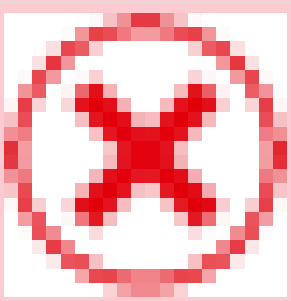
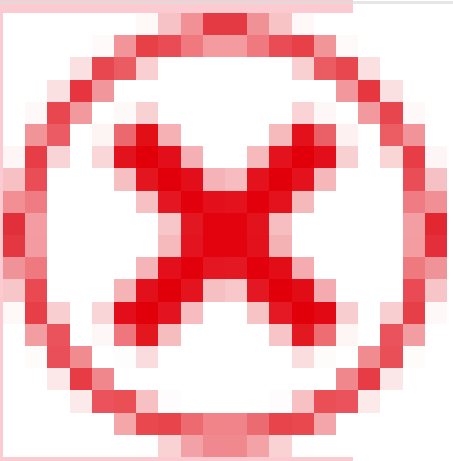
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
Acompanhamento de execução					
Exibir Fluxos de Trabalho de Segurança					
Gatilhos de Fluxo de Trabalho					
Utilitários					

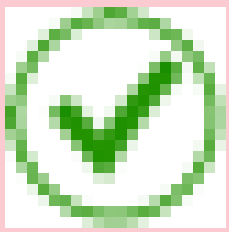
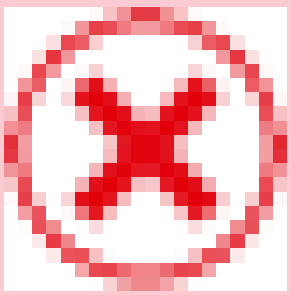
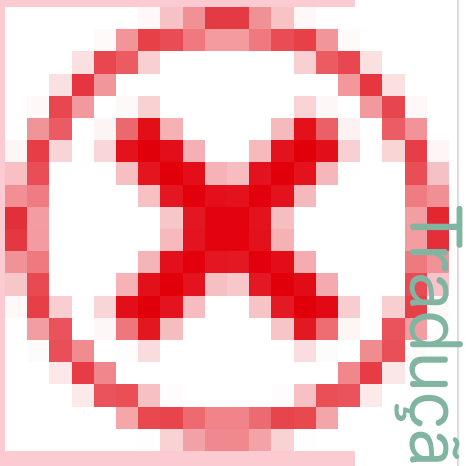
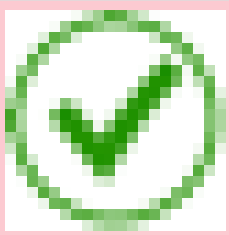
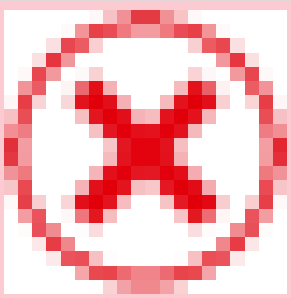
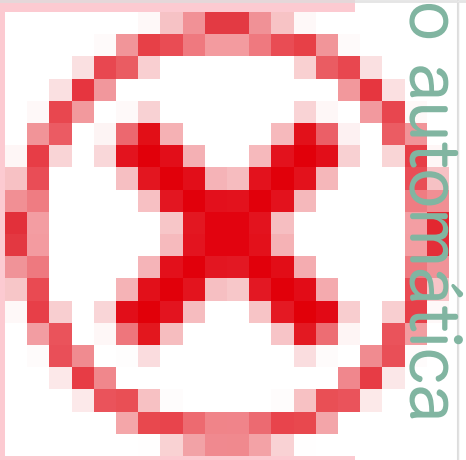
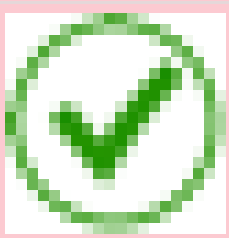
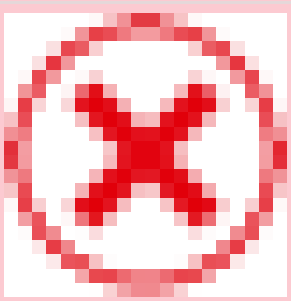
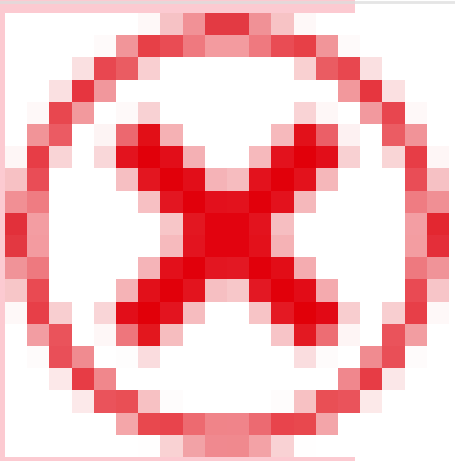
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
Mapeamento de Dados de Aprimoramento					
Transformações de Valores de campos					
Mapeamento de Campos					

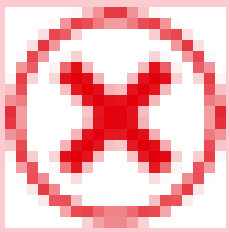
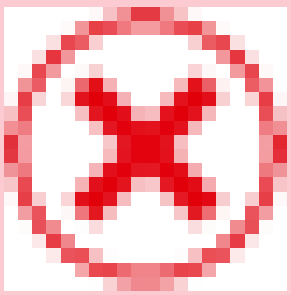
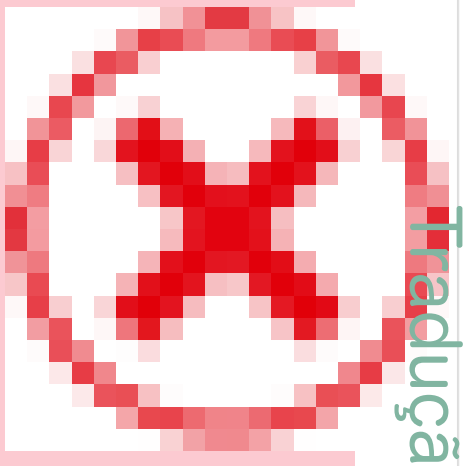
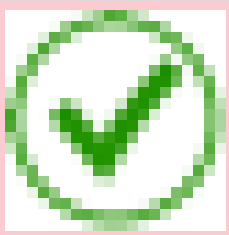
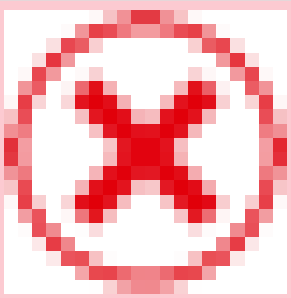
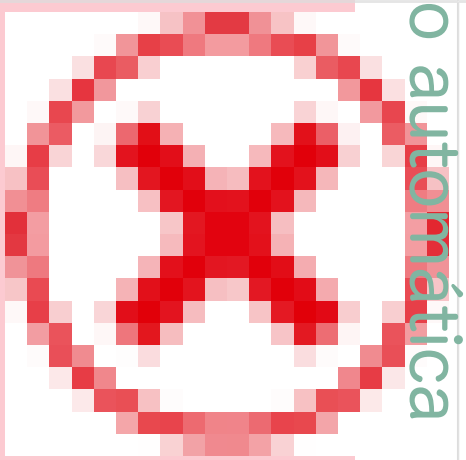
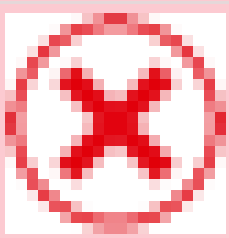
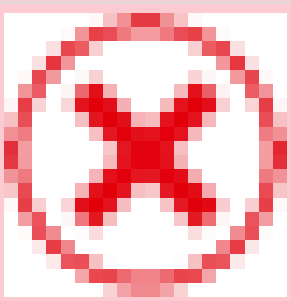
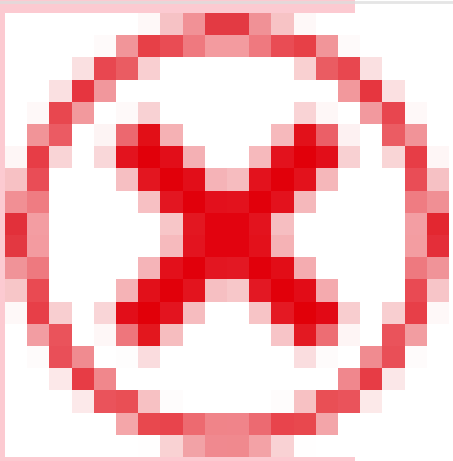
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
Orquestração sob demanda					
Grupos de Sistemas Operacionais					
Registro da aplicação SecOps					

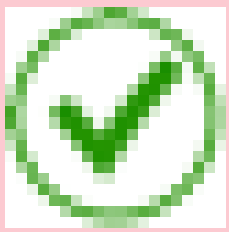
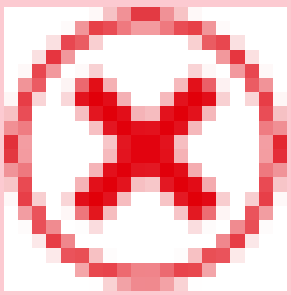
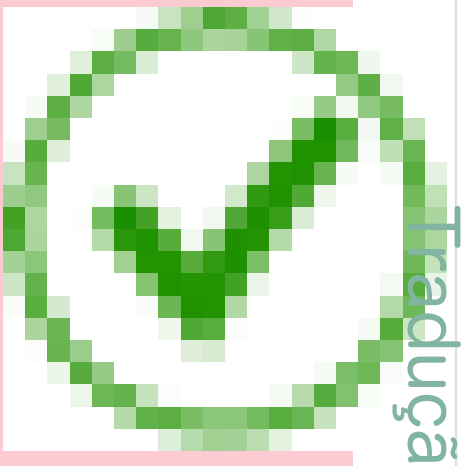
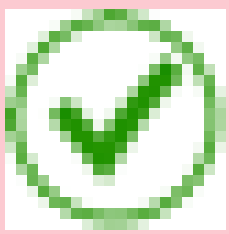
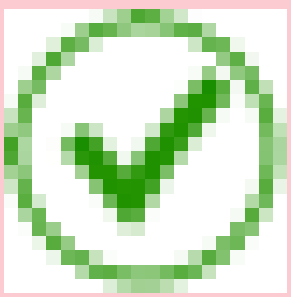
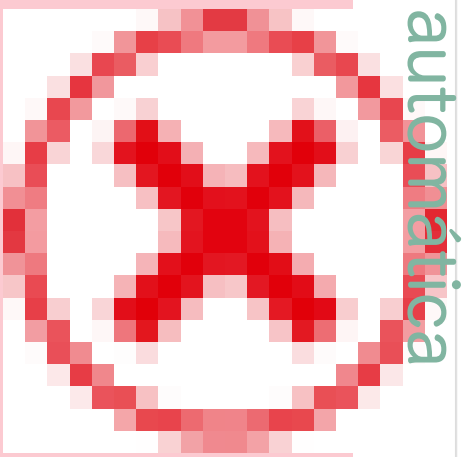
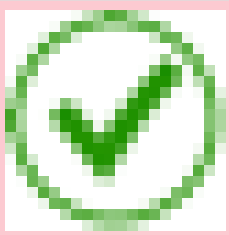
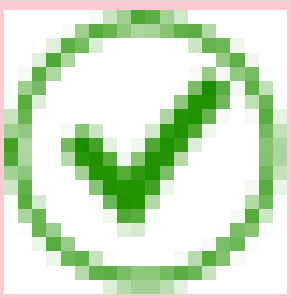
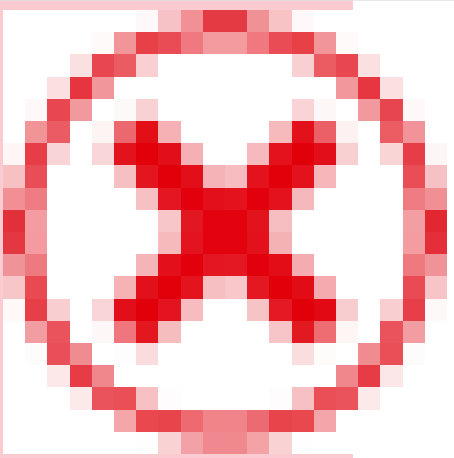
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
Configuração de trabalho em segundo plano					
CMDB					
Regras de Pesquisa de IC					
Itens Descobertos					

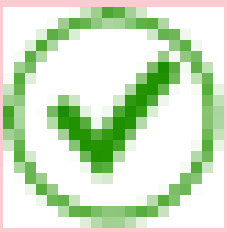
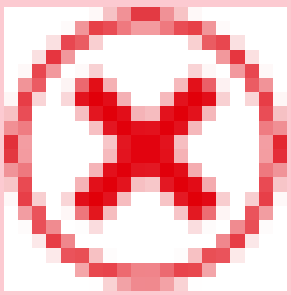
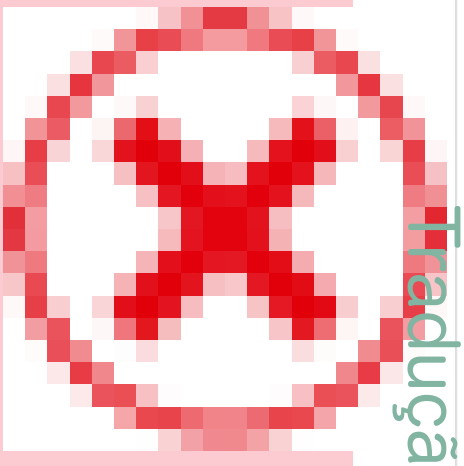
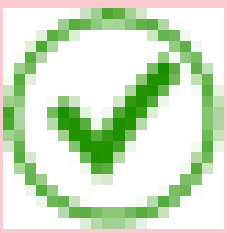
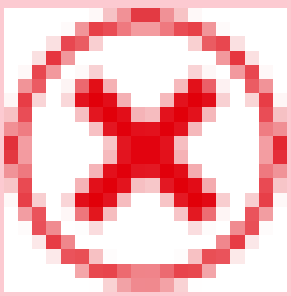
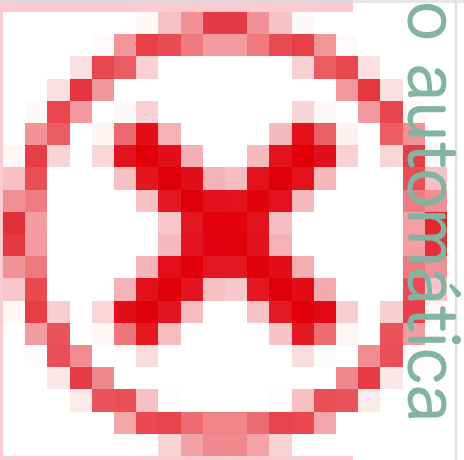
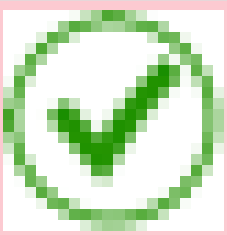
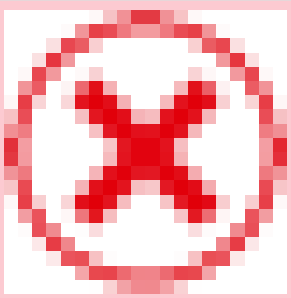
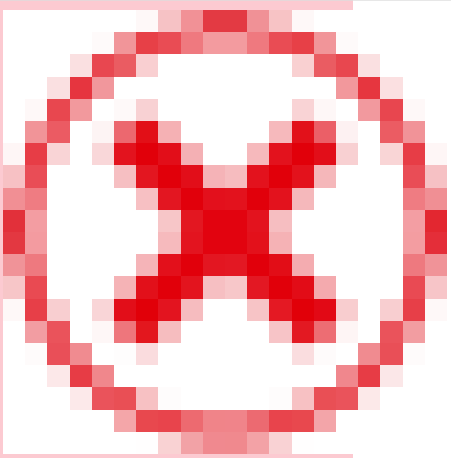
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
Reconciliar itens descobertos sem correspondência					
Imagens do contêiner descobertas					
WatchDog					
Configuração					

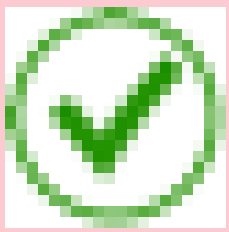
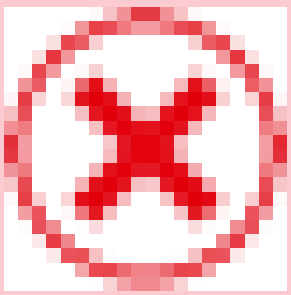
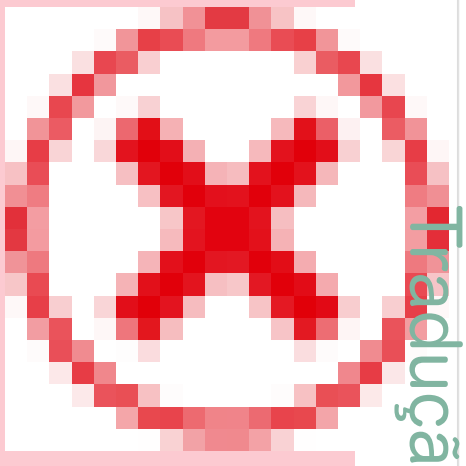
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Informações para outras funções:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Módulo	admin	sn_sec_cmn.admin	sn_sec_cmn.ci_manager	sn_sec_cmn.manage_background_job	sn_sec
Visão geral					

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
(Grupo de apps principal)					

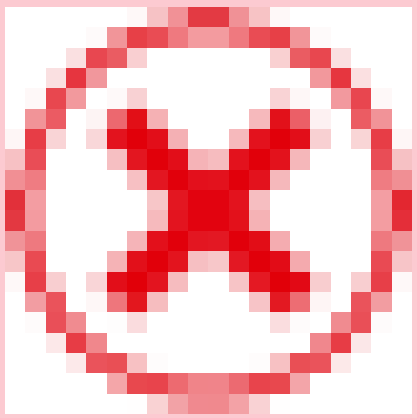
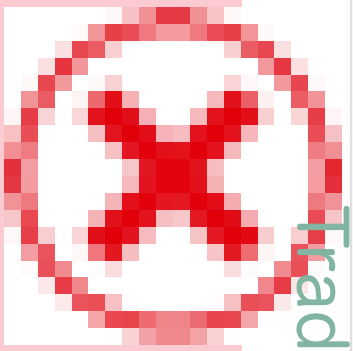
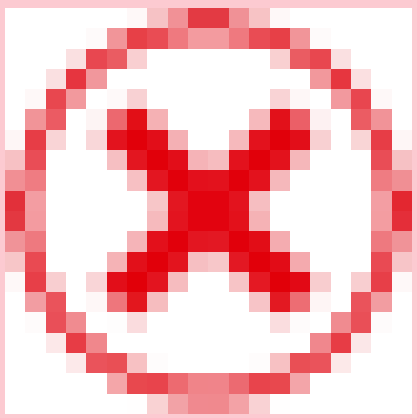
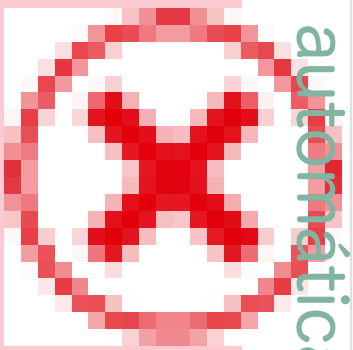
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Integrações					
Fluxos de capacidades de integração					

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Execuções de capacidade	✗	✓	✗	✗	
Limite de classificação da implementação da capacidade	✗	✓	✗	✗	

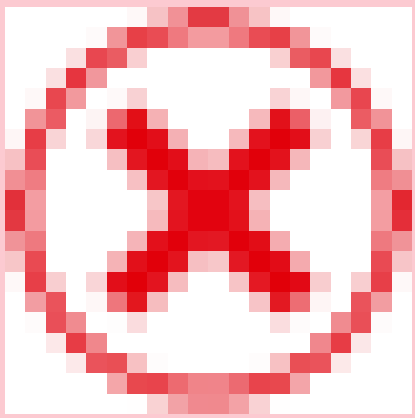
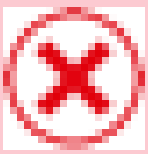
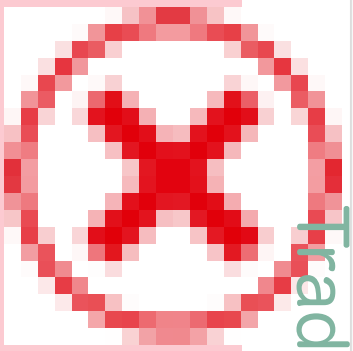
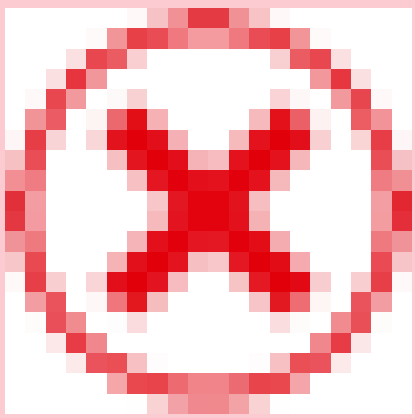
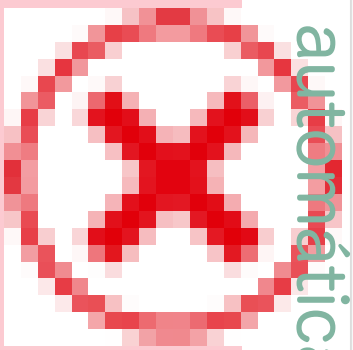
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Configurações de Integração					
Configuração de Pesquisa de Vistas					

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Capacidades de integração	✗	✓	✓	✗	
Integrações					
Fluxos de capacidades de integração	✗	✓	✗	✗	

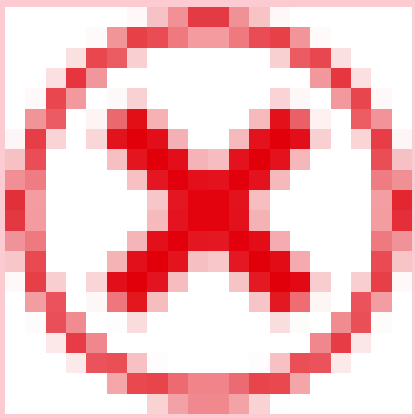
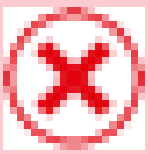
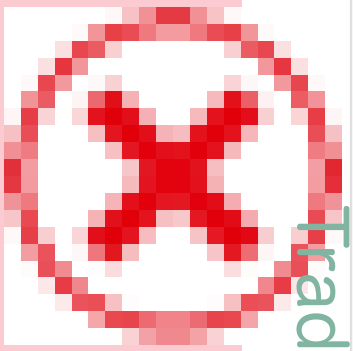
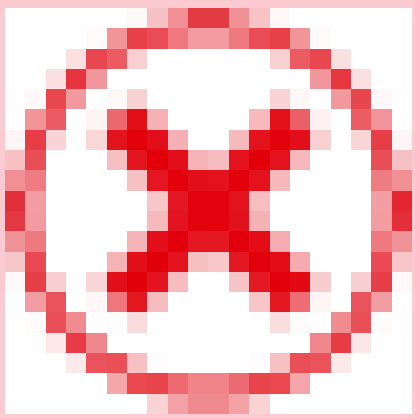
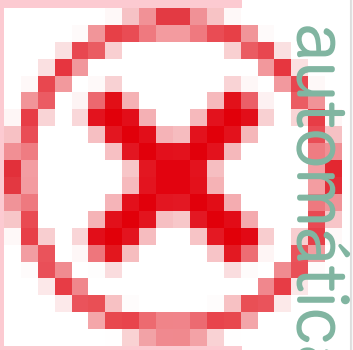
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Execuções de capacidade					
Limite de classificação da implementação da capacidade					

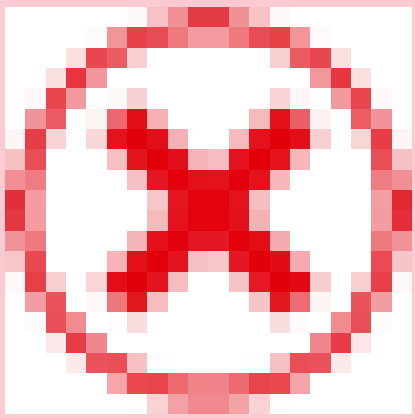
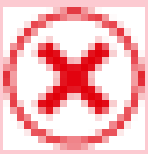
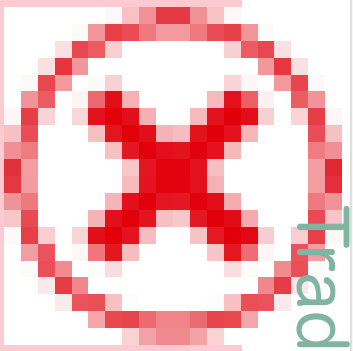
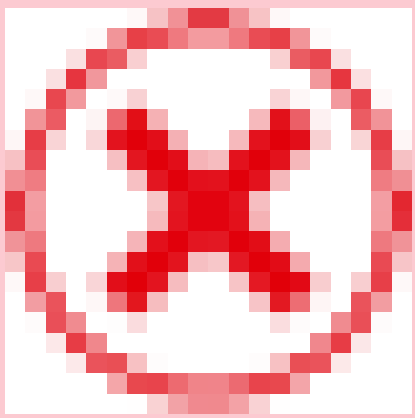
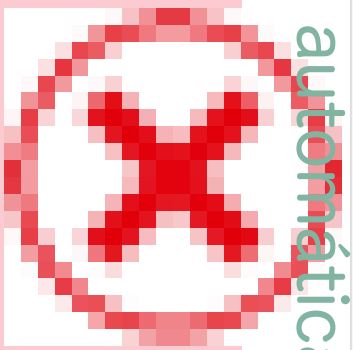
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Configurações de Integração					
Configuração de Pesquisa de Vistas					

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Capacidades de integração	✗	✓	✓	✗	
Processamento de E-mails					
Análise de E-mails	✗	✓	✗	✗	

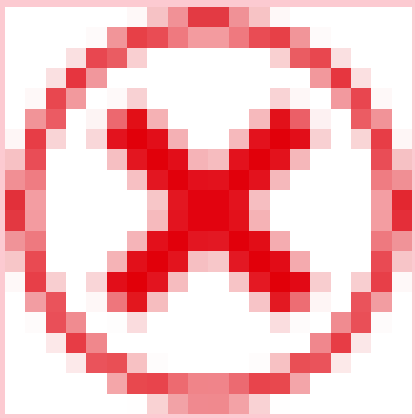
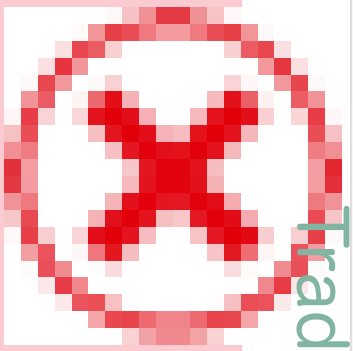
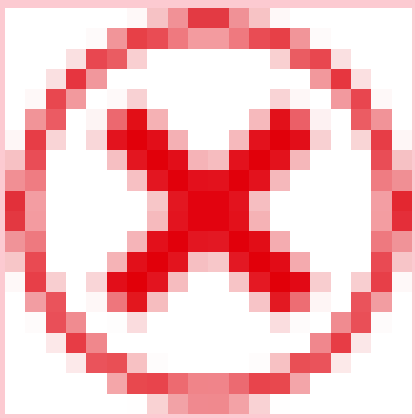
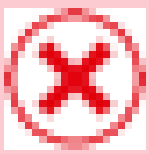
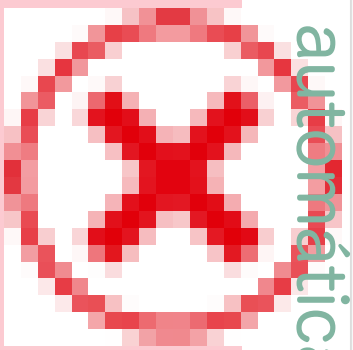
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Regras de Duplicação					
Propriedades					

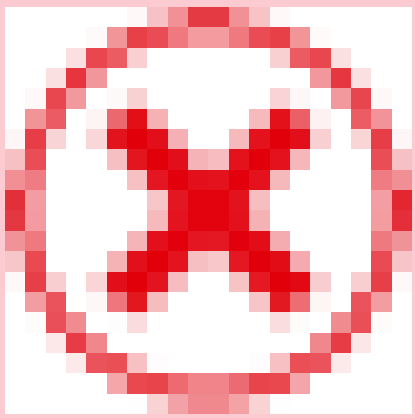
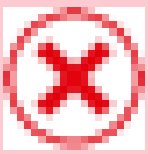
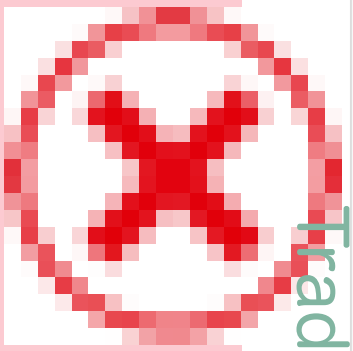
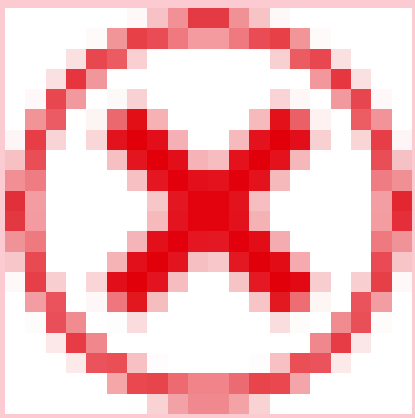
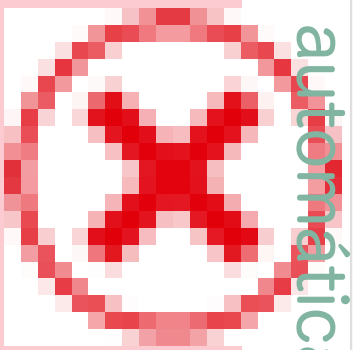
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
E-mails Incompatíveis					
Phishing relatado pelo usuário de regras de ingestão					

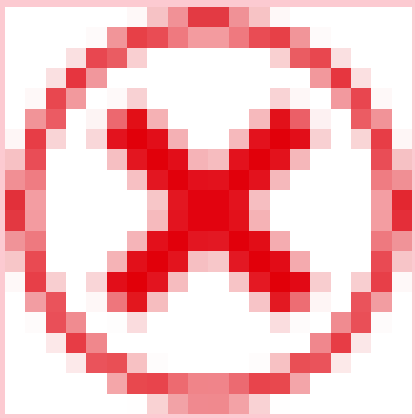
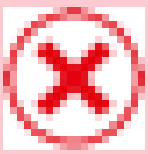
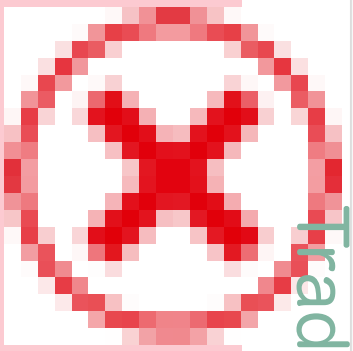
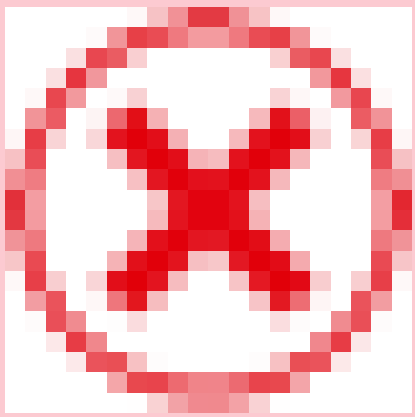
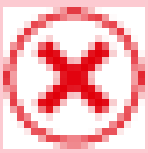
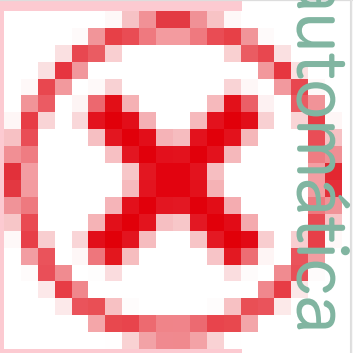
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Propriedades do Phishing Reportado pelo Usuário					
Grupos					
Grupos de Filtros					

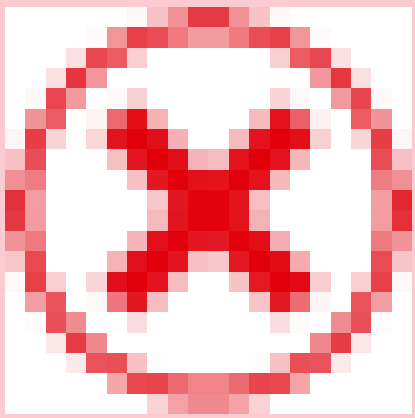
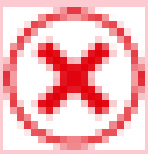
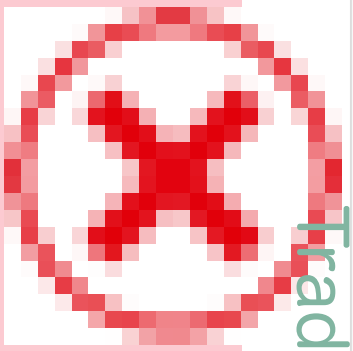
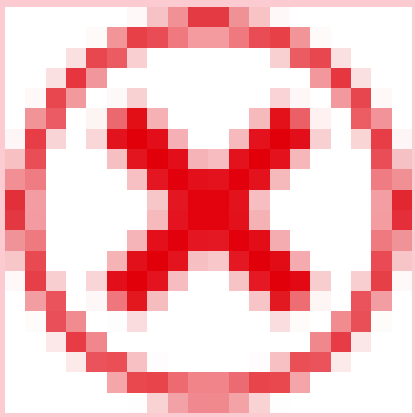
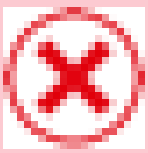
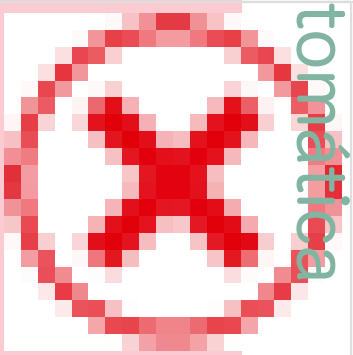
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Escalações					
Enriquecimentos de Dados					
Marcadores de Segurança					
Grupos					

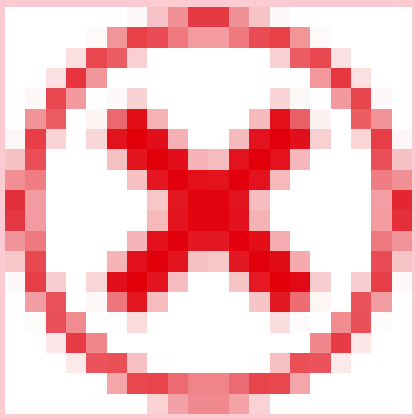
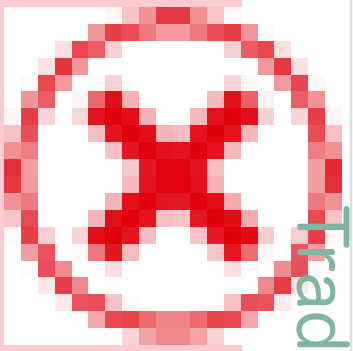
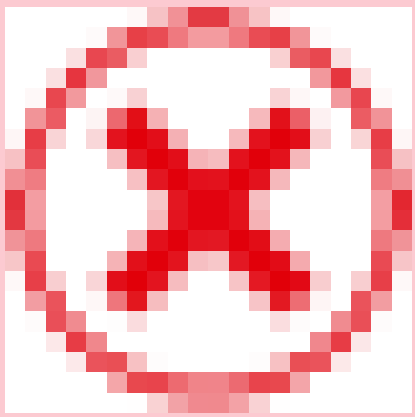
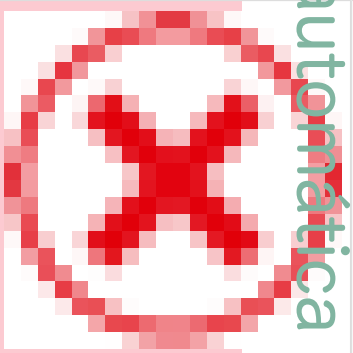
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Marcadores					
Workflows					
Acompanhamento de execução					

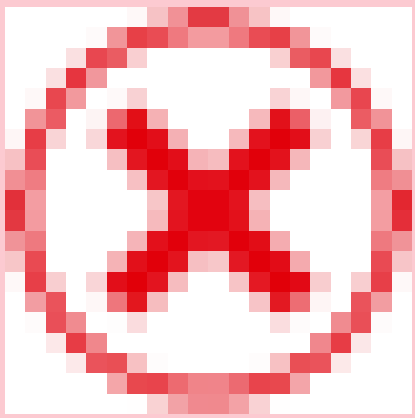
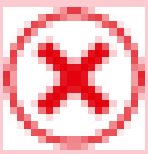
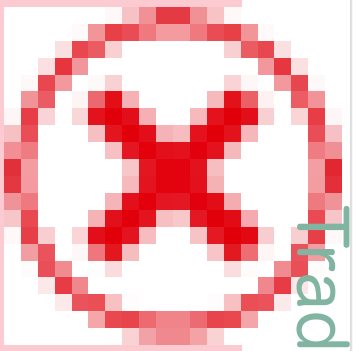
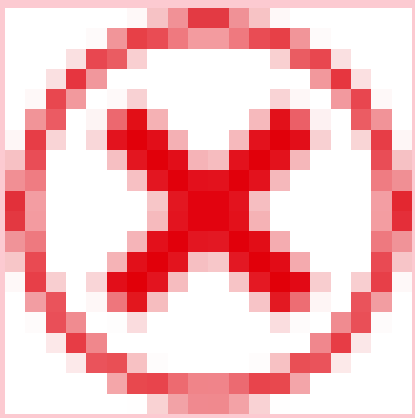
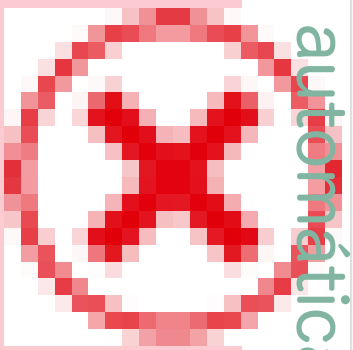
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Exibir Fluxos de Trabalho de Segurança					
Gatilhos de Fluxo de Trabalho					
Utilitários					

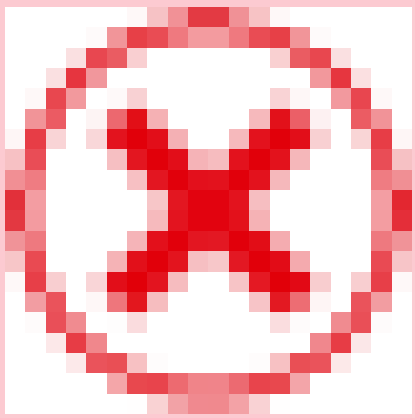
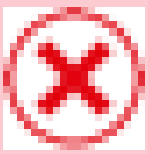
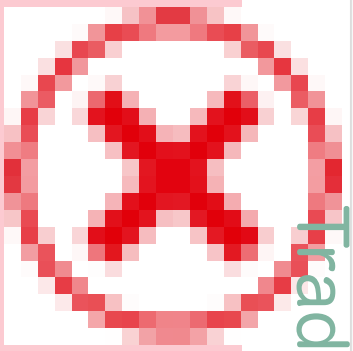
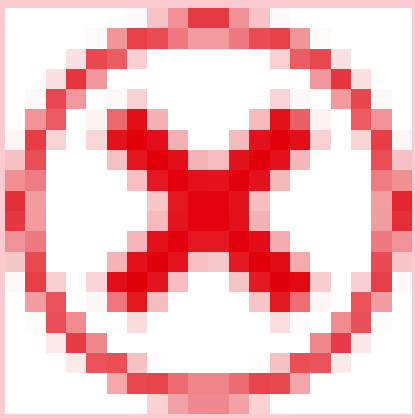
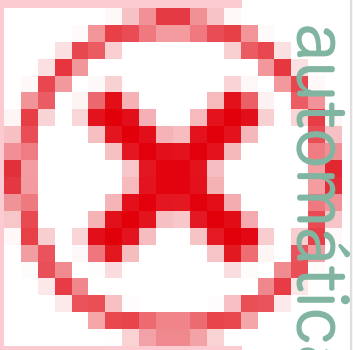
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Mapeamento de Dados de Aprimoramento					
Transformações de Valores de campos					

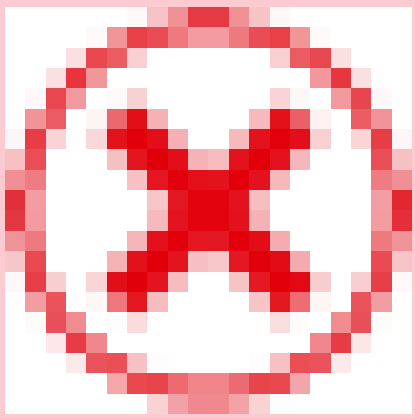
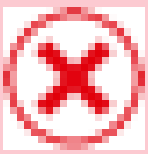
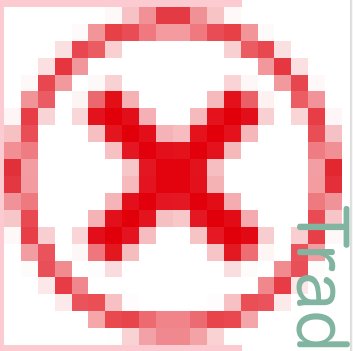
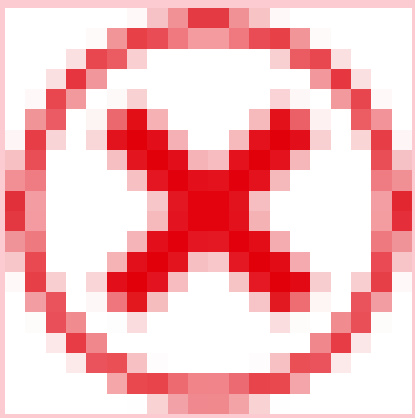
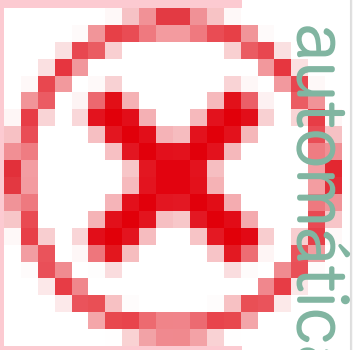
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Mapeamento de Campos					
Orquestração sob demanda					

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Grupos de Sistemas Operacionais	✗	✓	✗	✗	
Registro da aplicação SecOps	✗	✓	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Configuração de trabalho em segundo plano	✗	✓	✓	✗	
CMDB					
Regras de Pesquisa de IC	✗	✓	✗	✗	

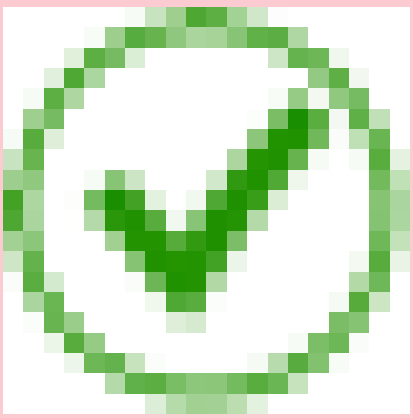
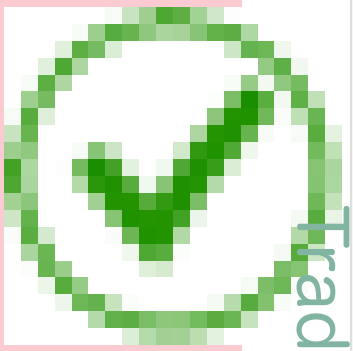
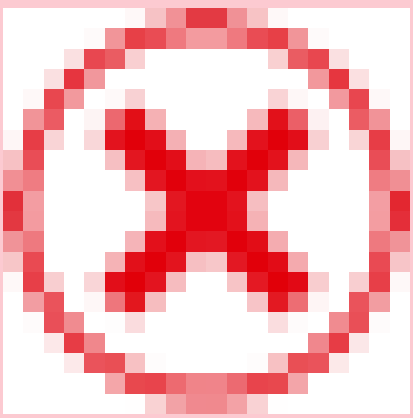
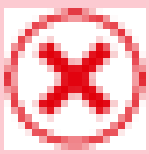
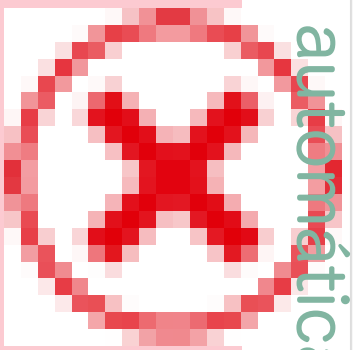
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Itens Descobertos					
Reconciliar itens descobertos sem correspondência					

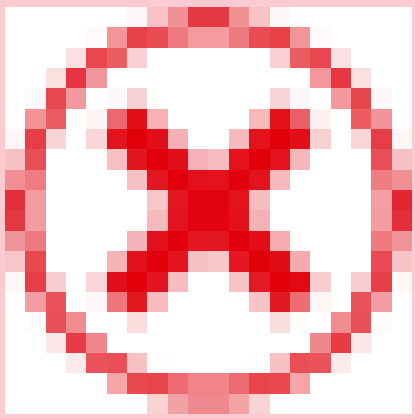
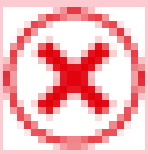
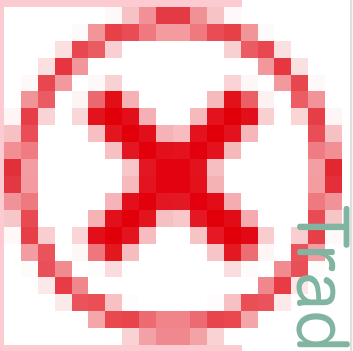
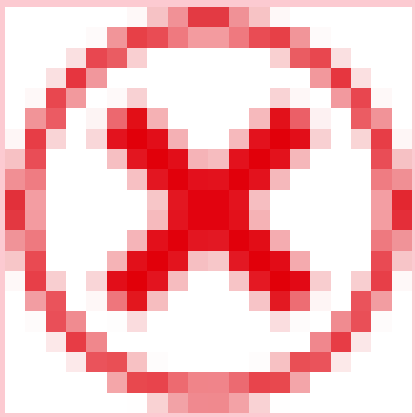
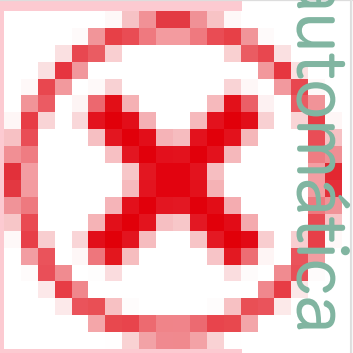
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Imagens do contêiner descobertas					
WatchDog					
Configuração					

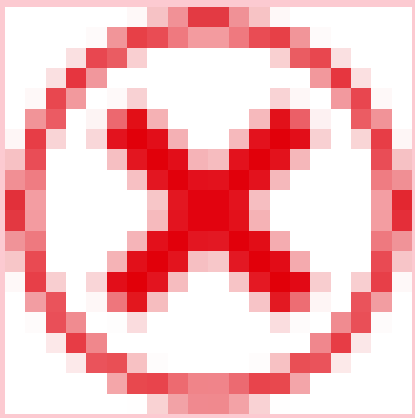
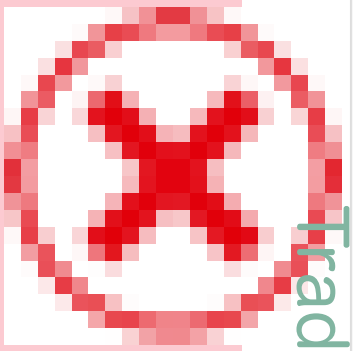
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.basic, sn_vul.read_discovered_item, sn_vul_container.read_discovered_image

Informações para outras funções:

admin, sn_sec_cmn.admin, sn_sec_cmn.ci_manager, sn_sec_cmn.manage_background_job, sn_sec_cmn.read, sn_sec_cmn.read_background_job

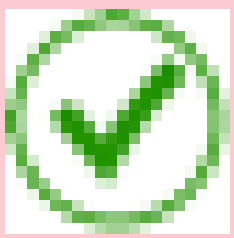
Módulo	sn_sec_cmn.reclassify_unmatch_ci	sn_si.admin	sn_si.básico	sn_vul.read_discovered_item	sn_vul
Visão geral					

[End]

[store-future: BEGIN review]

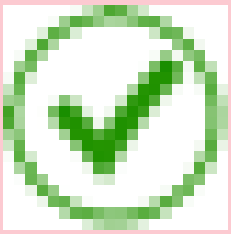
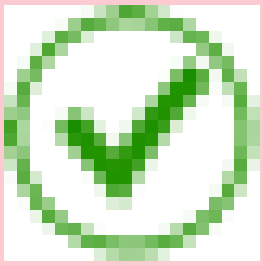
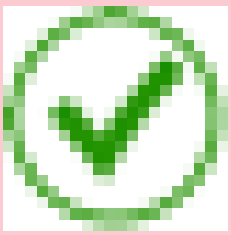
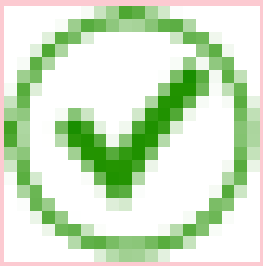
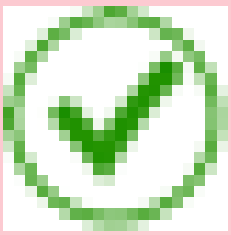
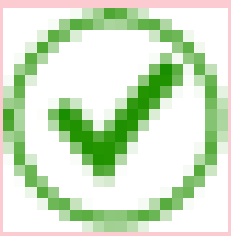
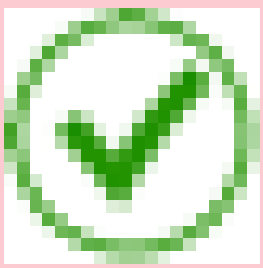
Acesso ao módulo por função para Splunk Integration

Para Splunk Integration, consulte os itens de menu que podem ser acessados por uma função específica.

Módulo	sn_si.admin	sn_si.analista
(Grupo de apps principal)		
Perfis de evento do Splunk		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

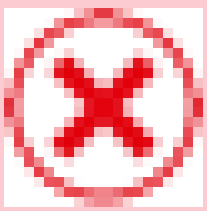
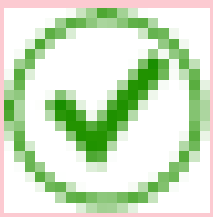
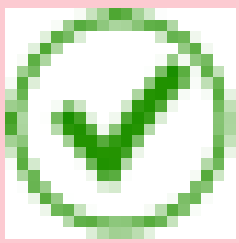
Módulo	sn_si.admin	sn_si.analista
Traduções de campo do Splunk		
Evento do Splunk para tarefas		
Importação de evento do Splunk		
Configurações de integração do Splunk		

[End]

[store-future: BEGIN review]

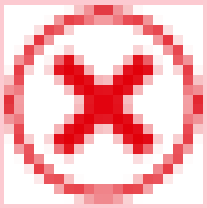
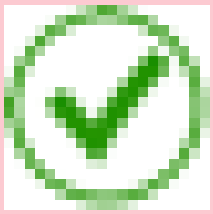
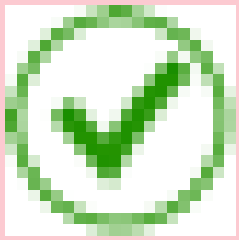
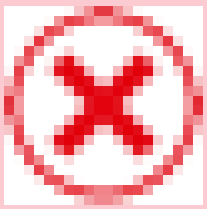
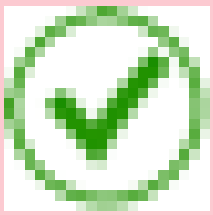
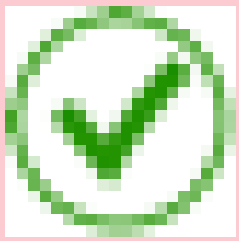
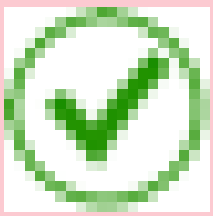
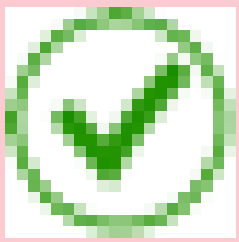
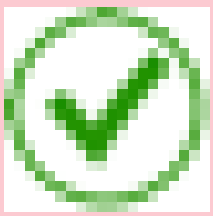
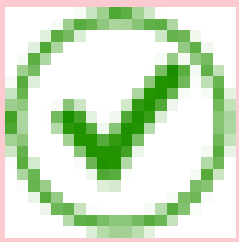
Acesso ao módulo por função da integração DLP da Symantec

Para o Symantec DLP Integration, consulte os itens de menu que podem ser acessados por uma função específica.

Módulo	agent_admin	sn_dlir.admin	sn_dlir.analista
(Grupo de apps principal)			
Perfil do incidente			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

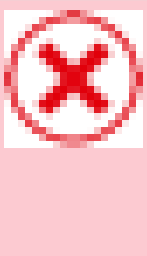
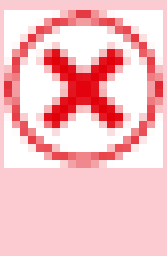
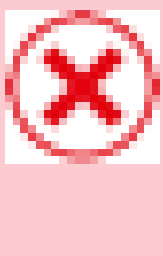
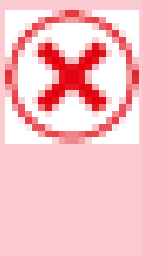
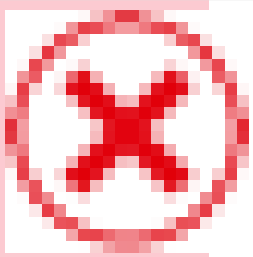
Módulo	agent_admin	sn_dlir.admin	sn_dlir.analista
Mapeamento do status do incidente			
Configurações			
Aplicação MID			
MID Server			

[End]

[store-future: BEGIN review]

Acesso ao módulo por função da Inteligência contra ameaças

Para Inteligência contra ameaças, consulte os itens de menu que podem ser acessados por uma função específica.

Módulo	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.gerente	sn_ti.admin	sn_ti.case_user_read	sn_ti.read
(Grupo de apps principal)							
Objetos							
Objetos							
Repositório LOC							

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.gerente	sn_ti.admin	sn_ti.case_user_read	sn_ti.read
Métodos de modo de ataque	✓	✓	✓	✓	✓	✓	✓
Indicadores	✓	✓	✓	✓	✓	✓	✓
Observáveis	✓	✓	✓	✓	✓	✓	✓
Padrões de ataque	✓	✓	✓	✓	✓	✓	✓
Campanhas	✓	✓	✓	✓	✓	✓	✓
Linha de ação	✓	✓	✓	✓	✓	✓	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.gerente	sn_ti.admin	sn_ti.case_user_read	sn_ti.read
Identidades	✓	✓	✓	✓	✓	✓	✓
Infraestrutura	✓	✓	✓	✓	✓	✓	✓
Locais	✓	✓	✓	✓	✓	✓	✓
Malware	✓	✓	✓	✓	✓	✓	✓
Conjunto de intrusão	✓	✓	✓	✓	✓	✓	✓
Agentes da ameaça	✓	✓	✓	✓	✓	✓	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.gerente	sn_ti.admin	sn_ti.case_user_read	sn_ti.read
Análise de malware	✓	✓	✓	✓	✓	✓	✓
Dados observados	✓	✓	✓	✓	✓	✓	✓
Grupos de ameaças	✓	✓	✓	✓	✓	✓	✓
Definições de marcação	✓	✓	✓	✓	✓	✓	✓
Anotações de ameaça	✓	✓	✓	✓	✓	✓	✓
Opiniões sobre ameaças	✓	✓	✓	✓	✓	✓	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.gerente	sn_ti.admin	sn_ti.case_user_read	sn_ti.read
Relatórios de ameaças	✓	✓	✓	✓	✓	✓	✓
Avistamentos do indicador	✓	✓	✓	✓	✓	✓	✓
Avistamentos de objeto	✓	✓	✓	✓	✓	✓	✓
Vulnerabilidades	✓	✓	✓	✓	✓	✓	✓
Ferramentas	✓	✓	✓	✓	✓	✓	✓
Relacionamentos objeto/objeto	✓	✓	✓	✓	✓	✓	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.gerente	sn_ti.admin	sn_ti.case_user_read	sn_ti.read
Relacionamentos de ObjectIndicator	✓	✓	✓	✓	✓	✓	✓
Relacionamentos de Observável de Objeto	✓	✓	✓	✓	✓	✓	✓
Origens							
Origens de Ameaças	✗	✗	✗	✗	✓	✗	✗
Perfis TAXII	✗	✗	✗	✗	✓	✗	✗
Inteligência Externa							
Biblioteca de Violação de Dados	✓	✓	✓	✓	✓	✓	✓
Biblioteca WHOIS	✓	✓	✓	✓	✓	✓	✓
Administração							

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.gerente	sn_ti.admin	sn_ti.case_user_read	sn_ti.read
Propriedades	✗	✗	✗	✗	✓	✗	✗
Mecanismos de Ataque	✗	✗	✗	✗	✓	✗	✗
Motivações de ataque	✗	✗	✗	✗	✓	✗	✗
Métodos de Descoberta	✗	✗	✗	✗	✓	✗	✗
Feeds	✗	✗	✗	✗	✓	✗	✗
Tipos de Indicador	✗	✗	✗	✗	✓	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.gerente	sn_ti.admin	sn_ti.case_user_read	sn_ti.read
Tipos de infraestrutura	✗	✗	✗	✗	✓	✗	✗
Efeitos Pretendidos	✗	✗	✗	✗	✓	✗	✗
Capacidades do malware	✗	✗	✗	✗	✓	✗	✗
Tipos de malware	✗	✗	✗	✗	✓	✗	✗
Notificações	✗	✗	✗	✗	✓	✗	✗
Tipos de observável	✗	✗	✗	✗	✓	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.gerente	sn_ti.admin	sn_ti.case_user_read	sn_ti.read
Definições de Limite de Taxa	✗	✗	✗	✗	✓	✗	✗
Tipos de relatório	✗	✗	✗	✗	✓	✗	✗
Funções de agente da ameaça	✗	✗	✗	✗	✓	✗	✗
Tipos de Agente da Ameaça	✗	✗	✗	✗	✓	✗	✗
Tipos de Ferramentas	✗	✗	✗	✗	✓	✗	✗
Gestão de casos							
Todos os Casos	✗	✗	✗	✗	✗	✓	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.gerente	sn_ti.admin	sn_ti.case_user_read	sn_ti.read
Casos em aberto	✗	✗	✗	✗	✗	✓	✗
Meus Casos	✗	✗	✗	✗	✗	✓	✗
Repositório do MITRE ATT&CK							
Visão geral	✓	✓	✓	✓	✓	✓	✓
Matrizes	✓	✓	✓	✓	✓	✓	✓
Técnicas	✓	✓	✓	✓	✓	✓	✓
Mitigações	✓	✓	✓	✓	✓	✓	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.gerente	sn_ti.admin	sn_ti.case_user_read	sn_ti.read
Grupos	✓	✓	✓	✓	✓	✓	✓
Malware	✓	✓	✓	✓	✓	✓	✓
Ferramentas	✓	✓	✓	✓	✓	✓	✓
Relações do MITRE	✓	✓	✓	✓	✓	✓	✓
Mapa térmico e Navegador	✓	✓	✓	✓	✓	✓	✓
Mapeamento de técnica de CVE	✓	✓	✓	✓	✓	✓	✓
Administração do MITRE ATT&CK							

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.gerente	sn_ti.admin	sn_ti.case_user_read	sn_ti.read
Mapeamento de fonte de dados	✓	✓	✓	✓	✓	✓	✓
Mapeamento de componente de dados	✓	✓	✓	✓	✓	✓	✓
Definição de cobertura de detecção	✓	✓	✓	✓	✓	✓	✓
Mapeamento de cobertura de detecção	✓	✓	✓	✓	✓	✓	✓
Definição de cobertura de mitigação	✓	✓	✓	✓	✓	✓	✓
Calculadora de cobertura de mitigação	✓	✓	✓	✓	✓	✓	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Módulo	sn_si.admin	sn_si.analista	sn_si.ciso	sn_si.gerente	sn_ti.admin	sn_ti.case_user_read	sn_ti.read
Mapeamento de cobertura de mitigação	✓	✓	✓	✓	✓	✓	✓
Regra de extração da técnica	✓	✓	✓	✓	✓	✓	✓
Mapeamento de regras de detecção MITRE ATTCK	✓	✓	✓	✓	✓	✓	✓
Definição de mapa térmico da técnica de grupo de ameaças	✓	✓	✓	✓	✓	✓	✓
Mapeamento da técnica MITRE ATTCK do grupo de ameaças	✓	✓	✓	✓	✓	✓	✓
Propriedades	✓	✗	✗	✗	✓	✗	✗

[End]

[store-future: BEGIN review]

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo por função do Vulnerability Response

Para Vulnerability Response, consulte os itens de menu que podem ser acessados por uma função específica.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

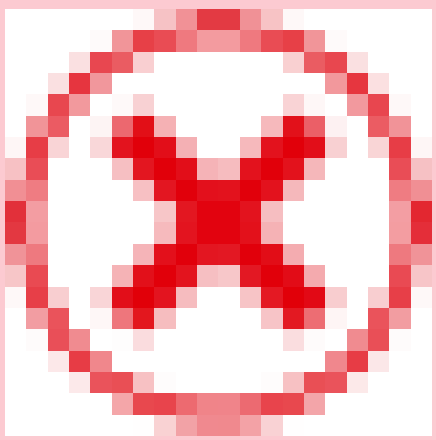
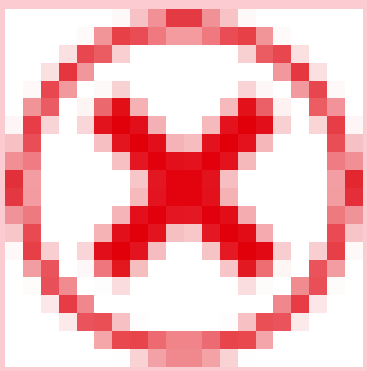
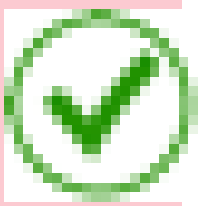
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.config
(Grupo de apps principal)				
Painel do CISO				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

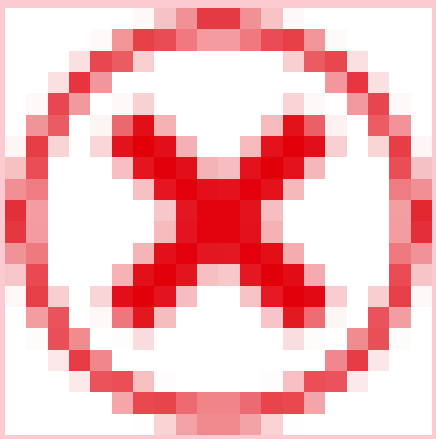
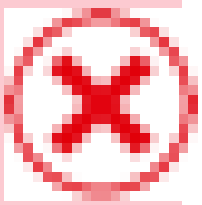
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Visão Geral da Correção				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Espaço para gerentes de vulnerabilidades	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Visão geral	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Espaço de correção de TI	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Visão geral do aprovador	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Visão geral	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

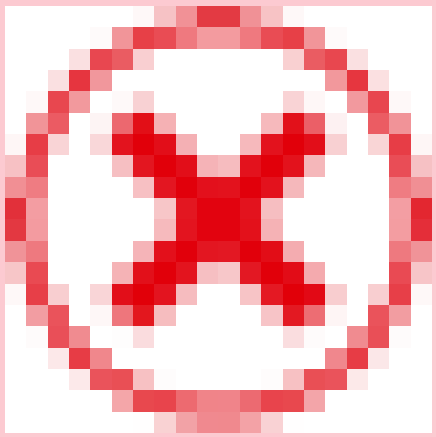
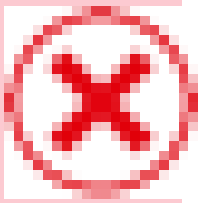
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Minhas aprovações				
Tarefas de correção				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Ativo	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Atribuídos a Mim	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Atribuído aos Meus grupos	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Todos	✗	✓	✗	✓
Itens vulneráveis				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Risco crítico	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Alto risco	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Explorável	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Perto da meta	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Meta não atingida	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Nos últimos 90 dias	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Há mais de 90 dias	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Não designado	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Desagrupado	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Desativado	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Vários adiamentos	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Todos	✗	✓	✗	✓
Soluções				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Todos	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Substituição mais alta	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Com itens vulneráveis	✗	✓	✗	✓
Bibliotecas				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
NVD	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
CWE	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Terceiros	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Software Vulnerável	✗	✓	✗	✓
Verificação de Vulnerabilidades				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Avaliação de Exposição	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Verificações	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Scanners	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Fila de Verificação	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Limites de Taxa do Scanner	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Definições de Limite de Taxa	✗	✓	✗	✓
Administração				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

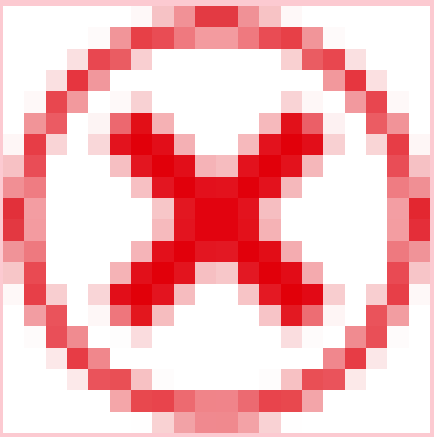
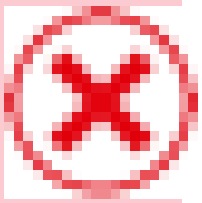
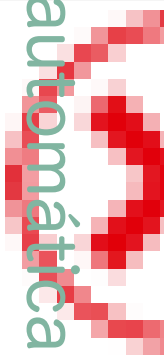
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Assistente de configuração				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Tópicos de observação	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

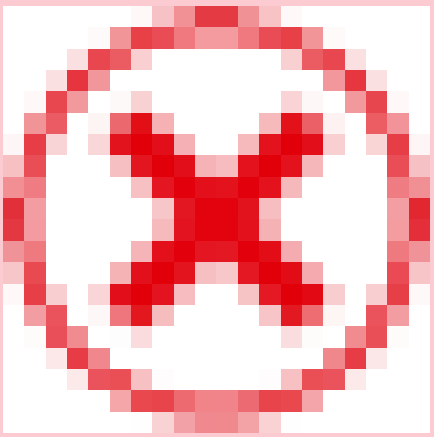
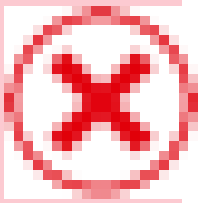
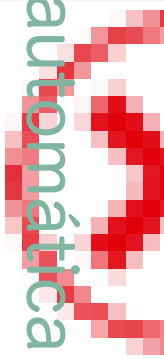
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Regras de atribuição				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Regras de tarefa de correção	✗	✓	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Recomendações de atribuição	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Calculadoras de vulnerabilidade	✗	✓	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.config
Calculadora de Rollup de Vulnerabilidade	✗	✓	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

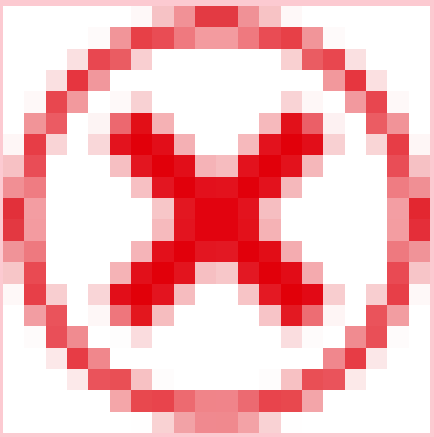
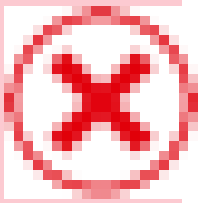
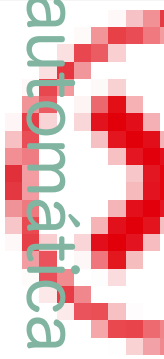
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Regras de destino de correção				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Configuração de fechamento automático	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Regras de exclusão automática	✗	✓	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

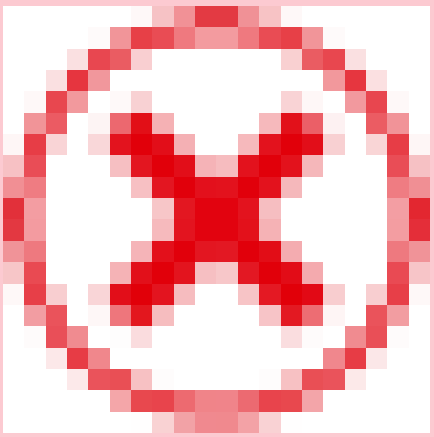
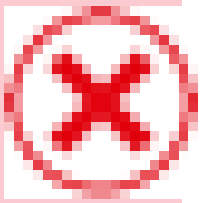
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Regras de exceção				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Regras de aprovação	✓	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Regras de classificação	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Configuração de desempenho	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Configurar granularidade de IV	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Notificações	✗	✓	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Modelos de e-mail	✗	✓	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Importar Fila	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Integrações	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

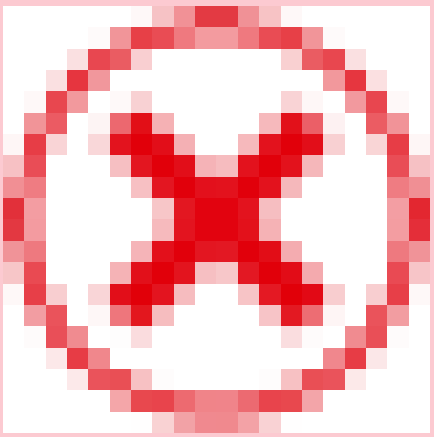
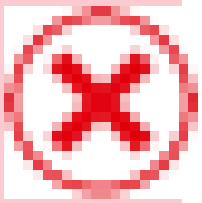
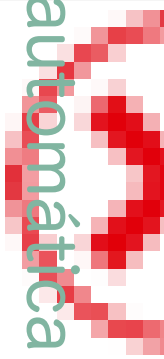
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Definições do ANS				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Configurar SAM NVD	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Mapas de Gravidade Normalizados	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Configuração de cobertura de verificação	✗	✓	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Gestão de exceção	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Relatório de uso	✗	✗	✗	✗
Diagnósticos				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

Informações para outras funções:

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_sec_cmn.manage_approval_rules	sn_vul.access_setup_assistant	sn_vul.ciso_read	sn_vul.configu
Verificações	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
(Grupo de apps principal)			
Painel do CISO	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Visão Geral da Correção	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Espaço para gerentes de vulnerabilidades	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Visão geral	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Espaço de correção de TI	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Visão geral do aprovador	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Visão geral	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Minhas aprovações	✗	✗	✗
Tarefas de correção			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Ativo	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Atribuídos a Mim	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Atribuído aos Meus grupos	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Todos	✗	✗	✗
Itens vulneráveis			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Risco crítico	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Alto risco	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Explorável	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Perto da meta	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Meta não atingida	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Nos últimos 90 dias	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Há mais de 90 dias	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Não designado	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Desagrupado	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Desativado	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Vários adiamentos	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Todos	✗	✗	✗
Soluções			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Todos	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Substituição mais alta	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Com itens vulneráveis	✗	✗	✗
Bibliotecas			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
NVD	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
CWE	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Terceiros	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Software Vulnerável	✗	✗	✗
Verificação de Vulnerabilidades			

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Avaliação de Exposição	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Verificações	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Scanners	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Fila de Verificação	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Limites de Taxa do Scanner	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Definições de Limite de Taxa	✗	✗	✗
Administração			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Assistente de configuração	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Tópicos de observação	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Regras de atribuição	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Regras de tarefa de correção	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Recomendações de atribuição	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Calculadoras de vulnerabilidade	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Calculadora de Rollup de Vulnerabilidade	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Regras de destino de correção	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Configuração de fechamento automático	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Regras de exclusão automática	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Regras de exceção	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Regras de aprovação	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Regras de classificação	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Configuração de desempenho	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Configurar granularidade de IV	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Notificações	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Modelos de e-mail	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Importar Fila	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Integrações	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Definições do ANS	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Configurar SAM NVD	✓	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Mapas de Gravidade Normalizados	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Configuração de cobertura de verificação	✗	✓	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Gestão de exceção	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Relatório de uso	✗	✗	✗
Diagnósticos			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.configure_nvd_integration	sn_vul.configure_scan_coverage_read	sn_vul.configure_vi_granula
Verificações	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

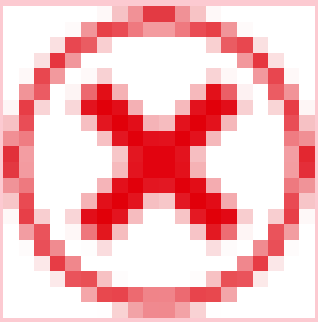
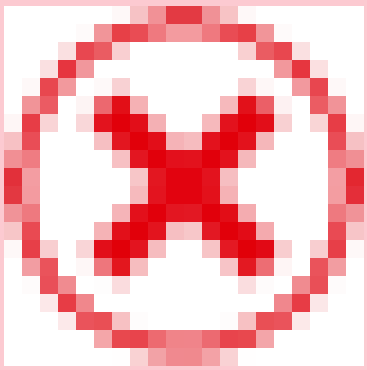
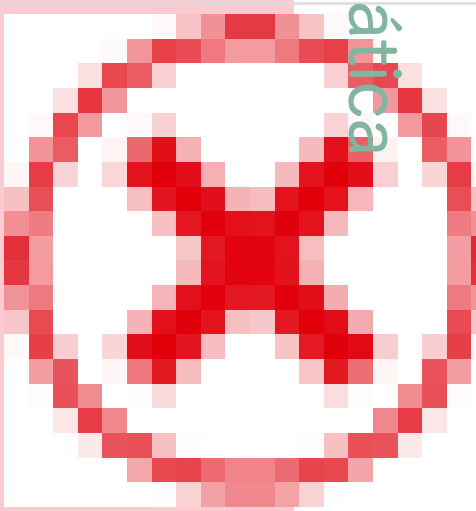
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
(Grupo de apps principal)			
Painel do CISO			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

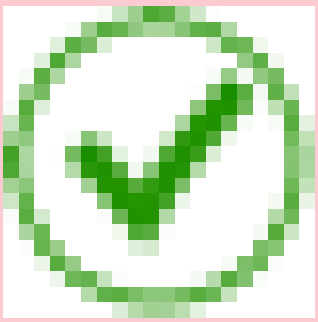
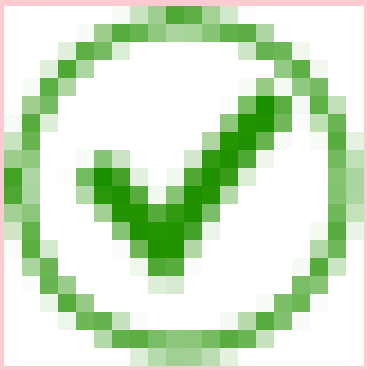
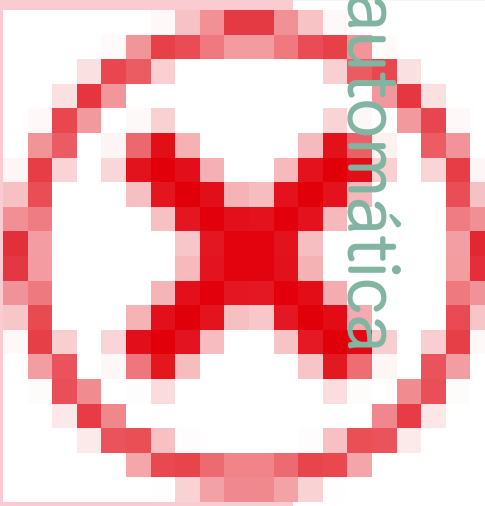
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Visão Geral da Correção			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

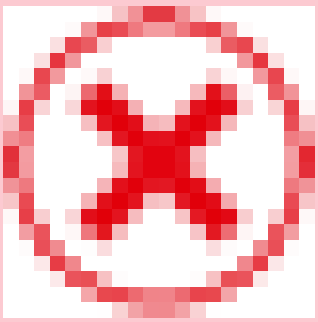
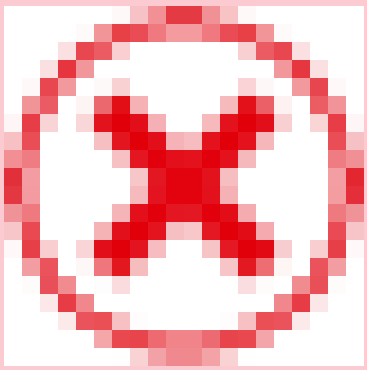
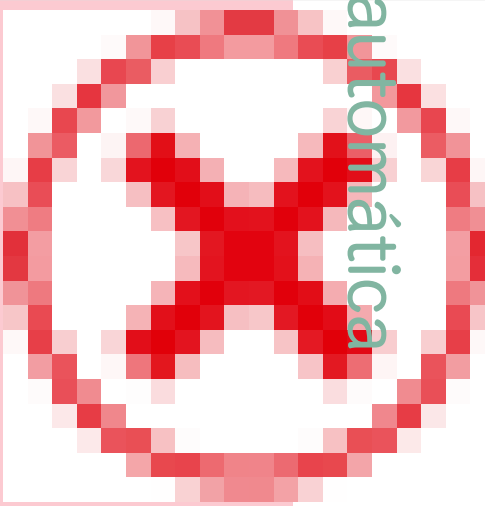
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Espaço para gerentes de vulnerabilidades			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

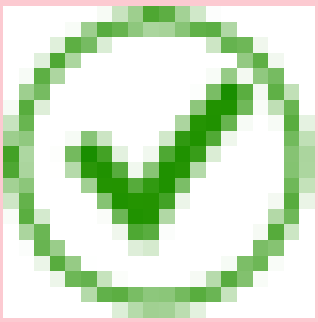
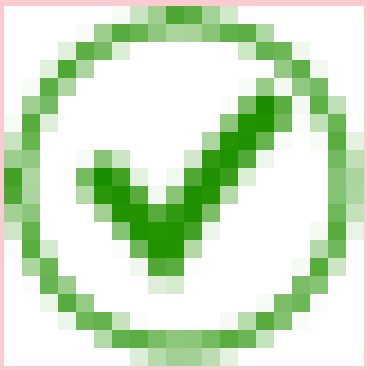
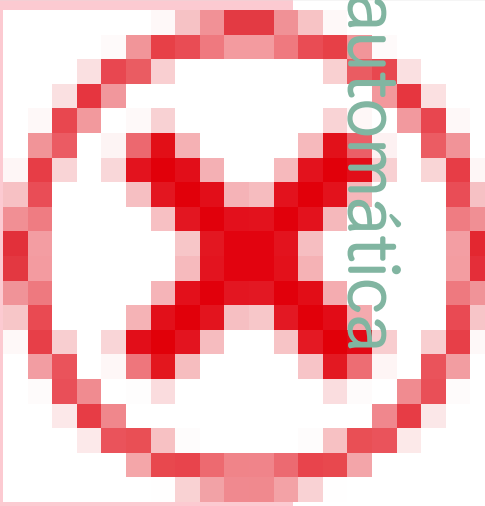
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Visão geral			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

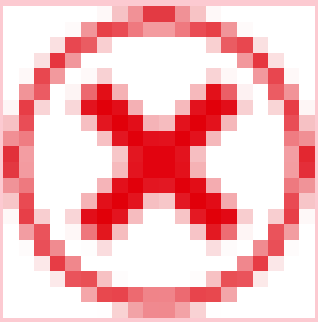
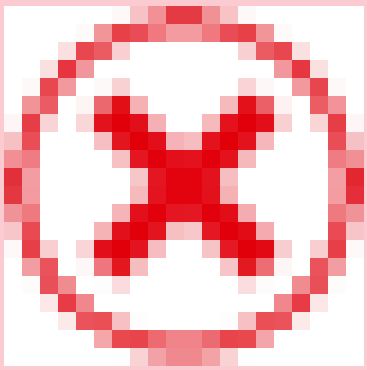
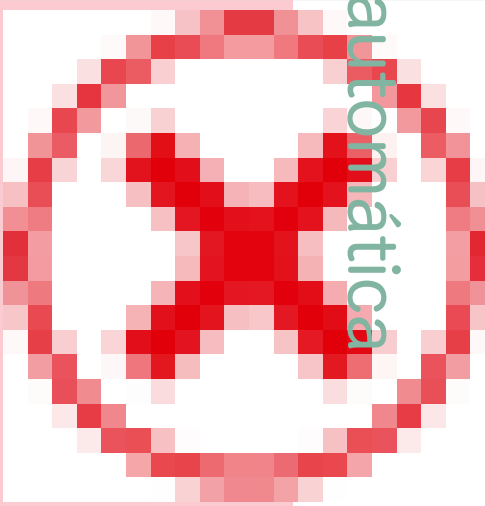
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Espaço de correção de TI			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

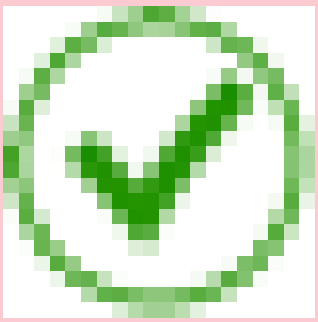
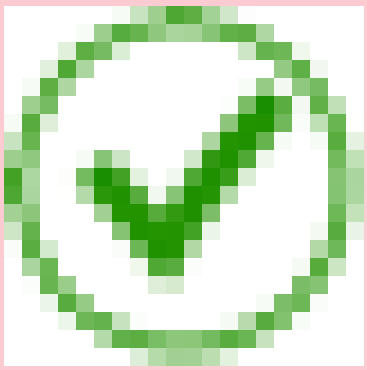
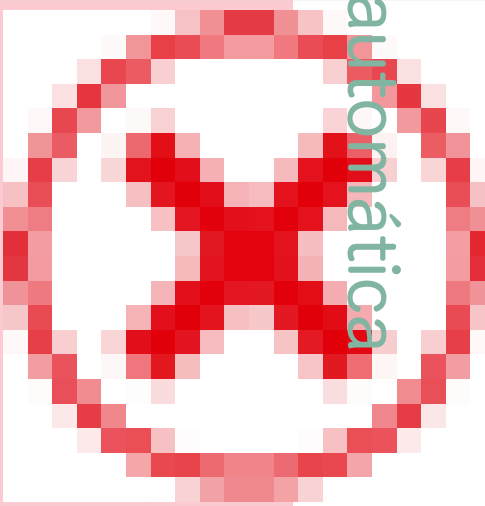
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Visão geral do aprovador			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

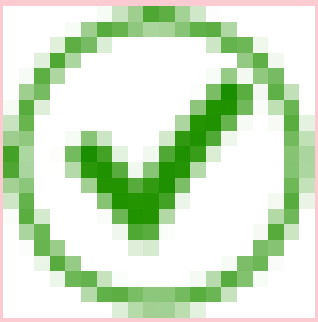
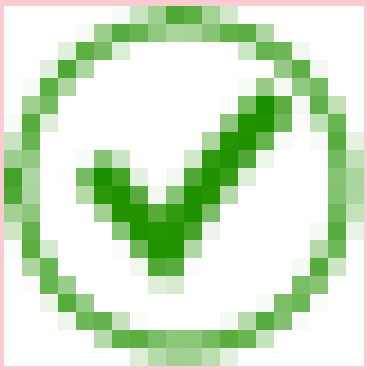
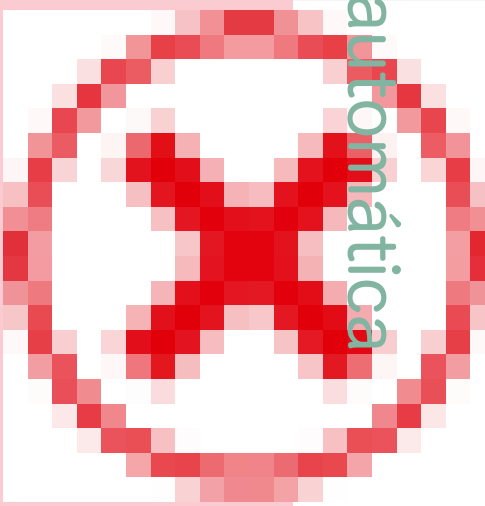
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Visão geral			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

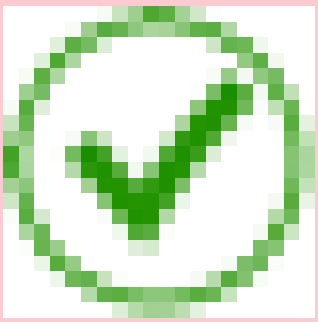
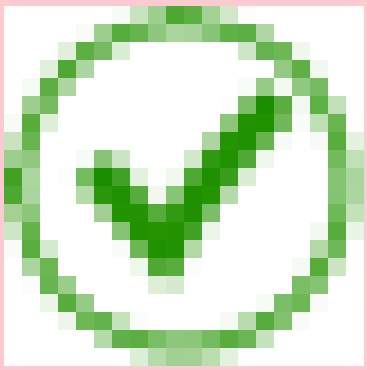
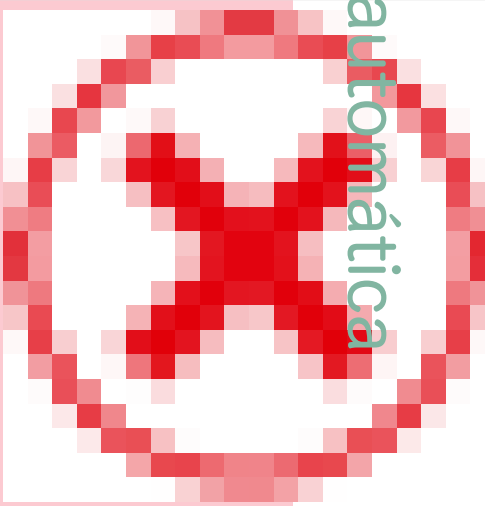
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Minhas aprovações			
Tarefas de correção			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

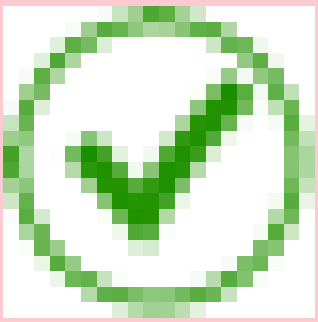
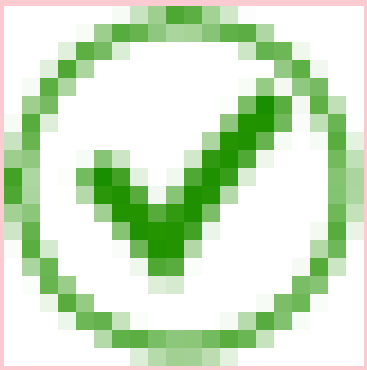
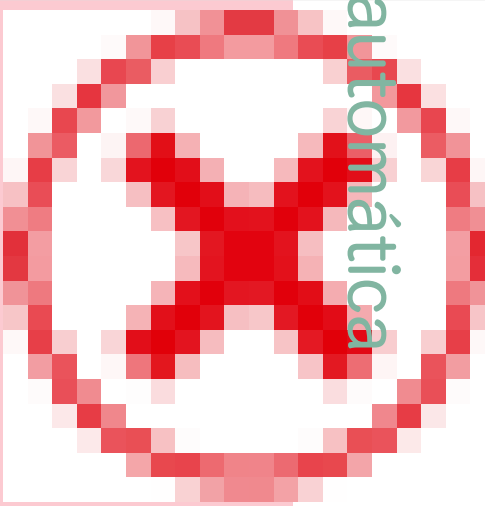
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Ativo			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

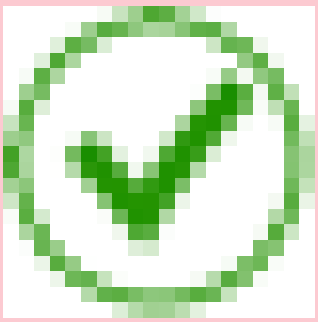
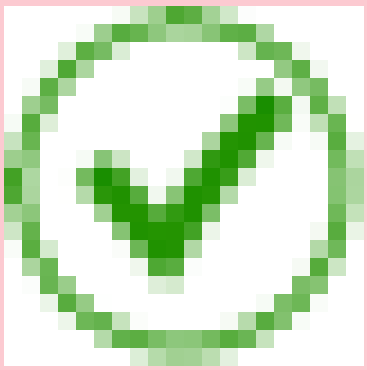
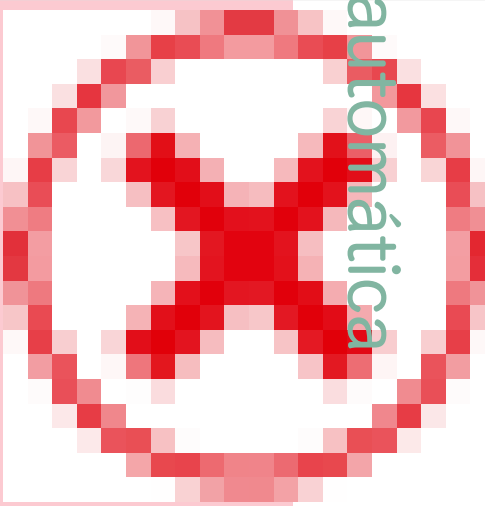
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Atribuídos a Mim			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

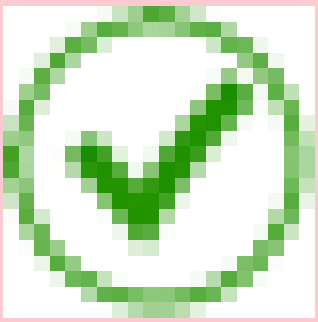
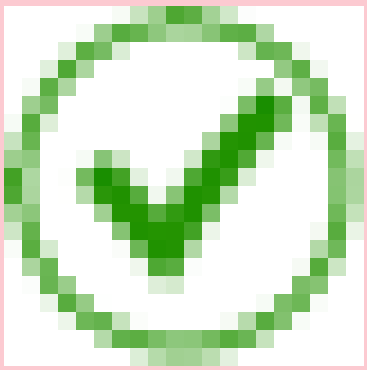
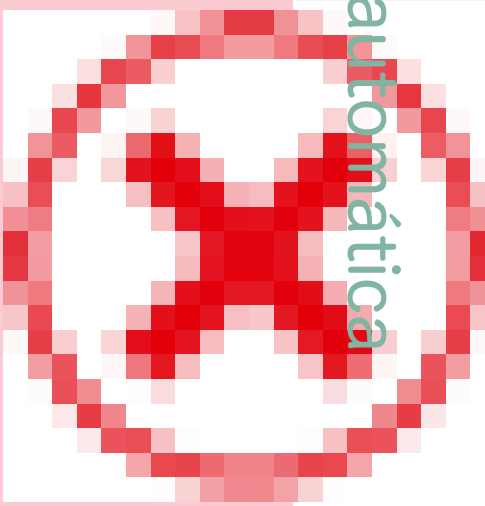
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Atribuído aos Meus grupos			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

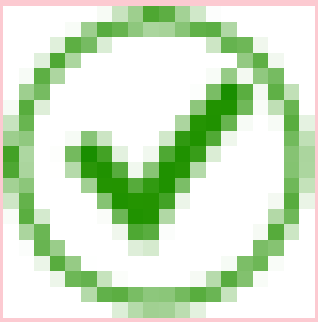
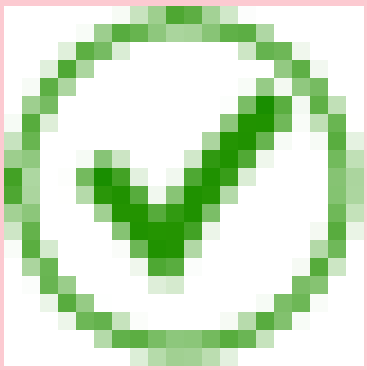
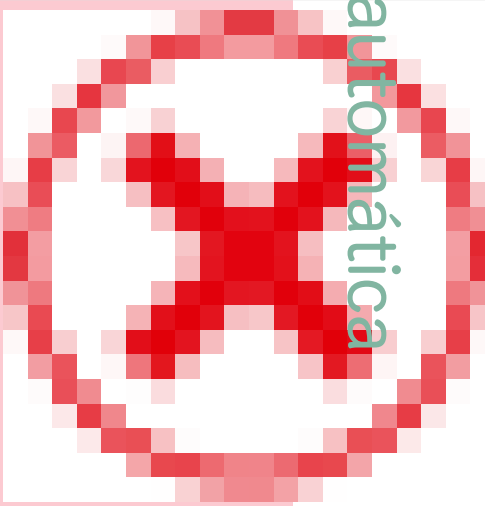
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Todos			
Itens vulneráveis			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

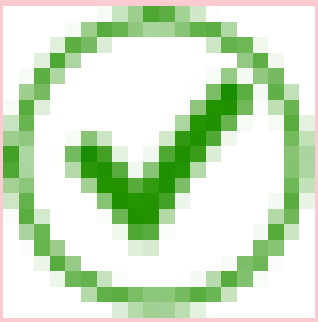
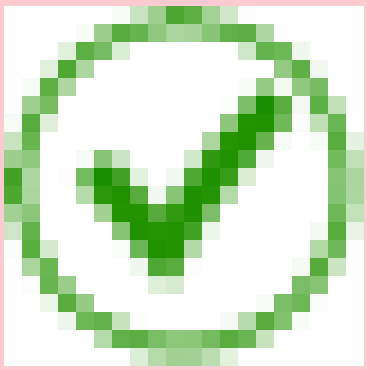
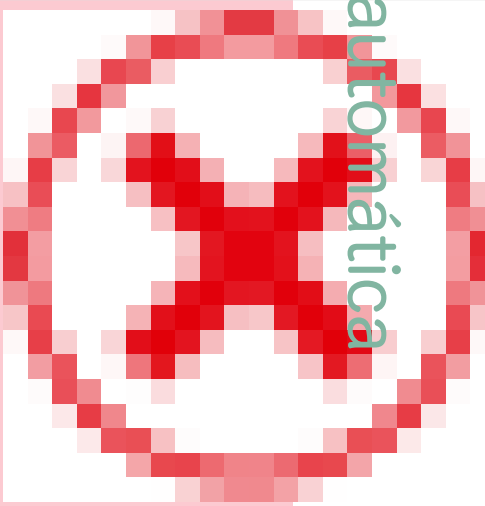
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Risco crítico			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

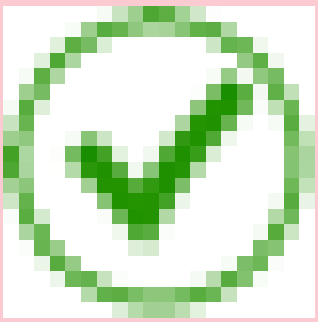
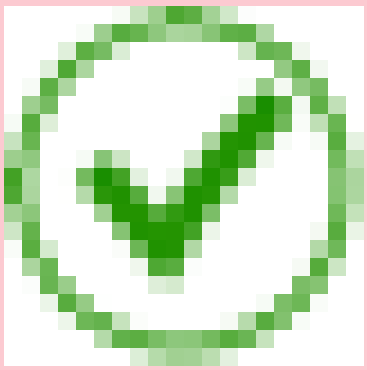
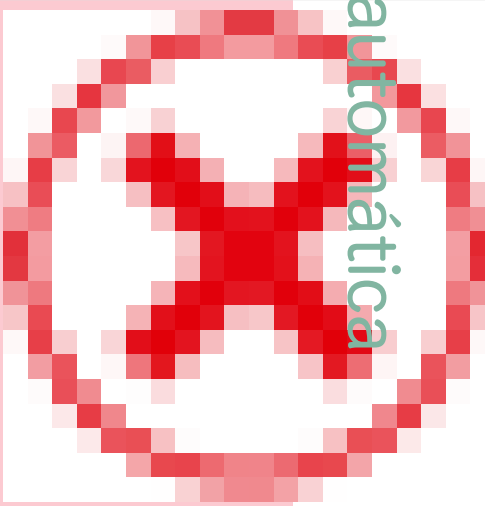
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Alto risco			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

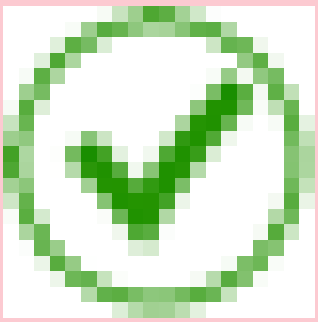
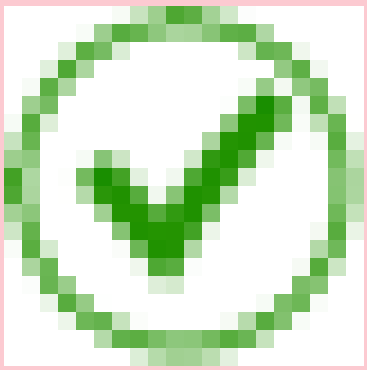
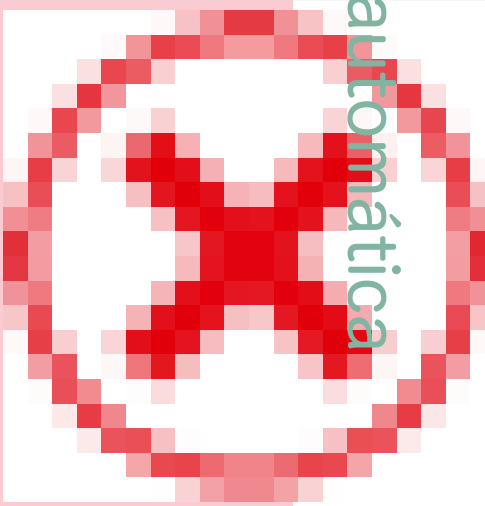
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Explorável			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

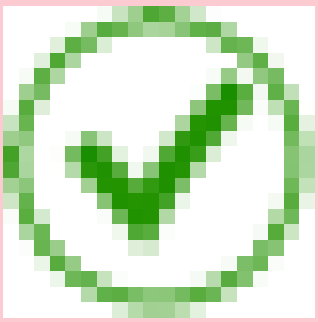
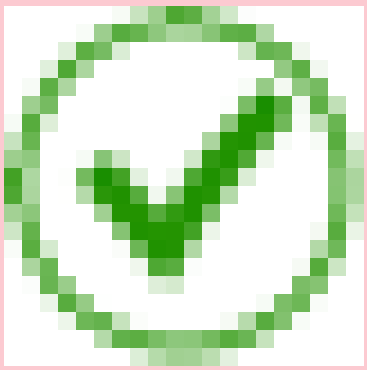
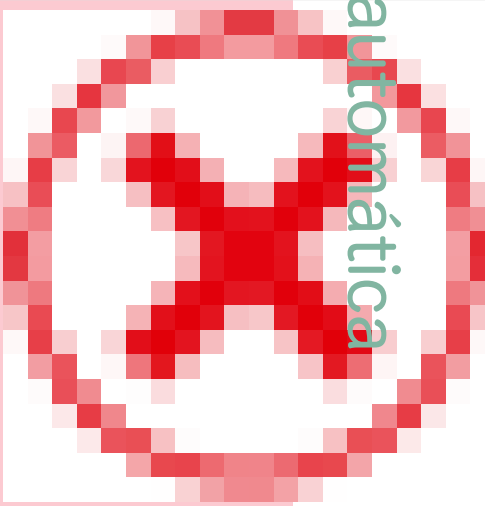
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Perto da meta			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

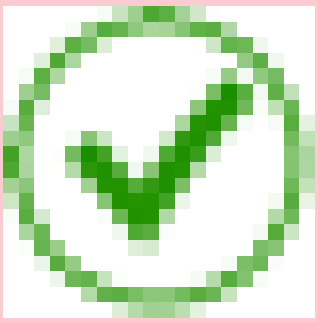
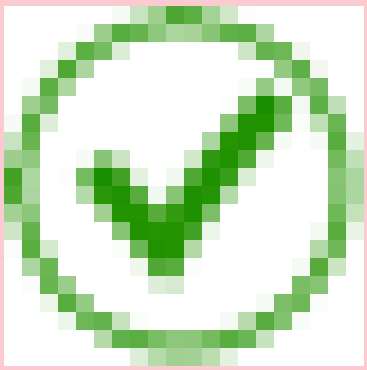
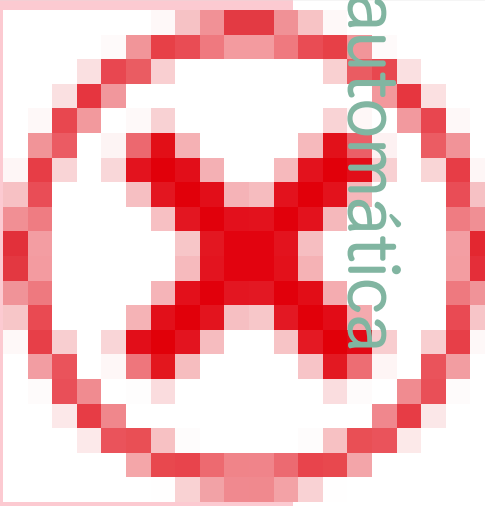
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Meta não atingida			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

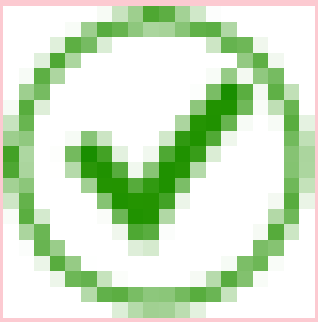
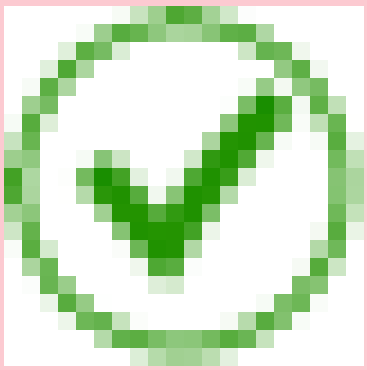
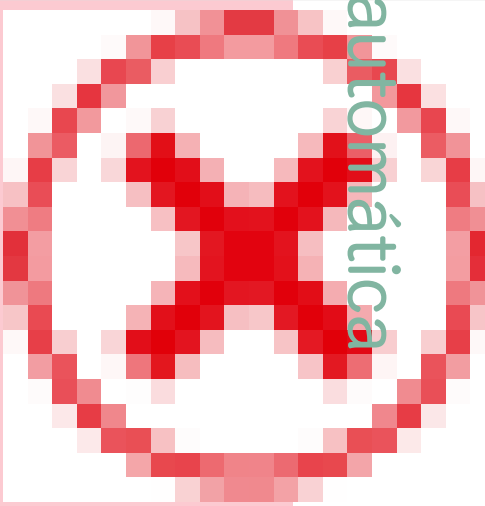
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Nos últimos 90 dias			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

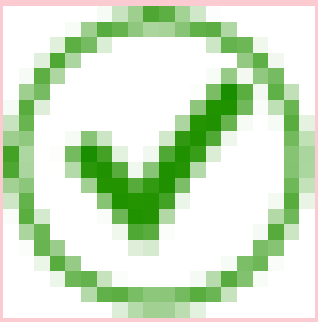
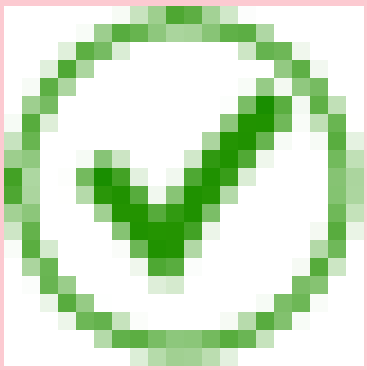
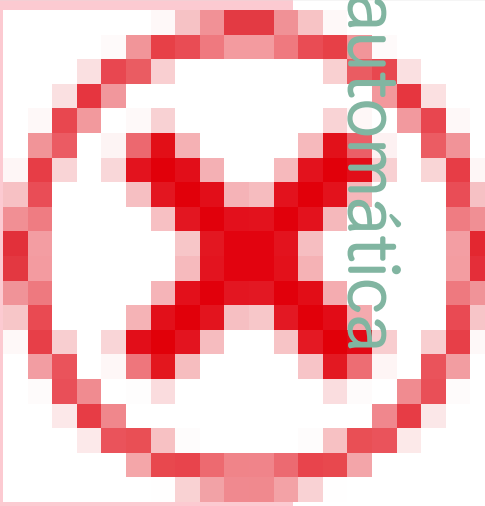
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Há mais de 90 dias			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

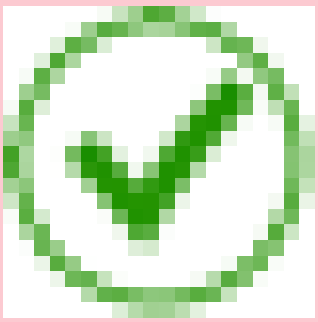
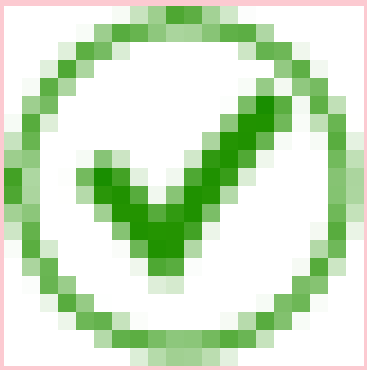
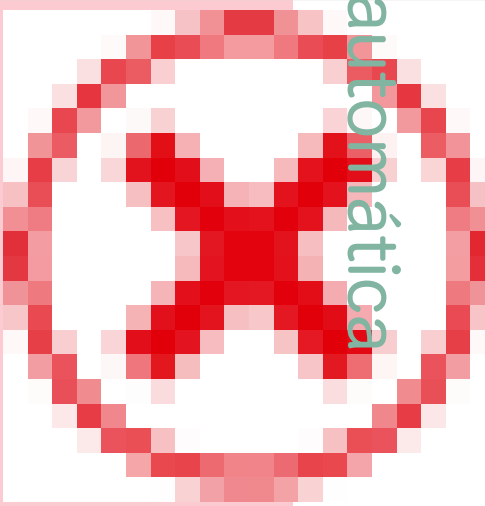
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Não designado			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

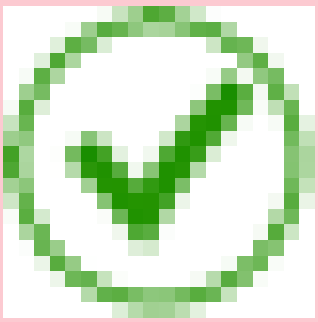
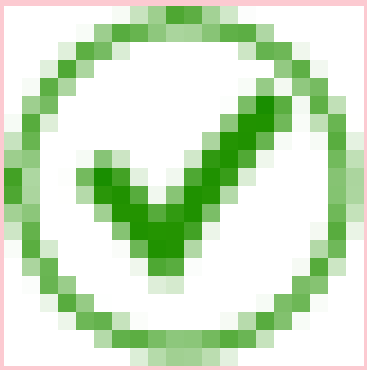
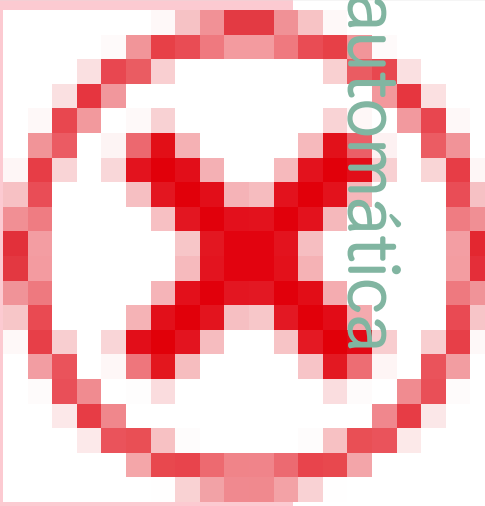
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Desagrupado			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

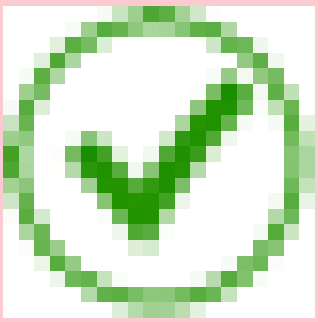
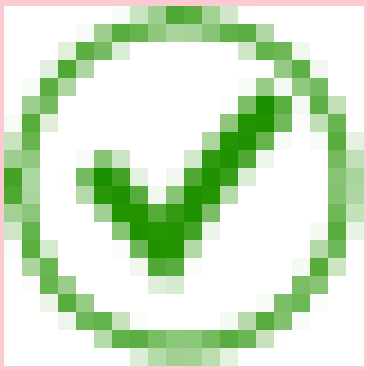
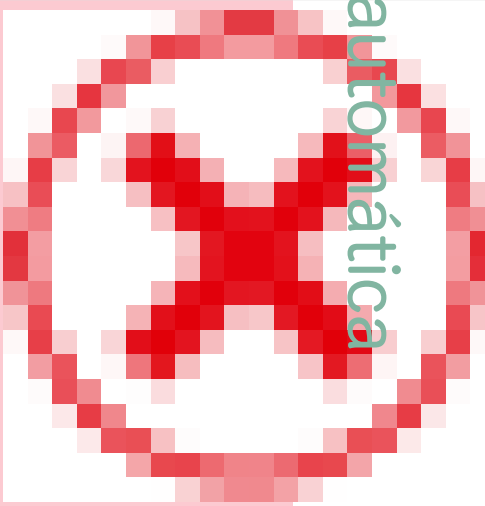
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Desativado			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

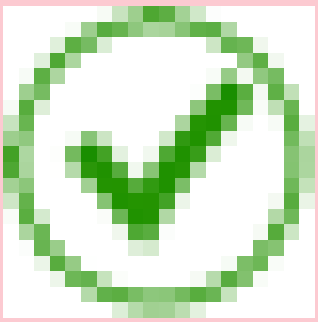
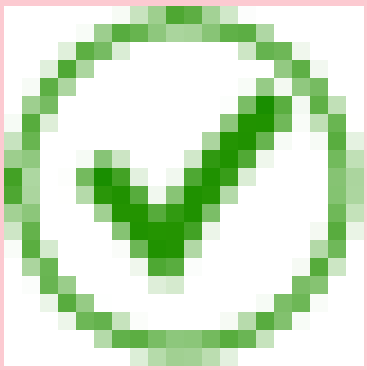
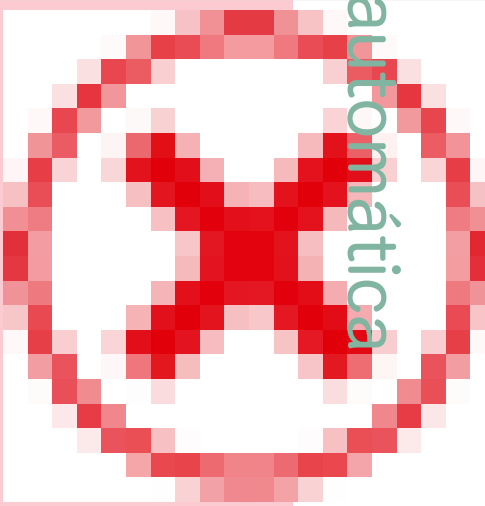
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Vários adiamentos			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

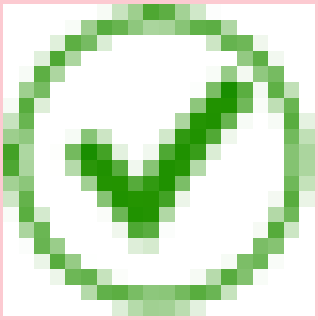
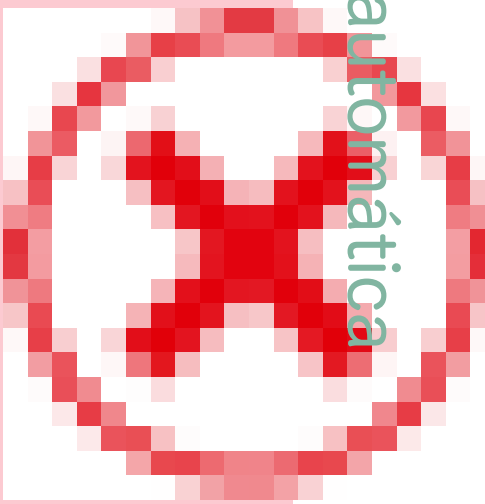
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Todos			
Soluções			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

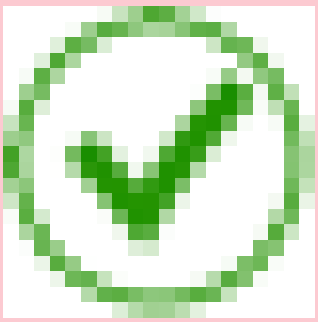
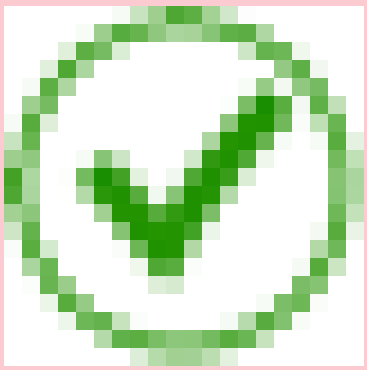
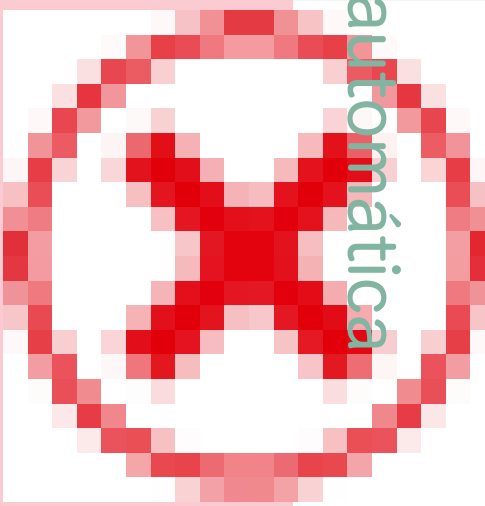
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Todos			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

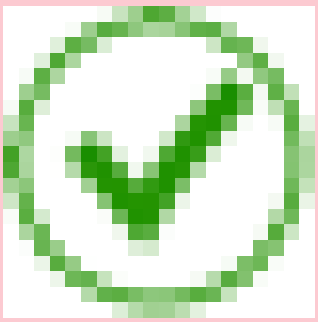
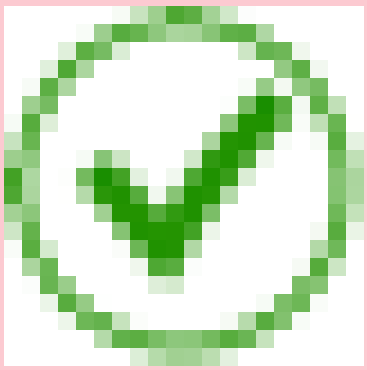
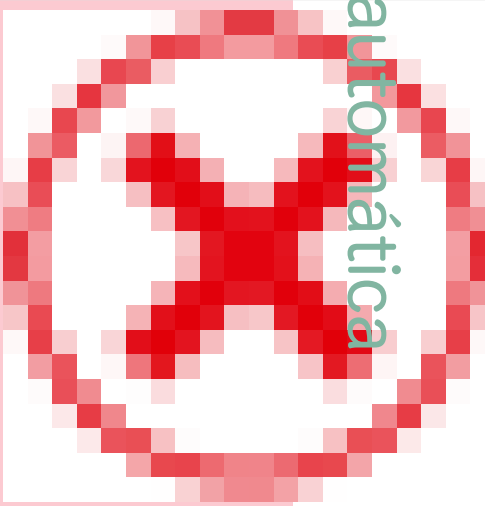
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Substituição mais alta			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

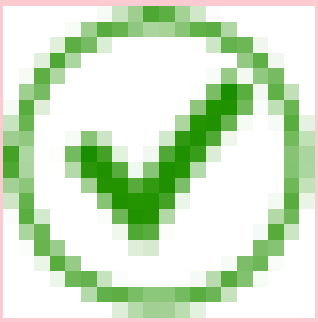
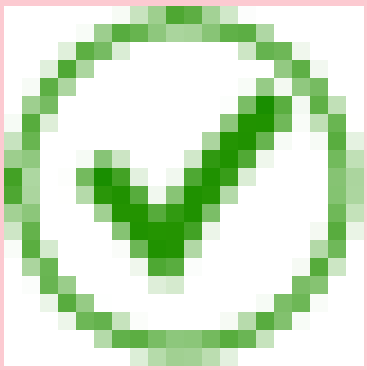
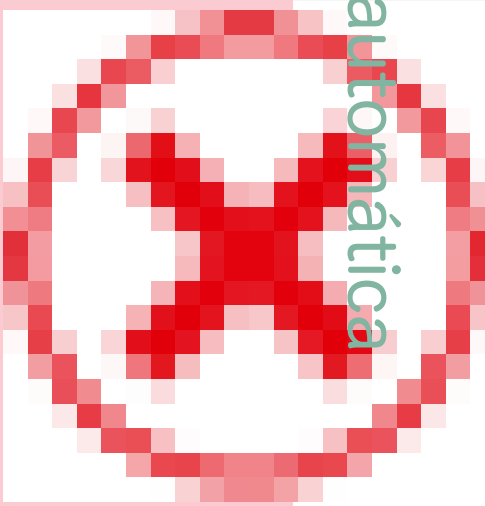
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Com itens vulneráveis			
Bibliotecas			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

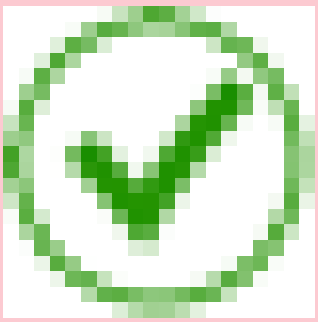
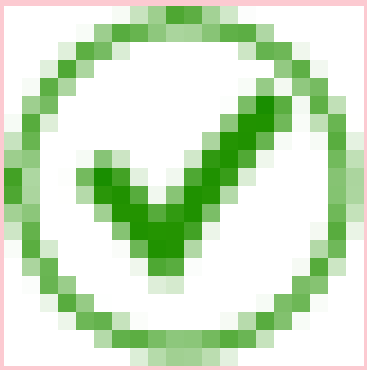
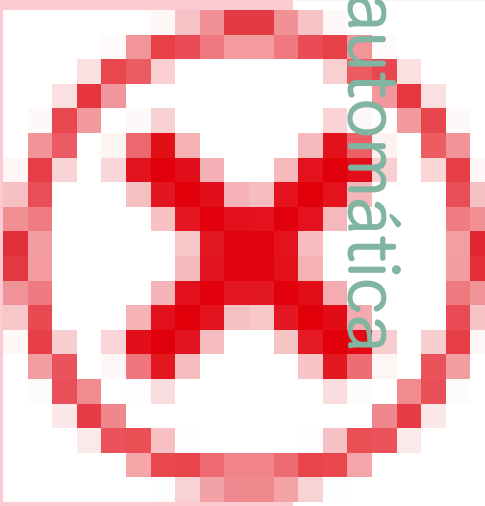
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
NVD			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

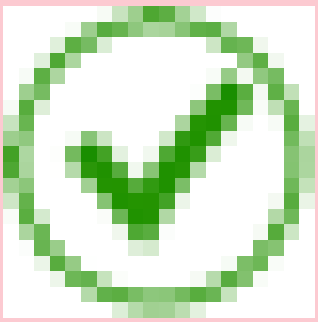
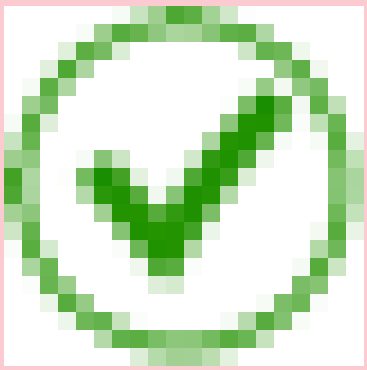
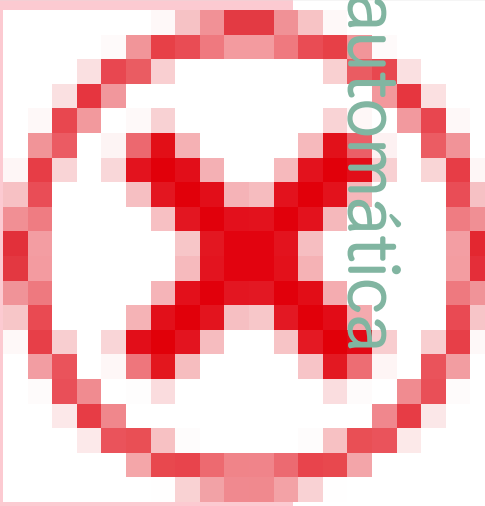
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
CWE			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

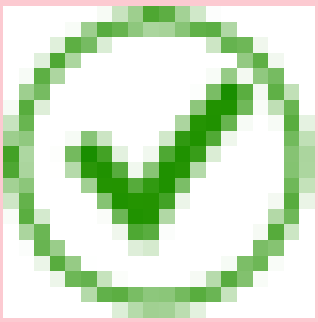
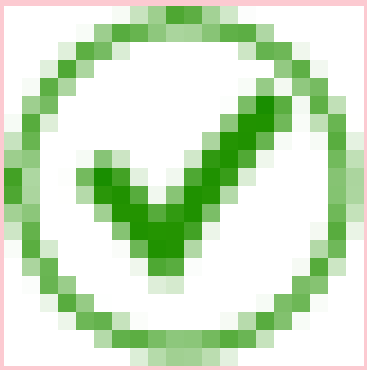
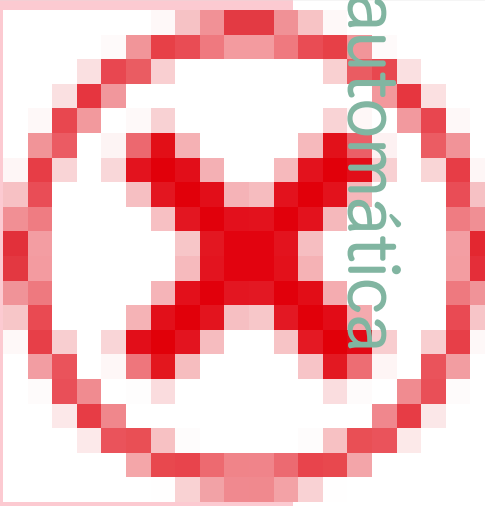
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Terceiros			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

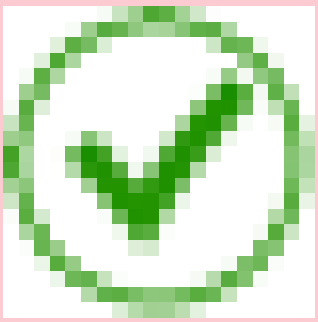
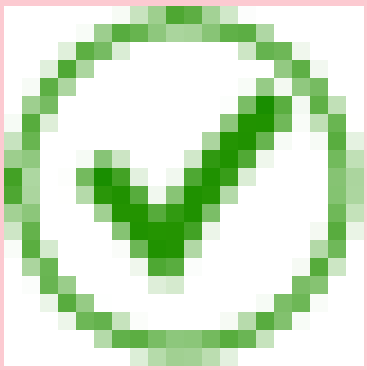
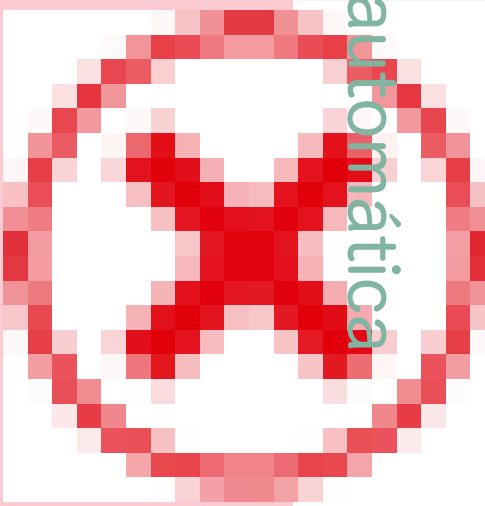
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Software Vulnerável			

Verificação de Vulnerabilidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

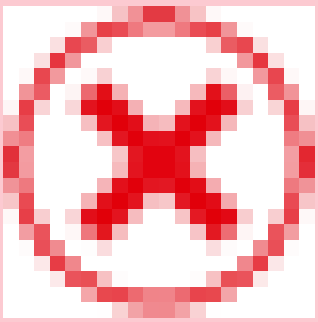
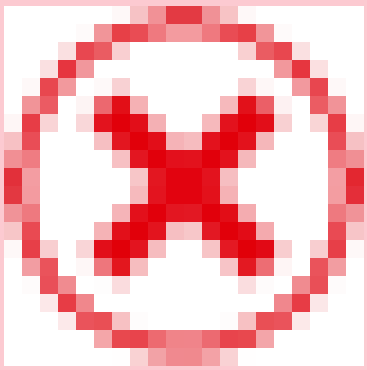
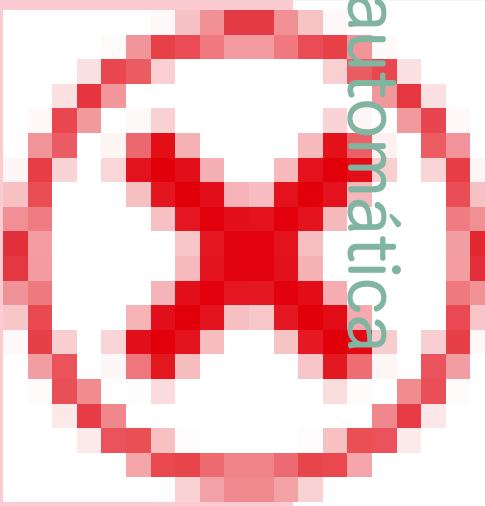
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Avaliação de Exposição			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

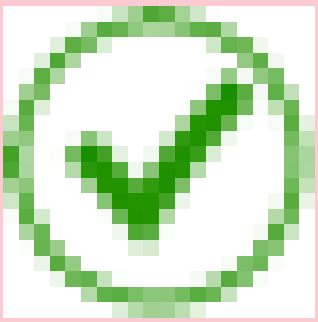
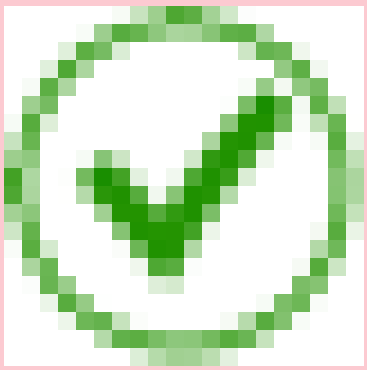
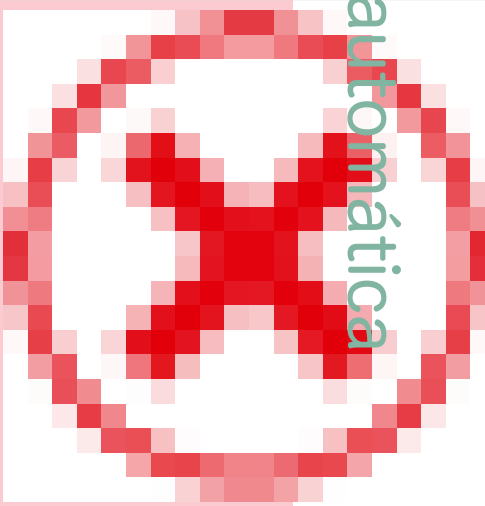
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Verificações			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

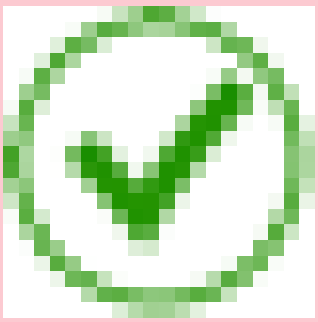
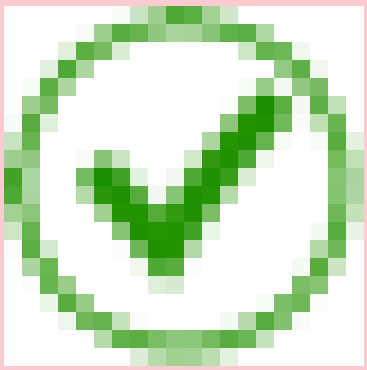
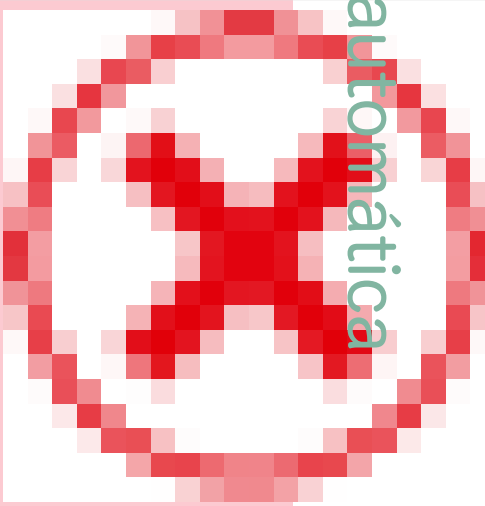
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Scanners			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

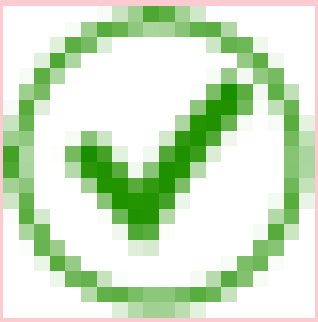
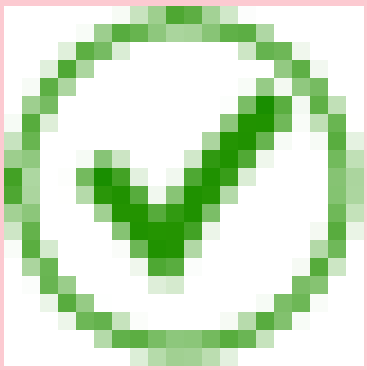
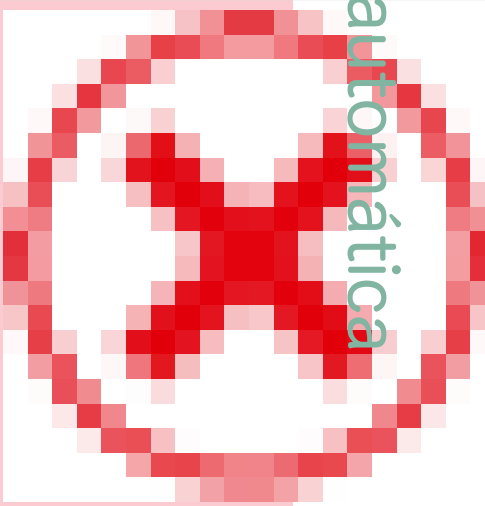
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Fila de Verificação			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

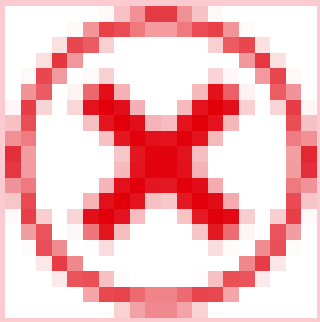
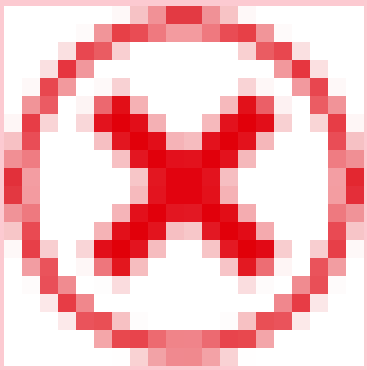
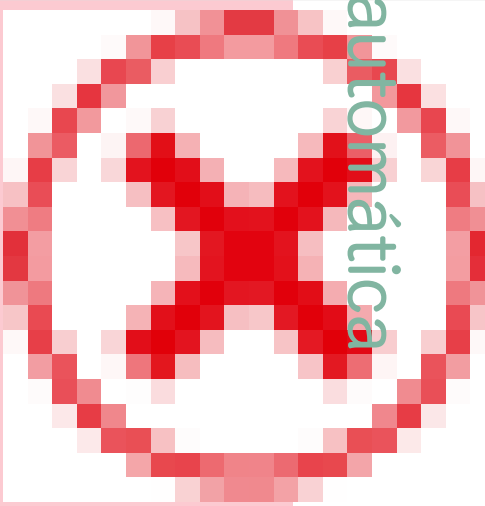
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Limites de Taxa do Scanner			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Definições de Limite de Taxa	✗	✗	✗
Administração			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

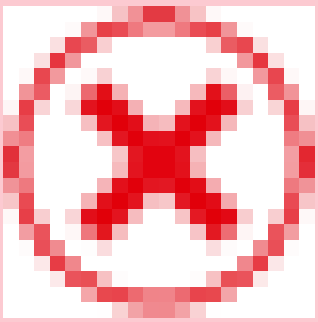
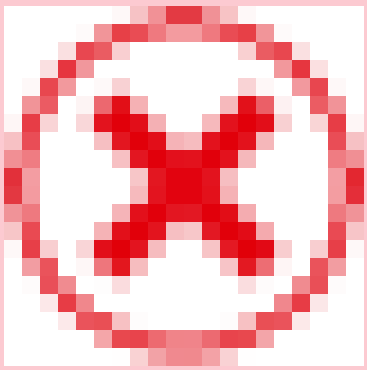
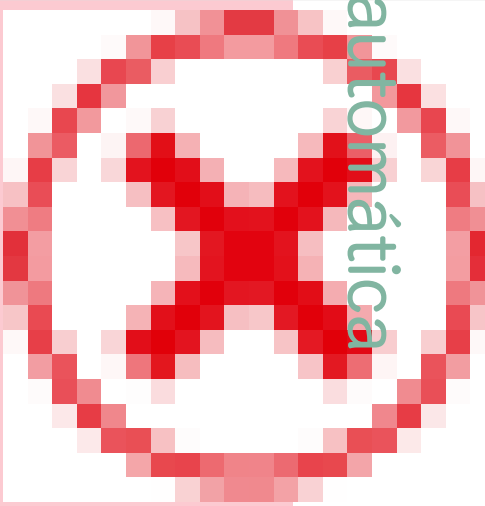
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Assistente de configuração			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

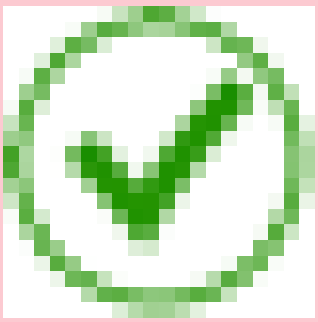
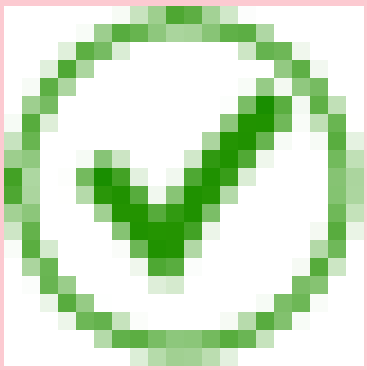
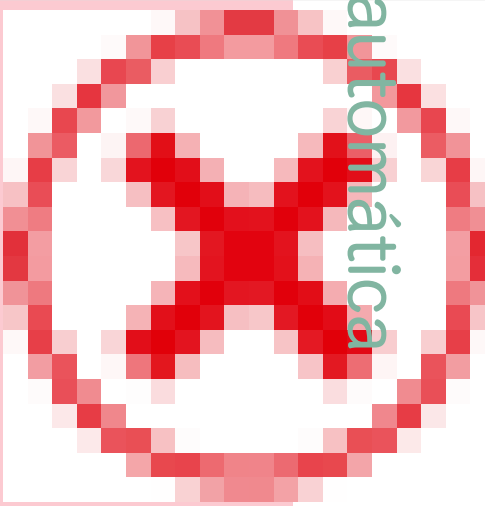
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Tópicos de observação			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

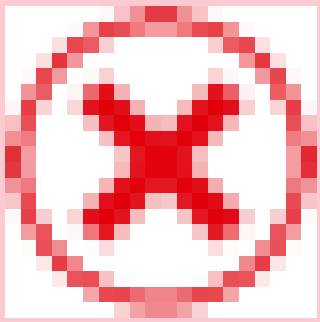
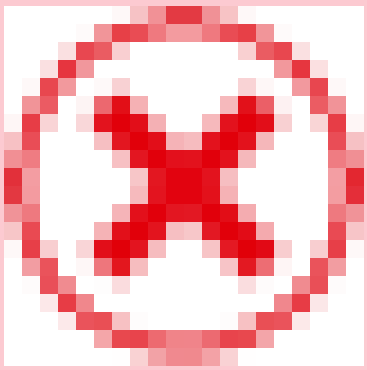
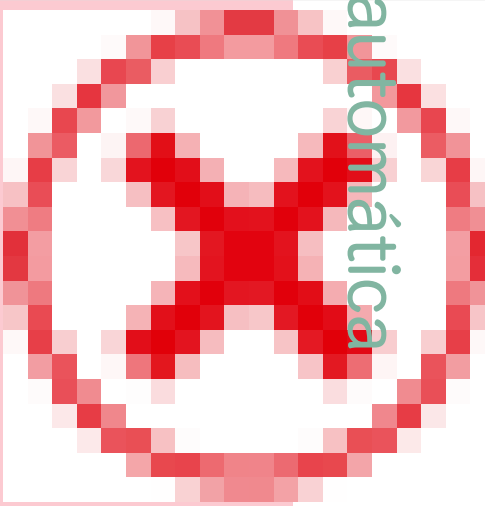
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Regras de atribuição			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

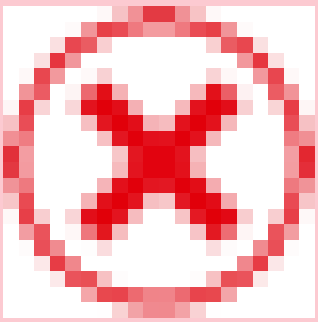
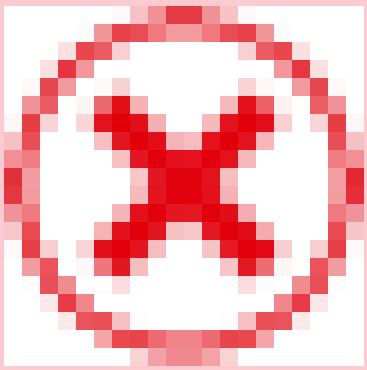
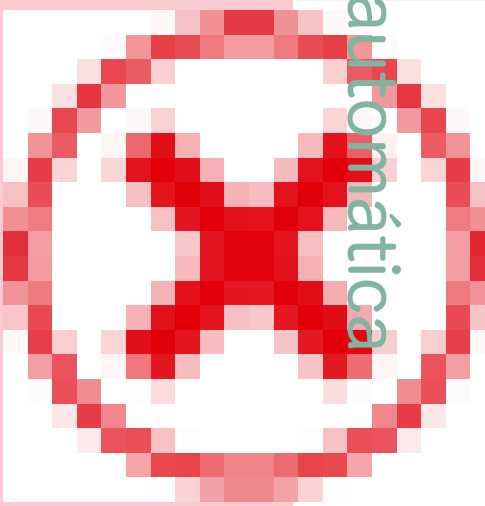
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Regras de tarefa de correção			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

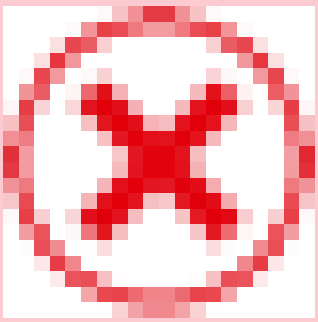
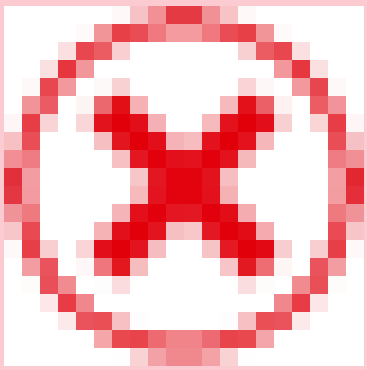
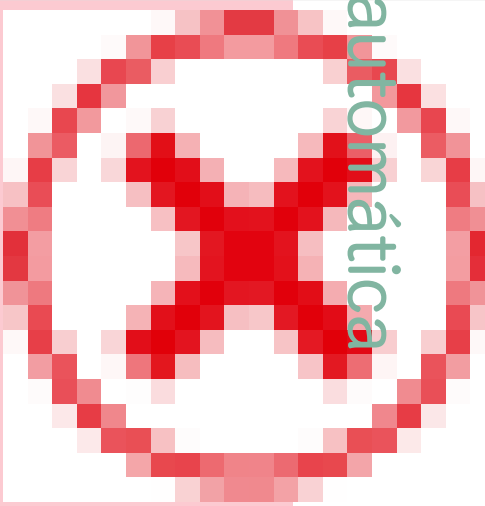
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Recomendações de atribuição			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

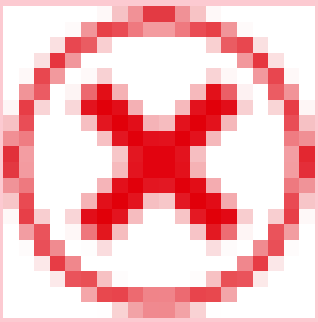
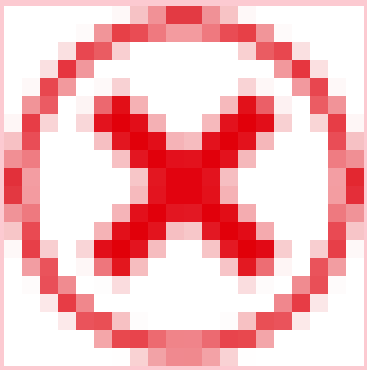
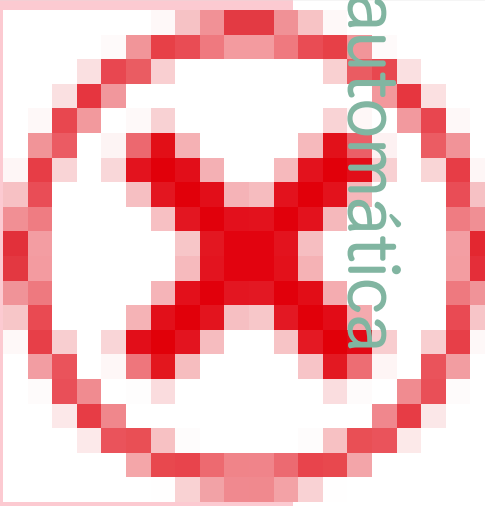
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Calculadoras de vulnerabilidade			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

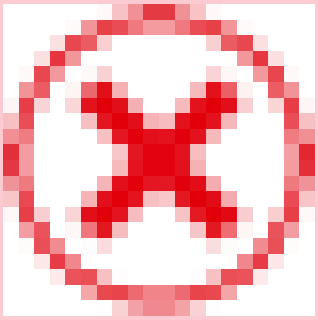
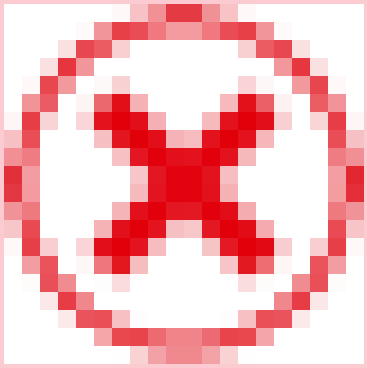
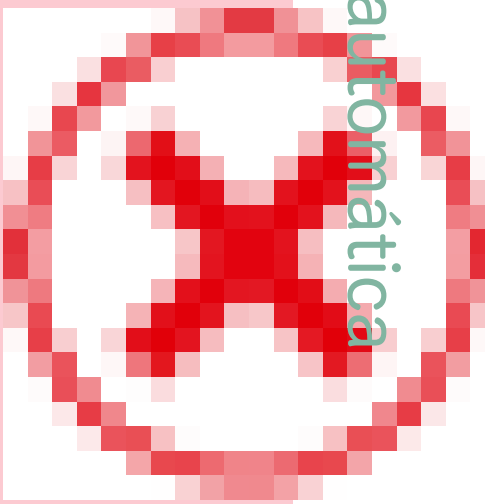
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Calculadora de Rollup de Vulnerabilidade			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

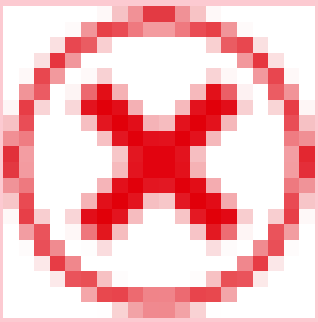
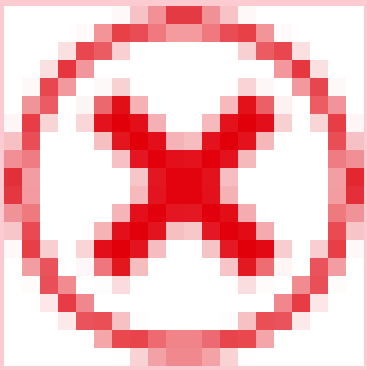
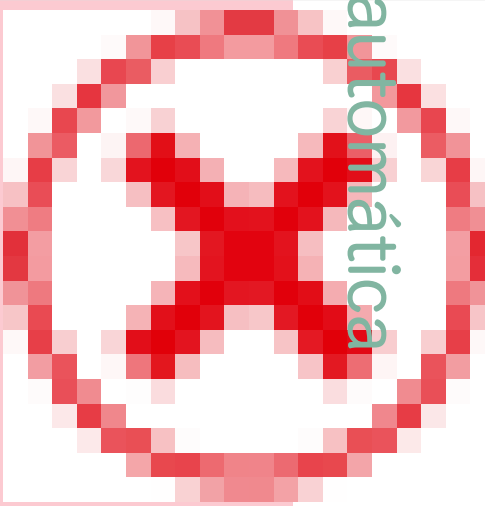
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Regras de destino de correção			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

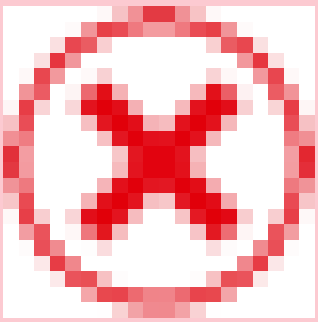
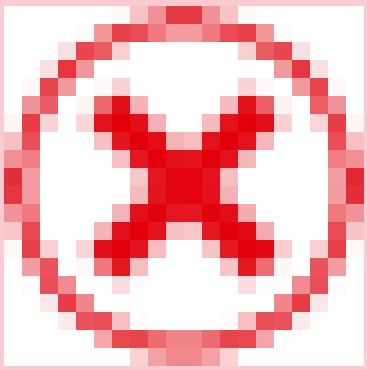
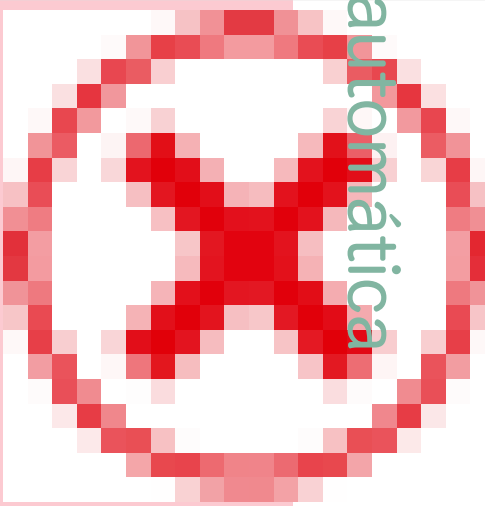
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Configuração de fechamento automático			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

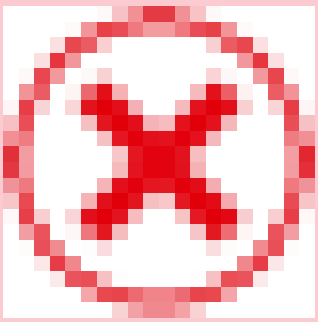
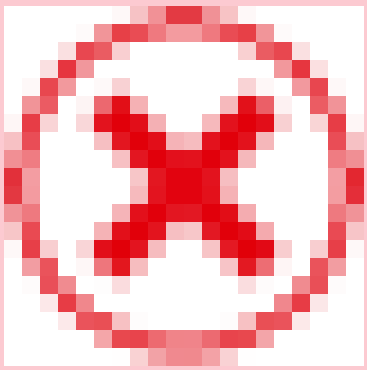
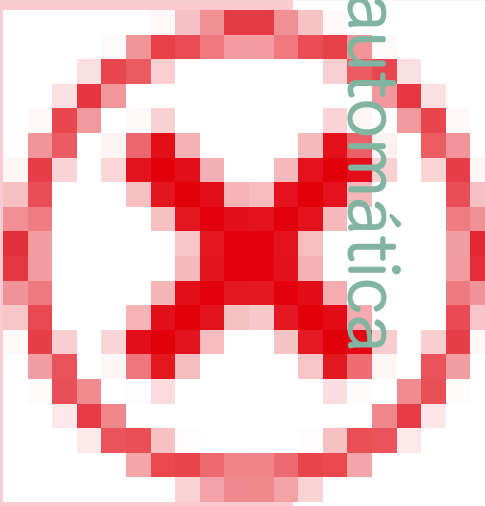
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Regras de exclusão automática			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

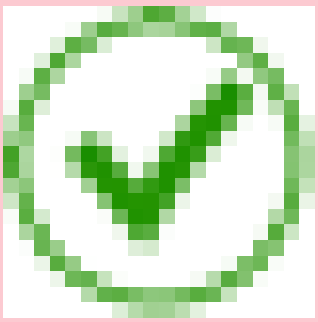
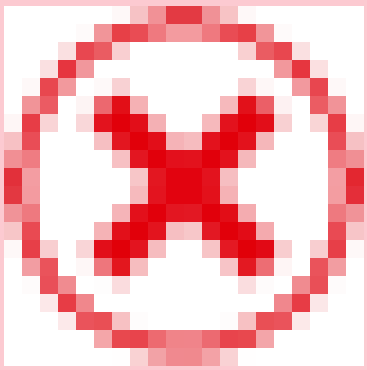
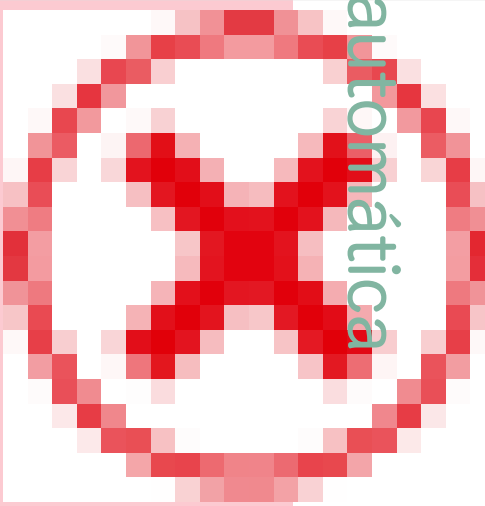
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Regras de exceção			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

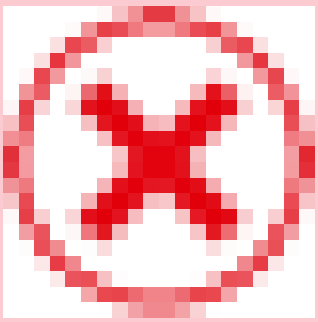
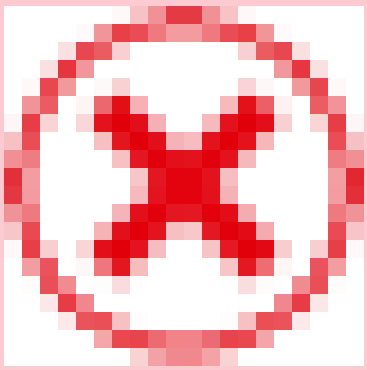
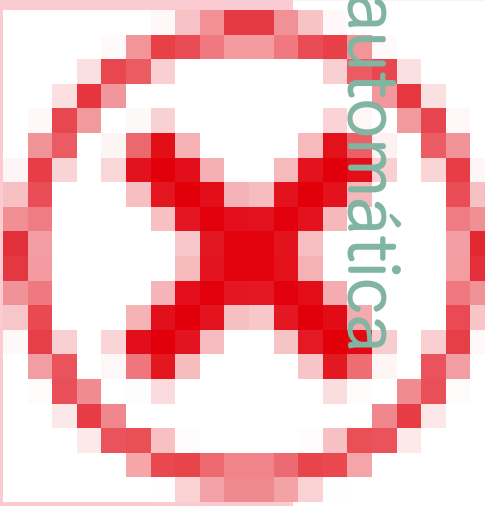
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Regras de aprovação			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

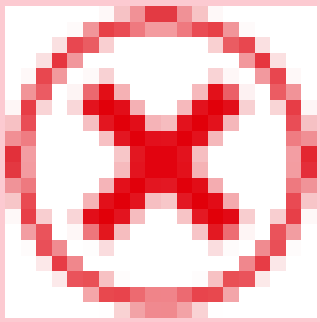
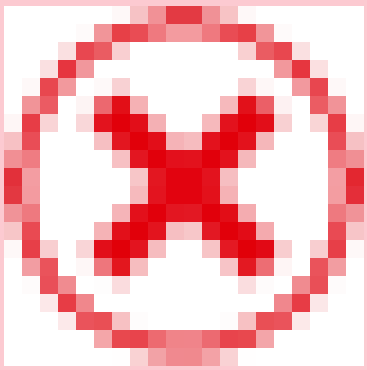
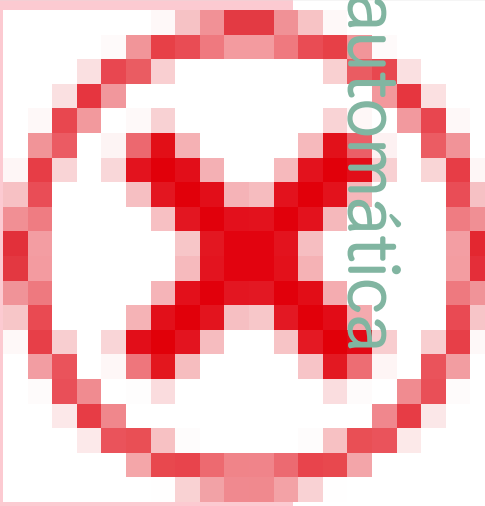
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Regras de classificação			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

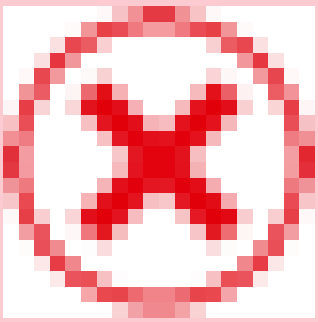
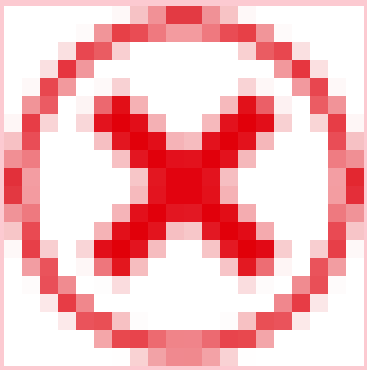
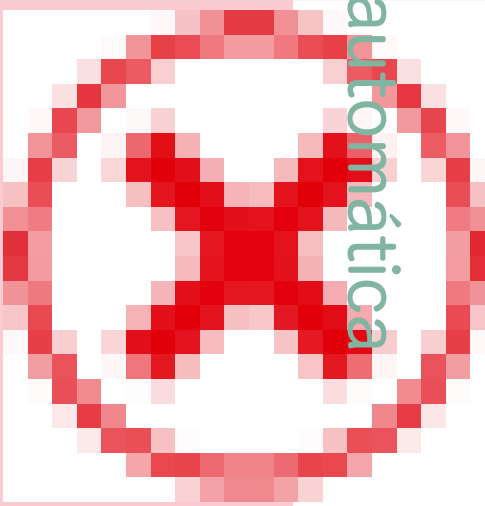
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Configuração de desempenho			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

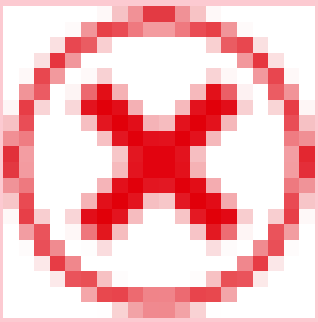
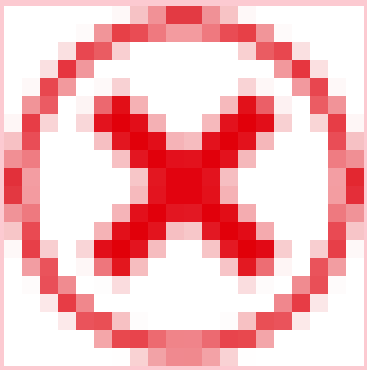
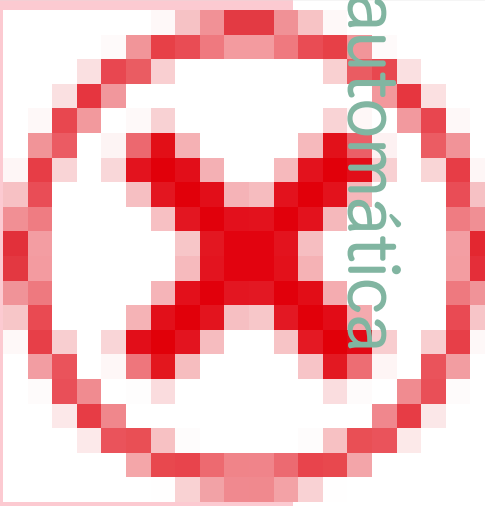
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Configurar granularidade de IV			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Notificações	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

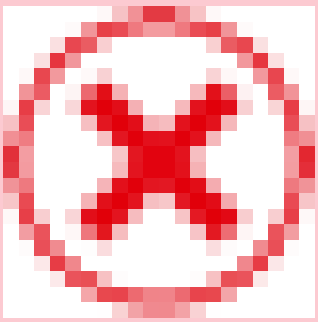
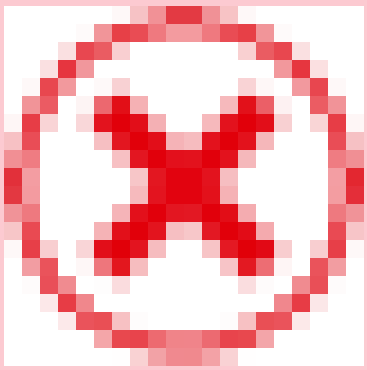
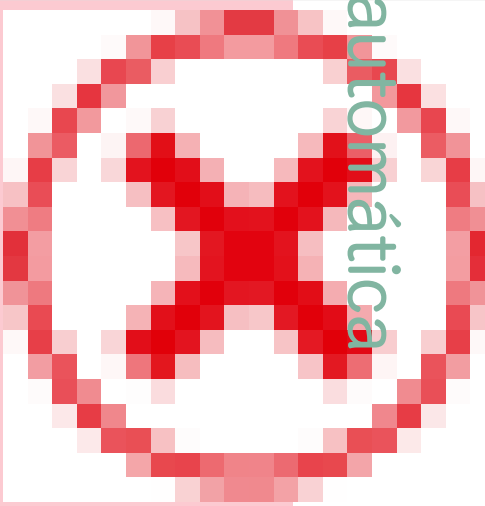
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Modelos de e-mail			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

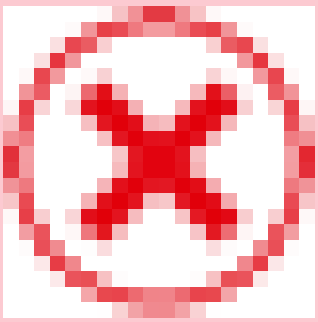
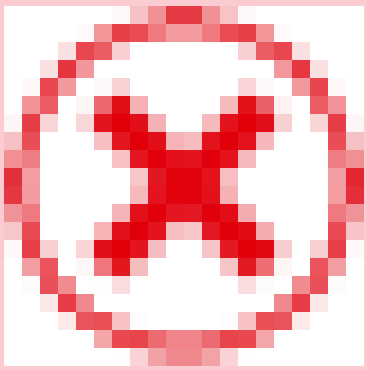
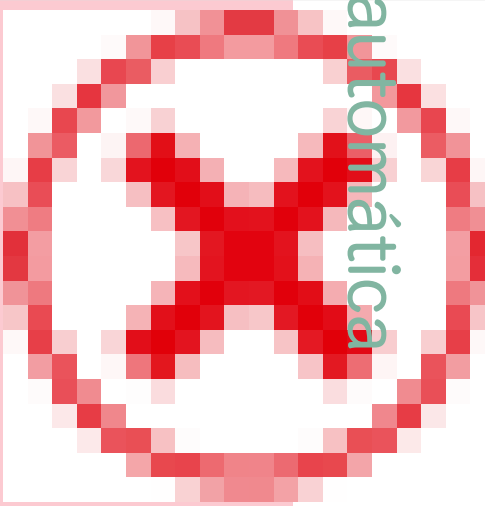
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Importar Fila			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

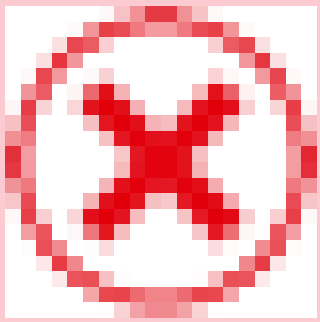
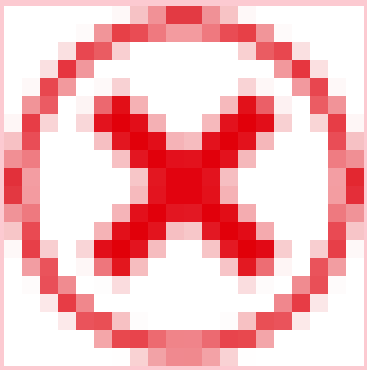
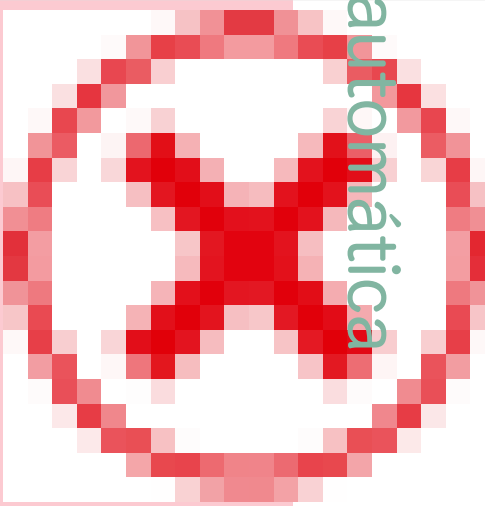
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Integrações			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

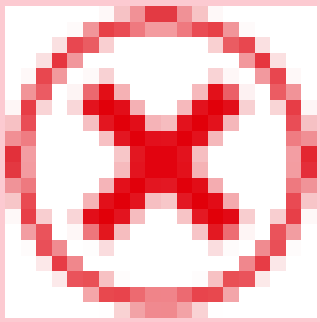
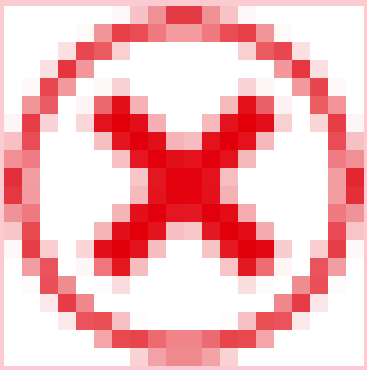
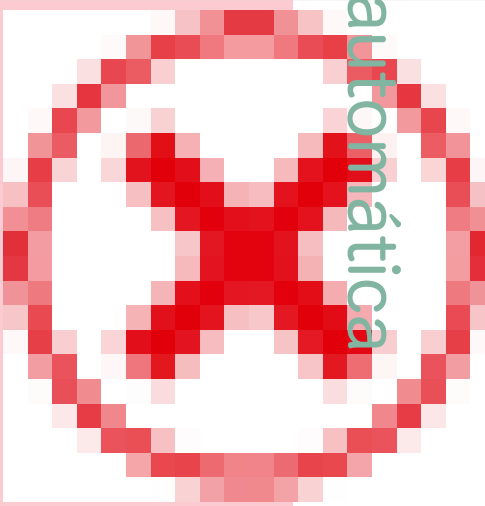
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Definições do ANS			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

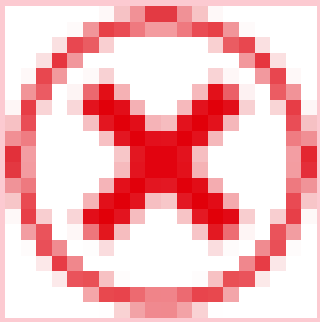
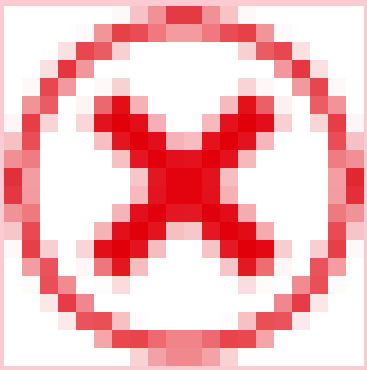
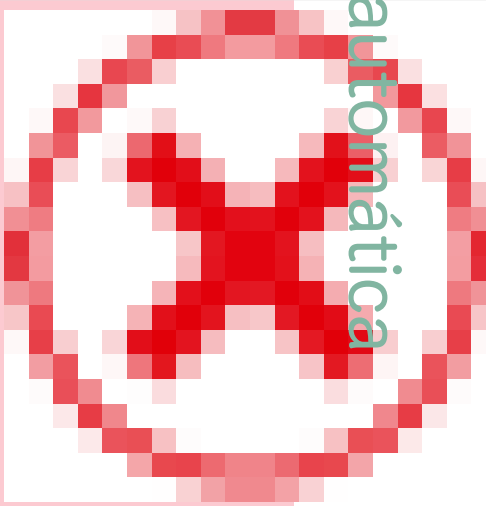
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Configurar SAM NVD			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

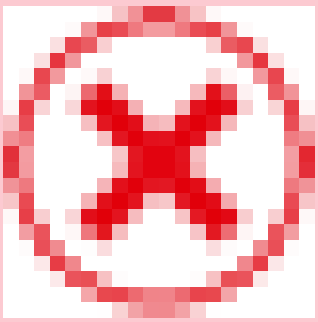
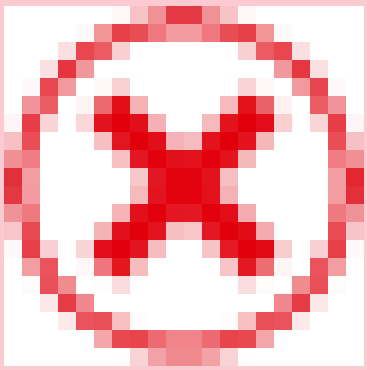
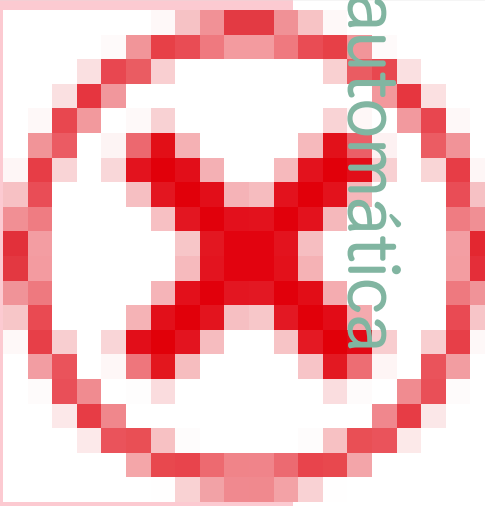
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Mapas de Gravidade Normalizados			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

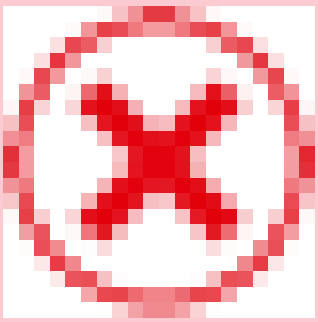
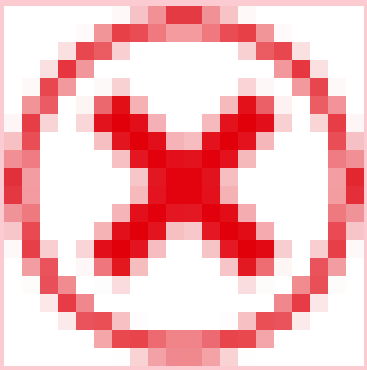
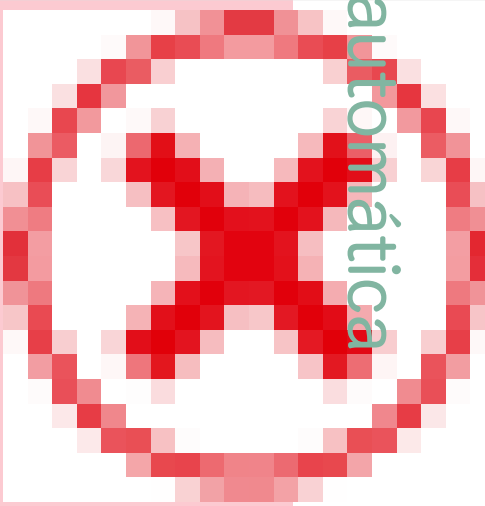
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Configuração de cobertura de verificação			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

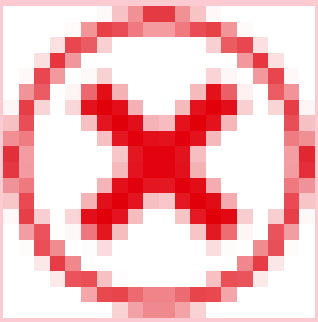
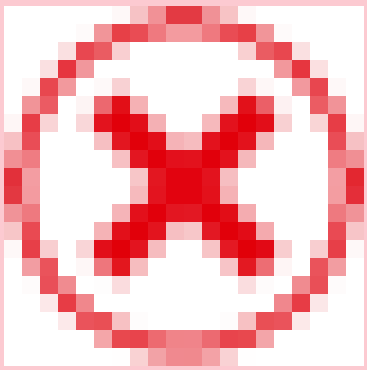
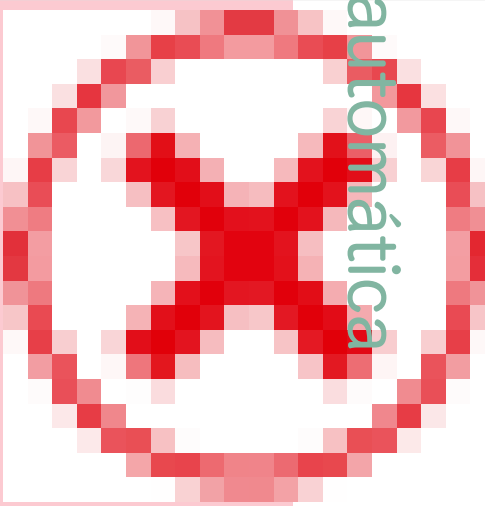
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Gestão de exceção			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

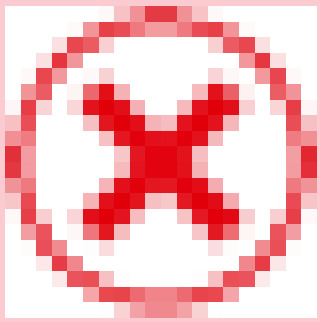
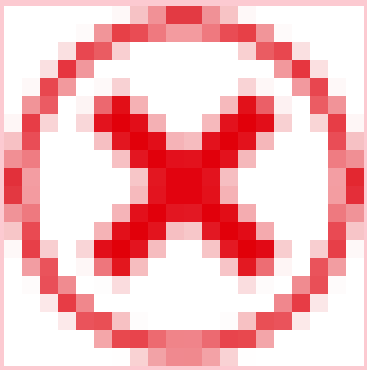
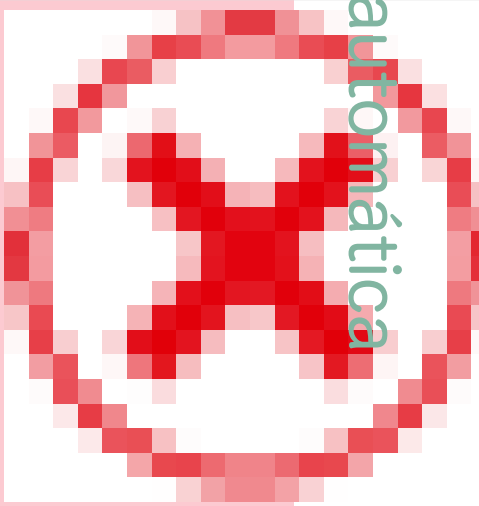
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Relatório de uso			
Diagnósticos			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

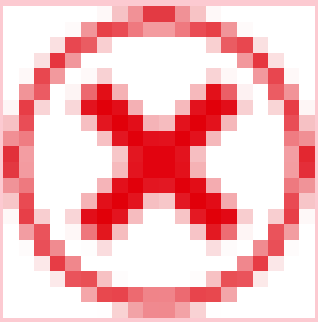
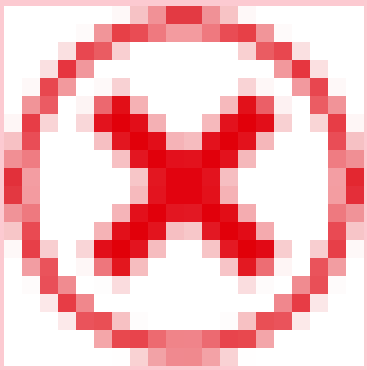
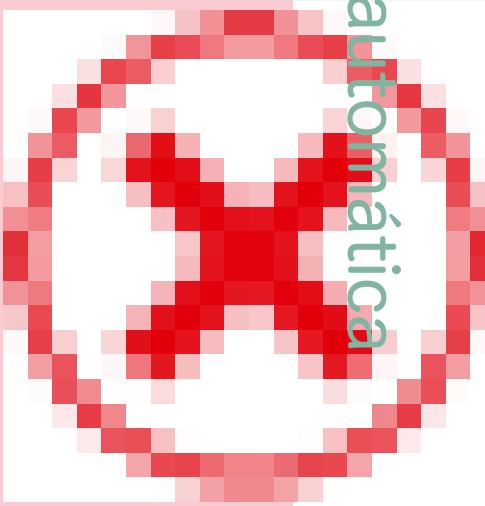
sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.exception_approver	sn_vul.false_positive_approver	sn_vul.manage_assignment_recom_confi
Verificações			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
(Grupo de apps principal)			
Painel do CISO	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Visão Geral da Correção	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Espaço para gerentes de vulnerabilidades	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Visão geral	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Espaço de correção de TI	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Visão geral do aprovador	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Visão geral	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Minhas aprovações	✗	✗	✗
Tarefas de correção			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Ativo	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Atribuídos a Mim	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Atribuído aos Meus grupos	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Todos	✗	✗	✓
Itens vulneráveis			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Risco crítico	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Alto risco	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Explorável	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Perto da meta	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Meta não atingida	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

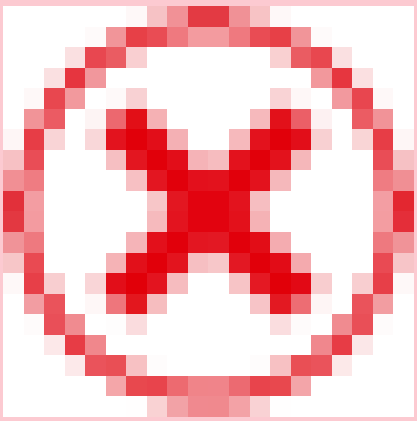
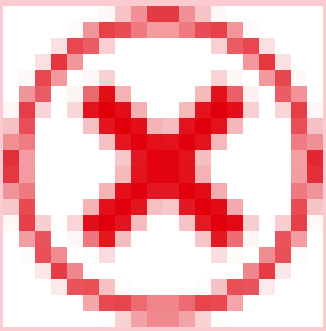
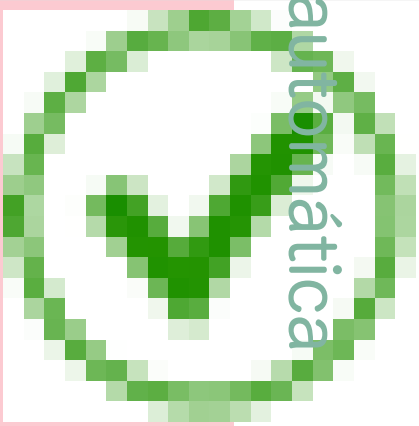
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Nos últimos 90 dias			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Há mais de 90 dias	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Não designado	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Desagrupado	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Desativado	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Vários adiamentos	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Todos	✗	✗	✓
Soluções			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Todos	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

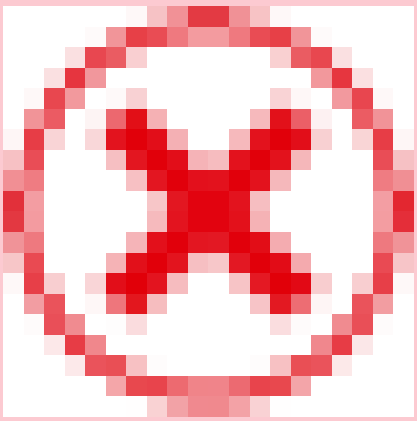
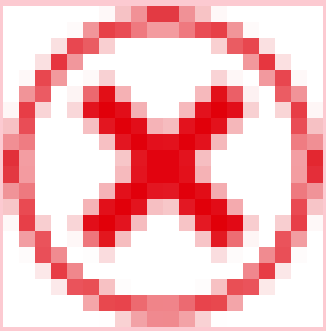
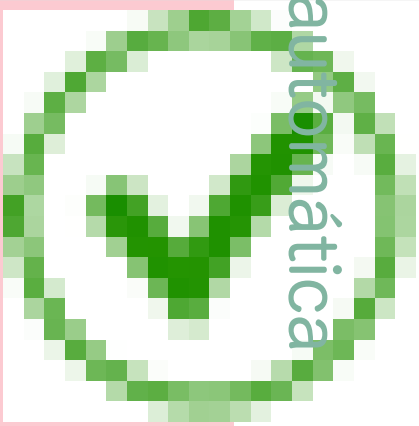
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Substituição mais alta			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Com itens vulneráveis	✗	✗	✓
Bibliotecas			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
NVD	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
CWE	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Terceiros	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Software Vulnerável	✗	✗	✓
Verificação de Vulnerabilidades			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Avaliação de Exposição	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Verificações	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Scanners	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Fila de Verificação	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Limites de Taxa do Scanner	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Definições de Limite de Taxa	✗	✗	✗
Administração			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Assistente de configuração	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Tópicos de observação	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Regras de atribuição	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Regras de tarefa de correção	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Recomendações de atribuição	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Calculadoras de vulnerabilidade	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Calculadora de Rollup de Vulnerabilidade	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Regras de destino de correção	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Configuração de fechamento automático	✓	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Regras de exclusão automática	✗	✓	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Regras de exceção	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Regras de aprovação	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Regras de classificação	✗	✗	✓

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Configuração de desempenho	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Configurar granularidade de IV	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Notificações	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Modelos de e-mail	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Importar Fila	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Integrações	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Definições do ANS	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Configurar SAM NVD	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Mapas de Gravidade Normalizados	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Configuração de cobertura de verificação	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Gestão de exceção	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Relatório de uso	✗	✗	✗
Diagnósticos			

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_auto_close_stale_vi	sn_vul.manage_auto_delete	sn_vul.manage_classification_rules
Verificações	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

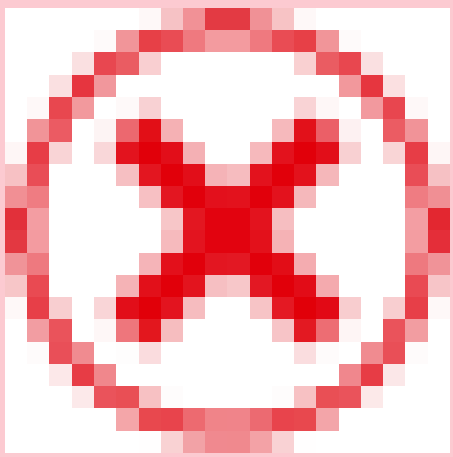
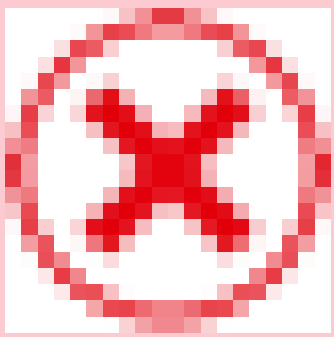
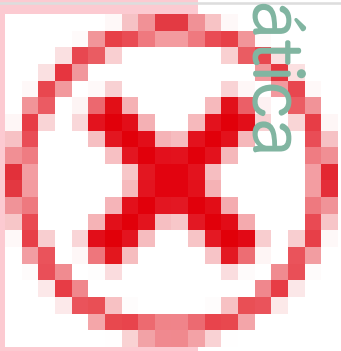
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
(Grupo de apps principal)				
Painel do CISO				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

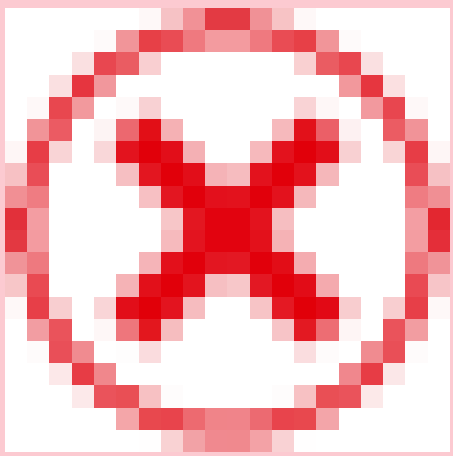
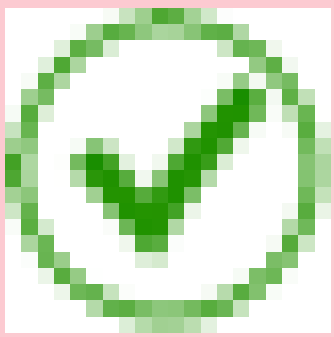
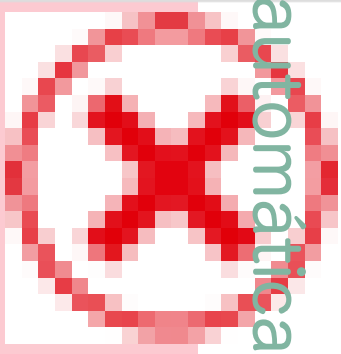
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Visão Geral da Correção				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

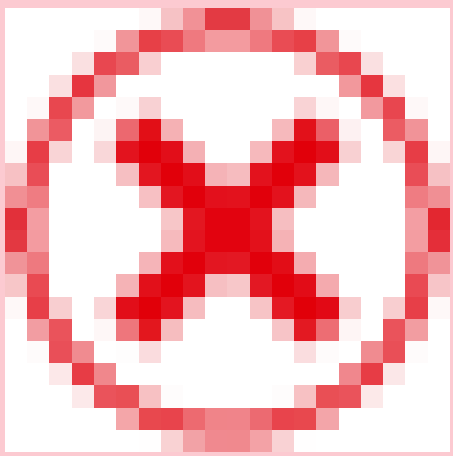
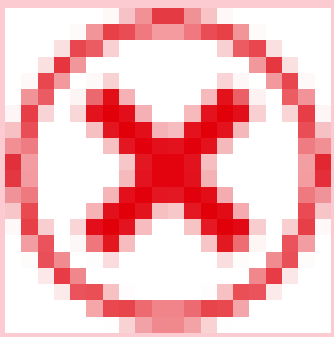
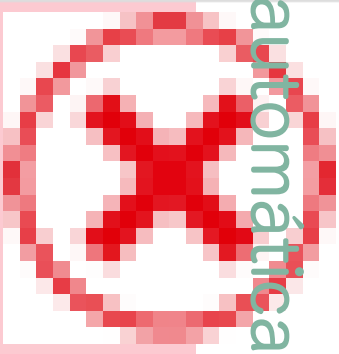
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Espaço para gerentes de vulnerabilidades				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

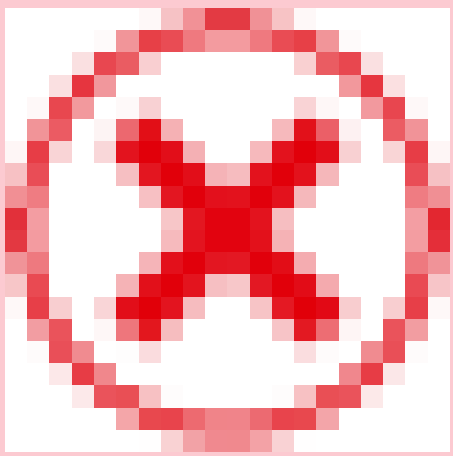
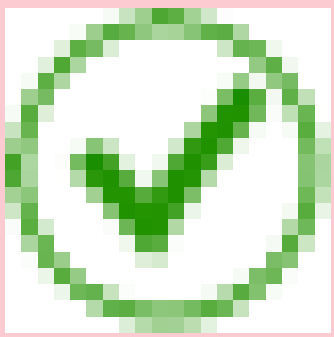
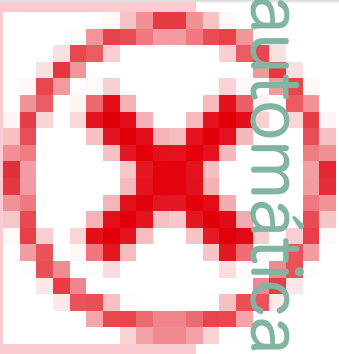
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Visão geral				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

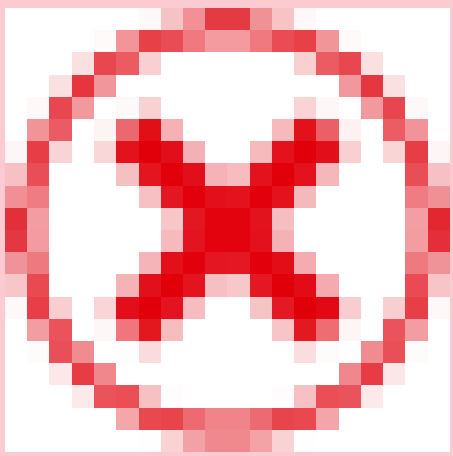
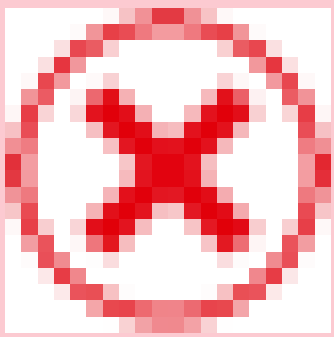
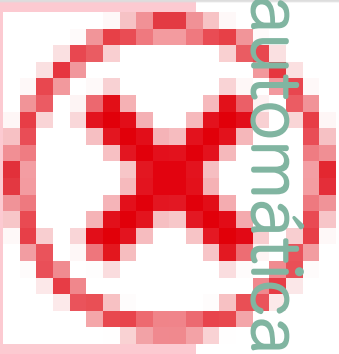
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Espaço de correção de TI				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

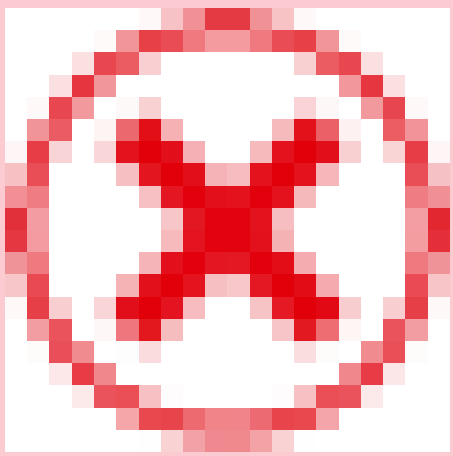
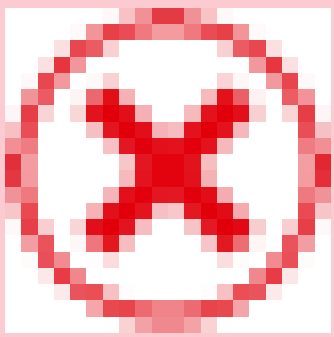
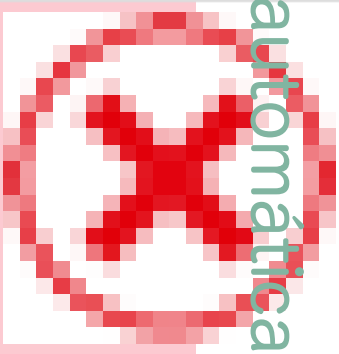
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Visão geral do aprovador				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

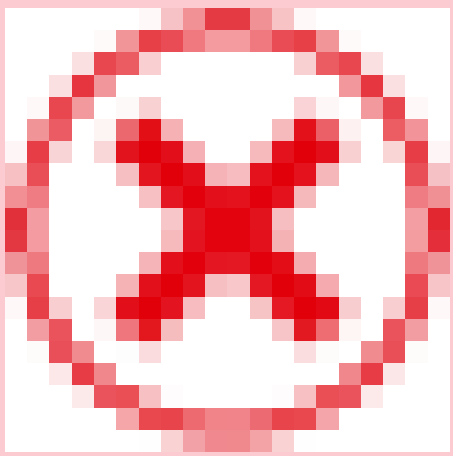
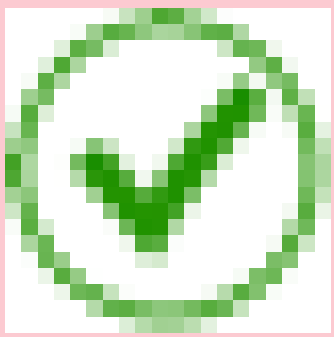
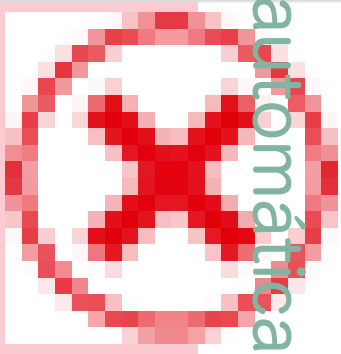
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Visão geral				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

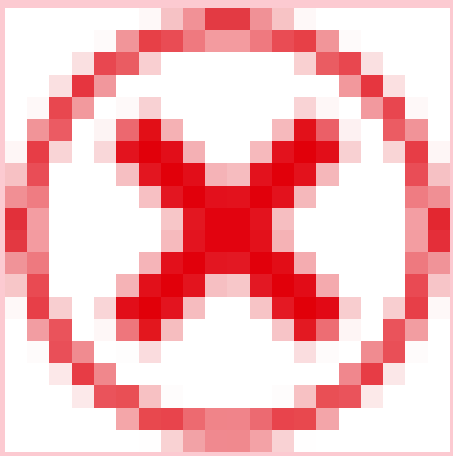
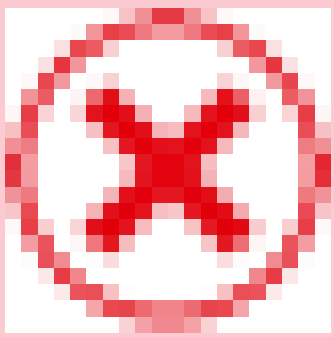
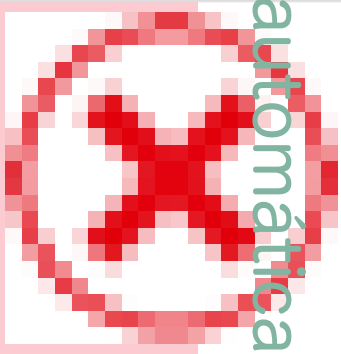
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Minhas aprovações				
Tarefas de correção				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

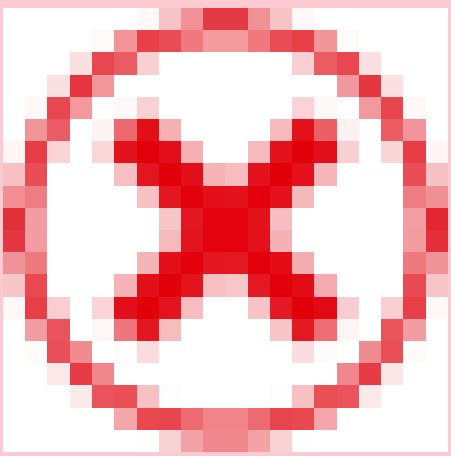
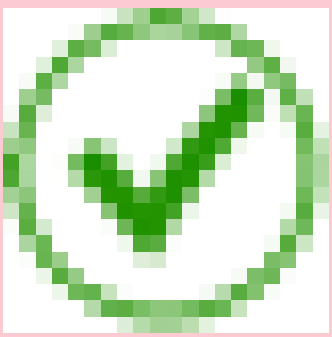
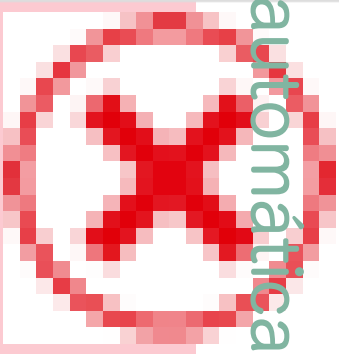
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Ativo				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

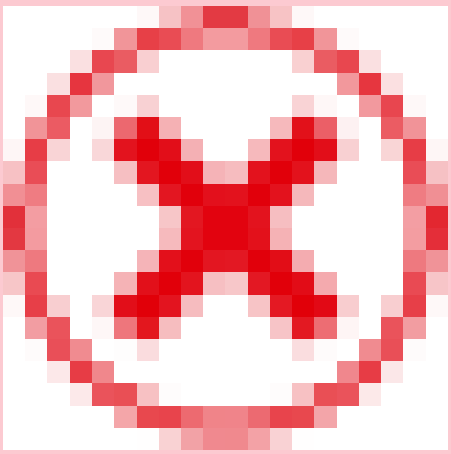
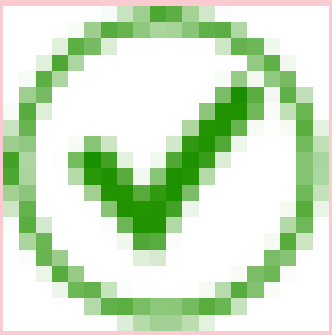
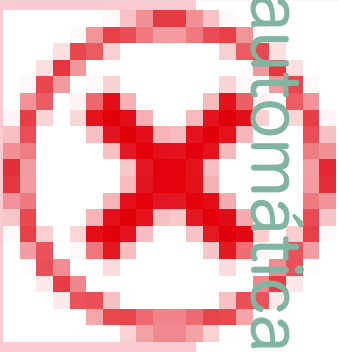
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Atribuídos a Mim				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

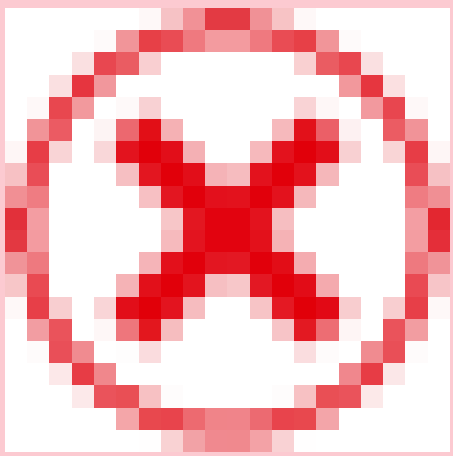
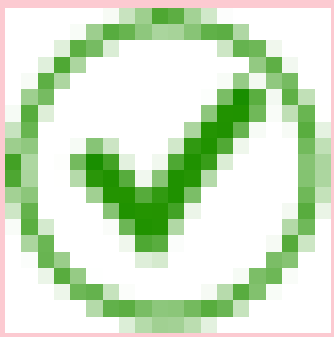
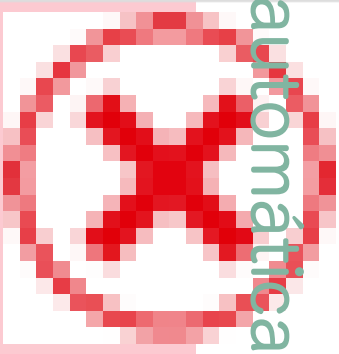
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Atribuído aos Meus grupos				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

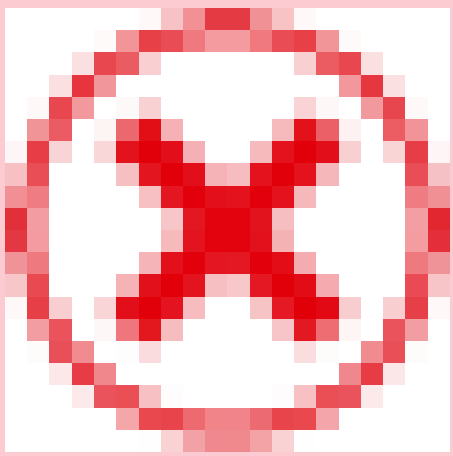
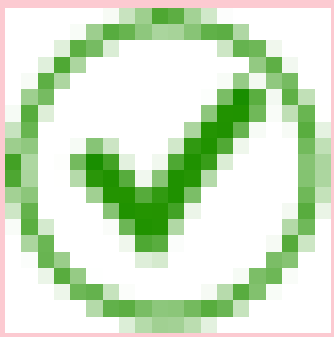
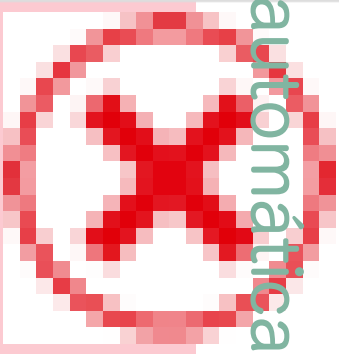
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Todos				
Itens vulneráveis				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

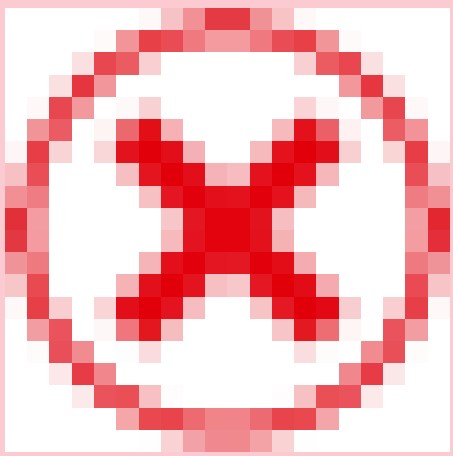
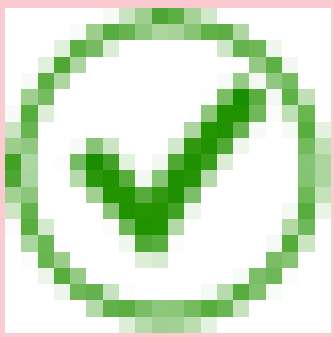
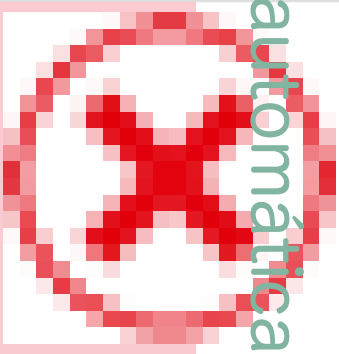
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Risco crítico				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

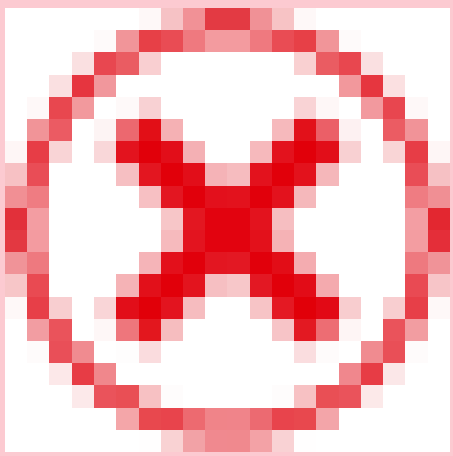
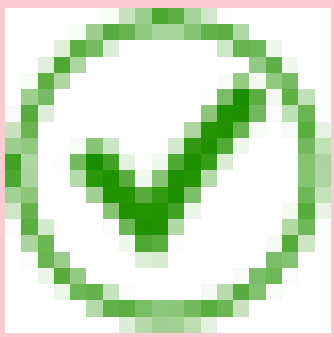
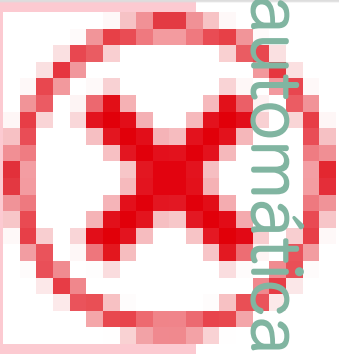
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Alto risco				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

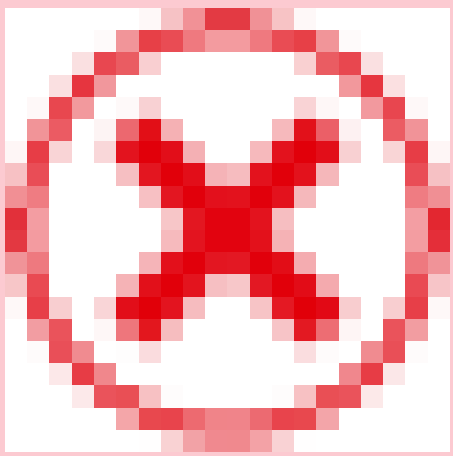
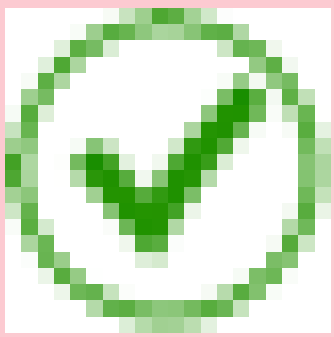
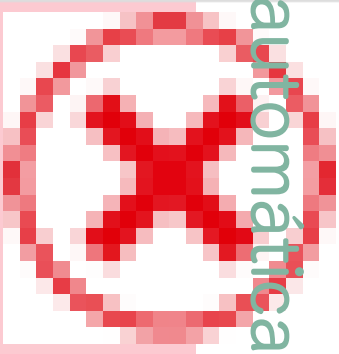
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Explorável				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

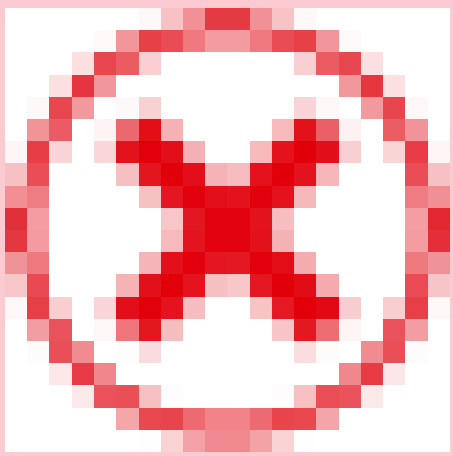
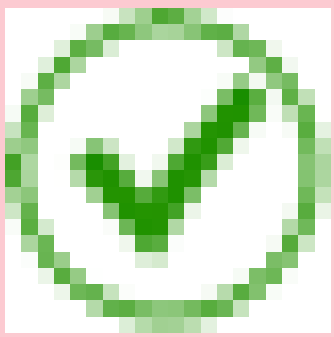
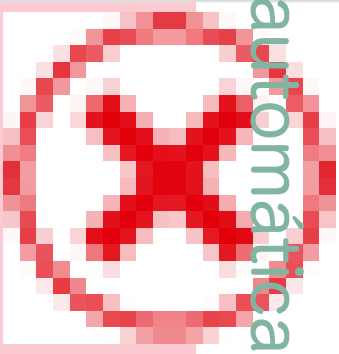
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Perto da meta				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

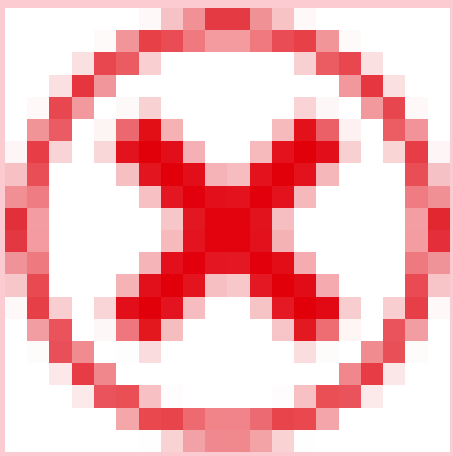
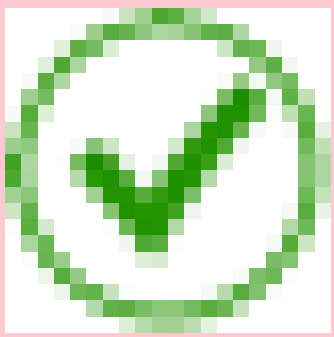
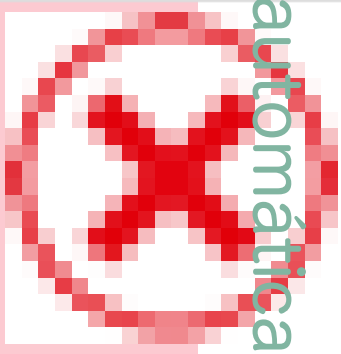
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Meta não atingida				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

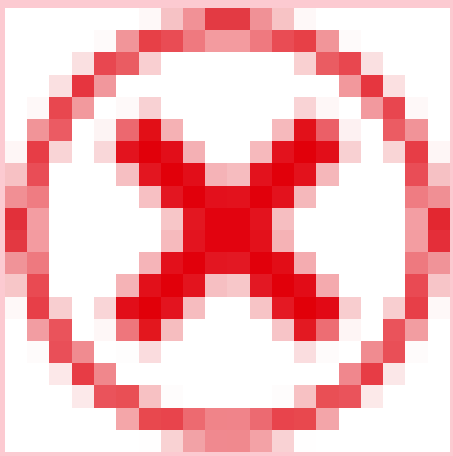
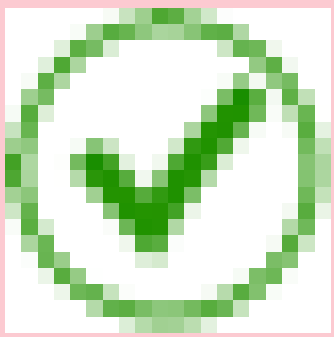
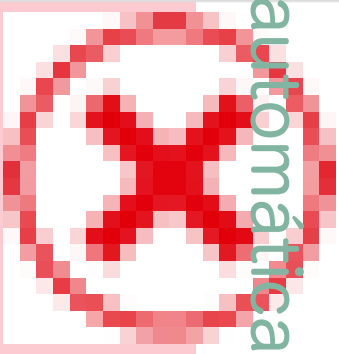
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Nos últimos 90 dias				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

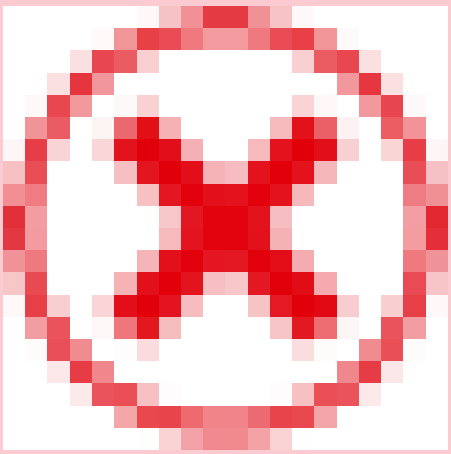
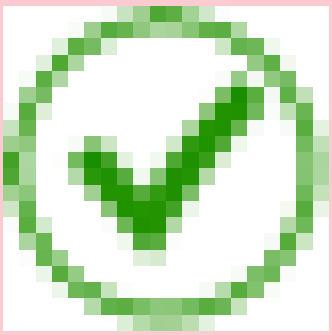
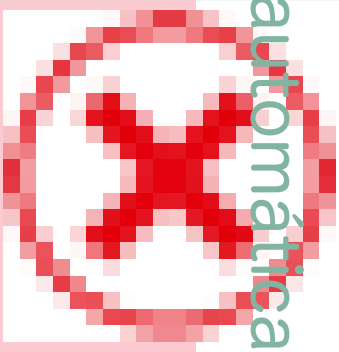
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Há mais de 90 dias				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Não designado	✗	✓	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

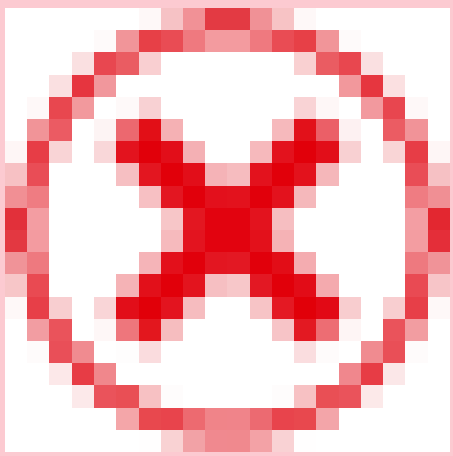
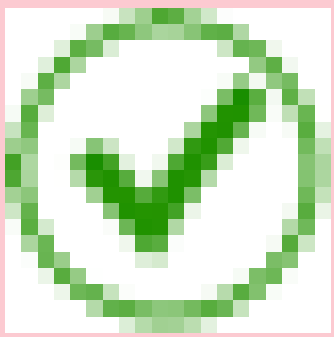
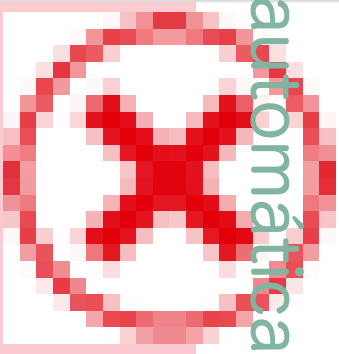
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Desagrupado				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

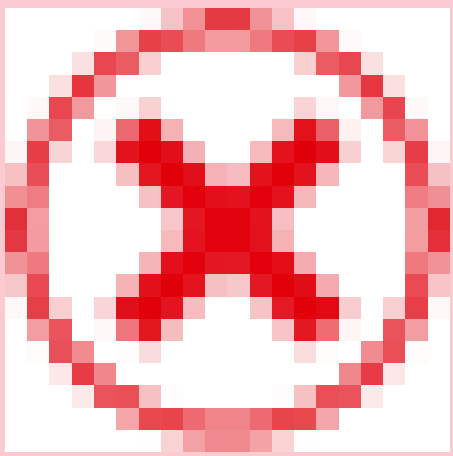
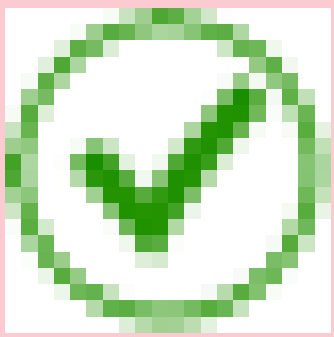
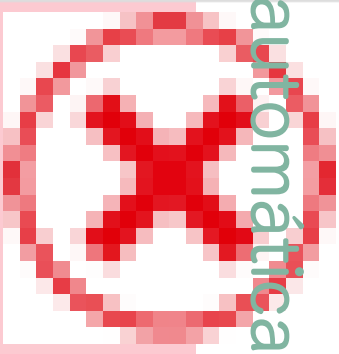
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Desativado				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

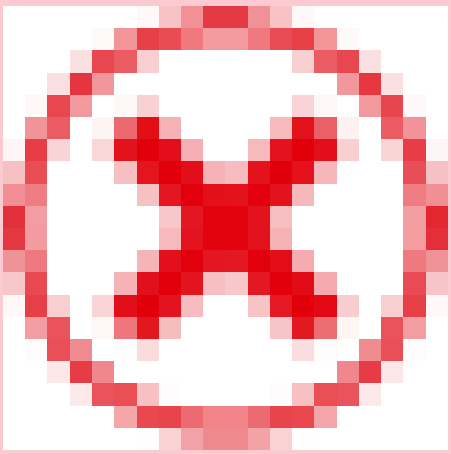
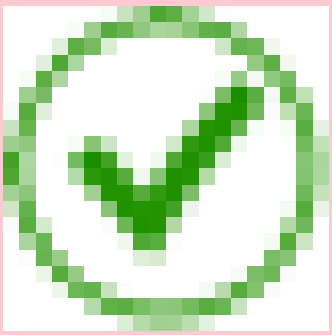
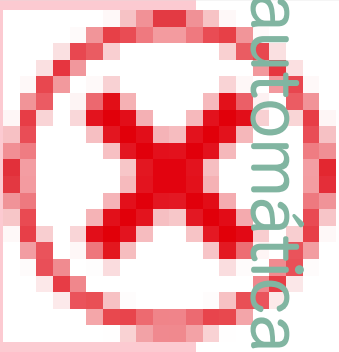
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Vários adiamentos				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

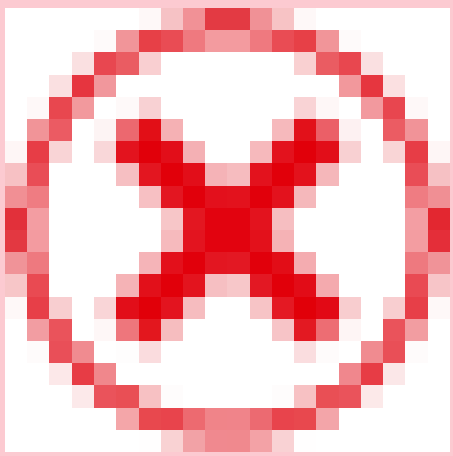
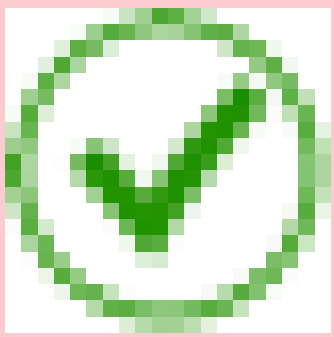
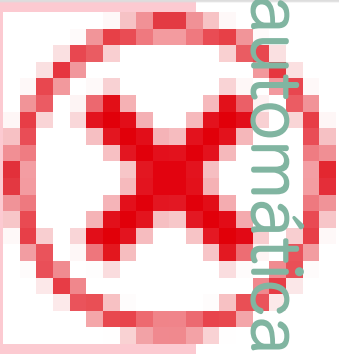
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Todos				
Soluções				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

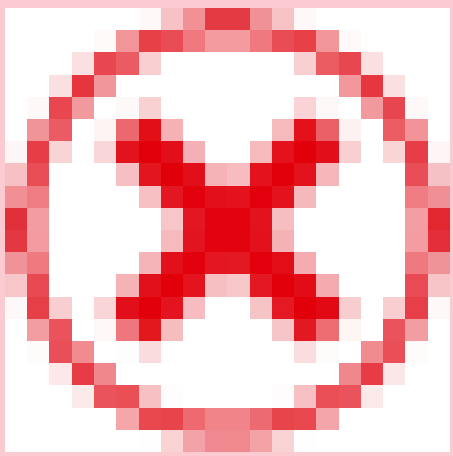
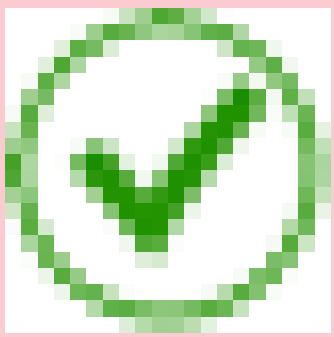
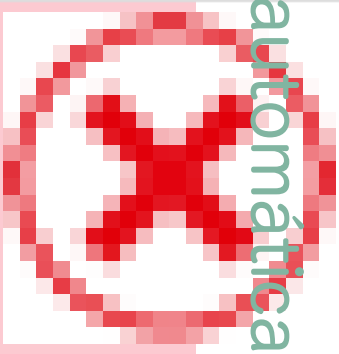
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Todos				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

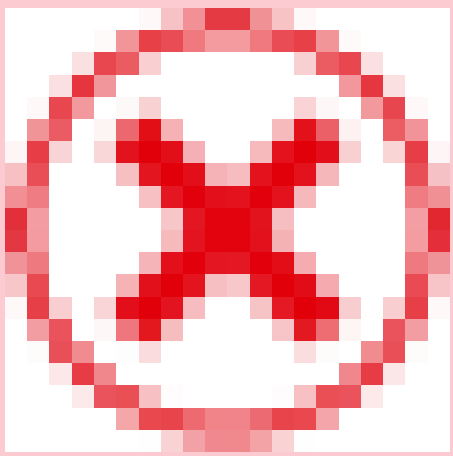
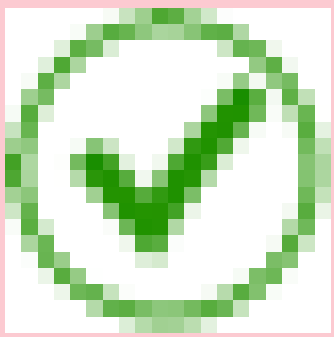
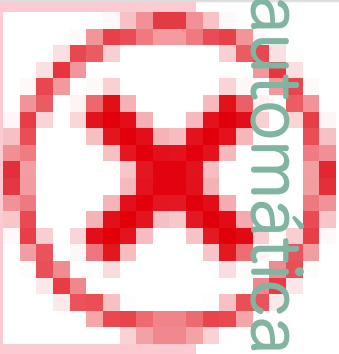
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Substituição mais alta				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

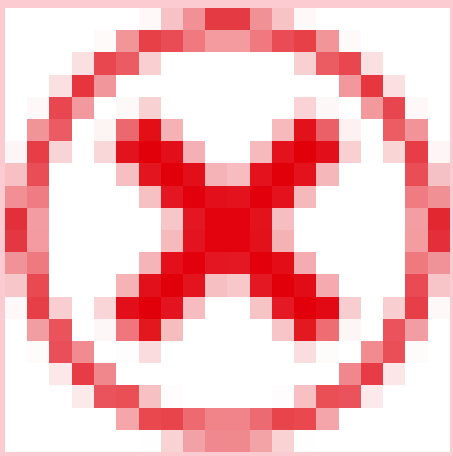
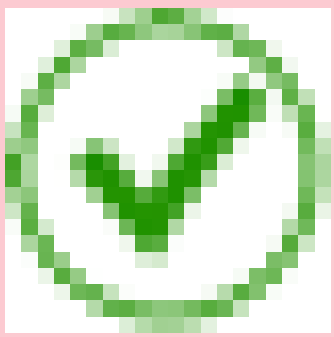
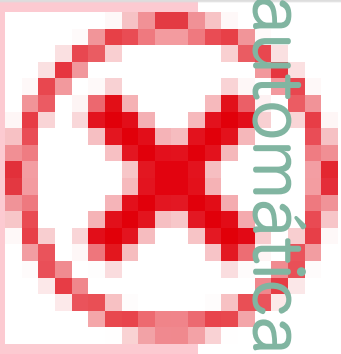
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Com itens vulneráveis				
Bibliotecas				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

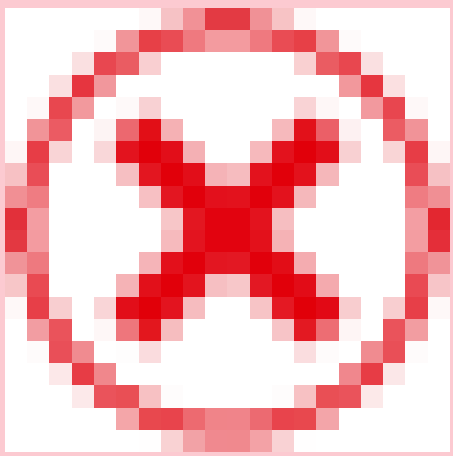
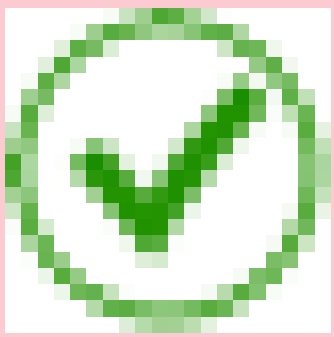
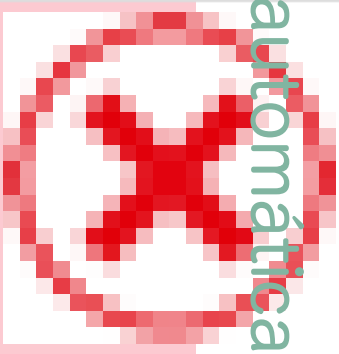
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
NVD				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

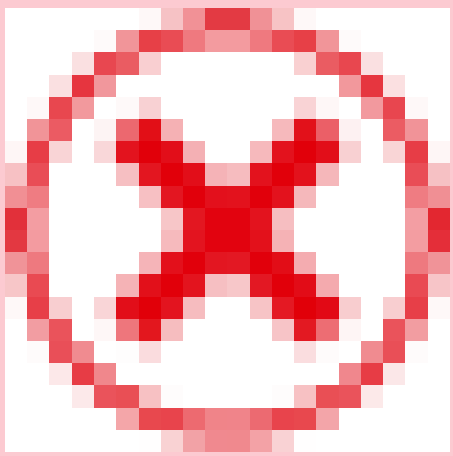
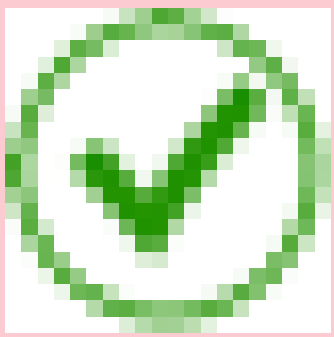
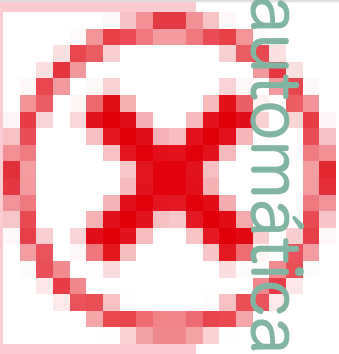
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
CWE				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

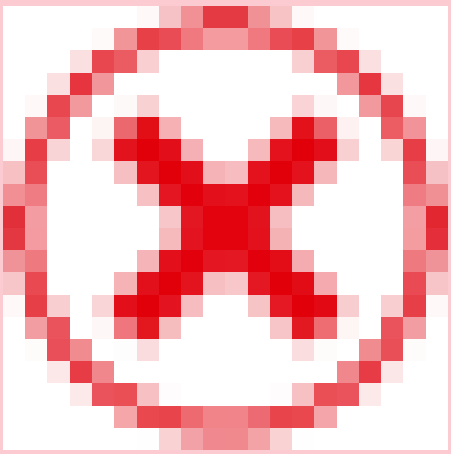
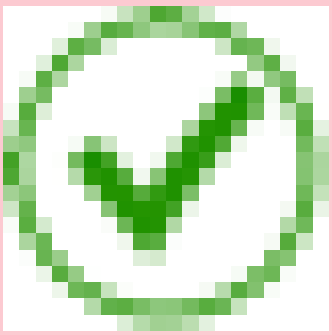
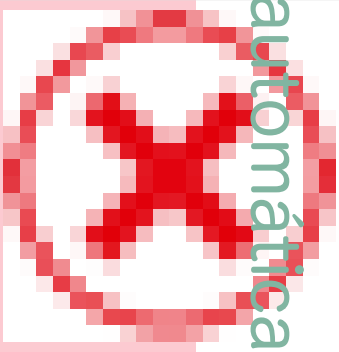
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Terceiros				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

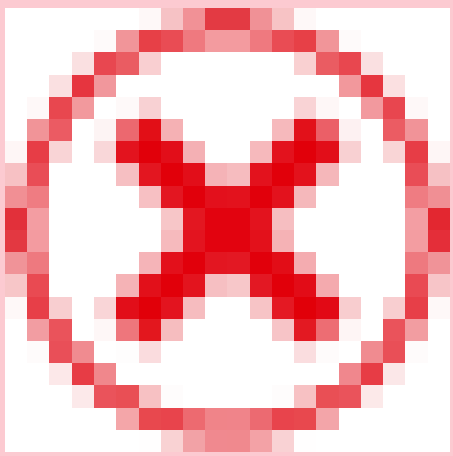
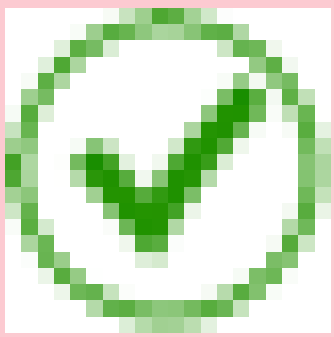
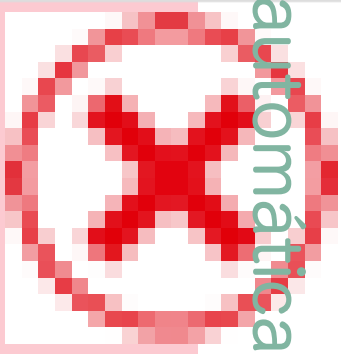
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Software Vulnerável				

Verificação de Vulnerabilidades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

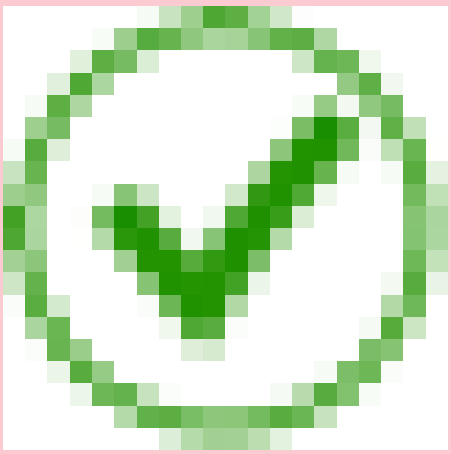
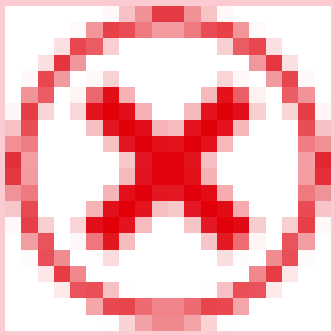
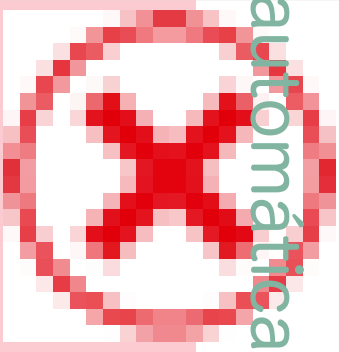
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Avaliação de Exposição				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

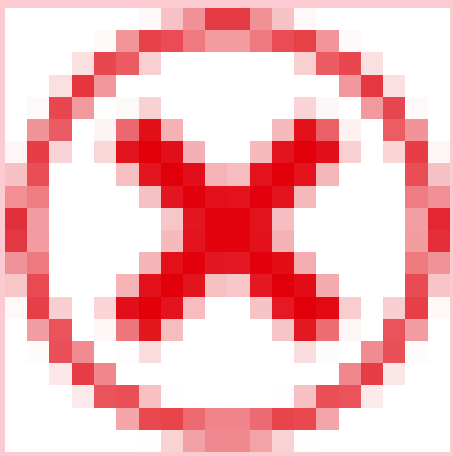
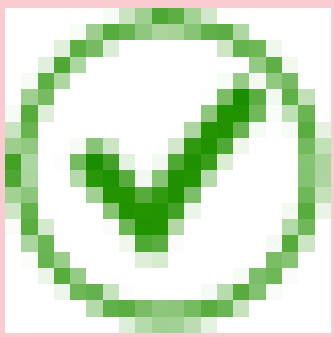
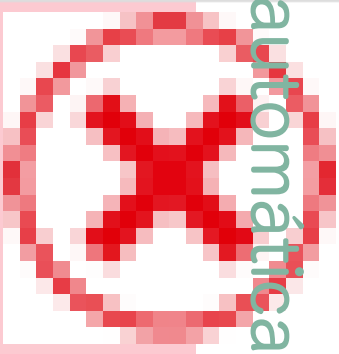
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Verificações				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

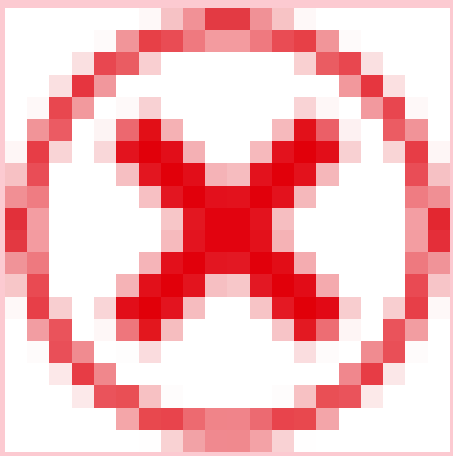
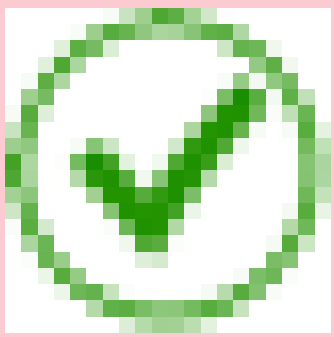
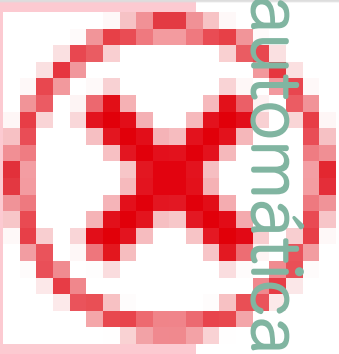
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Scanners				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

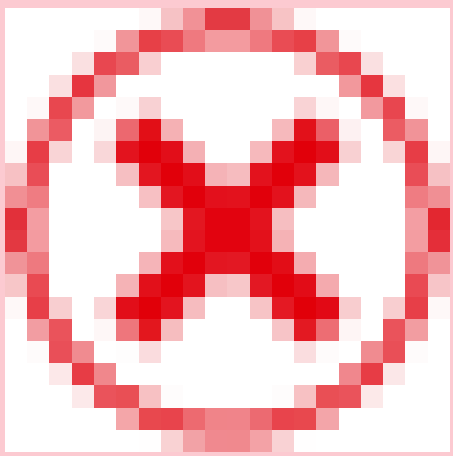
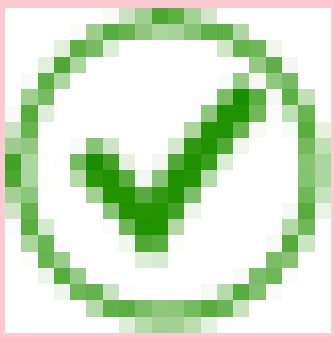
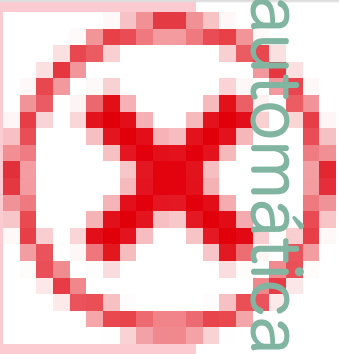
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Fila de Verificação				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

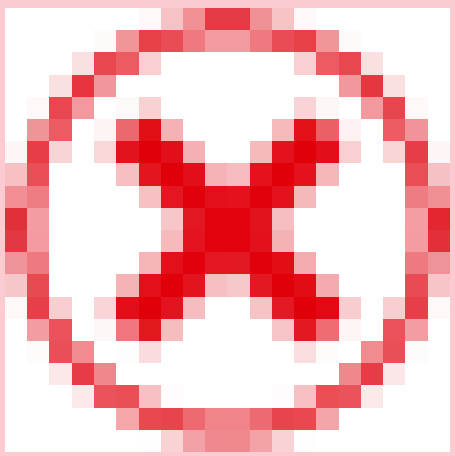
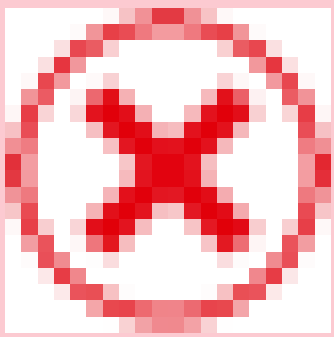
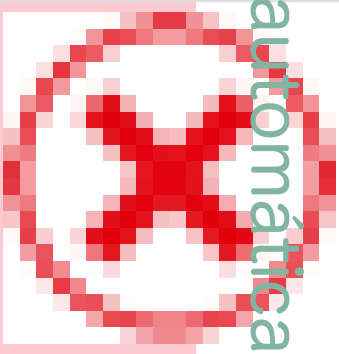
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Limites de Taxa do Scanner				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

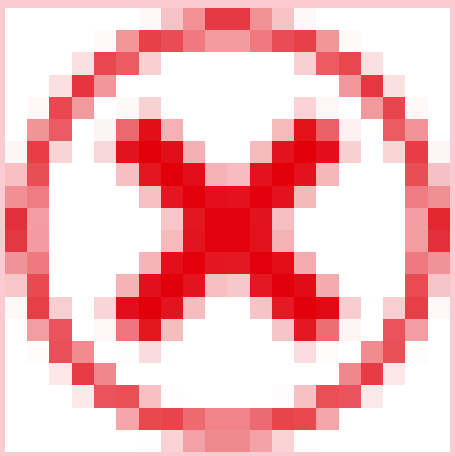
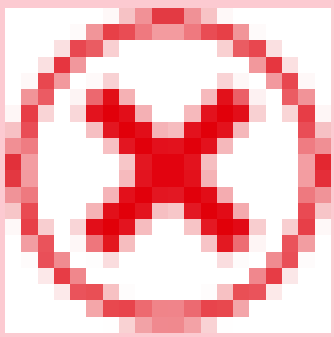
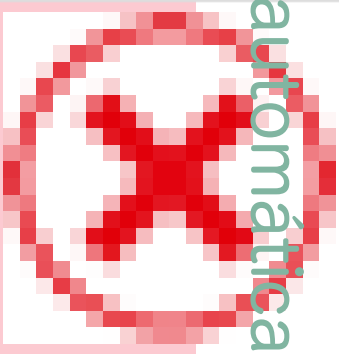
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Definições de Limite de Taxa				
Administração				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

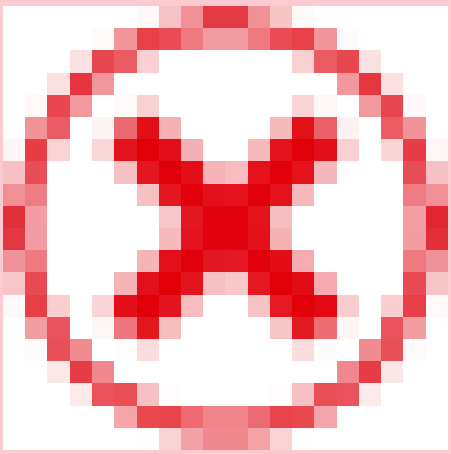
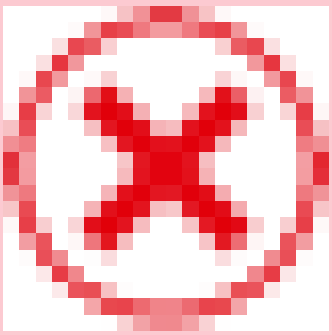
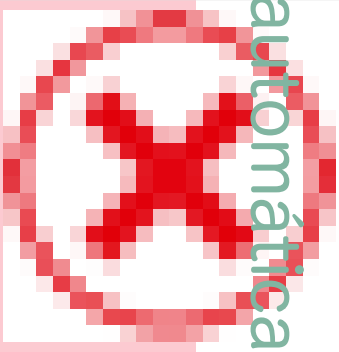
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Assistente de configuração				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

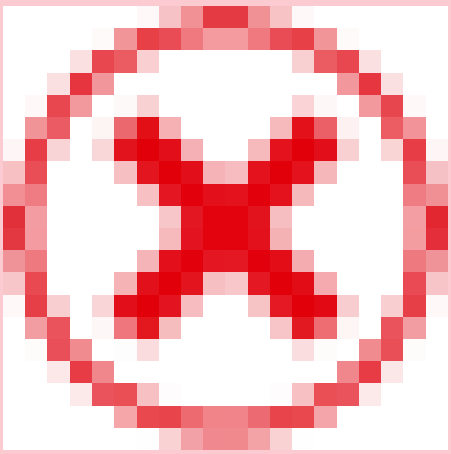
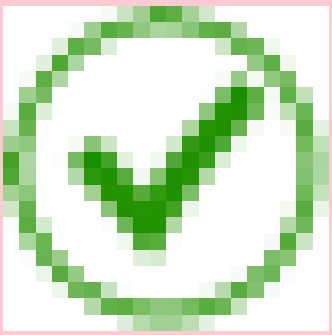
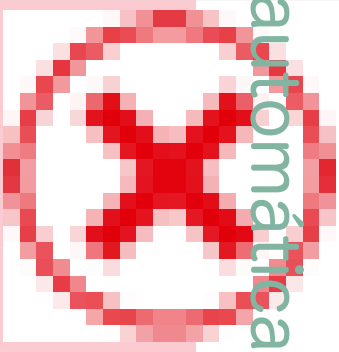
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Tópicos de observação				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

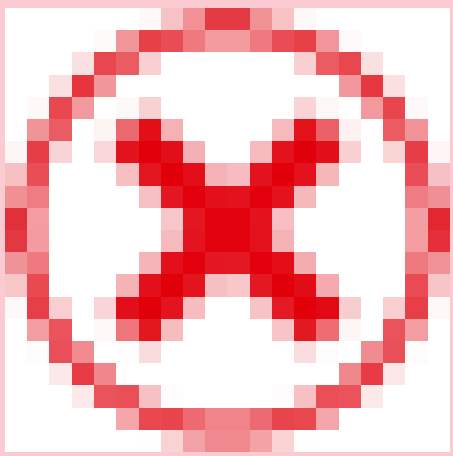
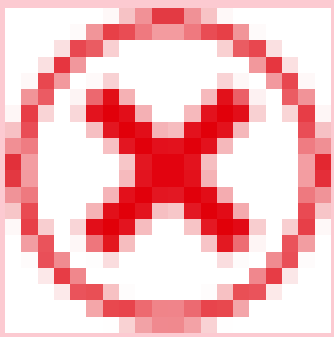
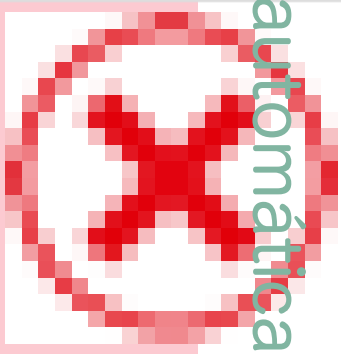
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Regras de atribuição				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

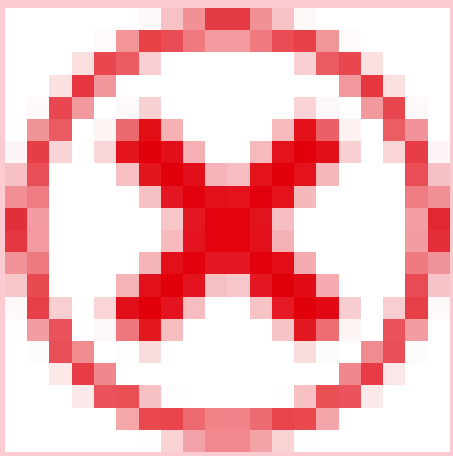
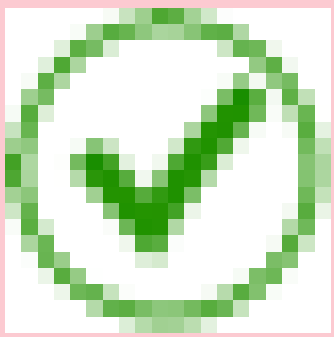
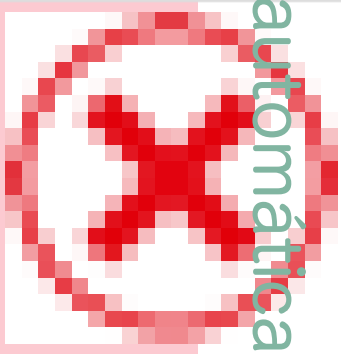
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Regras de tarefa de correção				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

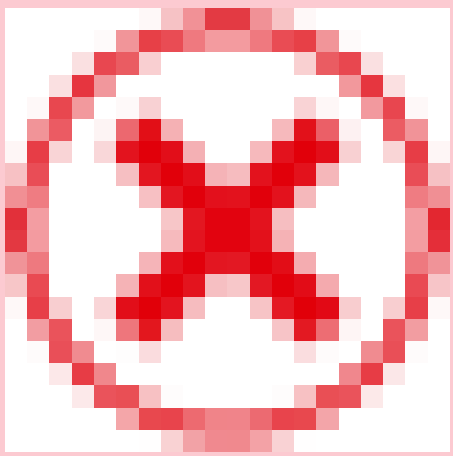
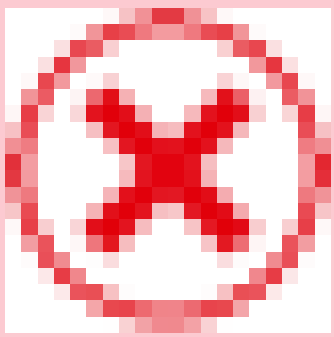
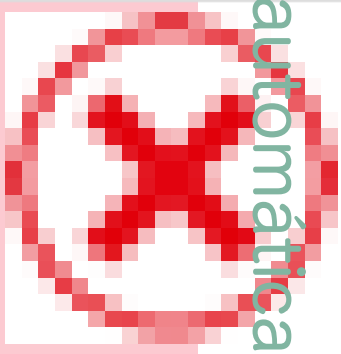
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Recomendações de atribuição				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

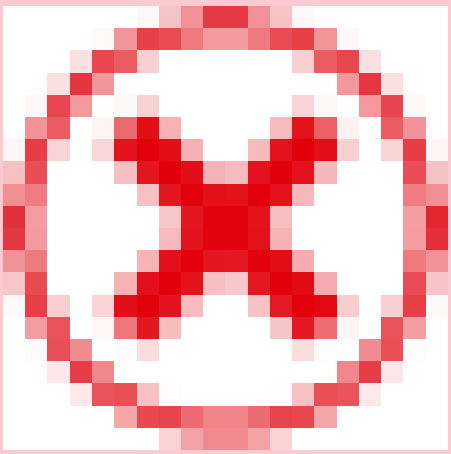
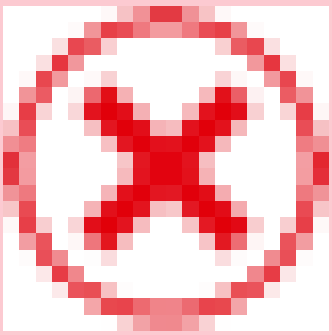
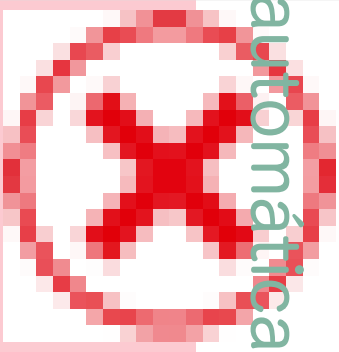
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Calculadoras de vulnerabilidade				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

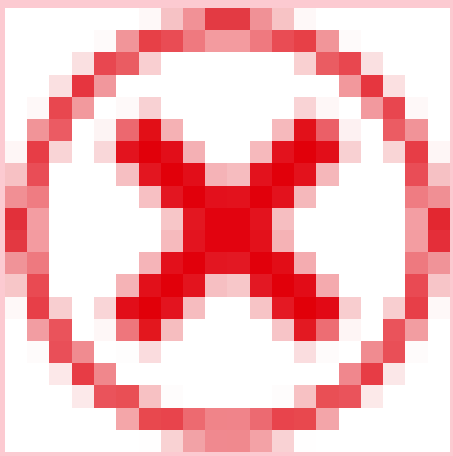
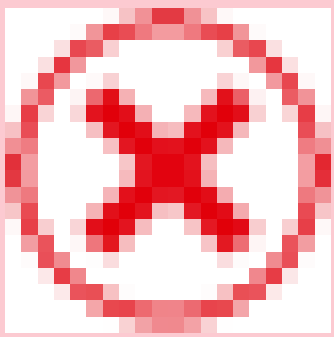
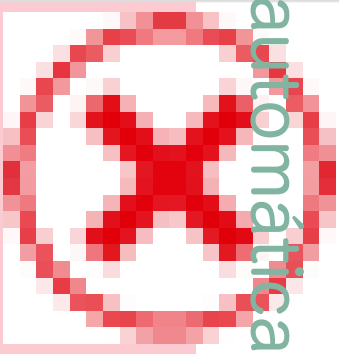
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Calculadora de Rollup de Vulnerabilidade				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

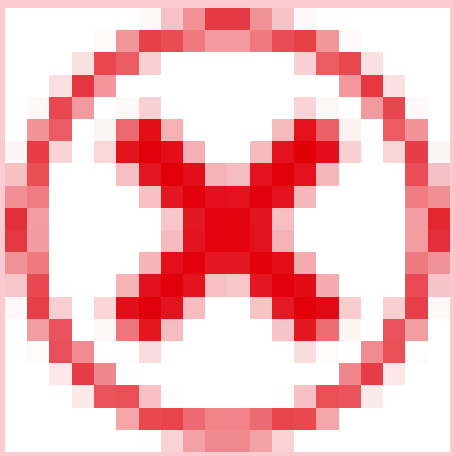
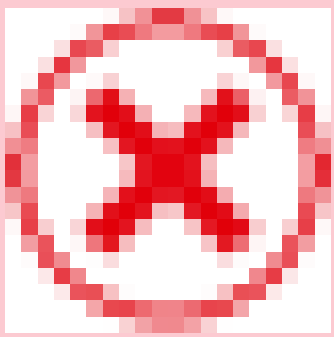
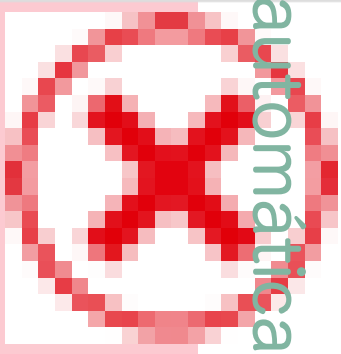
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Regras de destino de correção				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

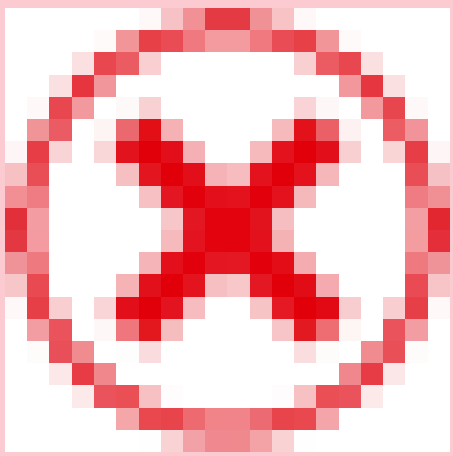
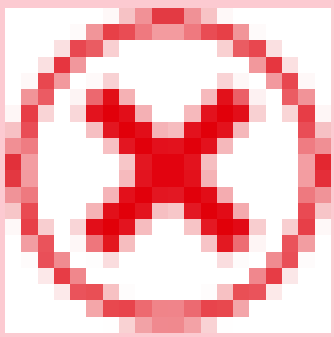
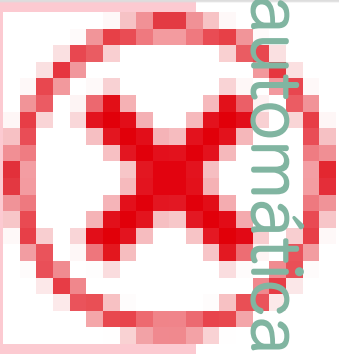
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Configuração de fechamento automático				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

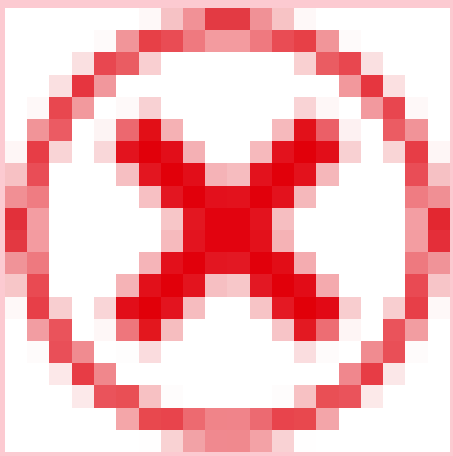
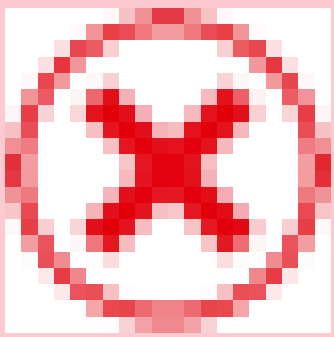
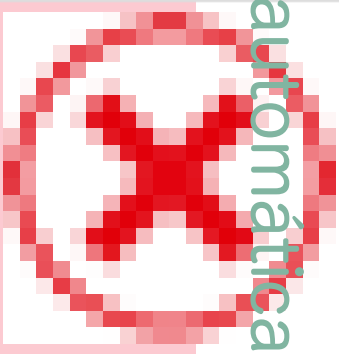
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Regras de exclusão automática				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

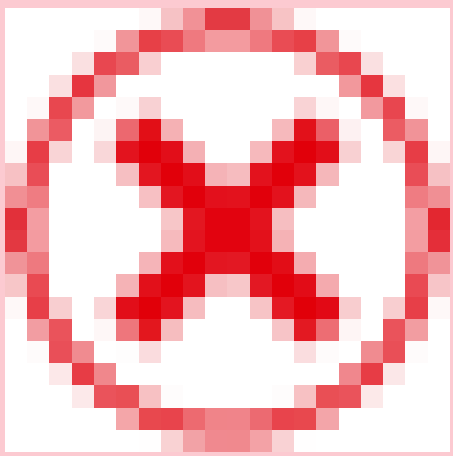
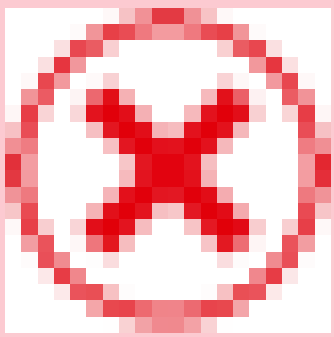
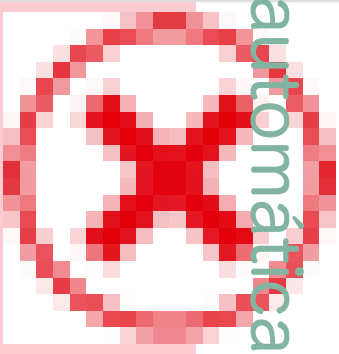
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Regras de exceção				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

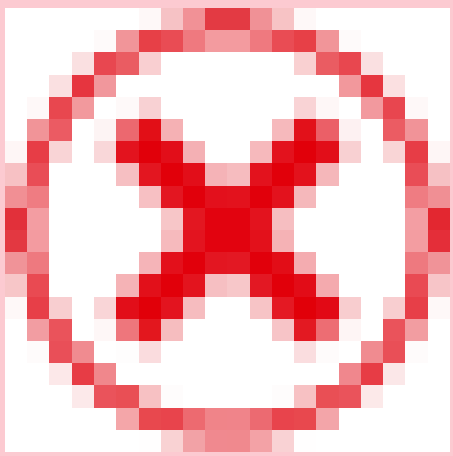
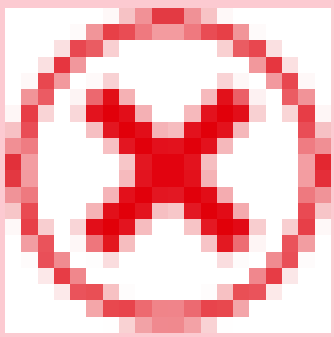
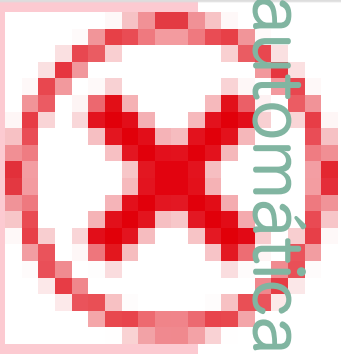
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Regras de aprovação				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

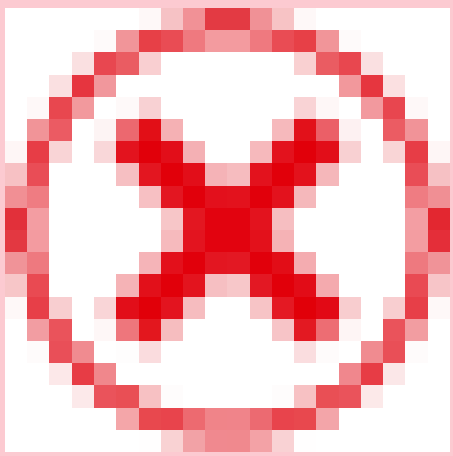
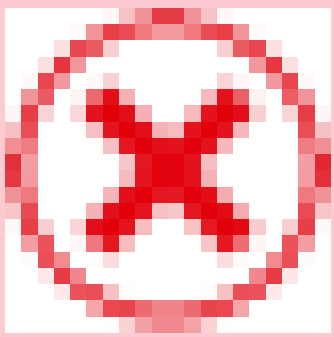
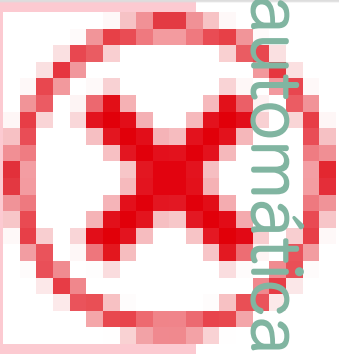
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Regras de classificação				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

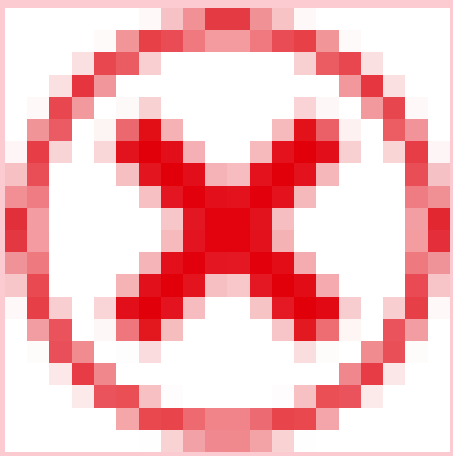
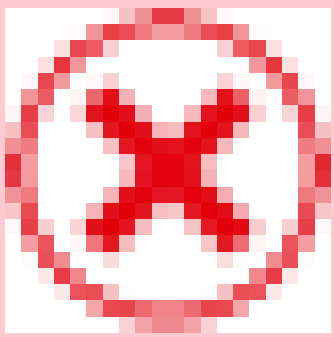
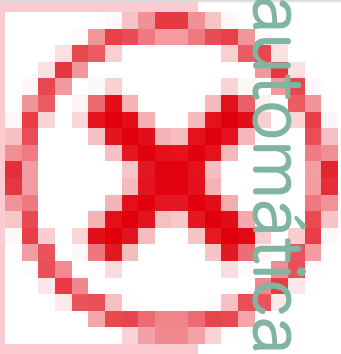
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Configuração de desempenho				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

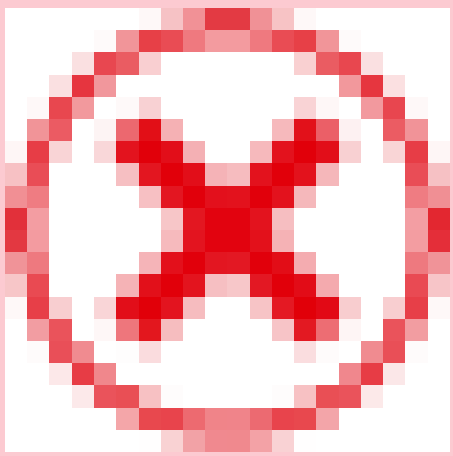
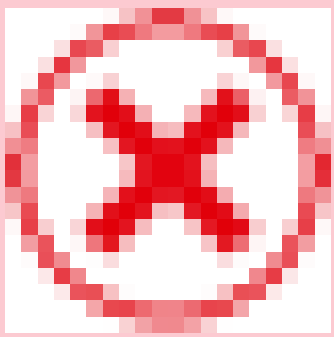
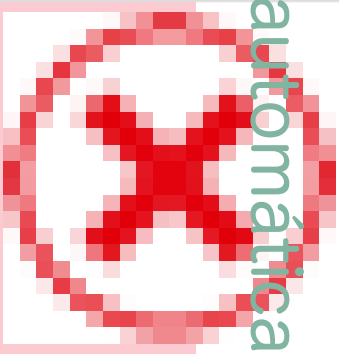
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Configurar granularidade de IV				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

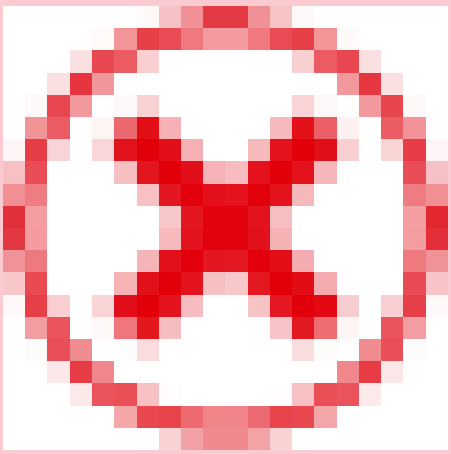
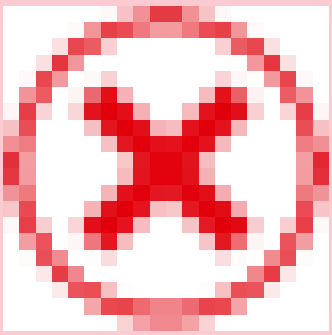
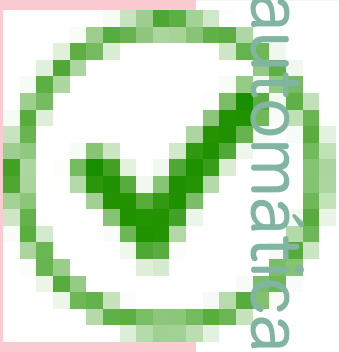
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Notificações				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

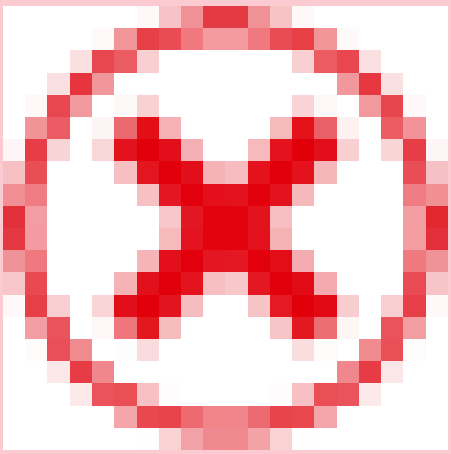
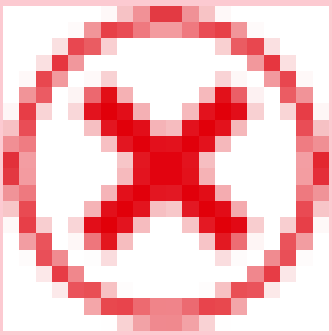
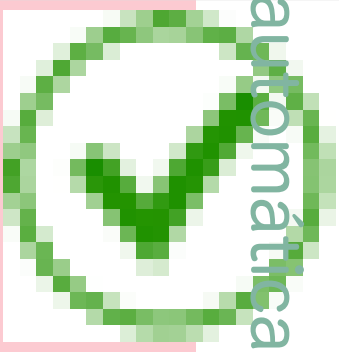
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Modelos de e-mail				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

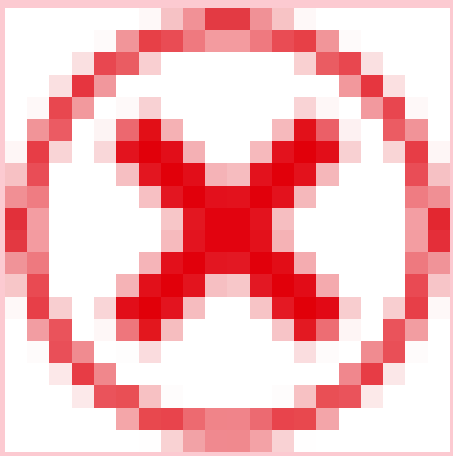
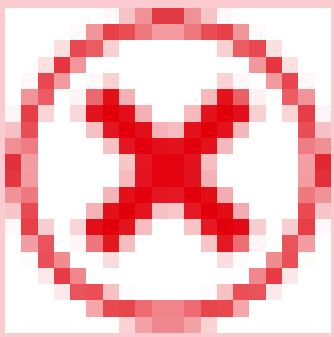
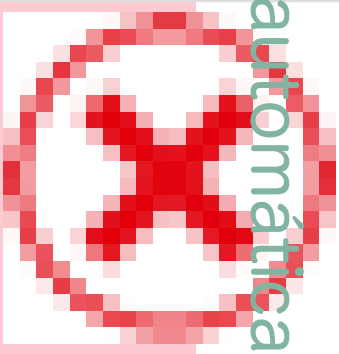
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Importar Fila				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

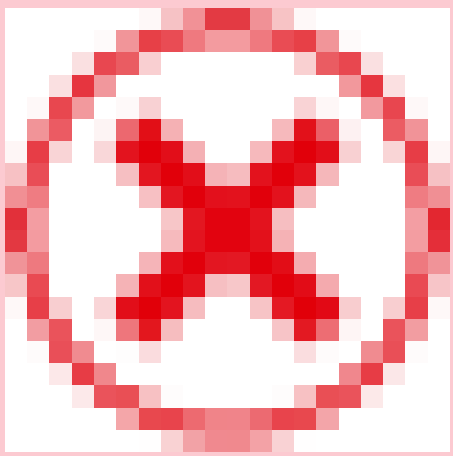
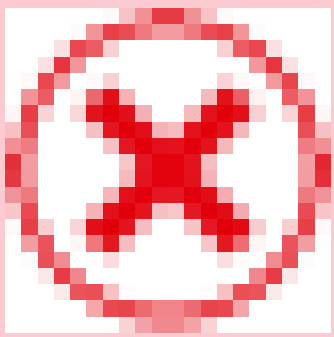
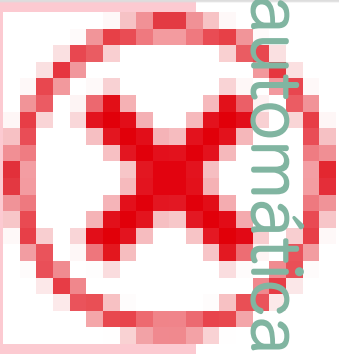
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Integrações				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

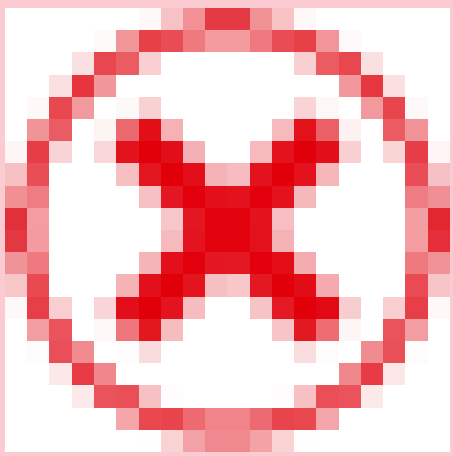
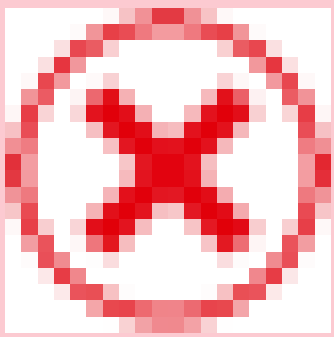
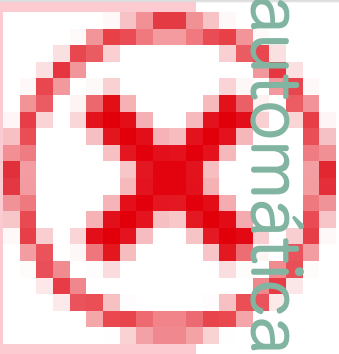
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Definições do ANS				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

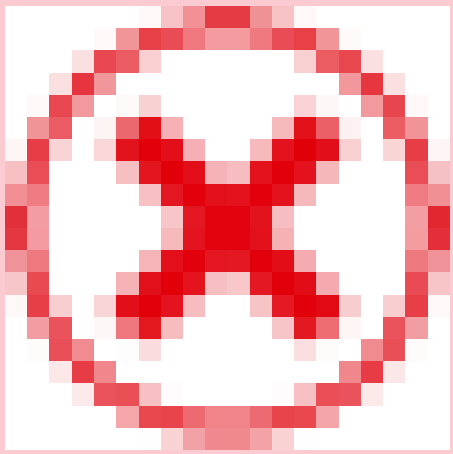
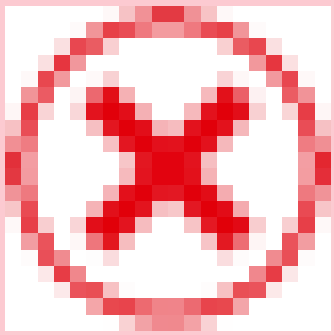
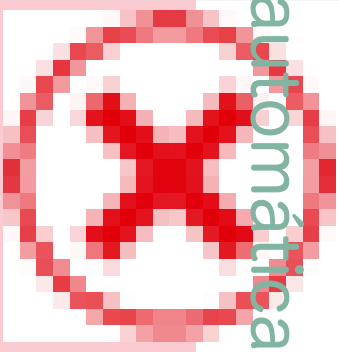
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Configurar SAM NVD				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

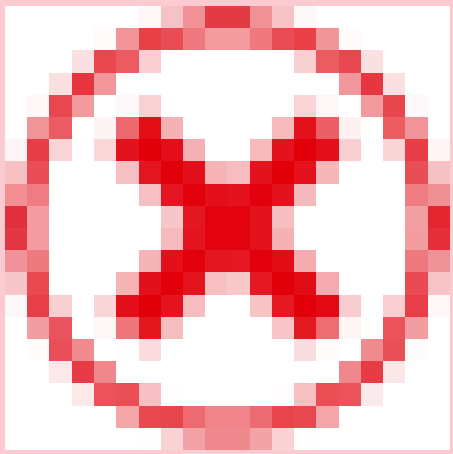
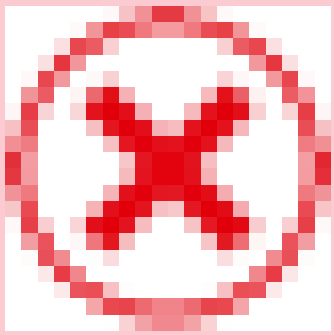
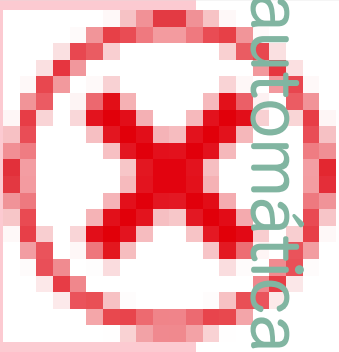
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Mapas de Gravidade Normalizados				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

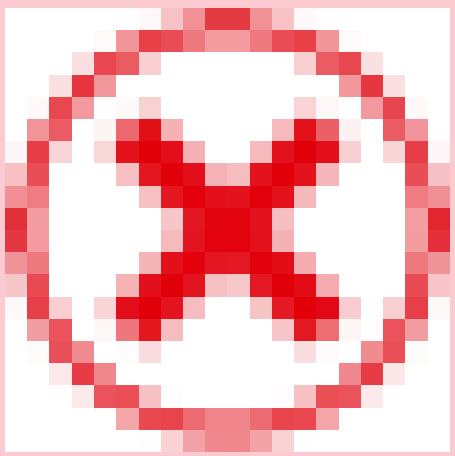
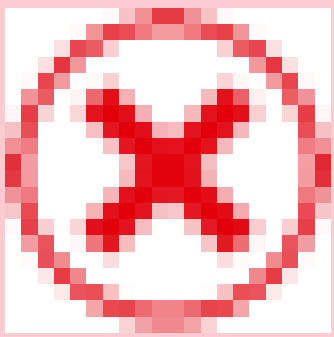
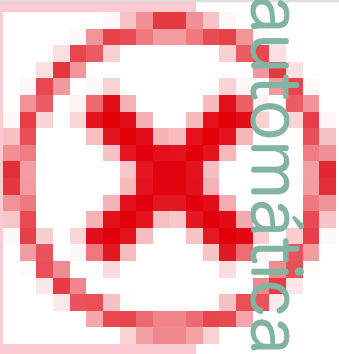
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Configuração de cobertura de verificação				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

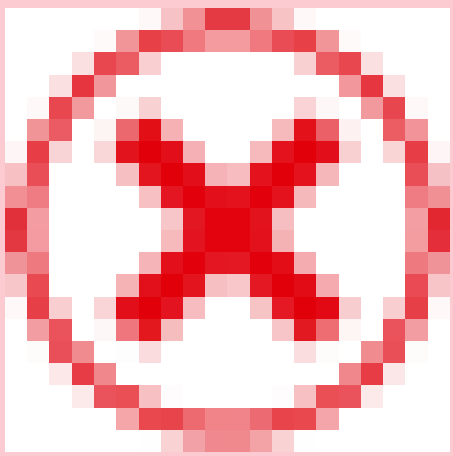
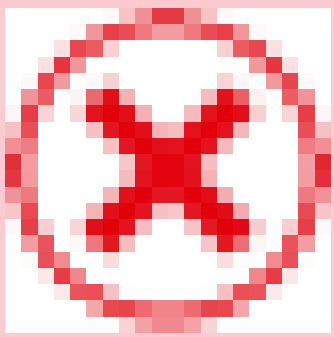
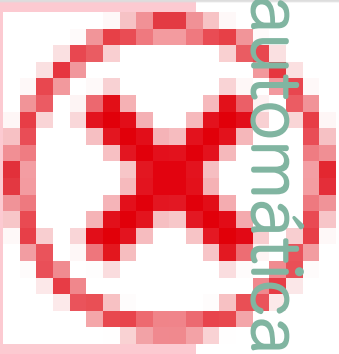
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Gestão de exceção				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

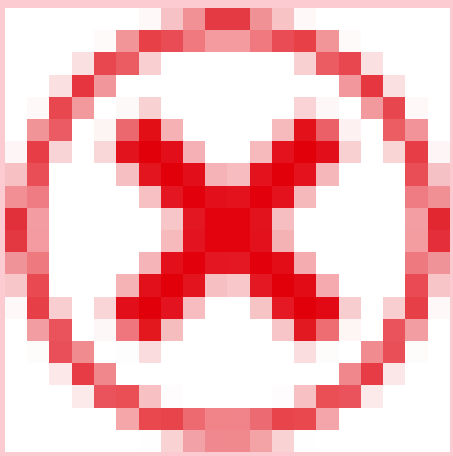
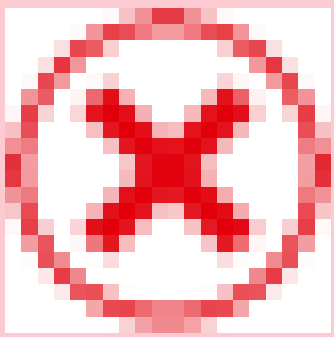
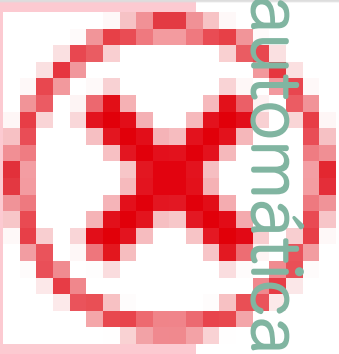
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Relatório de uso				
Diagnósticos				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

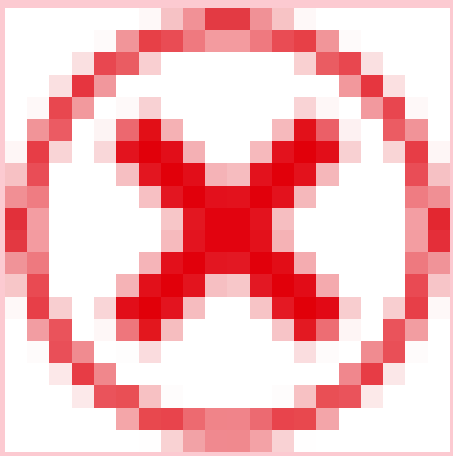
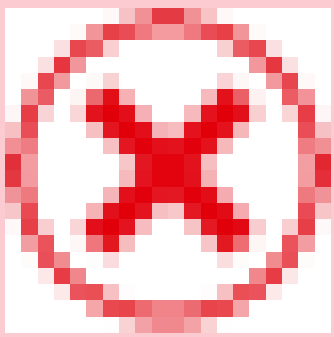
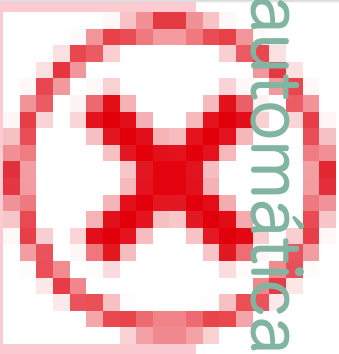
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_exposure_assessment	sn_vul.manage_group_rules	sn_vul.manage_notifications	sn_
Verificações				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
(Grupo de apps principal)				
Painel do CISO	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Visão Geral da Correção	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Espaço para gerentes de vulnerabilidades				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Visão geral	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Espaço de correção de TI	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Visão geral do aprovador	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Visão geral	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Minhas aprovações	✗	✗	✗	
Tarefas de correção				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Ativo	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Atribuídos a Mim	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Atribuído aos Meus grupos	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Todos	✓	✓	✓	
Itens vulneráveis				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Risco crítico	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Alto risco	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Explorável	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Perto da meta	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Meta não atingida	✓	✓	✓	

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Nos últimos 90 dias	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Há mais de 90 dias	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Não designado	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Desagrupado	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Desativado	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Vários adiamentos	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Todos	✓	✓	✓	
Soluções				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Todos	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Substituição mais alta	✓	✓	✓	

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Com itens vulneráveis	✓	✓	✓	
Bibliotecas				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
NVD	✓	✓		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
CWE	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Terceiros	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Software Vulnerável	✓	✓	✓	
Verificação de Vulnerabilidades				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Avaliação de Exposição	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Verificações	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Scanners	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Fila de Verificação	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Limites de Taxa do Scanner	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Definições de Limite de Taxa	✗	✗	✗	
Administração				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Assistente de configuração	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Tópicos de observação	✓	✓	✓	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Regras de atribuição	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Regras de tarefa de correção	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Recomendações de atribuição	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Calculadoras de vulnerabilidade	✗	✓	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Calculadora de Rollup de Vulnerabilidade	✗	✓	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Regras de destino de correção	✓	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Configuração de fechamento automático	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Regras de exclusão automática	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Regras de exceção	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Regras de aprovação	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Regras de classificação	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Configuração de desempenho	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Configurar granularidade de IV	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Notificações	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Modelos de e-mail				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Importar Fila	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Integrações	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Definições do ANS	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Configurar SAM NVD	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Mapas de Gravidade Normalizados	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Configuração de cobertura de verificação	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Gestão de exceção	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Relatório de uso	✗	✗	✗	
Diagnósticos				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.manage_remediation_target_rules	sn_vul.manage_risk_score_configuration	sn_vul.read_all	s
Verificações	✗	✗	✗	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

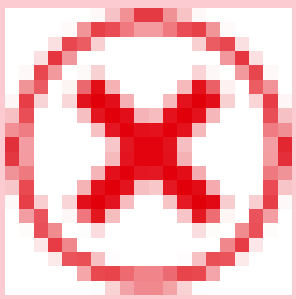
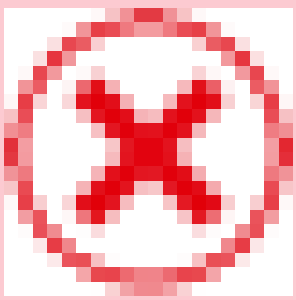
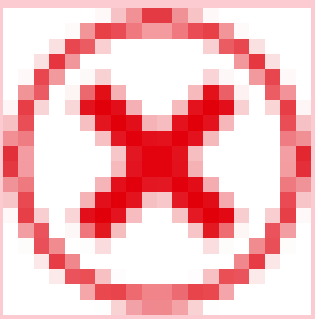
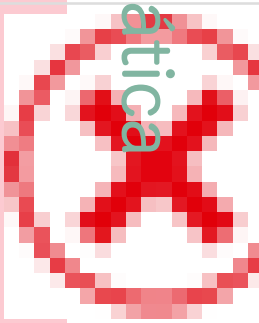
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
(Grupo de apps principal)				
Painel do CISO				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Visão Geral da Correção	✗	✗	✓	✗
Espaço para gerentes de vulnerabilidades	✗	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Visão geral	✗	✗	✗	✗
Espaço de correção de TI	✗	✗	✓	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Visão geral do aprovador	✗	✗	✗	✗
Visão geral	✗	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

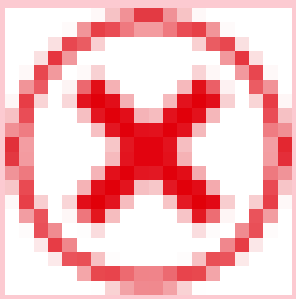
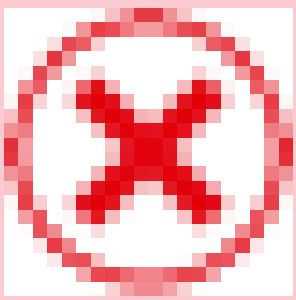
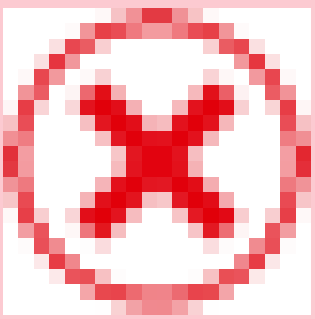
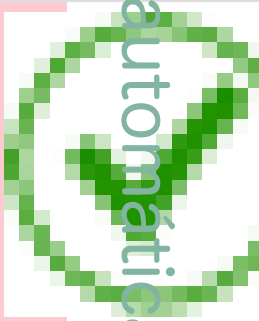
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Minhas aprovações				
Tarefas de correção				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Ativo	✗	✗	✗	✗
Atribuídos a Mim	✗	✗	✓	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Atribuído aos Meus grupos	✗	✗	✓	✗
Todos	✗	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Itens vulneráveis				
Risco crítico	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Alto risco	✗	✗	✗	✗
Explorável	✗	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Perto da meta	✗	✗	✗	✗
Meta não atingida	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Nos últimos 90 dias	✗	✗	✗	✗
Há mais de 90 dias	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Não designado	✗	✗	✓	✗
Desagrupado	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Desativado	✗	✗	✗	✗
Vários adiamentos	✗	✗	✓	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

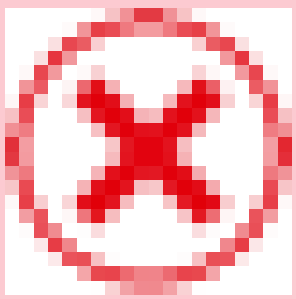
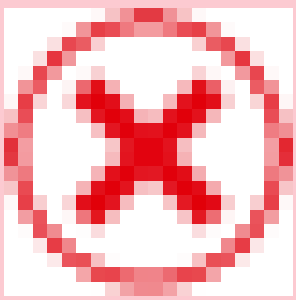
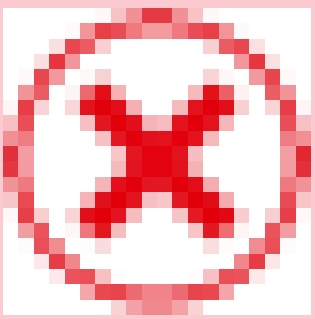
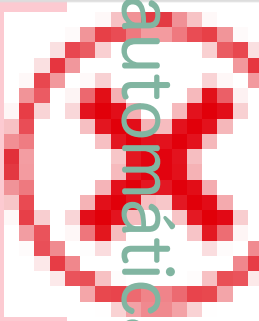
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Todos				
Soluções				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Todos	✗	✗	✓	✗
Substituição mais alta	✗	✗	✓	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

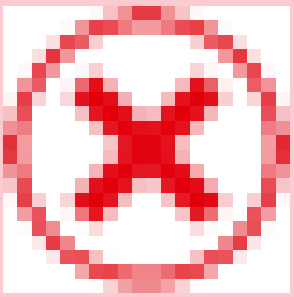
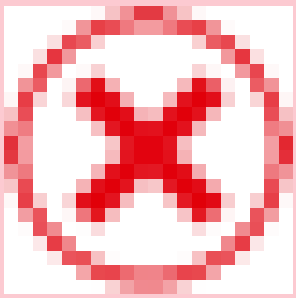
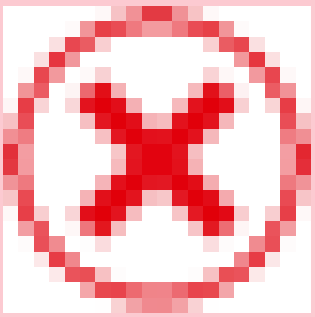
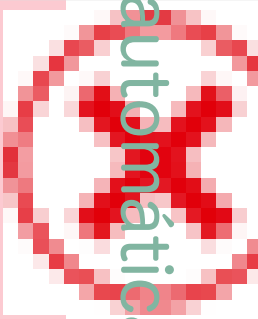
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Com itens vulneráveis				
Bibliotecas				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
NVD	✗	✗	✓	✗
CWE	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Terceiros	✗	✗	✓	✗
Software Vulnerável	✗	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Verificação de Vulnerabilidades				
Avaliação de Exposição	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Verificações	✗	✗	✗	✗
Scanners	✗	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Fila de Verificação	✓	✗	✗	✗
Limites de Taxa do Scanner	✗	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

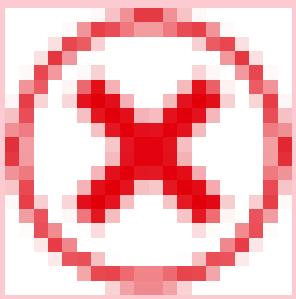
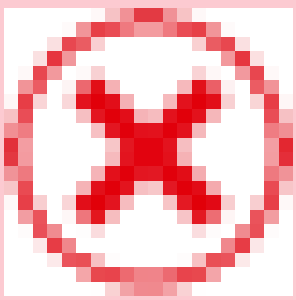
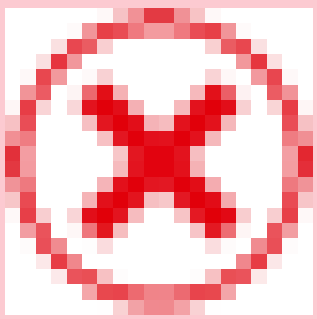
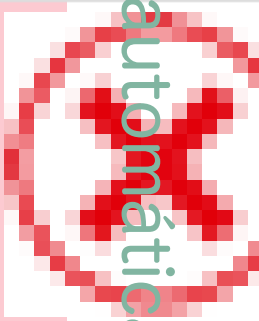
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Definições de Limite de Taxa				
Administração				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Assistente de configuração	✗	✗	✗	✗
Tópicos de observação	✗	✓	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Regras de atribuição	✗	✗	✗	✗
Regras de tarefa de correção	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Recomendações de atribuição	✗	✗	✗	✗
Calculadoras de vulnerabilidade	✗	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Calculadora de Rollup de Vulnerabilidade	✗	✗	✗	✗
Regras de destino de correção	✗	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Configuração de fechamento automático	✗	✗	✗	✗
Regras de exclusão automática	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Regras de exceção	✗	✗	✗	✗
Regras de aprovação	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Regras de classificação	✗	✗	✗	✗
Configuração de desempenho	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Configurar granularidade de IV	✗	✗	✗	✗
Notificações	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Modelos de e-mail	✗	✗	✗	✗
Importar Fila	✗	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Integrações	✗	✗	✗	✗
Definições do ANS	✗	✗	✗	✗

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Configurar SAM NVD	✗	✗	✗	✗
Mapas de Gravidade Normalizados	✗	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Tradução automática

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Configuração de cobertura de verificação	✗	✗	✗	✗
Gestão de exceção	✗	✗	✗	✗

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

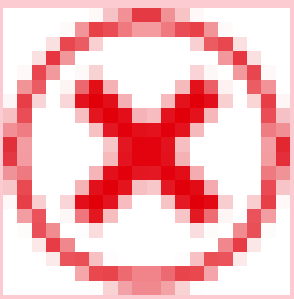
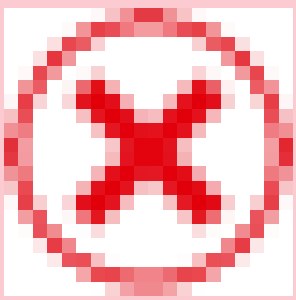
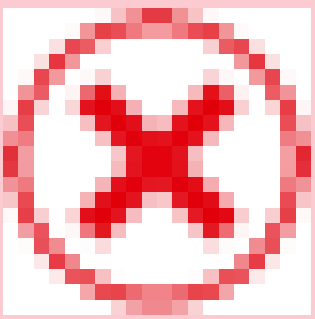
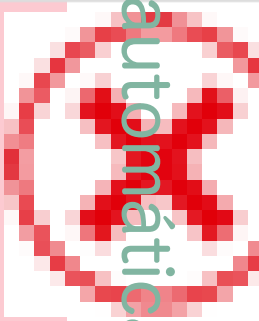
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Relatório de uso				
Diagnósticos				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

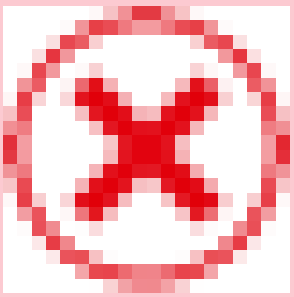
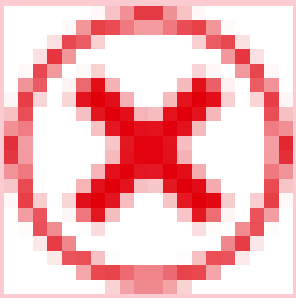
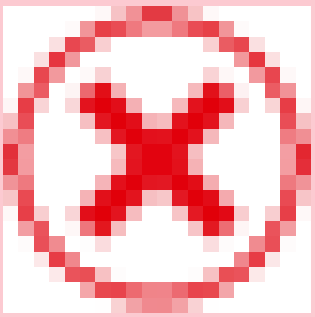
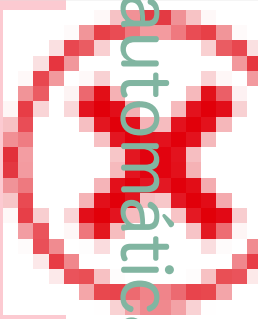
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Módulo	sn_vul.read_integrations	sn_vul.read_watch_topic	sn_vul.remediation_owner	sn_vul.unassign_appr
Verificações				

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

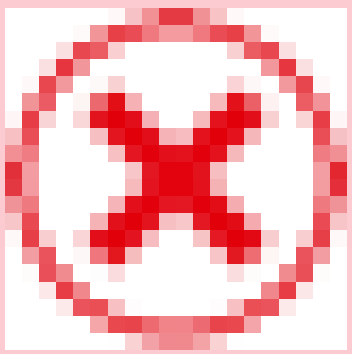
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
(Grupo de apps principal)		
Painel do CISO		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

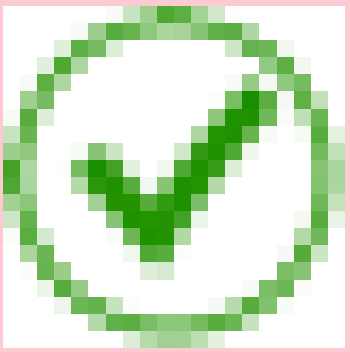
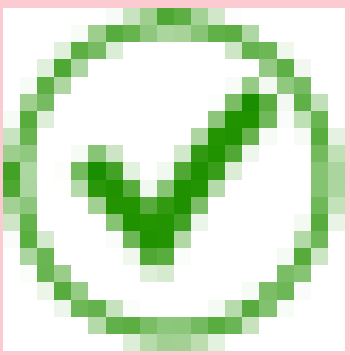
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Visão Geral da Correção		
Espaço para gerentes de vulnerabilidades		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

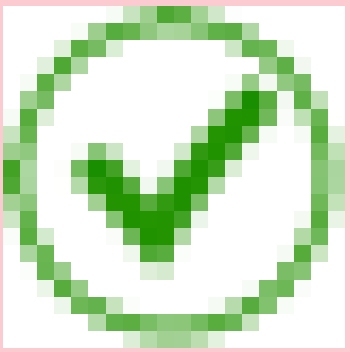
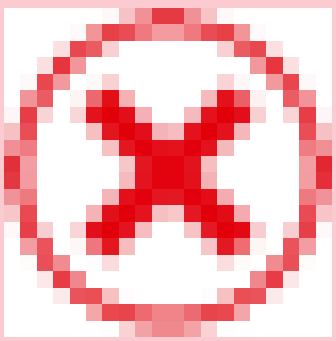
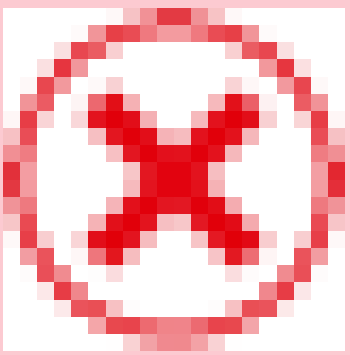
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Visão geral		
Espaço de correção de TI		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

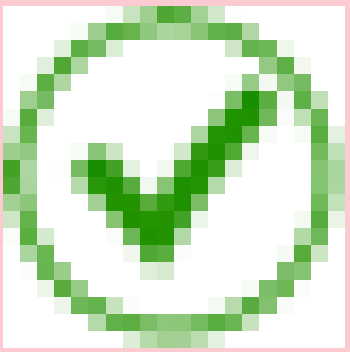
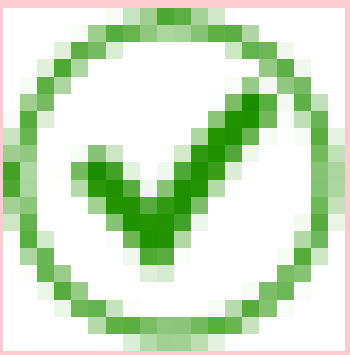
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Visão geral do aprovador		
Visão geral		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

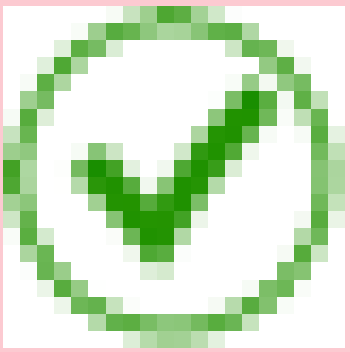
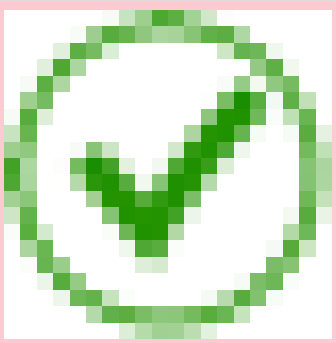
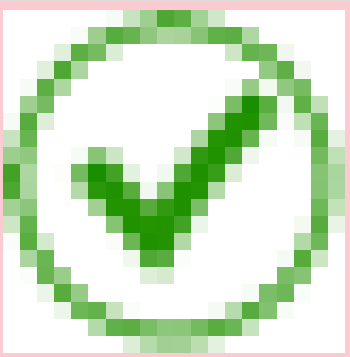
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Minhas aprovações		
Tarefas de correção		
Ativo		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

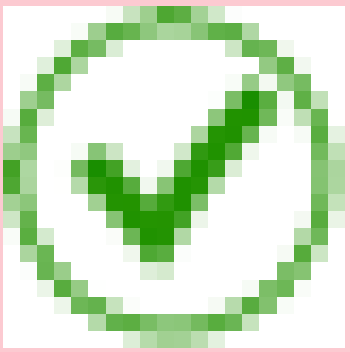
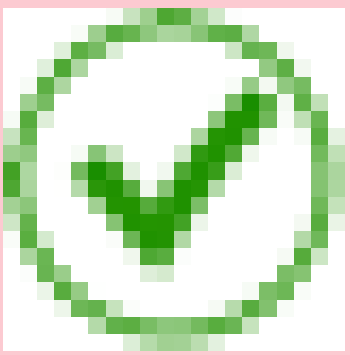
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Atribuídos a Mim		
Atribuído aos Meus grupos		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

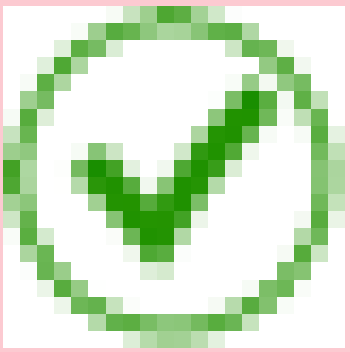
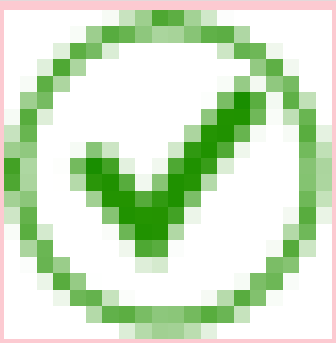
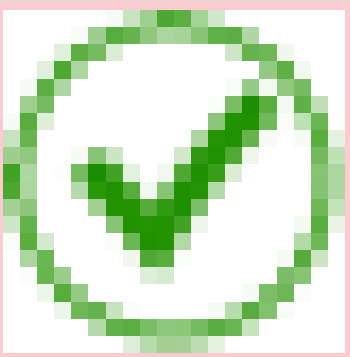
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Todos		
Itens vulneráveis		
Risco crítico		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

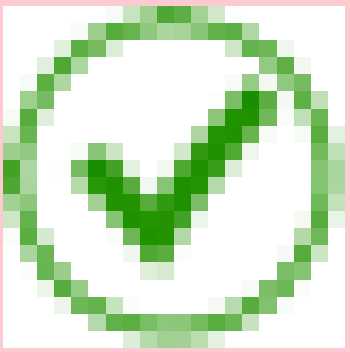
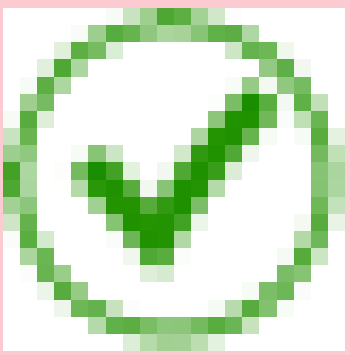
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Alto risco		
Explorável		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

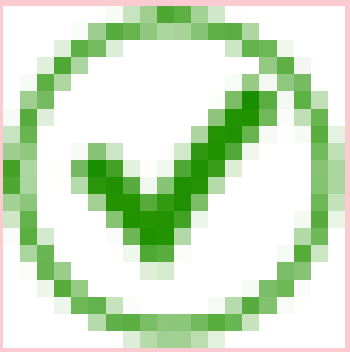
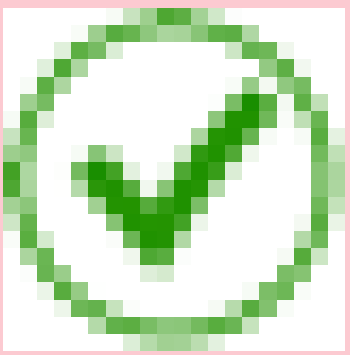
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Perto da meta		
Meta não atingida		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

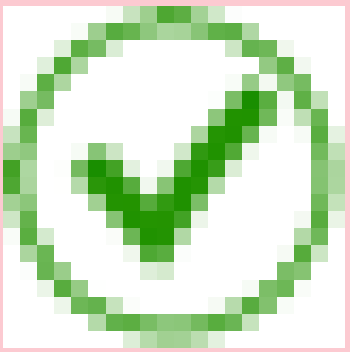
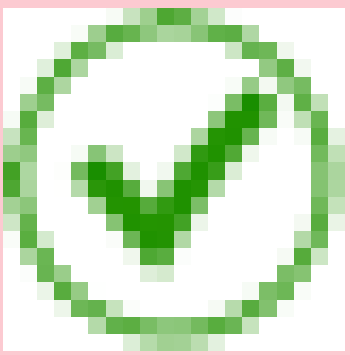
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Nos últimos 90 dias		
Há mais de 90 dias		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

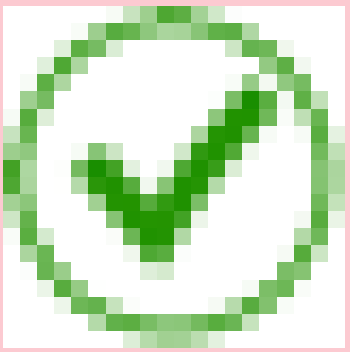
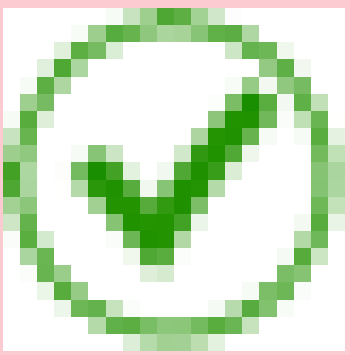
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Não designado		
Desagrupado		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

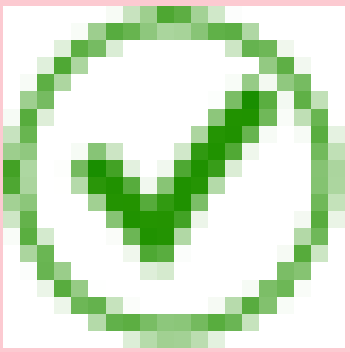
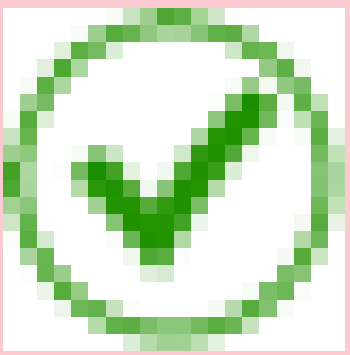
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Desativado		
Vários adiamentos		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

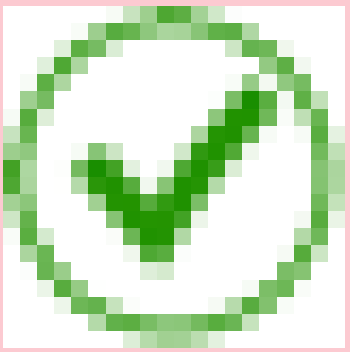
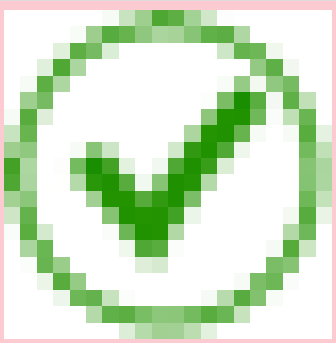
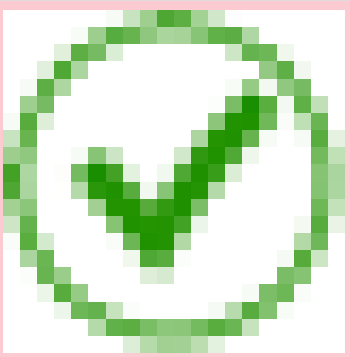
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Todos		
Soluções		
Todos		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

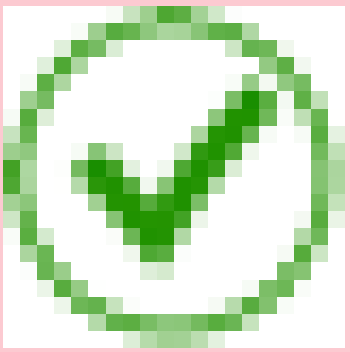
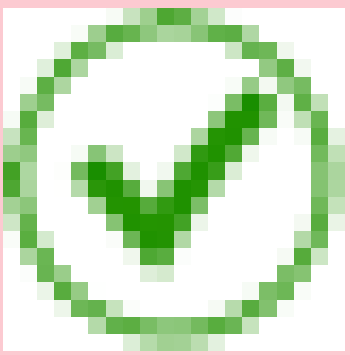
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Substituição mais alta		
Com itens vulneráveis		
Bibliotecas		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

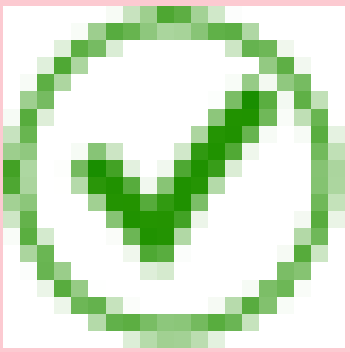
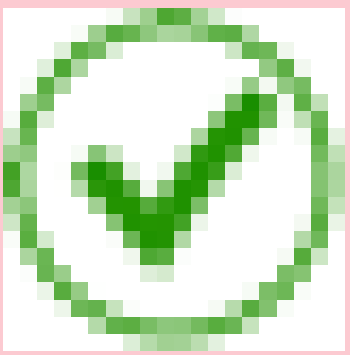
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
NVD		
CWE		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

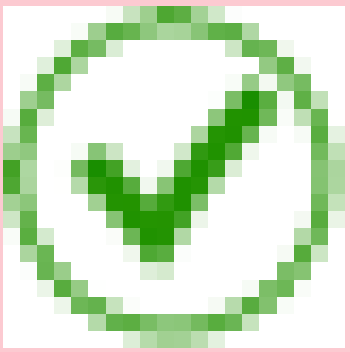
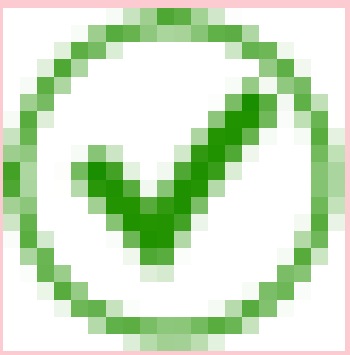
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Terceiros		
Software Vulnerável		
Verificação de Vulnerabilidades		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

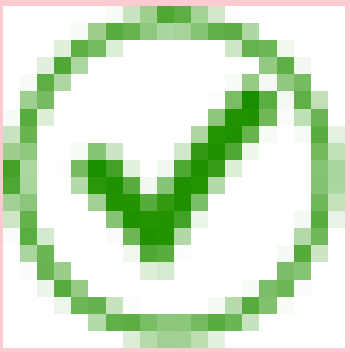
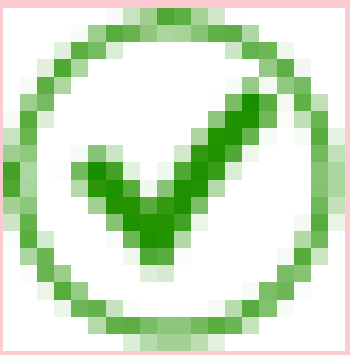
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Avaliação de Exposição		
Verificações		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

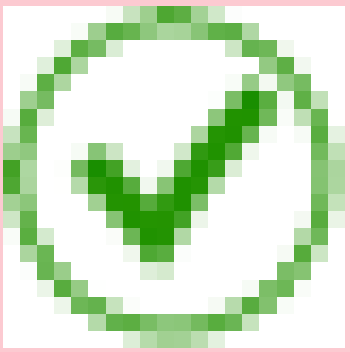
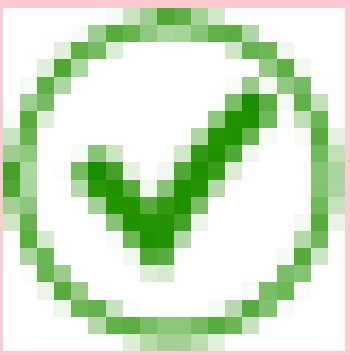
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Scanners		
Fila de Verificação		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

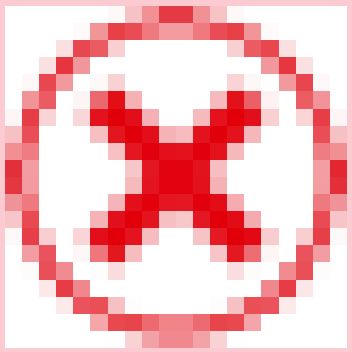
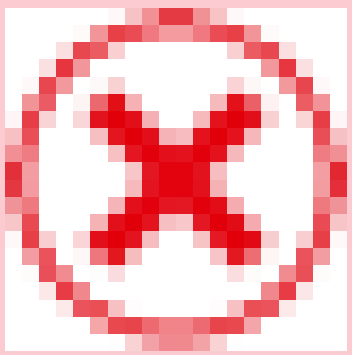
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Limites de Taxa do Scanner		
Definições de Limite de Taxa		
Administração		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

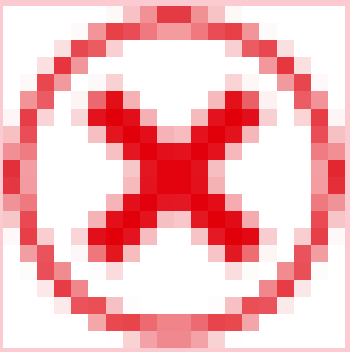
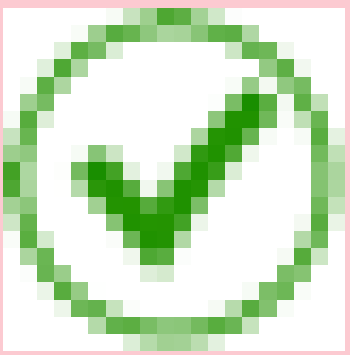
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Assistente de configuração		
Tópicos de observação		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

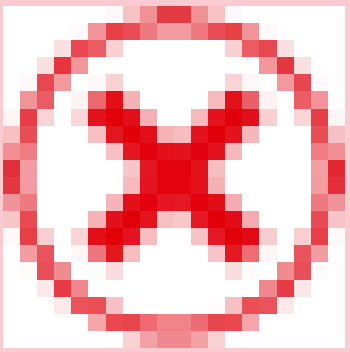
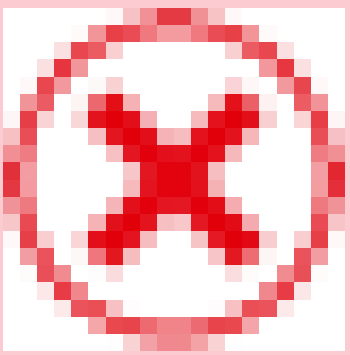
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Regras de atribuição		
Regras de tarefa de correção		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

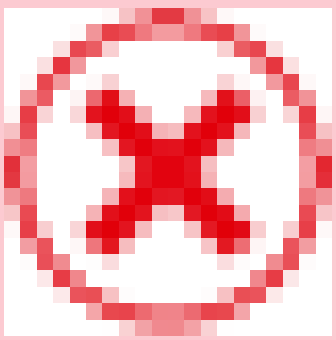
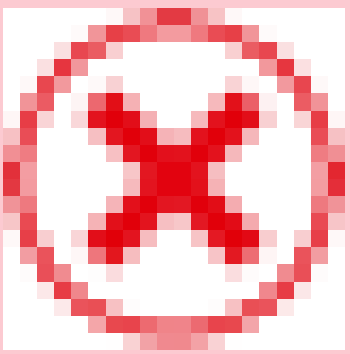
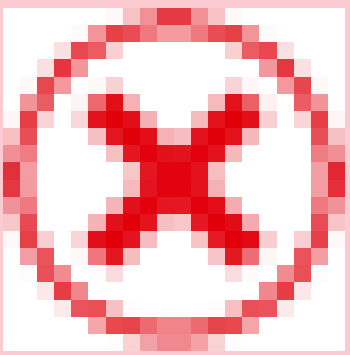
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Recomendações de atribuição		
Calculadoras de vulnerabilidade		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

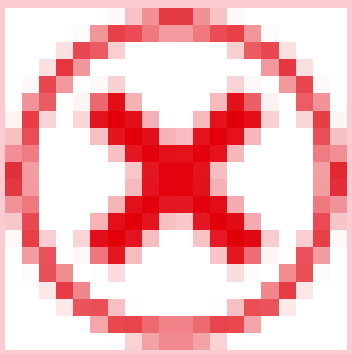
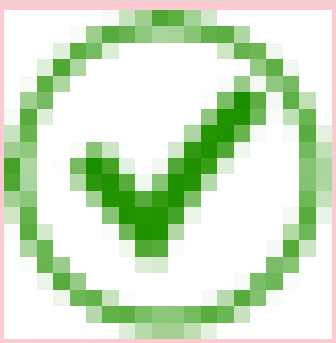
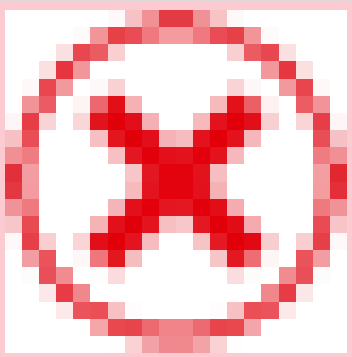
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Calculadora de Rollup de Vulnerabilidade		
Regras de destino de correção		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

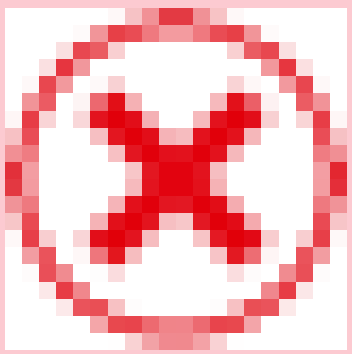
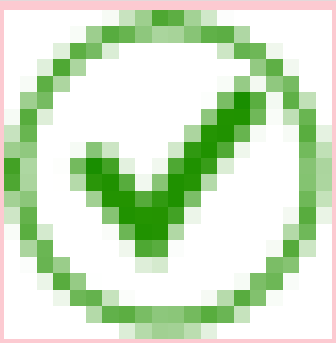
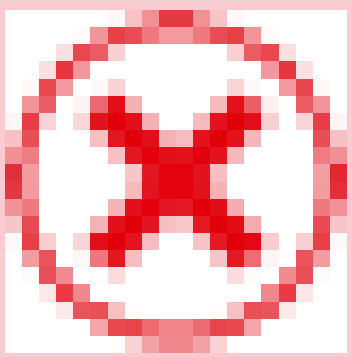
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Configuração de fechamento automático		
Regras de exclusão automática		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

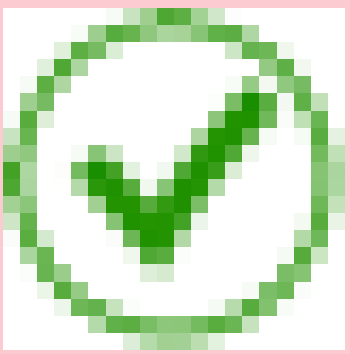
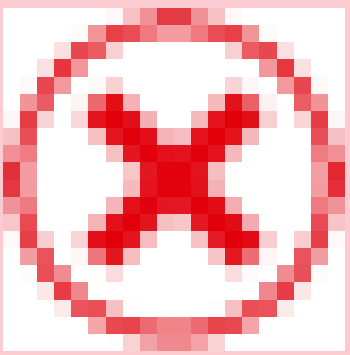
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Regras de exceção		
Regras de aprovação		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

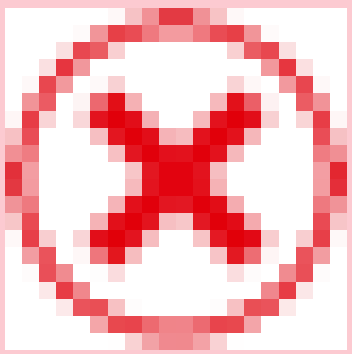
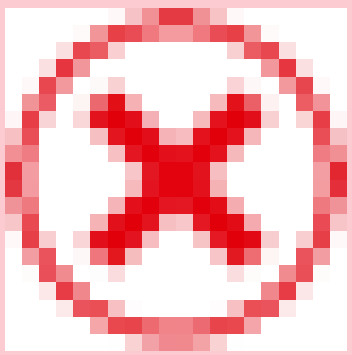
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Regras de classificação		
Configuração de desempenho		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

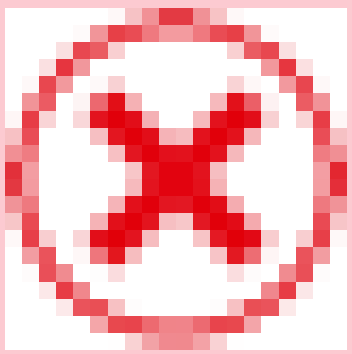
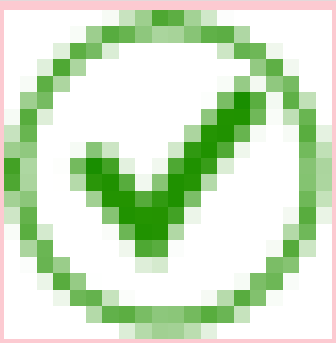
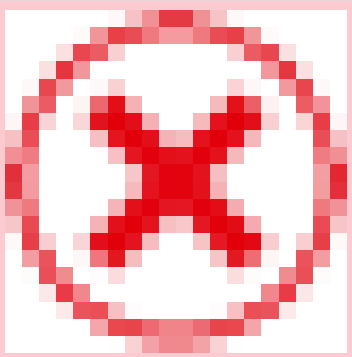
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Configurar granularidade de IV		
Notificações		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

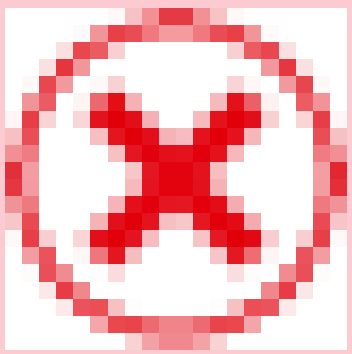
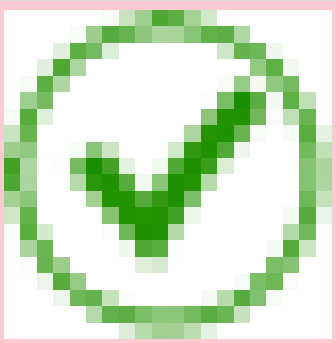
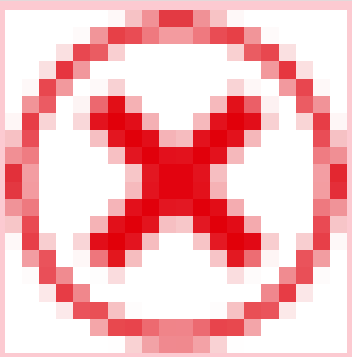
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Modelos de e-mail		
Importar Fila		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

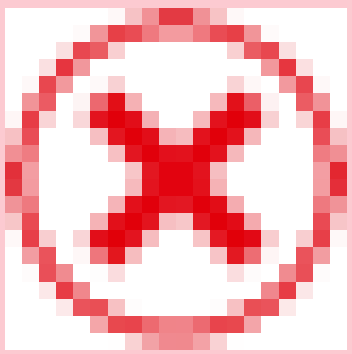
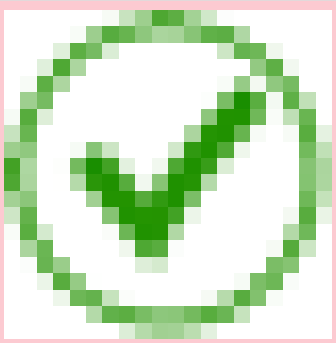
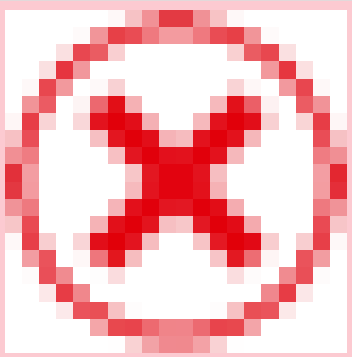
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Integrações		
Definições do ANS		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

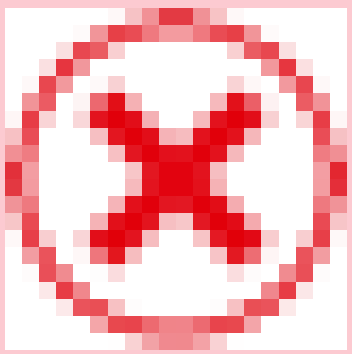
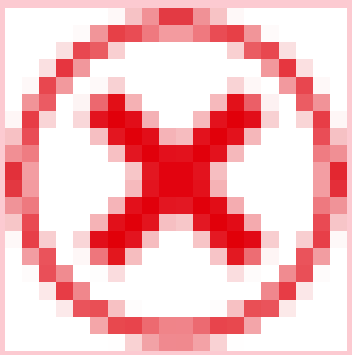
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Configurar SAM NVD		
Mapas de Gravidade Normalizados		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

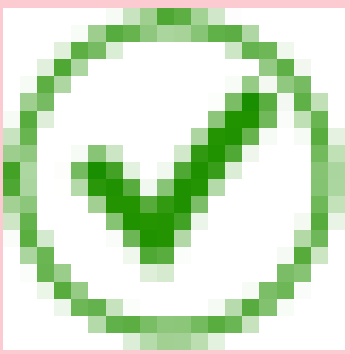
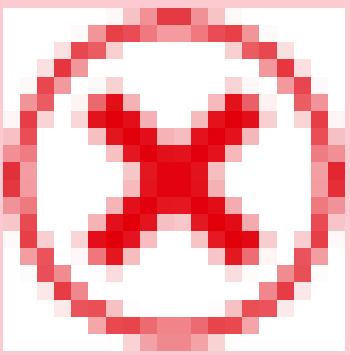
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Configuração de cobertura de verificação		
Gestão de exceção		

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Acesso ao módulo para: sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Informações para outras funções:

sn_sec_cmn.manage_approval_rules, sn_vul.access_setup_assistant, sn_vul.ciso_read, sn_vul.configure_integrations

sn_vul.configure_nvd_integration, sn_vul.configure_scan_coverage_read, sn_vul.configure_vi_granularity, sn_vul.configure_vr_performance

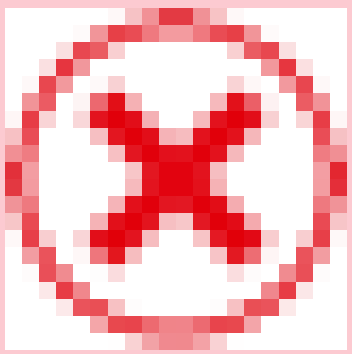
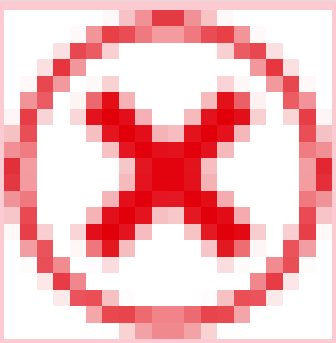
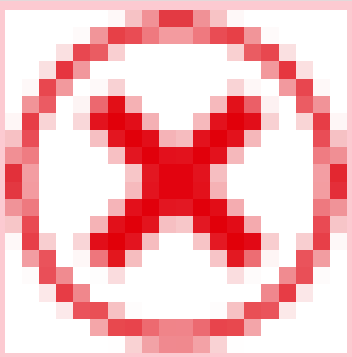
sn_vul.exception_approver, sn_vul.false_positive_approver, sn_vul.manage_assignment_recom_config, sn_vul.manage_assignment_rules

sn_vul.manage_auto_close_stale_vi, sn_vul.manage_auto_delete, sn_vul.manage_classification_rules, sn_vul.manage_exception_configuration

sn_vul.manage_exposure_assessment, sn_vul.manage_group_rules, sn_vul.manage_notifications, sn_vul.manage_permissions

sn_vul.manage_remediation_target_rules, sn_vul.manage_risk_score_configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_auto_exception_rule

sn_vul.read_integrations, sn_vul.read_watch_topic, sn_vul.remediation_owner, sn_vul.unassign_approver, sn_vul.view_enterprise_wide_stats

Módulo	sn_vul.vulnerability_admin	sn_vul.vulnerability_analyst
Relatório de uso		
Diagnósticos		
Verificações		

[End]

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisar Security Operations

Você pode encontrar informações rapidamente em qualquer aplicação Security Operations usando o ícone de pesquisa no cabeçalho da tela. O Zing é o mecanismo de indexação e pesquisa de texto que executa todas as pesquisas de texto em sua instância.

Antes de Iniciar

Função necessária: sn_si.read ou superior

Procedimento

1. Clique no ícone de pesquisa ( ) no canto superior direito da tela.
2. Digite os critérios pelos quais você deseja pesquisar e pressione **Enter**.
   Se você tiver o plug-in Security Incident Response ativado, os critérios de pesquisa inseridos apresentarão qualquer texto de descrição resumida, ICs, endereços IP ou URLs correspondentes em seus incidentes de segurança, Security Incident Response tarefas ou solicitações de segurança. Se você tiver os plug-ins Vulnerability Response ou Inteligência contra ameaças ativados, os resultados da pesquisa incluirão vulnerabilidades, itens vulneráveis, entradas vulneráveis, observáveis, IoCs e modo/métodos de ataque.

Tópicos relacionados

Introdução à pesquisa

Pesquisa de texto do Zing

Referência do Security Operations Integrations

Os desenvolvedores e parceiros da ServiceNow podem usar as informações nesta seção para entender a funcionalidade oculta de integrações de terceiros, incluindo diretrizes de desenvolvimento, recursos de integração e fluxos de trabalho.

ServiceNow Security Operations diretrizes de desenvolvimento de integração

A plataforma ServiceNow fornece vários mecanismos para desenvolver integrações com sistemas externos. O pacote de produtos ServiceNow Security Operations adiciona recursos de integração destinados a simplificar o processo de integração com sistemas externos focados na segurança.

A maioria dos conceitos neste guia pressupõe alguma familiaridade com a funcionalidade ServiceNow padrão. Para integrar com o pacote Security Operations], é necessário conhecimento dos seguintes conceitos ServiceNow :

- Script Includes
- Serviços Web de entrada/saída
- Fontes de dados
- Conjuntos de importação
- Mapas de transformação

Programa de parceiros de tecnologia

Quaisquer requisitos para certificação de aplicação ou diretrizes fornecidas na documentação do Programa de parceiros de tecnologia substituem qualquer informação neste guia. Este guia não substitui a documentação do Programa de parceiros de tecnologia e serve apenas como um complemento para a documentação existente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações, consulte a publicação do blog do curso de treinamento do Technology Partner Program .

Tipos de ServiceNow integrações fornecidas

As aplicações [Security Operations (Security Incident Response, Inteligência contra ameaçase Vulnerability Response) podem ser integradas perfeitamente a outras aplicações ServiceNow para aprimorar sua funcionalidade.

As integrações a seguir são fornecidas no sistema de base Security Operations.

Security Incident Response – Integração da Gestão de eventos

Os recursos da aplicação Gestão de eventos foram expandidos para oferecer suporte a Security Incident Response. O plug-in de suporte Security Incident Response Gestão de eventos analisa automaticamente o conteúdo de eventos em Gestão de eventos para preencher campos em incidentes de segurança.

Caso de uso coberto:

Criação de eventos de segurança no sistema Gestão de eventos a partir das ferramentas Security Information and Gestão de eventos (SIEM)

Recursos úteis fornecidos:

- Funcionalidade de gestão de eventos - correlação de eventos, regras de evento e regras de alerta
- Mapeamento automático de valores de additional_information para o incidente de segurança resultante

Recursos:

Documentação de suporte da Gestão de eventos de incidentes de segurança

Documentação da Gestão de eventos

Security Incident Response - Import Set API integration

Além de usar Gestão de eventos para enviar eventos relacionados à segurança, a aplicação Security Incident Response fornece uma API Import Set que permite a criação direta de incidentes de segurança. O endpoint REST do conjunto de importação de incidente de segurança é http://localhost:8080/api/now/import/sn_si_incident_import.

Esta técnica de integração é útil quando a) Gestão de eventos não está instalado ou b) é desejado simplesmente criar incidentes de segurança sem passar pelo evento > alerta > fluxo de incidente de segurança que é necessário ao usar Gestão de eventos.

Caso de uso coberto:

Criação de incidentes de segurança diretamente das ferramentas SIEM.

Recursos úteis fornecidos:

Correspondência automática de IC na criação do Incidente de segurança com base em IP, NetBIOS ou nome de domínio totalmente qualificado.

Recursos:

Documentação da API do conjunto de importação da plataforma

Documentação do conjunto de importação do serviço Web de incidente de segurança

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Inteligência contra ameaças - integração de origem de pesquisa

As origens de pesquisa fornecem a capacidade de enviar dados para origens de pesquisa externas para determinar se esses dados são mal-intencionados. Geralmente, esses dados são um endereço IP, URL, arquivo ou hash de arquivo.

Caso de uso coberto:

Pesquise um endereço IP, URL, arquivo ou hash com um serviço de pesquisa externo.

Recursos úteis fornecidos:

- Maneira consistente de solicitar pesquisas de itens do catálogo e incidentes de segurança.
- Capacidades de limitação de taxa e limitação fornecidas com pouca/nenhuma codificação.
- Criação automática de entradas observáveis de Indicadores de comprometimento (IoC) para todos os problemas encontrados pelas origens de pesquisa.

Inteligência contra ameaças - integração da origem da ameaça

As origens de ameaça fornecem a capacidade de extrair dados de repositórios externos de inteligência contra ameaças. Esses dados são importados para as várias tabelas de indicadores de compromisso existentes no sistema. Coleções TAXII e listas de bloqueio simples são compatíveis nativamente. Para adicionar novas coletas TAXII (ou perfis baseados em um serviço de gestão de coleta ou descoberta), basta adicionar uma entrada. Da mesma forma, adicionar uma nova lista de bloqueios simples de coluna única é uma questão de inserir um novo registro e fornecer o URL da lista de bloqueios. Para conjuntos de dados mais complexos, uma integração personalizada pode ser fornecida para fazer uma chamada para um URL e analisar a resposta.

Caso de uso coberto:

Recupere dados de uma fonte de inteligência contra ameaças para carregar em tabelas IoC.

Recursos úteis fornecidos:

- Suporte para listas de bloqueio simples e coleções TAXII sem codificação.
- Mecanismo simples para executar mensagens REST para recuperar dados.
- Recuperação/processamento de dados desacoplados para reutilização do componente de integração.
- Suporte nativo para processamento de dados de passagem retornados para fontes de dados (e conjuntos de importação/mapas de transformação).
- Oferece suporte a várias solicitações de dados por integração (para chamadas paginadas) com a capacidade de passar contexto para chamadas subsequentes

Recursos:

Definir uma origem de ameaça

Vulnerability Response - integração de invocação do scanner

O Vulnerability Scanner Invocation é um ponto de entrada de integração leve que oferece suporte à invocação de verificações de vulnerabilidade da instância. Um scanner de vulnerabilidade de terceiros é chamado de forma assíncrona para programar uma verificação de itens de configuração ou endereços IP.

Caso de uso coberto:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Faça uma solicitação ao scanner de terceiros para verificar um IC (usando informações de host derivadas do IC) ou endereço IP/endereços IP.

Recursos úteis fornecidos:

- Estrutura simples para definir implementações de scanner.
- Maneira consistente de solicitar verificações de itens do catálogo, incidentes de segurança e itens vulneráveis.
- Atualização automática de tarefas com o resultado da invocação de verificação.

Vulnerability Response - integração de dados

As integrações de dados de vulnerabilidade têm como objetivo recuperar dados de vulnerabilidade de sistemas de vulnerabilidade de terceiros. As saídas esperadas dessas integrações são entradas de vulnerabilidade e itens vulneráveis. Essa integração permite que os scanners de vulnerabilidade de terceiros funcionem de forma independente, com a expectativa de que as vulnerabilidades possam ser trabalhadas e rastreadas na instância.

Casos de uso cobertos:

- Recuperar bibliotecas de vulnerabilidades
- Recuperar emparelhamentos de vulnerabilidade/IC
- Sincronizar ICs com o sistema de gestão de vulnerabilidades

Recursos úteis fornecidos:

- Recuperação/processamento de dados desacoplados para reutilização do componente de integração.
- Suporte nativo para processamento de dados de passagem retornados para fontes de dados (e conjuntos de importação/mapas de transformação).
- Oferece suporte a várias solicitações de dados por integração (para chamadas paginadas) com a capacidade de passar contexto para chamadas subsequentes.

Recursos:

Documentação de integração de dados de vulnerabilidade

Security Operations Configurações de integração

Muitas das integrações incluídas no sistema básico exigem pouca ou nenhuma configuração e funcionam da mesma forma. Certas integrações, como Qualys Cloud Platform, no entanto, exigem etapas separadas para configurar a integração. Outros oferecem suporte a diferentes conjuntos de tipos de verificação e pesquisa e diferentes limites de taxa.

Esta seção descreve as diferenças entre as integrações compatíveis e indica mais documentações, conforme necessário.

- Integração do Carbon Black: permite que você investigue e responda a incidentes de segurança usando as APIs Carbon Black para consultar e interagir com endpoints associados a incidentes de segurança.
- Antibot Check Point - Integração do analisador de e-mails: usa um analisador de e-mail que consome notificações por e-mail do antibot Check Point para criar incidentes de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Integração do Elasticsearch Incident Enrichment: pesquisa seus logs e adiciona informações de vista relevantes aos seus incidentes de segurança.
- Integração de Have I been pwned?: permite que a lista de contas violadas (endereços de e-mail e nomes de usuário) seja pesquisada rapidamente por meio de um serviço RESTful.
- HPE Security ArcSight ESM - Integração do analisador de e-mails: usa um analisador de e-mail que consome notificações por e-mail do HPE ArcSight ESM para criar incidentes de segurança.
- HPE ArcSight Logger - Integração de Aprimoramento de incidente: pesquisa seus logs e adiciona informações de vista relevantes aos seus incidentes de segurança.
- IBM QRadar - Integração de aprimoramento de incidente: pesquisa seus logs e adiciona informações de vista relevantes aos seus incidentes de segurança.
- McAfee ESM - Integração do analisador de e-mail: usa um analisador de e-mail que consome notificações por e-mail do McAfee ESM para criar incidentes de segurança.
- McAfee ESM - Integração de aprimoramento de incidente: pesquisa seus logs e adiciona informações de vista relevantes aos seus incidentes de segurança.
- OPSWAT Metadefender visão geral da integração: permite que os dados de ameaça, detectados pelo scanner Metadefender de terceiros, sejam baixados para a aplicação Inteligência contra ameaças para acompanhamento, priorização e resolução.
- Integração de Palo Alto Networks - AutoFocus: o Palo Alto Networks AutoFocus, um serviço em nuvem de inteligência contra ameaças, permite pesquisar informações de sessão relacionadas a observáveis de incidentes de segurança.
- Integração de Palo Alto Networks - Firewall: o Firewall da Palo Alto Networks permite configurar e manter firewalls para impedir ameaças conhecidas e desconhecidas na rede, na nuvem e nos endpoints.
- Integração de Palo Alto Networks - WildFire: a integração do Wildfire permite que você consulte programaticamente trabalhos de análise no Wildfire e recupere resultados históricos por meio de uma interface de API XML simples.
- Noções básicas sobre o Qualys Vulnerability Integration: Qualys Cloud Platform é usado em Vulnerability Response.
- Splunk - Integração de aprimoramento de incidentes: pesquisa seus logs e adiciona informações de vista relevantes aos seus incidentes de segurança.
- Integração de Plataforma de ponto de extremidade Tanium: a integração do Security Operations Tanium usa um fluxo de trabalho e atividades de fluxo de trabalho para retornar processos em execução para ICs afetados.
- Integração do VirusTotal: usado em Inteligência contra ameaças. Para usar esta origem de pesquisa, você deve ativar o plug-in VirusTotal Integration.
- Configuração da integração da API WhoisXML: fornece dados consistentes e bem estruturados de uma pesquisa Whois. Mantém dados Whois precisos acessíveis 24 horas por dia, 7 dias por semana.

Ativar e configurar integrações de terceiros

Você pode ativar os plug-ins para integrações de terceiros e configurá-los para uso na mesma tela.

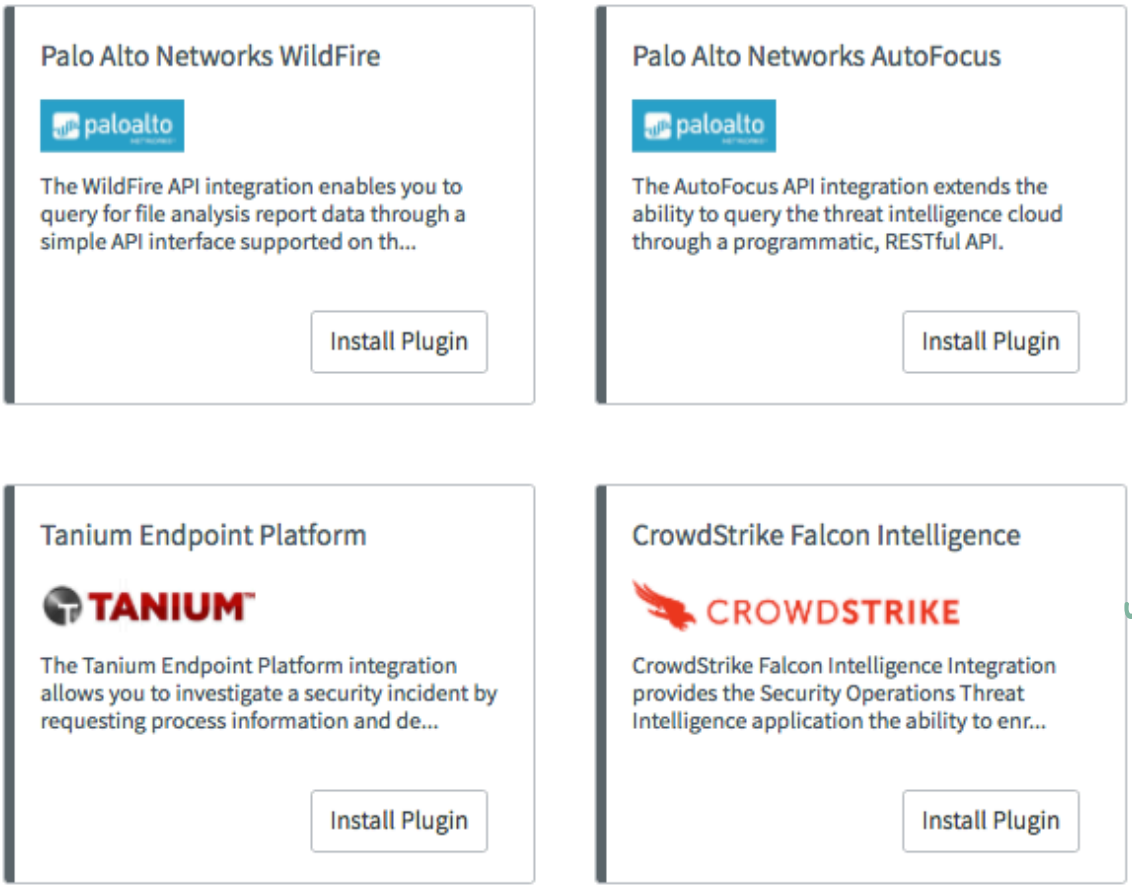
Antes de Iniciar
Função necessária: sn_sec_cmn.admin

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Configuração de Integração**.
   As integrações de segurança disponíveis aparecem como uma série de cartões, semelhantes ao grupo de cartões a seguir. Você pode apontar para qualquer cartão para obter uma descrição da integração.



2. Para instalar o plug-in de uma determinada integração, clique em **Instalar plug**-in.

   a. No formulário Plug-in do sistema, revise os detalhes do plug-in e clique no link relacionado **Ativar/ Atualizar**.

   b. Clique em **Ativar**.
   Quando a ativação estiver concluída, a tela Integração de segurança será reaberta e o botão da integração que você ativou será rotulado como **Configurar**.

3. Clique em **Configurar**.

   Nota:
   Se você estiver configurando o Qualys Vulnerability Integration, consulte Instalação de Vulnerability Response e aplicações compatíveis.

4. Insira a **Chave de API**.
5. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar uma integração

Você pode criar uma integração e adicionar o cartão de integração associado à tela Integrações de segurança. Este procedimento é destinado a parceiros que criam integrações de terceiros.

Antes de Iniciar

Função necessária: sn_sec_cmn.admin

Público:parceiros que criam integrações de terceiros.

Procedimento

1. No filtro de navegação, digite sn_sec_core_integration_item.list e pressione a tecla **Enter**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Nome	O nome da integração.
ID do plug-in	O plug-in que deve ser ativado para usar a integração.
Ordem	Indica a ordem em que este cartão de integração aparece.
Texto da faixa	Clique no link, selecione uma imagem ou logotipo a ser exibido no cartão de integração e clique em **OK**.
Instalada	Campo somente leitura que indica se o plug-in já foi instalado.
Configurável	Indica se você pode configurar a integração.
Categorias	Usado para filtrar os cartões de integração.
Descrição resumida	Uma descrição da integração que aparece na dica da ferramenta do cartão.
Descrição	Uma descrição mais longa da integração.

4. Clique com o botão direito no cabeçalho do formulário e selecione **Salvar**.
   A lista relacionada **Integração e configurações** é exibida. Você pode usar esta lista relacionada para definir opções de configuração para a integração. Essas opções aparecem quando você clica no botão **Configuração** no cartão de integração associado.
5. Clique em **Nova**.
6. Preencha os campos no formulário, conforme apropriado.

Campo	Descrição
Rótulo	O nome do item de integração.
Nome	O plug-in que deve ser ativado para usar a integração.
Integração	Exibe a integração para a qual você está definindo itens de integração
Ordem	Indica a ordem na qual este item de integração aparece.
Tipo	Na lista, selecione o tipo de campo:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Cadeia de caracteres ○ Inteiro ○ Decimal ○ Data ○ Booliano ○ Senha ○ IPv4 ○ IPv6 ○ URL
Valor	Insira o valor associado ao **Tipo** selecionado. Se um valor inválido para o **Tipo** selecionado for inserido, nenhum registro será recuperado quando a integração for executada. Por exemplo, se você selecionar o tipo de URL e inserir um valor de 12.32.23.10, nenhum registro será recuperado.

7. Clique em **Enviar**.

Dicas para escrever integrações

Evite algumas das dificuldades que você pode encontrar ao escrever suas próprias integrações, seguindo estas diretrizes.

Use a funcionalidade da plataforma ServiceNow sempre que possível

Em sua maioria, as capacidades de integração integradas nas aplicações [Security Operations (Security Incident Response, Inteligência contra ameaçase Vulnerability Response) têm como objetivo aprimorar ou simplificar a funcionalidade de integração da plataforma ServiceNow existente. Ao escrever integrações, sempre use a funcionalidade da plataforma quando ela existir. Estas são algumas funcionalidades ServiceNow comuns que podem ser usadas em vez de "criar o seu próprio".

- Serviços Web de saída - para a maioria das interações com sistemas de terceiros, a comunicação é por meio de serviços Web. Nesses casos, utilize os serviços Web de saída da plataforma (REST e SOAP são compatíveis).
- Fontes de dados/conjuntos de importação/mapa de transformação – para processar dados e inserir em tabelas ServiceNow, o mecanismo preferencial é usar fontes de dados e componentes associados.

Use estruturas de integração do Security Operations sempre que possível

Como os mecanismos de integração Security Operations resolveram muitos problemas comuns, não é necessário reimplementar as funcionalidades básicas para cada integração. Por exemplo, os dados de vulnerabilidade e as estruturas de origem da ameaça oferecem suporte à manipulação de várias páginas e à passagem desses dados para fontes de dados/transformações/conjuntos de importação. Da mesma forma, a estrutura de origem de verificação ou pesquisa fornece funcionalidade de limitação de taxa configurável. Como regra, ao implementar um recurso ou conjunto de recursos, verifique se a estrutura de integração Security Operations existente cobre seu caso de uso. Em caso afirmativo, use essa estrutura.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Estenda as estruturas de integração do Security Operations existentes conforme necessário

A maioria das tabelas e scripts usados pelas estruturas de integração Security Operations foram estendidas para atender às necessidades futuras. Se um caso de uso for encontrado enquanto você estiver gravando uma integração, estenda uma tabela de integração ou script para melhor atender a esse caso de uso.

Forneça feedback para a ServiceNow sobre problemas encontrados durante a integração

Conforme uma integração está sendo desenvolvida ou testada, forneça feedback quando forem encontrados problemas. Mesmo que uma solução alternativa seja necessária, a equipe de Suporte e atendimento ao cliente pode fornecer uma melhoria em versões futuras que podem atenuar o problema para integrações futuras.

Testar com carga razoável

Um problema comum com integrações é que elas não estão preparadas para lidar com cargas realistas. Como cada integração é uma aplicação com escopo, há mais limitações impostas pela plataforma para garantir a estabilidade do sistema. Essas limitações podem resultar no encerramento de trabalhos de longa execução ou de chamadas de API. Você pode garantir que processos de longa execução ou processos que processam muitos dados sejam tratados normalmente, reduzindo o tempo que cada chamada ou processo leva (geralmente fornecendo um meio de paginar solicitações de API ou agrupando grandes conjuntos de dados).

Solução de problemas de integração

Essas sugestões de solução de problemas podem ajudar a resolver problemas comuns que podem ser encontrados ao configurar ou executar integrações.

Substituir um certificado SSL de terceiros não confiável ou expirado

Quando uma conexão SSL é necessária em uma integração, há circunstâncias em que o certificado fornecido pelo fornecedor terceirizado ainda não é confiável em ServiceNow ou expirou. Você pode substituí-lo ou adicionar um novo certificado.

Antes de Iniciar
Função necessária: sn_ti.write

Procedimento

1. Adquira o certificado SSL do fornecedor terceirizado.
   Por exemplo, você pode importar um Certificado X.509 (PEM) de um endpoint SSL no navegador Firefox, da seguinte forma.

   a. Insira o URL do endpoint na barra de endereço do navegador.
      Por exemplo: https://<3rdparty>/.

   b. Clique no ícone de cadeado na linha de endereço.

   c. Clique em **Mais informações** e na guia **Segurança**.

   d. Clique em **Exibir certificado** e na guia **Detalhe**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

e. Clique em **Exportar** para salvar o PEM em seu sistema de arquivos local.

f. Abra o arquivo salvo em qualquer ferramenta de editor de texto e copie o conteúdo para a área de transferência.
Ele deve começar com `-----BEGIN CERTIFICATE-----` e terminar com `-----END CERTIFICATE-----`.

2. Navegar até **Definição do Sistema** > **Certificados**.
3. Clique em **Novo** e crie um novo registro para a integração.
4. Em **Certificado PEM**, cole o certificado que você baixou e copiou para a área de transferência anteriormente.
5. Clique em **Salvar**.
Os outros campos no registro são gerados automaticamente.

Estrutura de capacidades de integrações 2.0

O novo Integration Capabilities Framework 2.0 foi reprojetado para permitir a implementação de integrações de maneira simples e consistente. Isso garante uma experiência consistente para tipos semelhantes de integrações (por exemplo: pesquisa de reputação de observável).

A nova estrutura tem recursos implementados usando fluxos.

Os benefícios da implementação da estrutura aprimorada incluem:

- Os fluxos de capacidade que incluem somente componentes de nível de negócios sem qualquer lógica específica de implementação.
- Os fluxos de capacidade agora aceitam uma ampla matriz de entradas e formatos para máxima flexibilidade (por exemplo, referências observáveis, referências de IC, tarefas, qualquer tabela ou combinações de sys_id).
- A limitação ou limitação de taxa nas execuções de integração agora são fáceis de configurar (removendo a necessidade de fazer isso usando código personalizado ou mudanças nos fluxos de trabalho de implementação).
- As capacidades aprimoradas de auditoria e acompanhamento de execução agora permitem relatórios melhores e uma solução de problemas mais fácil.
- Funções robustas de tratamento de erros são integradas aos fluxos de capacidade para evitar a duplicação de rotinas de implementação.
- Capacidade de configurar o gatilho condicional dos recursos ou das integrações. Isso fornece flexibilidade para iniciar automaticamente automações com base na categoria de incidente.
- Uma condição de filtro padrão foi introduzida em todos os recursos para filtrar observáveis listados antes que as entradas sejam fornecidas para as integrações.

Nota:
Esta nova estrutura de recursos não atualiza a estrutura de recursos atual. Ambas as estruturas podem funcionar em paralelo. Para obter instruções sobre como aproveitar a nova estrutura de recursos, consulte Usando o novo Capability Framework com uma integração instalada e Como usar o novo Capability Framework com um fluxo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Integrações e componentes compatíveis

O plug-in Security Incident Response inclui todos os fluxos de recursos listados no Integration Capabilities Framework 2.0 e filtros de alto nível padrão que você pode habilitar ou desabilitar, dependendo do seu requisito.

Nota:
Se você quiser usar o novo Capability Integration Framework com a versão New York, deverá instalar o plug-in ServiceNow IntegrationHub Starter Pack Installer. Entre em contato com o Suporte ao cliente para obter assistência com a instalação.

Versões da aplicação compatíveis

A partir do Security Incident Response 10.0, as seguintes integrações são compatíveis:

Aplicação	Versão mínima necessária
Security Operations Hybrid Analysis Integration	10.0.0
Security Operations PhishTank Integration	10.0.0
Security Operations ThreatCrowd Integration	10.0.0
Security Operations CrowdStrike Intelligence Integration	10.0.0
Security Operations "Recebi uma doação?" Integração	10.0.0
Integração do Metadefender do Security Operations	10.0.0
Integração futura registrada do Security Operations	10.0.0
Security Operations VirusTotal Integration	10.0.0
Integração reversa de WhoIs do Security Operations	10.0.0

A partir do Security Incident Response 10.4, as seguintes integrações são compatíveis:

Aplicação	Versão mínima necessária
Security Operations RiskIQ Integration	10.0.0
Security Operations Shodan Integration	10.0.0
Integração WhoIs do Security Operations	10.0.0
Security Operations Carbon Black Integration	10.3.1
Security Operations Splunk Search Integration	10.3.0
Security Operations ArcSight Logger Integration	10.3.0
Security Operations McAfee ESM Integration	10.3.0
Security Operations Elasticsearch Integration	10.3.0
Security Operations IBM QRadar Integration	10.3.1
Host CrowdStrike Falcon do Security Operations	10.3.0

Componentes incluídos

O novo Capability Integration Framework inclui os seguintes componentes:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Recursos**: todos os recursos a seguir que existem no produto hoje como fluxos de trabalho foram reprojetados usando fluxos :
  - **Solicitação de bloqueio**: fornece uma maneira de bloquear observáveis associados a um incidente de segurança em um firewall, proxy da web ou algum outro ponto de controle. Essa capacidade é usada durante as investigações de resposta do incidente com uma ameaça identificada.
  - **Pesquisa e exclusão de e-mail**: fornece uma maneira de pesquisar um servidor de e-mail durante uma investigação de segurança e, se necessário, excluir e-mails do servidor.
  - **Aprimorar item de configuração**: fornece uma maneira geral de aprimorar itens de configuração com informações adicionais de várias fontes. Esta capacidade é usada durante as investigações de resposta do incidente para aprimorar os dados associados a um incidente de segurança.
  - **Aprimorar observável**: fornece uma maneira geral de aprimorar observáveis com informações adicionais de várias fontes. Essa capacidade é usada durante as investigações de resposta do incidente com uma ameaça identificada.
  - **Ingestão de eventos**: fornece uma maneira geral de criar um incidente de segurança mapeando eventos de uma origem de integração para um incidente de segurança.
  - **Obter estatísticas de rede**: recupera uma lista de conexões de rede ativas de um endpoint ou host. Essa capacidade é usada para aprimoramento de incidentes durante as investigações.
  - **Obter processos em execução**: recupera uma lista de processos em execução de um endpoint ou host. Essa capacidade é usada para aprimoramento de incidentes durante as investigações.
  - **Isolar host**: fornece uma maneira de isolar um endpoint ou um host associado a um incidente de segurança. Isolar host é executado em um item de configuração (IC).
  - **Publicar na lista**de observação: fornece uma maneira de adicionar observáveis associados a um incidente de segurança a uma lista de observação que monitora eventos de segurança e gera alertas. Essa capacidade é usada como parte da resposta do incidente durante as investigações.
  - Pesquisa de vistas: pesquisa vários**SIEMs**ou outros armazenamentos de log para instâncias de observáveis. Esta funcionalidade é usada para determinar a presença de IoCs mal-intencionados em seu ambiente.
  - **Pesquisa de ameaças**: executa pesquisas de inteligência contra ameaças para determinar se um determinado observável está associado a uma ameaça à segurança conhecida. Essa capacidade é usada como parte da resposta do incidente durante as investigações.
- **Novas tabelas**:
  - sn_sec_cmn_capability: recurso e fluxo que implementa o recurso.
  - sn_sec_cmn_capability_implementation: o fluxo de implementação real que fornece os serviços da funcionalidade.
  - sn_sec_cmn_capability_execution: o registro de execução de uma capacidade no tempo de execução.
  - sn_sec_cmn_capability_implementation_execution: o registro de execução de uma implementação de recurso no tempo de execução.
  - sn_sec_cmn_filter_condition: as condições de filtro que podem ser aplicadas no tempo de execução à funcionalidade ou a uma implementação de funcionalidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Incluir script**: CapabilityProcessor: lida com todo o código de processamento da estrutura.
- **Limite de taxa**: capacidade máxima de solicitações simultâneas por período: define quantas integrações podem ser executadas em paralelo.
- **Implementação da capacidade do processo de trabalho programado**: é executado a cada 15 segundos e pode ser desabilitado na página Propriedades de administração de segurança (**Incidente de segurança** > **Administração** > **Propriedades**.
  - Habilita ou desabilita o trabalho programado, Processar implementações de capacidade: este trabalho programa e gerencia automaticamente os fluxos de execução de implementação de capacidade.
  - Habilita ou desabilita pesquisas ou aprimoramentos automatizados: configuração que ativa ou desativa o trabalho programado que executa a pesquisa de ameaças automatizada ou o aprimoramento de observáveis quando observáveis são adicionados a incidentes de segurança na estrutura de recursos atual.
  - Habilita ou desabilita o trabalho programado, Pesquisar observáveis de incidente de segurança: este trabalho programa automaticamente uma Pesquisa de ameaças ou Aprimorar observáveis quando observáveis são adicionados a um incidente de segurança.

Configurações no novo Capability Framework

Esta seção descreve as configurações disponíveis na nova estrutura.

Antes de Iniciar

Função necessária: sn_si.admin, flow_designer, action_designer

Procedimento

1. Navegar até **Tudo** > **Security Operations** > **Integrações** > **Habilidades**.

> **Nota:**
> Versão 10.4: a partir do Security Incident Response 10.4, o nome do menu **Recursos** foi alterado para **Recursos de integração (fluxos)**.

2. Os recursos disponíveis com o sistema de base são exibidos.

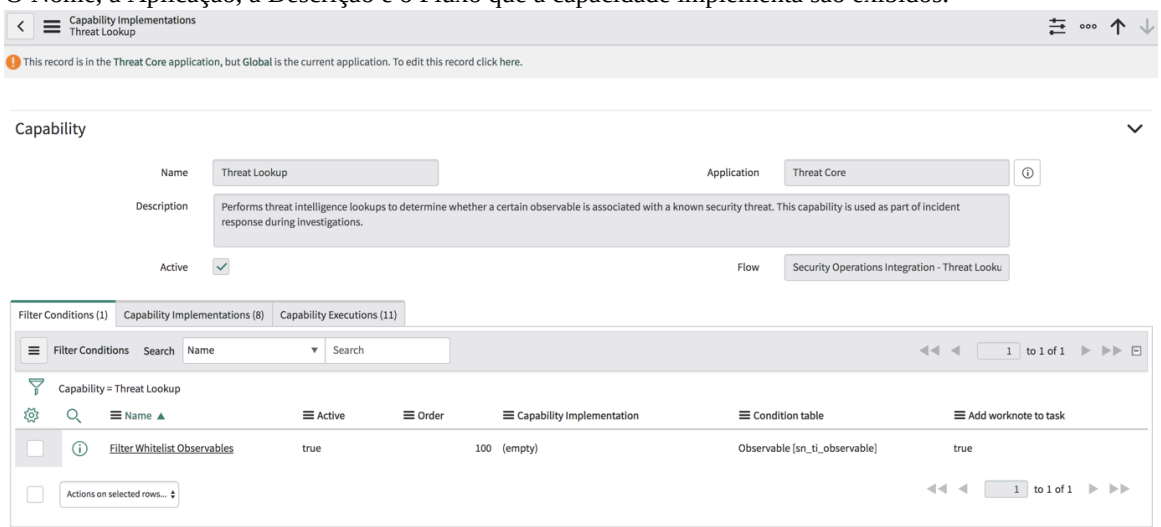
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:

Esses são os recursos fornecidos com o sistema de base. Você pode usar os recursos ou personalizá-los conforme necessário. As etapas a seguir descrevem como configurar um recurso e as integrações implementadas para o recurso.

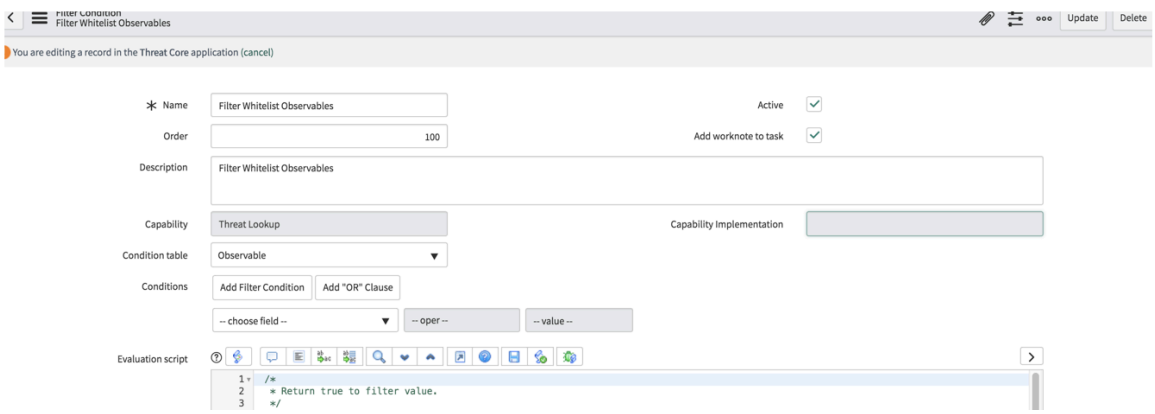
3. Clique no link na coluna Nome para configurar um recurso.
   O Nome, a Aplicação, a Descrição e o Fluxo que a capacidade implementa são exibidos.



4. Marque a caixa de seleção **Ativo** para ativar o recurso.

   - **Condições de filtro no nível de recurso**: quando um recurso de integração implementa um fluxo, as condições de filtro associadas ao fluxo serão executadas antes que o fluxo de recurso seja iniciado. Por exemplo, a funcionalidade Pesquisa de ameaças inclui a condição Filtrar observáveis na lista de permissões, conforme mostrado acima. Clique no link Nome para editar a condição do filtro.

     Nota:
     Marque a caixa de seleção **Adicionar anotação de trabalho à tarefa** para adicionar anotações de trabalho e incluir informações sobre as condições de filtro usadas.



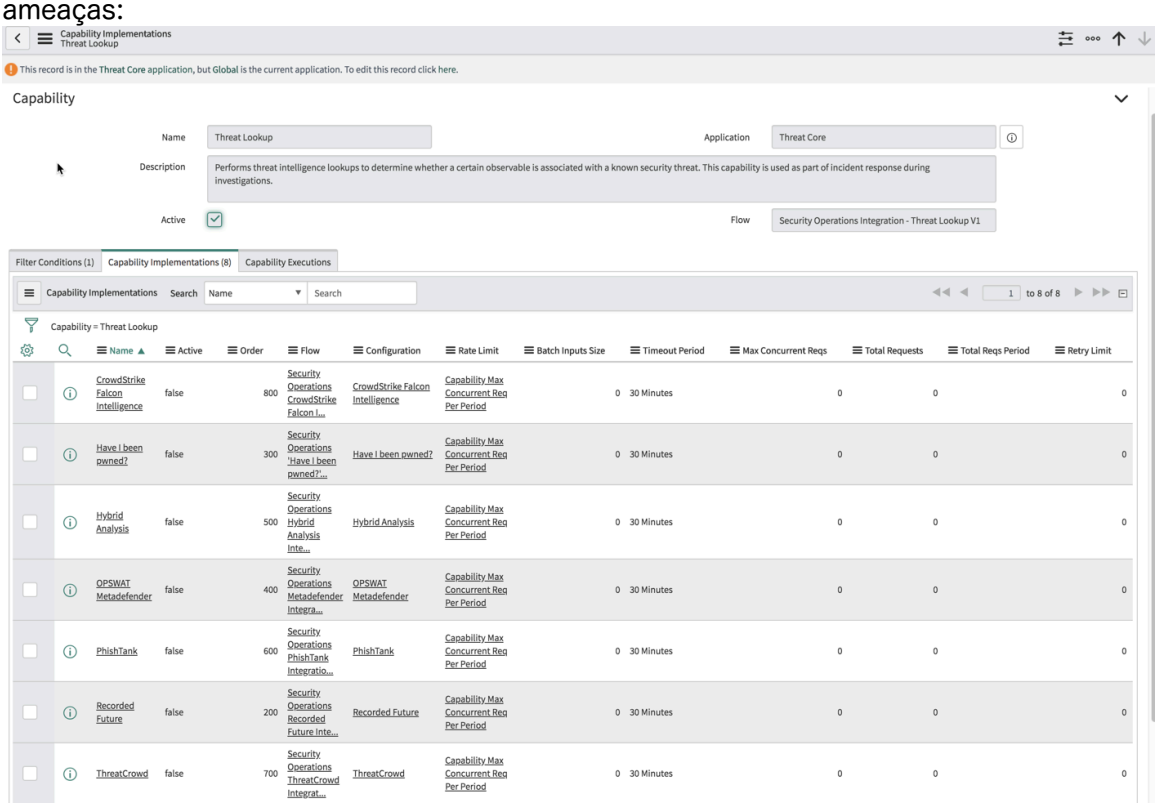
   Você pode definir condições de filtro ou um script ou uma combinação de ambos. No exemplo acima, um script é usado para definir as condições do filtro. Quando o fluxo de recursos é executado, o script pesquisa observáveis da lista de permissões e os remove da tabela.

Tradução automática

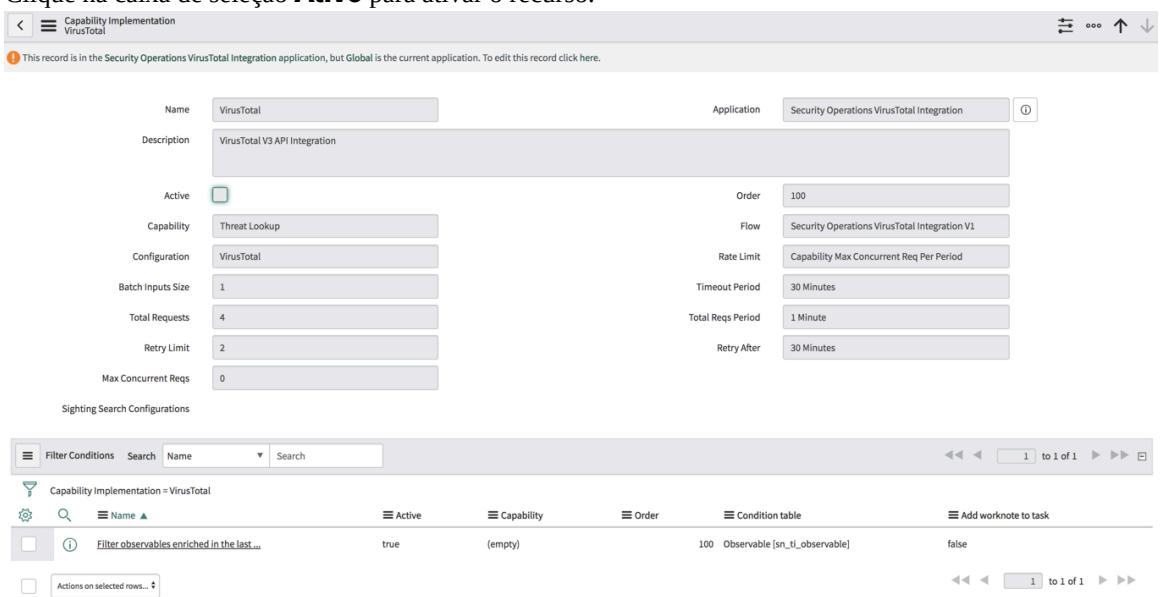
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
As condições de filtro definidas aqui são aplicáveis a todas as integrações ativas definidas na guia **Implementações de capacidade**.

- **Implementações de capacidade**: clique na guia **Implementações de capacidade**. As implementações (integrações) que foram configuradas para o recurso são exibidas. O exemplo abaixo mostra as integrações configuradas para a funcionalidade Pesquisa de ameaças:



5. Clique no link Nome para exibir a Implementação de capacidade.
   O Nome, a Aplicação, a Descrição e o Fluxo que a funcionalidade implementa são exibidos.
6. Clique na caixa de seleção **Ativo** para ativar o recurso.

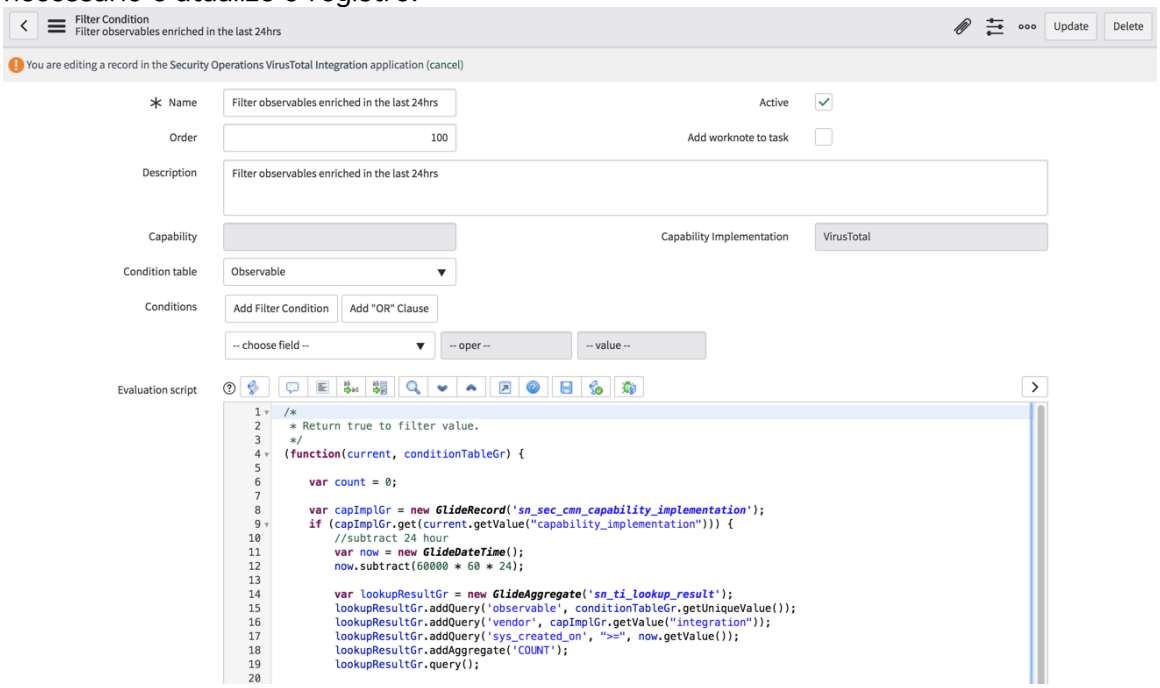


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você pode especificar os seguintes detalhes:

Clique no link Nome na seção Condições do filtro para configurar as condições definidas para a implementação. Adicione ou exclua condições de filtro, modifique o script se necessário e atualize o registro.



Usando o novo Capability Framework com uma integração instalada

Esta seção descreve como usar a nova estrutura para uma integração existente.

Use as etapas abaixo para habilitar uma integração já instalada e configurada (consulte a lista de integrações compatíveis em Integrações e componentes compatíveis) para usar a nova estrutura de recursos.

Nota:
O Integration Capability Framework 2.0 disponível com o Security Incident Response 10.0.2 oferece suporte a implementações dos recursos **Pesquisa de ameaças** e **Aprimorar observável**. Implementações para outros recursos serão disponibilizadas em uma versão futura.

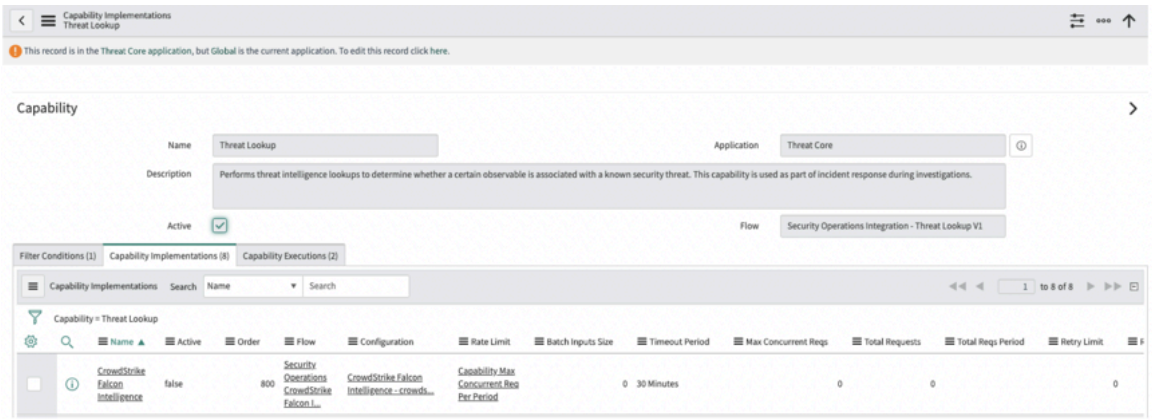
Antes de começar

- Função necessária: sn_si.admin
- Security Incident Response 10.0.2

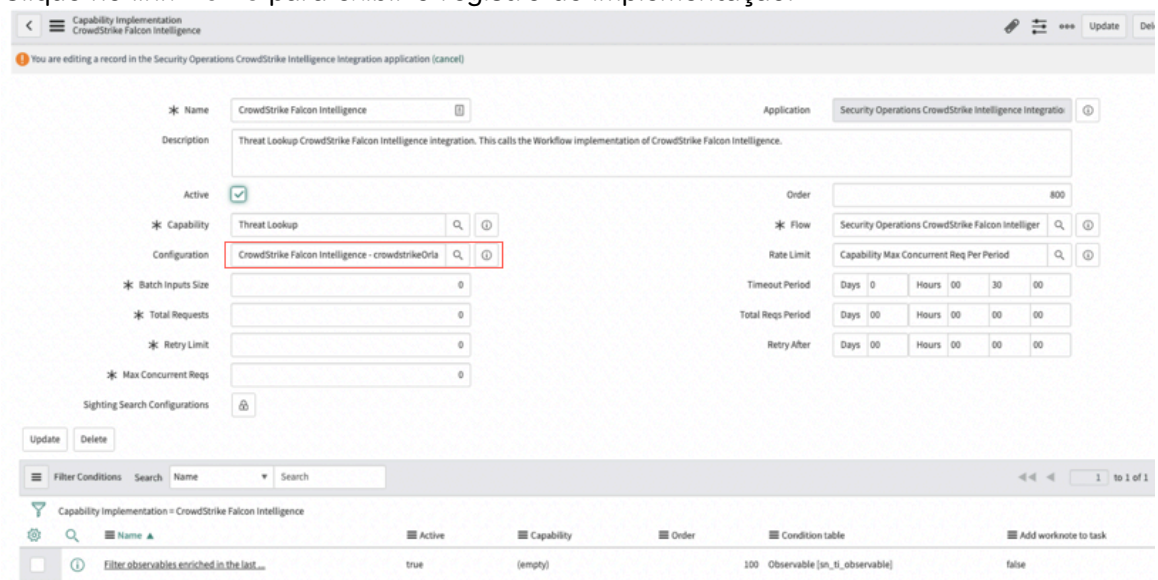
1. Navegar até **Security Operations** > **Integrações** > **Habilidades**.
2. Clique no recurso **Pesquisa de ameaças**.
3. Clique na guia Implementação de recursos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



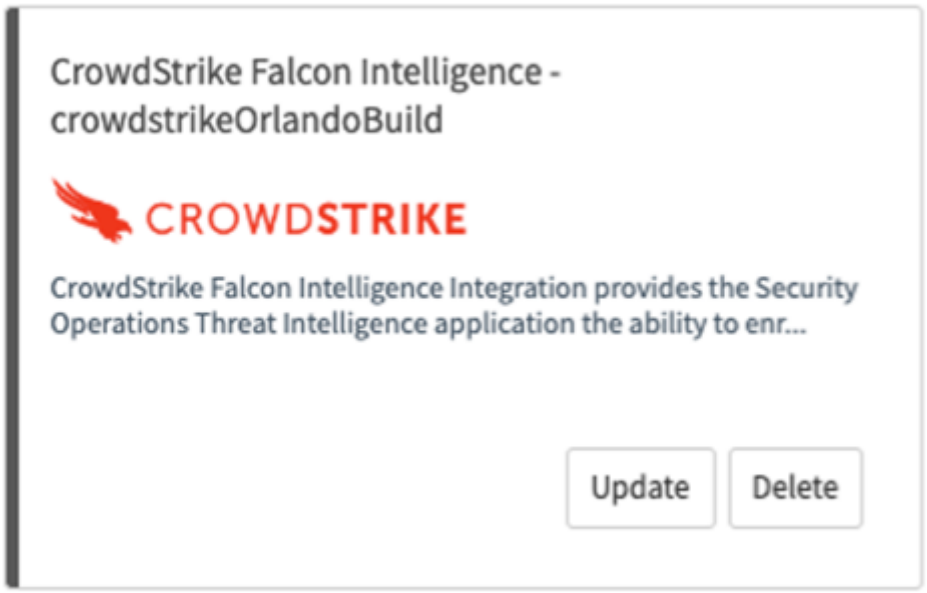
4. 4. Exiba o registro de implementação de capacidade da integração de interesse (exemplo: Crowdstrike Falcon Intelligence). A coluna **Ativa** deve ter o valor **Falso**.
5. Clique no link **Nome** para exibir o registro de implementação.



6. Marque a caixa de seleção **Ativo**.
7. Certifique-se de que o registro de implementação esteja apontando para o registro de configuração correto (o nome do bloco para a integração em **Configurações de Integração** > **Mostrar configurações (Sim)**).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



8. A implementação está habilitada para uso com a nova estrutura.

Nota:
Todas as integrações compatíveis quando instaladas com o Security Incident Response 10.0.2 serão habilitadas automaticamente na nova estrutura de capacidade de integração.

Como usar o novo Capability Framework com um fluxo

Use as etapas abaixo para criar um fluxo e chamar o subfluxo fornecido pela nova estrutura de recursos.

Antes de Iniciar

- Função necessária: sn_si.admin, flow_designer, action_designer
- Instale uma das integrações compatíveis (consulte Integrações e componentes compatíveis)

As etapas abaixo descrevem como criar um fluxo de amostra e chamar um dos subfluxos fornecidos com a nova estrutura de recursos.

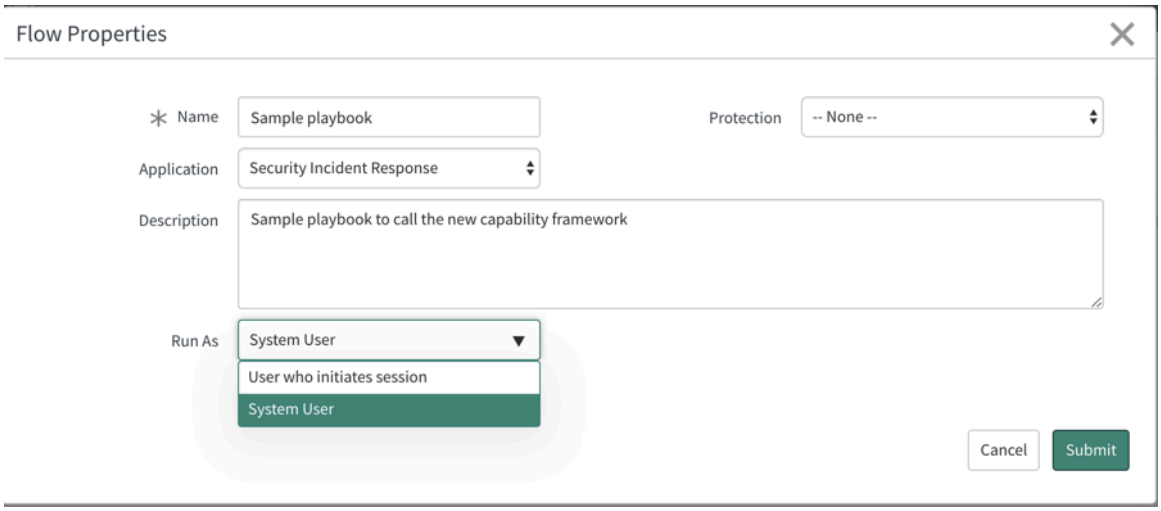
Procedimento

1. Navegar até **Tudo** > **Flow Designer** > **Designer**.

2. Clique em **Novo** para criar um novo fluxo e fornecer as informações necessárias para as propriedades.

Tradução automática

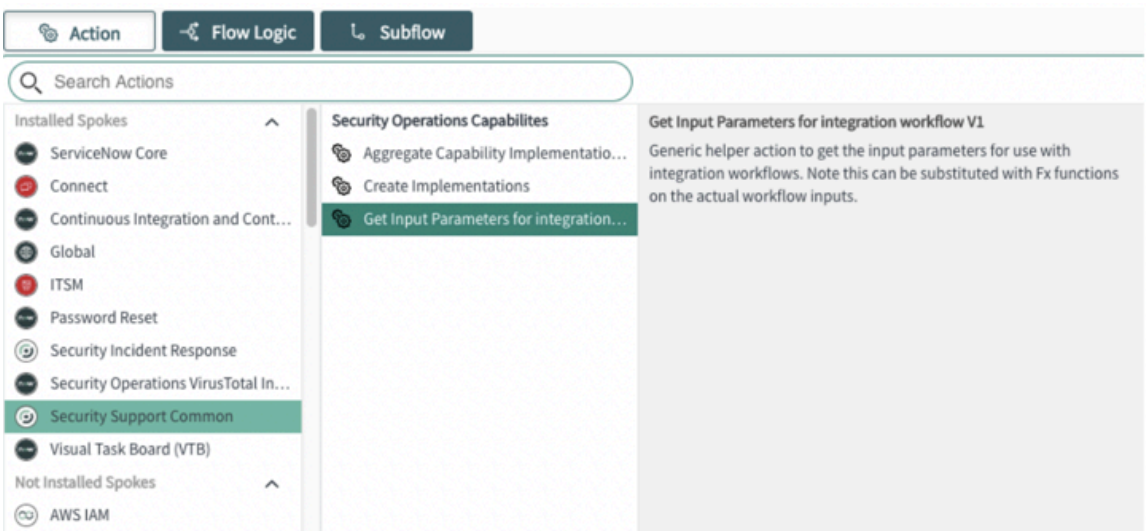
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Nota:
Selecione **Usuário do sistema** na lista de seleção Executar como, conforme mostrado na imagem acima.

3. Selecione uma condição do gatilho para o fluxo (um gatilho comum é a criação de um registro de incidente de segurança para uma determinada categoria de incidente).

4. Na etapa 1 do fluxo, selecione uma ação para obter entradas do incidente de segurança (por exemplo, observáveis).
Você pode selecionar uma ação das ações fornecidas com o sistema de base com o Security Support Common Spoke.

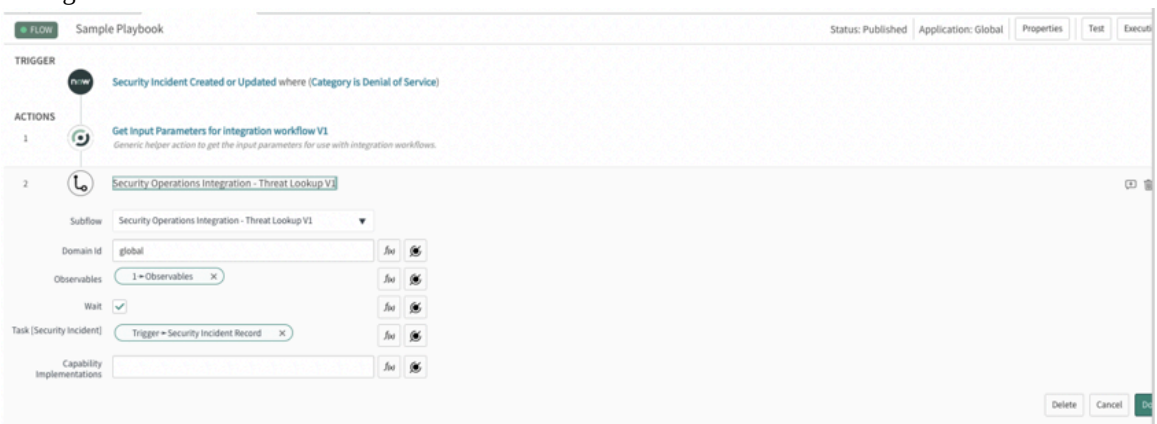


5. Na etapa 2, selecione um subfluxo (por exemplo, Pesquisa de ameaças).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

6. Configure o subfluxo selecionado conforme mostrado abaixo:



7. Salve e publique o fluxo.

Fluxos de capacidade de integração de solução de problemas

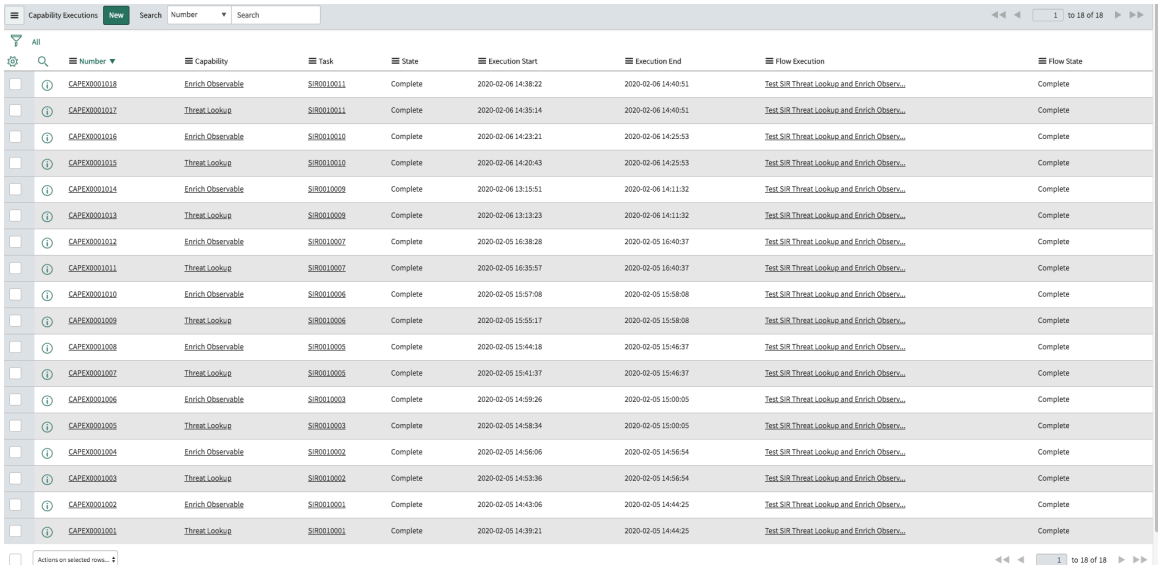
A opção Execuções de capacidade fornece informações detalhadas sobre cada capacidade que foi executada.

Nota:
As execuções concluídas são arquivadas após 30 dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

1. Navegar até **Security Operations** > **Integrações** > **Execuções de capacidade.**.



2. Clique no link Execuções de capacidade para exibir detalhes adicionais.

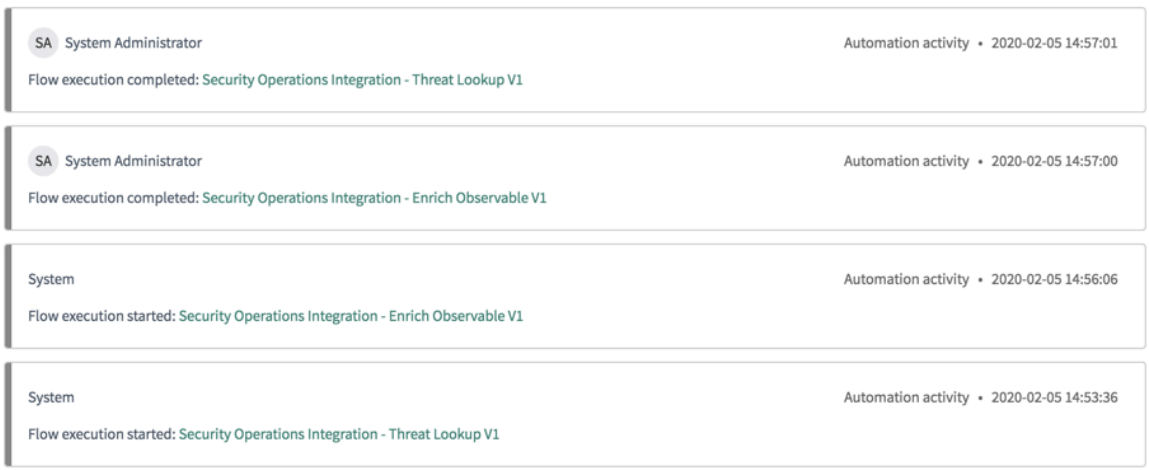
Anotações de trabalho de registro de incidente de segurança

Quando os observáveis são adicionados a um incidente de segurança e a condição do gatilho para o fluxo é atendida, os subfluxos Pesquisa de ameaças e Aprimorar observável são iniciados e as seguintes anotações de trabalho são adicionadas ao incidente de segurança:

- Execução de fluxo iniciada: Security Operations Integration - Aprimorar observável V1
- Execução de fluxo concluída: Security Operations Integration - Enrich Observable V1
- Execução de fluxo iniciada: Security Operations Integration – Pesquisa de ameaças V1
- Execução de fluxo concluída: Security Operations Integration – Pesquisa de ameaças V1

Para exibir essas anotações de trabalho, faça login como um usuário com as *funções* `sn_si.admin` ou `sn_si.analyste` `flow_designer`e `action_designer`.

Navegue até a página de registro do incidente de segurança e clique nessas anotações de trabalho para exibir os detalhes da execução do fluxo.



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

REST APIs para integração de terceiros com Security Operations

O sistema base Security Operations inclui uma série de REST APIs de script que permitem que clientes e parceiros se integrem facilmente a uma implantação Security Operations existente. As APIs permitem coletar dados de fora do seu sistema (por exemplo, um script Python é usado para receber dados do VirusTotal) e enviá-los de volta para sua instância.

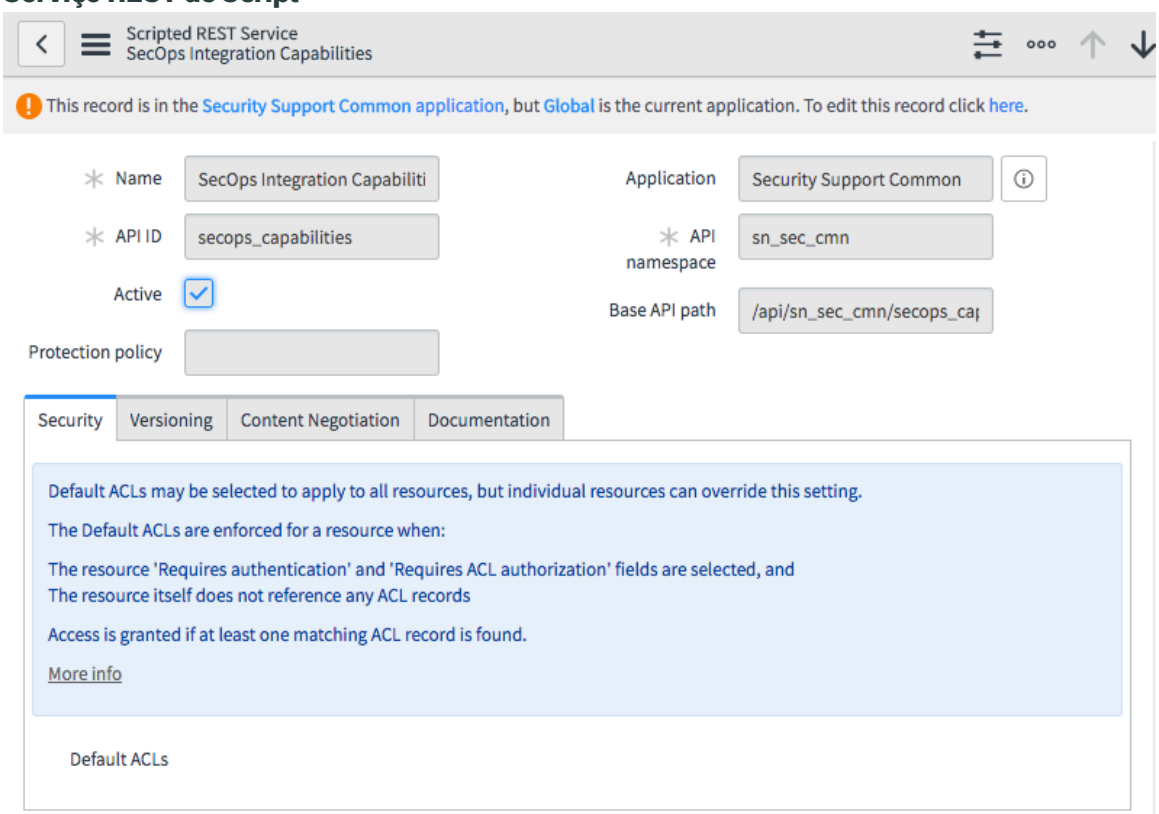
Scripts escritos em praticamente qualquer linguagem (Python, por exemplo) podem ser usados com as APIs para executar processos específicos do cliente. Os scripts devem ser escritos em um idioma capaz de fazer uma chamada HTTP Post externa. Por exemplo, se você tiver uma aplicação Java, deverá usar uma biblioteca, como o pacote java.net.HttpUrlConnection, para construir uma chamada HTTP e passar uma cadeia de caracteres JSON como corpo da mensagem.

A API é usada exclusivamente para adicionar dados que foram coletados fora do nosso sistema. Por exemplo, se você inseriu o script python do VT e recebeu dados do VT, poderá enviar esses dados de volta para a instância SN.

Autenticação

Todas as operações nas definições de API usam a autenticação de plataforma fornecida pelo Recurso de operação deScripted REST APIs . Para acessar, navegue até **Serviços web do sistema** > **Scripted Web Services** > **Scripted REST APIs** e localize a API **de capacidades de integração de SecOps**.

Serviço REST de Script



O usuário e o domínio do usuário estão prontamente disponíveis no contexto da API. Os registros podem ser vinculados a um usuário, um caminho de auditoria a ser estabelecido e a separação de domínio realizada. Além disso, como você está autenticado como um usuário específico, pode usar Usando GlideRecordSecure para impedir qualquer acesso não autorizado aos dados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Autorização

Para proteger o processo de criação de registros de usuários fora da aplicação Security Operations, você deve ter a função sn_sec_cmn.api_write. Somente usuários com esta função podem acessar as APIs.

Parâmetros de solicitação de configuração

Os parâmetros de solicitação a seguir estão disponíveis.

Nome	Padrão	Descrição
ignore_mandatory_fields	falso	Se definido como verdadeiro, o registro persistirá mesmo se os campos obrigatórios não forem preenchidos.
include_wrap	falso	Se definido como verdadeiro, a resposta incluirá o wrapper padrão fornecido pela instância para Scripted REST APIs.
resposta_simples	falso	Se definido como verdadeiro, a resposta incluirá somente se a operação foi bem-sucedida.

Respostas de erro

As seguintes respostas de erro podem ocorrer.

Mensagem de erro	Quando isso ocorre?	Solução
Acesso insuficiente	O usuário não tem a função sn_sec_cmn.api_write.	Adicione a função ao usuário.
Corpo de publicação inválido	O corpo da solicitação está vazio ou é um objeto vazio.	Em conformidade com a definição da API.
Nenhum campo fornecido	Os campos de dados fornecidos para persistir estão vazios.	Em conformidade com a definição da API.
Campos obrigatórios ausentes: x, y, z	Os campos obrigatórios estão ausentes.	Cumpra a definição da tabela de destino ou defina **ignore_mandatory_fields** como verdadeiro.
Não é possível manter o registro	Não é possível manter o registro analisado.	Falha ao inserir GlideRecord (), análise adicional é necessária.
Erro desconhecido	Ocorre se nenhum caminho de erro conhecido tiver sido seguido.	Uma análise mais aprofundada é necessária.

caso de uso de aprimoramento de IC

Usando seus scripts de terceiros, você pode gravar na tabela Aprimoramento de item de configuração [sn_sec_cmn_ci_enrichment_result] para aprimoramento de IC. Os registros de aprimoramento são baseados em recursos existentes que fornecem informações detalhadas sobre um registro de uma fonte de terceiros.

Solicitação de amostra e respostas para o caso de uso de aprimoramento de IC são mostradas aqui.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar solicitação para aprimoramento de IC


```
{
   "ignore_mandatory_fields": true,
   "payload": [
      {
         "configuration_item_id": "2dfd7c8437201000deeabfc8bcbe5d56",
         "data": [
             {
               "external_link": "http://www.servicenow.com",
               "vendor": "aafbf46ad72212007a6de294de6103a2",
               "data_type": null,
               "source": null,
               "name": null,
               "parent": null,
               "summary": "Found 1000 open vulnerabilities on the specified
               configuration item",
               "retrieval_date": "2017-09-05 08:56:28"
             }
          ]
      }
   ]
}
```


Criar resposta para aprimoramento de IC


```
{
   "success": true,
   "status": "success",
   "payload": {
        "results": [
            {
                "sys_id": "2dfd7c8437201000deeabfc8bcbe5d56",
                "reference_url":
                "http://10.0.214.15:8080/nav_to.do?uri=cmdb_ci.do?sys_id=2dfd7c8437201000
                deeabfc8bcbe5d56",
                    "results": [
                        {
                            "sys_id": "4a8b92fb0b410300263a089b37673a33",
                            "reference_url":
                            "http://10.0.214.15:8080/nav_to.do?uri=sn_sec_cmn_ci_
                        enrichment_result.do?sys_id=4a8b92fb0b410300263a089b37673a33"}
                    ]
                }
            ],
            "domain": "global",
            "configuration_item_ids": [
            "2dfd7c8437201000deeabfc8bcbe5d56"
        ]
    }
}
```


Tradução automática

Caso de uso de aprimoramento de observável

Usando seus scripts de terceiros, você pode gravar na tabela Resultado de aprimoramento observável [sn_ti_observable_enrichment_result] para aprimoramento observável. Os registros de aprimoramento são baseados em recursos existentes que fornecem informações detalhadas sobre um registro de uma fonte de terceiros.

Solicitação de amostra e respostas para o caso de uso de aprimoramento observável são mostradas aqui.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar-Solicitação de aprimoramento observável

```
"ignore_mandatory_fields": true,
  "payload": [
    {
      "observable_value": "http://www.google.com",
      "security_incident_ids": [
        "9424d4e10b110300263a089b37673a21"
      ],
      "enrichment_mapping_id": "9fa7d4590b622200263a089b37673a1d",
      "data": [{
        "vendor": "f15a46140b622200263a089b37673a7e",
        "summary": "Registrar:MarkMonitor, Inc., Registration Date:1997-09-15,
            Expiration Date:2020-09-14, Registrant country:UNITED STATES",
        "data_type": "json",
        "retrieval_date": "2017-08-30 10:35:02",
        "raw_data": "{\"WhoisRecord\":{\"administrativeContact\":{\"city\":
            \"Mountain View\",\"country\":\"UNITED STATES\",\"email\":
            \"dns-admin@google.com\",\"fax\":\"16506188571\",\"name\":
            \"DNS Admin\",\"organization\":\"Google Inc.\"}"
      }]
    }
  ]
}
```

Criar resposta para aprimoramento de observável

```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "43bd3f210b510300263a089b37673ac6",
                "reference_url": "http://10.0.65.185:8080/sn_ti_observable.do?
                    sys_id=43bd3f210b510300263a089b37673ac6&sys_target=&XML",
                "results": [
                    {
                        "sys_id": "0bbd3f210b510300263a089b37673acc",
                        "reference_url": "http://10.0.65.185:8080/sn_ti_observable_
                            enrichment_result.do?sys_id=0bbd3f210b510300263a089b37673acc
                                &sys_target=&XML"
                    }
                ]
            }
        ],
        "domain": "global",
        "observable_ids": [
            "43bd3f210b510300263a089b37673ac6"
        ]
    }
}
```

Nota:
Além de aprimorar os registros existentes, você também pode usar Security Operations mapeamento de dados de aprimoramento para adicionar novos registros a tabelas passando em um **richment_mapping_id** para um mapeamento de aprimoramento existente e uma cadeia de caracteres **bruta_data** correspondente que pode ser analisada pelo processo de mapeamento.

Caso de uso de pesquisa de ameaças

Usando seus scripts de terceiros, você pode gravar na tabela Resultado de pesquisa de ameaças [sn_ti_lookup_result] para obter resultados de pesquisa de ameaças. Os registros

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

de pesquisa são baseados em recursos existentes que fornecem informações detalhadas sobre um registro de uma fonte de terceiros.

Solicitação de amostra e respostas para o caso de uso de pesquisa de ameaça são mostradas aqui.

Criar solicitação para pesquisas de ameaças


```
{
"simple_response": false,
"include_wrapper": true,
  "ignore_mandatory_fields": false,
  "payload": [
    {
      "request_element_correlation_id": "1",
      "observable_value": "128.214.67.80",
      "data": [
        {
          "request_element_correlation_id": "2",
          "finding": "Malicious6",
          "source_engine": "VirusTotal API",
          "vendor": "aafbf46ad72212007a6de294de6103a2",
          "data_type": null,
          "source": null,
          "name": null,
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        },
        {
          "finding": "Malicious8",
          "source_engine": "VirusTotal API",
          "source_engine_version": "v2",
          "first_found": "2000-09-05 15:56:28",
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        }
      ]
    }
  ]
}
```


Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar resposta para pesquisas de ameaças


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "a0bddafb0b410300263a089b37673a93",
                "reference_url":
                    http://10.0.214.15:8080/nav_to.do?uri=sn_ti_observable.do?sys_id=
                        a0bddafb0b410300263a089b37673a93,
                    "request_element_correlation_id": "1",
                    "results": [
                        {
                            "sys_id": "24bddafb0b410300263a089b37673a95",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?sys
                            _id=24bddafb0b410300263a089b37673a95,
                    "request_element_correlation_id": "2",
                },
                {
                    "sys_id": "e8bddafb0b410300263a089b37673a96",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?
                            sys_id=e8bddafb0b410300263a089b37673a96
                            }
                        ]
                    }        ],
                "domain": "global",
                "observable_ids": [
                    "a0bddafb0b410300263a089b37673a93"        ]
    }
}
```


Capacidades de integração

A estrutura Capacidades de integração fornece uma arquitetura consistente para oferecer suporte à interoperabilidade com integrações de terceiros. Essa interface e modelo de dados abstratos isolam as integrações de mudanças na aplicação principal e garantem uma experiência consistente para tipos semelhantes de integrações.

Cada capacidade de integração persiste na tabela Capacidade de integração [sn_sec_cmn_integration_capability]. Os fluxos de trabalho de capacidade de integração não podem ser executados sozinhos e exigem o início de um fluxo de trabalho de implementação. Qualquer plug-in que forneça uma implementação da funcionalidade adiciona sua implementação à tabela secundária: Integration Capability execution [sn_sec_cmn_integration_capability_implementation].

A implementação especifica o fluxo de trabalho a ser executado, a integração relacionada (ID do plug-in) e a capacidade que ele implementa. Esses fluxos de trabalho podem ser executados em paralelo usando o inicializador de fluxo de trabalho paralelo; no entanto, a execução sequencial é o padrão no sistema de base. Se necessário, você pode mudar a ordem de execução.

Nota:
Se não houver implementações disponíveis, as ações de recurso não serão exibidas nos menus do produto.

Integração do Security Operations - Capacidade de solicitação de bloqueio

A capacidade Bloquear Ação bloqueia observáveis associados a um incidente de segurança em um firewall, proxy da web ou outro ponto de controle, usando fluxos de trabalho de implementação. Essa capacidade é usada durante as investigações de resposta do incidente com uma ameaça identificada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A funcionalidade Solicitação de Bloqueio tem um fluxo de trabalho, Integração do Security Operations - Fluxo de trabalho de solicitação de bloqueio, que executa a solicitação para bloquear. Este fluxo de trabalho aceita uma lista de observáveis, encontra todos os recursos de implementação e executa a solicitação com base no fluxo de trabalho configurado.

A capacidade também usa outras implementações:

- Fluxo de trabalho de integração do Security Operations Palo Alto Networks inicializador de firewall
- Security Operations Palo Alto Networks - Fluxo de trabalho de verificar e bloquear valor

Nota:
Se não houver implementações disponíveis, as ações de recurso não serão exibidas nos menus do produto.

Executar bloqueio de solicitação

Bloqueia a comunicação com observáveis associados a um incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

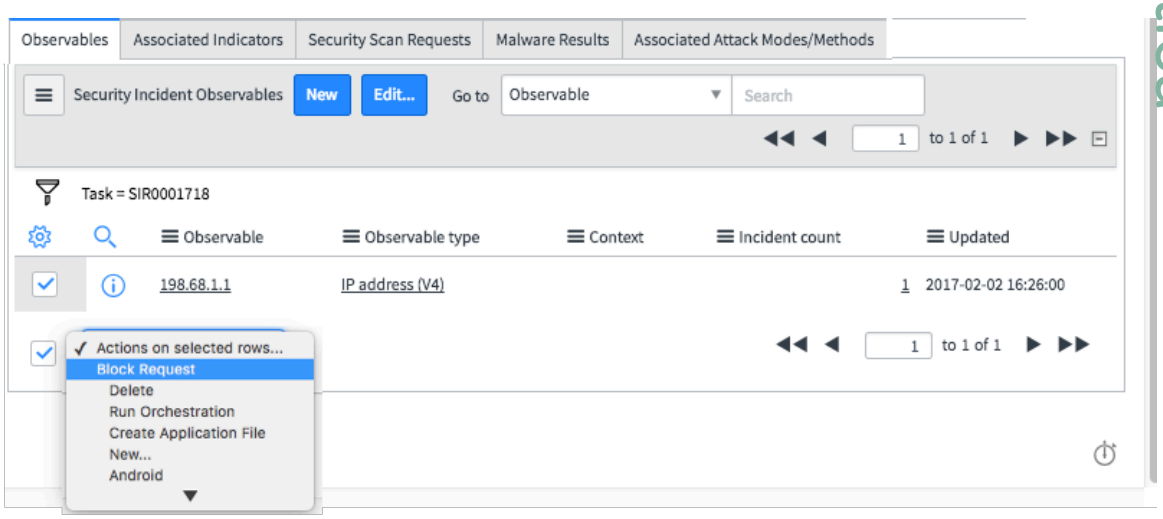
Nota:
Se não houver implementações disponíveis, as ações de recurso não serão exibidas nos menus do produto.

O fluxo de trabalho **Integração do Security Operations - Solicitação de bloqueio**pode ser acionado a partir de um formulário observável ou da lista relacionada **de Observáveis** de incidente de segurança em um incidente de segurança.

Este exemplo mostra uma Solicitação de Bloqueio de um incidente de segurança.

Procedimento

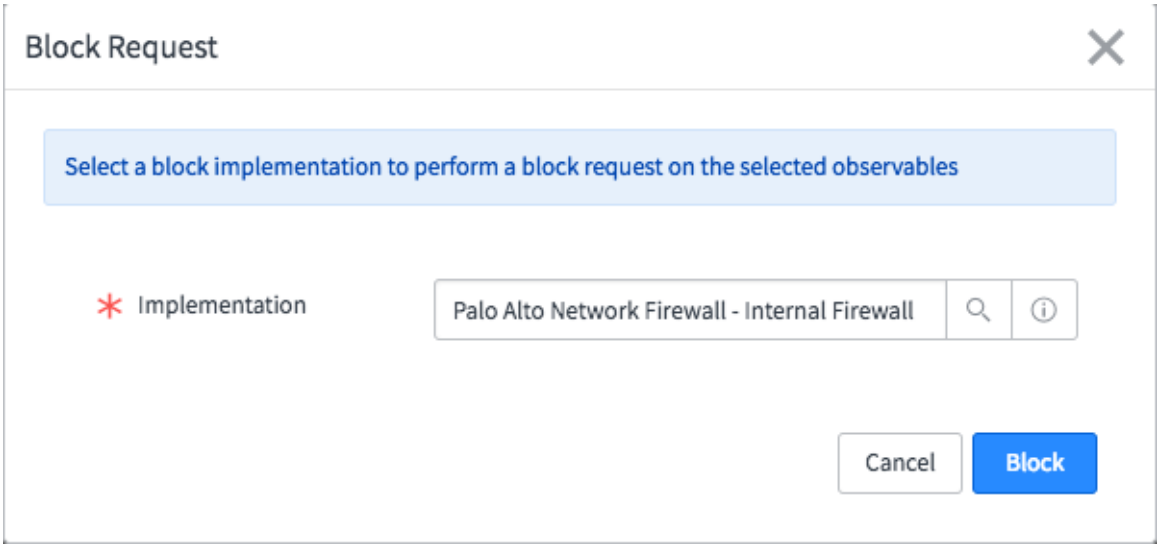
1. Navegue até um incidente de segurança.
2. Selecione observáveis na guia **Lista relacionada**.
3. Clique em **Bloquear solicitação** no menu suspenso **Ações nas linhas selecionadas...**



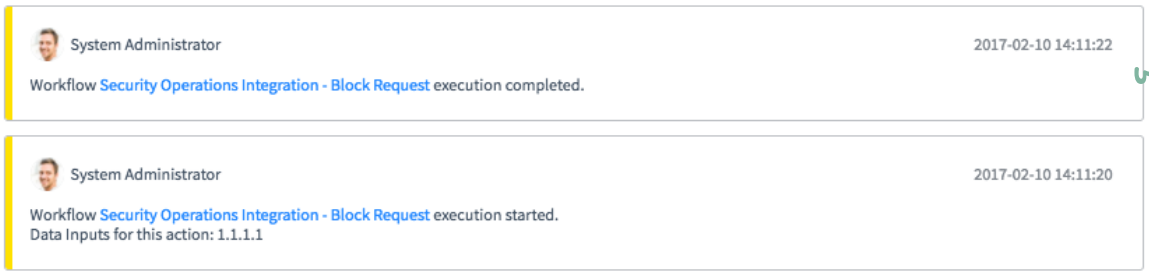
A caixa de diálogo é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Escolha a implementação.
5. Clique **em Bloquear**.
   A auditoria de execução do fluxo de trabalho é exibida na seção de anotações de trabalho.



Integração do Security Operations - Fluxo de trabalho de solicitação de bloqueio

O fluxo de trabalho Integração do Security Operations - Solicitação de bloqueio é um fluxo de trabalho de alto nível independente de integrações. Ele bloqueia observáveis associados a um incidente de segurança. Use-o para realizar uma integração como Palo Alto Networks - Firewall.

Antes de Iniciar

Função necessária: sn_si.analyst

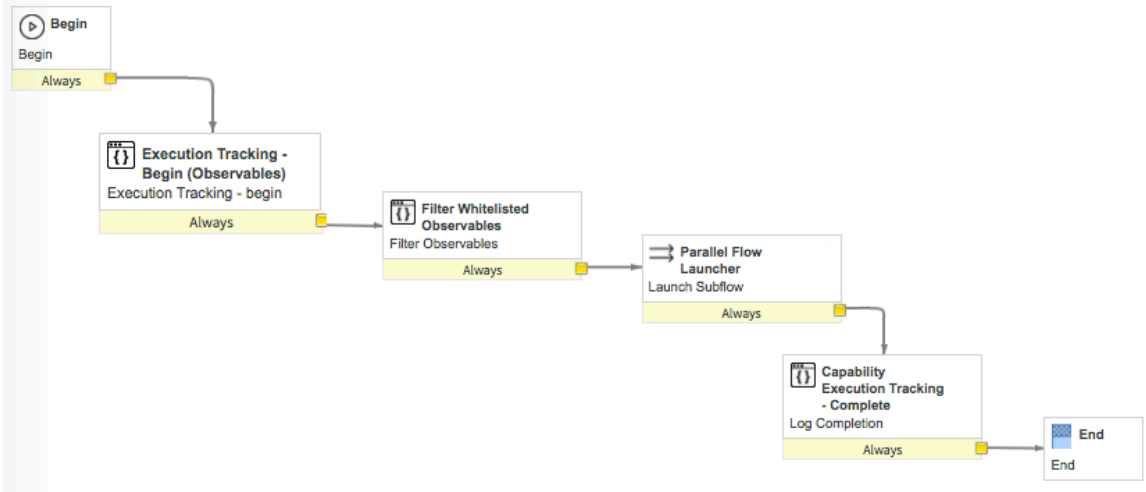
Por Que e Quando Desempenhar Esta Tarefa

O fluxo de trabalho **Integração do Security Operations - Solicitação de bloqueio**pode ser acionado em um formulário observável ou na lista relacionada **de Observáveis** de incidente de segurança em um incidente de segurança. Em uma lista, ele está no menu de ação suspenso. Em um formulário, é um link relacionado. O bloqueio de uma solicitação está disponível somente quando você tem uma implementação instalada para o recurso de solicitação de bloqueio.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Bloquear Solicitação



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Atividade Filtrar observáveis na lista de permissões

A atividade de fluxo de trabalho Observáveis na lista de permissões filtrados remove observáveis que podem ser ignorados da lista de observáveis. Esta atividade pode acelerar o processo de investigação e correção.

A atividade Filtrar observáveis na lista de permissões pode ser usada com qualquer fluxo de trabalho para filtrar observáveis antes de executar qualquer ação.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Lista de filtros criada.
Falha	Ocorreu um erro ao tentar filtrar os observáveis. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
observáveis	Lista de observáveis disponíveis.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
observáveis filtrados	Observáveis filtrados.

Integração do Security Operations - Capacidade de pesquisa e exclusão de e-mail

A funcionalidade Pesquisa e exclusão de e-mail retorna o número de e-mails de ameaça de uma pesquisa de servidor de e-mail e, opcionalmente, retorna detalhes de cada e-mail encontrado. Depois que a pesquisa de e-mail for concluída, você poderá excluir os e-mails.

A funcionalidade Pesquisa e exclusão de e-mail tem um fluxo de trabalho que executa os processos de pesquisa e exclusão de e-mail.

Nota:
Se não houver implementações disponíveis, as ações de recurso não serão exibidas nos menus do produto. Além disso, se nenhuma das implementações de capacidade de **pesquisa e exclusão de e-mail** estiver ativa, o link relacionado à **pesquisa** de e-mail em um incidente de segurança não será exibido.

Integração do Security Operations - Fluxo de trabalho de pesquisa e exclusão de e-mails

O fluxo de trabalho Integração do Security Operations - Pesquisa e exclusão de e-mails retorna o número de e-mails de ameaça de uma pesquisa de servidor de e-mail e, opcionalmente, retorna detalhes de cada e-mail encontrado. Depois que a pesquisa de e-mail for concluída, você poderá excluir os e-mails.

Antes de Iniciar
Função necessária: sn_si.analyst

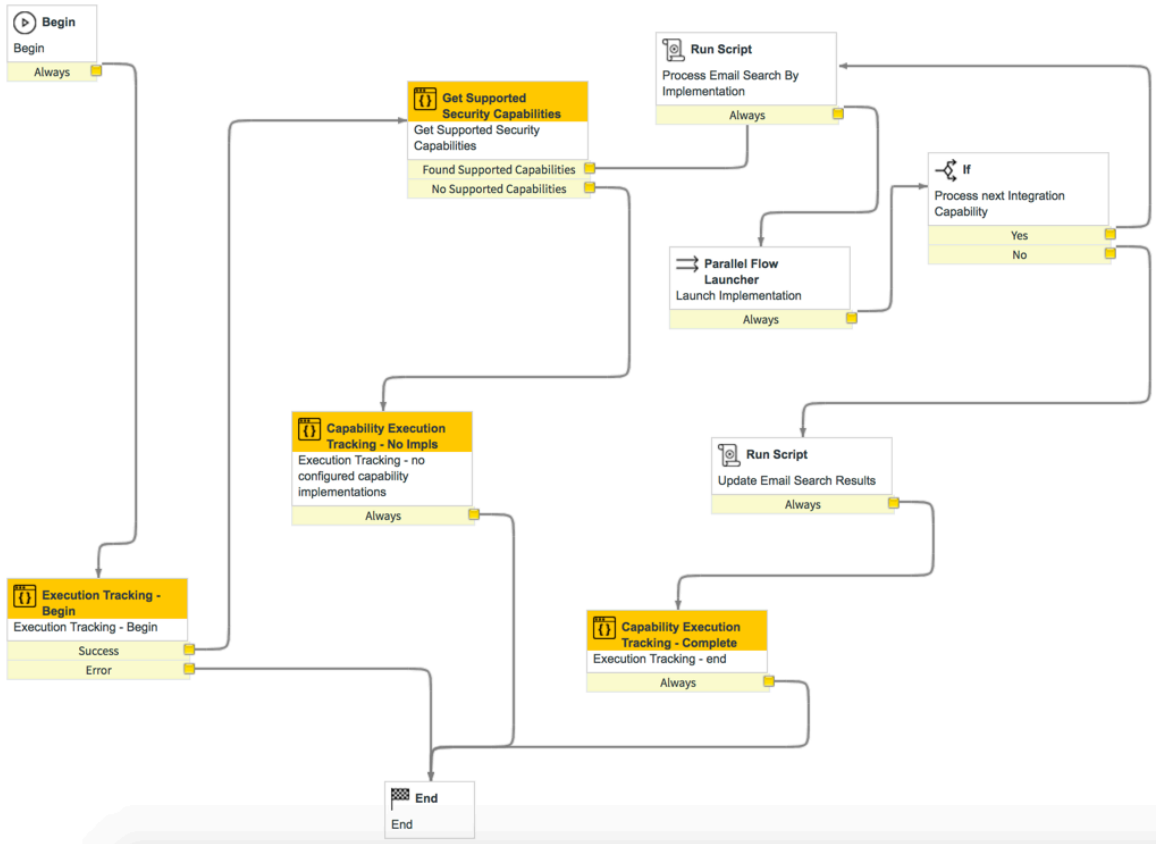
Por Que e Quando Desempenhar Esta Tarefa
A consulta de pesquisa pode levar algum tempo para ser concluída. Depois que a contagem é recebida, a aprovação é necessária para excluir e-mails de um servidor de e-mail.

Este fluxo de trabalho é acionado pelos botões **Excluir do(s) servidor(es)** de e **-mail e Pesquisar no(s)** servidor(es) de e-mail no formulário **Pesquisa** de e-mail em um incidente de segurança. Para obter mais informações, consulte Pesquisar e excluir e-mails de phishing.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa e Exclusão de E-mails



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Atividade Início do acompanhamento de execução (pesquisa de e-mail)

A atividade de execução do recurso Rastreamento de execução - Início (pesquisa de e-mail) cria um registro de acompanhamento de execução e marca o estado do registro como Iniciado. Esta atividade é usada por todos os fluxos de trabalho de capacidade e implementação para rastrear seu estado.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O registro de acompanhamento de execução foi criado.
Falha	Não foi possível criar registro de acompanhamento de execução.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityId	Identificador do sistema da capacidade de integração que está sendo executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
IdDeimplementação	Identificador do sistema da implementação da capacidade de integração que está sendo executada.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
workflowContextId	Identificador do sistema do registro de contexto de fluxo de trabalho associado. Fornecido pelo sistema.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.
parentCapabilityExcutionId	Identificador do sistema do registro de auditoria que iniciou o fluxo de trabalho de implementação. Necessário somente para fluxos de trabalho de implementação da capacidade de integração, como Splunk, Elasticsearch.
emailsearchId	O sysid do registro de pesquisa de e-mail na tabela Pesquisa de e-mail [sn_sec_cmn_email_search].

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
capacidadeExecutionId	Identificador do sistema do registro de acompanhamento de execução.

Atividade Obter capacidades de segurança compatíveis

A atividade de fluxo de trabalho Obter capacidades compatíveis recupera o nome e o número de integrações que estão ativas e oferecem suporte à funcionalidade solicitada.

A atividade Obter capacidades compatíveis pode ser usada com qualquer fluxo de trabalho para determinar quais recursos são compatíveis.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Integração que oferece suporte ao recurso encontrado.
Falha	Ocorreu um erro ao tentar encontrar uma integração ativa que ofereça suporte ao recurso. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityName	Nome da capacidade.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
domainId	Identificador do sistema para qualquer domínio associado ao fluxo de trabalho.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
SupportedCapabilities	Lista de integrações compatíveis com a funcionalidade.
capacidadeContagem	Número de integrações compatíveis com a funcionalidade.

Rastreamento de execução de capacidade - Nenhuma atividade de implementação

A atividade de fluxo de trabalho Rastreamento de execução de capacidade - sem implementações cria um registro de erro quando nenhuma implementação de capacidade de integração é encontrada.

A atividade Rastreamento de execução de capacidade - Sem Impls pode ser usada com qualquer fluxo de trabalho de capacidade de integração abstrata para lidar com a condição de erro quando nenhuma implementação de capacidade configurada estiver disponível.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de acompanhamento de execução é definido como **Erro** e uma mensagem indicando o erro é registrada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capacidadeExecutionId	Identificador do sistema para o registro de auditoria. Saída da atividade usada para iniciar o acompanhamento de execução.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Variáveis de saída

Não há variáveis de saída.

Integração do Security Operations - Aprimorar capacidade de IC

A funcionalidade Aprimorar IC permite aprimorar os dados de itens de configuração associados a um incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A capacidade **Aprimorar IC** tem um fluxo de trabalho, Integração do Security Operations - Fluxo de trabalho de Aprimoramento de IC. Quando o fluxo de trabalho do recurso é executado, ele executa fluxos de trabalho adicionais para as implementações ativadas. Você pode especificar uma implementação a ser usada para executar o aprimoramento nos ICs selecionados ou pode executar o aprimoramento usando todas as implementações.

Nota:
Esses dados aprimorados não são o tipo de dados que você deseja armazenar no seu CMDB, pois são dados forenses específicos de uma determinada investigação, por exemplo, executar um despejo de memória de um IC. Em vez disso, os dados são armazenados na tabela Aprimoramento do item de configuração [sn_sec_cmn_ci_enrichment_result].

Nota:
Se não houver implementações disponíveis, as ações de recurso não serão exibidas nos menus do produto.

Integração do Security Operations - Fluxo de trabalho de Aprimoramento de IC

O fluxo de trabalho Integração do Security Operations - Aprimoramento de IC permite aprimorar os dados em itens de configuração (IC) associados a um incidente de segurança.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado de Security Incident Response de duas maneiras.

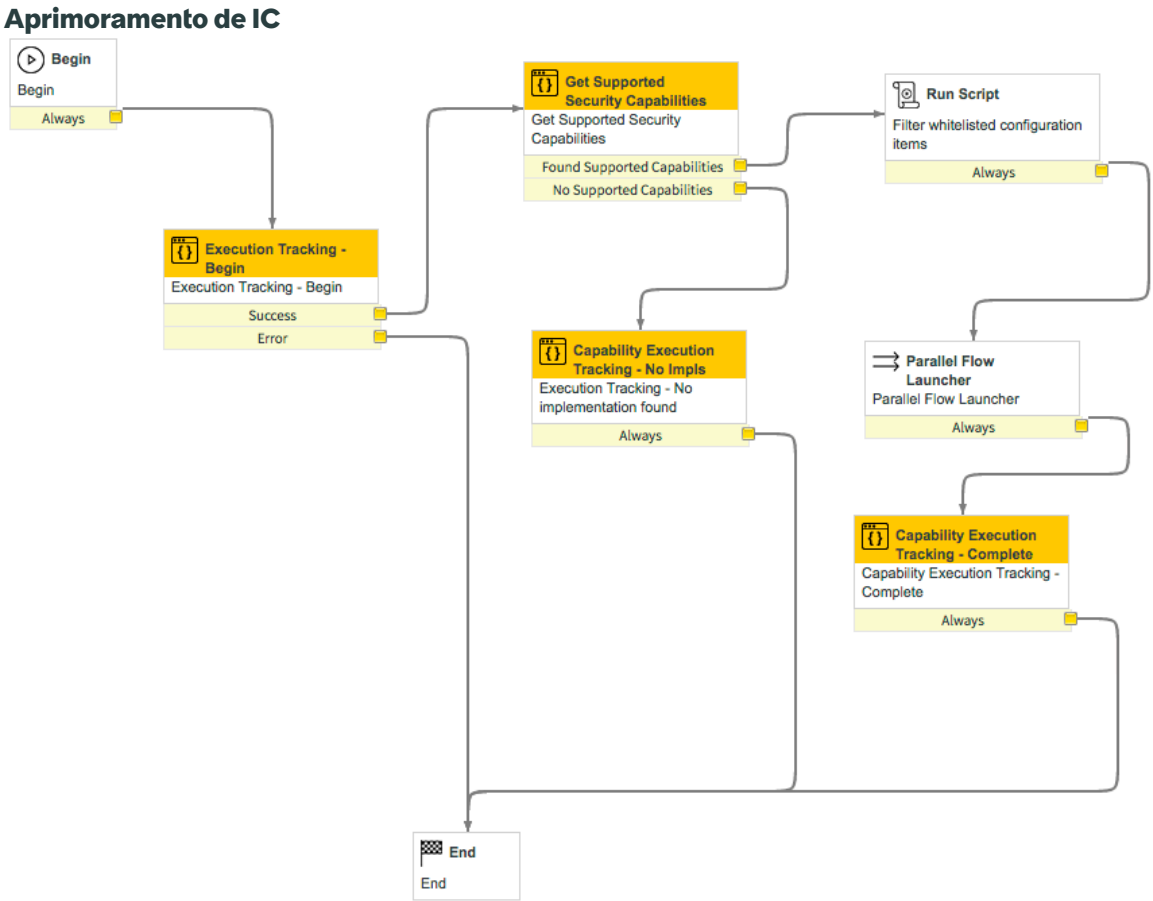
- selecionando um ou mais ICs na guia **Itens de configuração** (no link relacionado **Itens afetados**) e selecionando **Executar aprimoramento de IC** na lista de seleção **Ações nas linhas selecionadas**.
- abrindo um registro de IC e clicando no link relacionado **Executar aprimoramento de IC**.

Qualquer um dos métodos permite especificar quais implementações serão usadas para aprimorar os ICs selecionados. Os fluxos de trabalho de implementação associados são executados para realizar o aprimoramento.

Nota:
O sistema de base não inclui um fluxo de trabalho de implementação para esta capacidade. Para aprimorar ICs, você deve criar seu próprio fluxo de trabalho de implementação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Acompanhamento de execução - Iniciar atividade

A atividade de fluxo de trabalho Acompanhamento de execução - Iniciar inicia o processo de auditoria para um fluxo de trabalho de integração Security Operations que opera em observáveis.

A atividade Acompanhamento de execução - Início pode ser usada com qualquer fluxo de trabalho para começar a registrar o andamento do fluxo de trabalho em uma auditoria.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Um registro de auditoria é criado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
capabilityId	Identificador do sistema da capacidade de integração que está sendo executada.
isImpl	Sinalizador que especifica se a auditoria é feita para um fluxo de trabalho de capacidade de integração ou um fluxo de trabalho de implementação de capacidade de integração. Os valores possíveis são: • falso - denota auditoria em um fluxo de trabalho de capacidade de integração abstrato, como pesquisa de vistas. (padrão.) • verdadeiro: denota auditoria em um fluxo de trabalho de implementação de capacidade de integração. Por exemplo, Splunk ou Elasticsearch.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
observávelLista	Um ou mais SysIDs observáveis para executar a ação desejada. Usado como uma entrada de fluxo de trabalho.
workflowContextId	Identificador do sistema do registro de contexto de fluxo de trabalho associado. Fornecido pelo sistema.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.
parentCapabilityExcutionId	Identificador do sistema do registro de auditoria que iniciou o fluxo de trabalho de implementação. Necessário somente para fluxos de trabalho de implementação da capacidade de integração, como Splunk, Elasticsearch e VirusTotal.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
capacidadeExecutionId	Identificador do sistema do registro de auditoria.

Atividade Obter capacidades de segurança compatíveis

A atividade de fluxo de trabalho Obter capacidades compatíveis recupera o nome e o número de integrações que estão ativas e oferecem suporte à funcionalidade solicitada.

A atividade Obter capacidades compatíveis pode ser usada com qualquer fluxo de trabalho para determinar quais recursos são compatíveis.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Integração que oferece suporte ao recurso encontrado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Falha	Ocorreu um erro ao tentar encontrar uma integração ativa que ofereça suporte ao recurso. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityName	Nome da capacidade.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
domainId	Identificador do sistema para qualquer domínio associado ao fluxo de trabalho.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
SupportedCapabilities	Lista de integrações compatíveis com a funcionalidade.
capacidadeContagem	Número de integrações compatíveis com a funcionalidade.

Rastreamento de execução de capacidade - Nenhuma atividade de implementação

A atividade de fluxo de trabalho Rastreamento de execução de capacidade - sem implementações cria um registro de erro quando nenhuma implementação de capacidade de integração é encontrada.

A atividade Rastreamento de execução de capacidade - Sem Impls pode ser usada com qualquer fluxo de trabalho de capacidade de integração abstrata para lidar com a condição de erro quando nenhuma implementação de capacidade configurada estiver disponível.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de acompanhamento de execução é definido como **Erro** e uma mensagem indicando o erro é registrada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
capacidadeExecutionId	Identificador do sistema para o registro de auditoria. Saída da atividade usada para iniciar o acompanhamento de execução.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Variáveis de saída

Não há variáveis de saída.

Integração do Security Operations - Capacidade Aprimorar observável

A funcionalidade Aprimorar observável permite aprimorar observáveis com informações adicionais de várias fontes usando fluxos de trabalho de implementação. Essa capacidade é usada durante as investigações de resposta do incidente com uma ameaça identificada.

A capacidade Aprimorar observável tem um fluxo de trabalho, Security Operations Integration - Aprimorar fluxo de trabalho de observável. Quando o fluxo de trabalho do recurso é executado, ele executa fluxos de trabalho adicionais para as implementações ativadas. Você pode especificar uma implementação a ser usada para executar o aprimoramento nos observáveis selecionados ou pode executar o aprimoramento usando todas as implementações que correspondem aos tipos de observáveis compatíveis.

Nota:
Se não houver implementações disponíveis, as ações de recurso não serão exibidas nos menus do produto.

Security Operations Integration - Aprimorar fluxo de trabalho de observável

O fluxo de trabalho Integração do Security Operations - Aprimorar observável permite aprimorar observáveis com informações adicionais de várias fontes usando fluxos de trabalho de implementação.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho pode ser acionado de Security Incident Response ou Inteligência contra ameaças de duas maneiras.

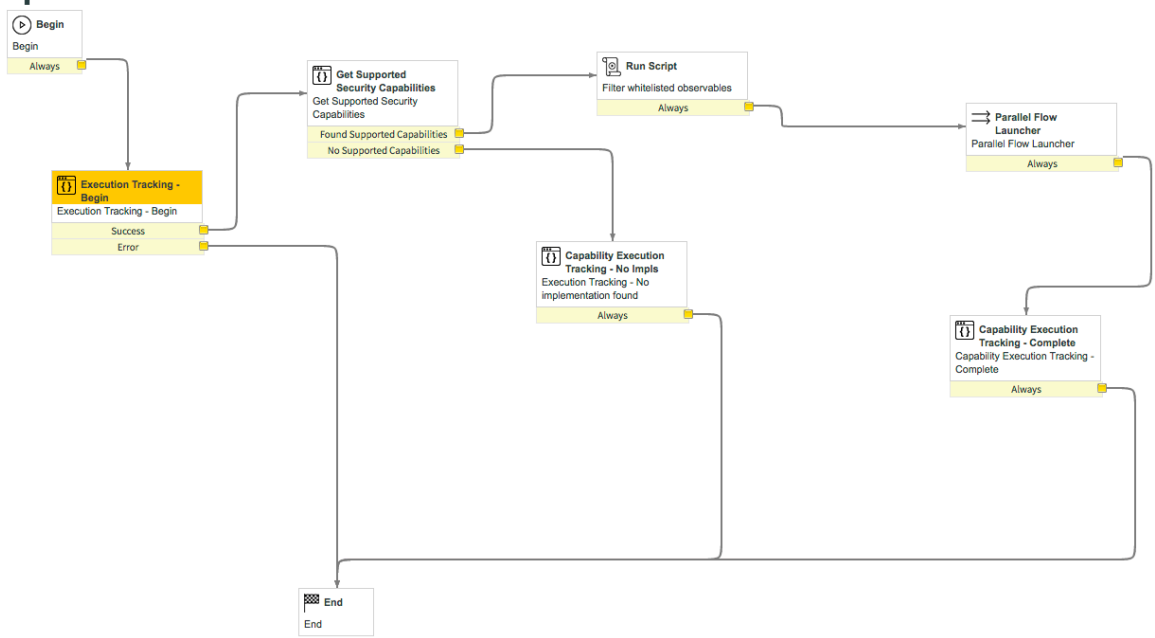
- selecionando um ou mais observáveis na lista Observáveis e selecionando **Executar aprimoramento** de observável na lista de seleção **Ações nas linhas selecionadas**.
- abrindo um registro de observável e clicando no link relacionado **Executar aprimoramento de observável**.

Qualquer um dos métodos permite especificar quais implementações serão usadas para aprimorar os observáveis selecionados. Os fluxos de trabalho de implementação associados são executados para realizar o aprimoramento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aprimorar Observável



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Atividade Obter capacidades de segurança compatíveis

A atividade de fluxo de trabalho Obter capacidades compatíveis recupera o nome e o número de integrações que estão ativas e oferecem suporte à funcionalidade solicitada.

A atividade Obter capacidades compatíveis pode ser usada com qualquer fluxo de trabalho para determinar quais recursos são compatíveis.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Integração que oferece suporte ao recurso encontrado.
Falha	Ocorreu um erro ao tentar encontrar uma integração ativa que ofereça suporte ao recurso. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityName	Nome da capacidade.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
domainId	Identificador do sistema para qualquer domínio associado ao fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
SupportedCapabilities	Lista de integrações compatíveis com a funcionalidade.
capacidadeContagem	Número de integrações compatíveis com a funcionalidade.

Rastreamento de execução de capacidade - Nenhuma atividade de implementação

A atividade de fluxo de trabalho Rastreamento de execução de capacidade - sem implementações cria um registro de erro quando nenhuma implementação de capacidade de integração é encontrada.

A atividade Rastreamento de execução de capacidade - Sem Impls pode ser usada com qualquer fluxo de trabalho de capacidade de integração abstrata para lidar com a condição de erro quando nenhuma implementação de capacidade configurada estiver disponível.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de acompanhamento de execução é definido como **Erro** e uma mensagem indicando o erro é registrada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capacidadeExecutionId	Identificador do sistema para o registro de auditoria. Saída da atividade usada para iniciar o acompanhamento de execução.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Variáveis de saída

Não há variáveis de saída.

Integração do Security Operations - Obter recurso de estatísticas de rede

O recurso Obter estatísticas de rede recupera uma lista de conexões de rede ativas de um host ou endpoint. Ele pode ser usado para aprimoramento de incidentes durante as investigações. Esta capacidade é acionada automaticamente quando um item de configuração é adicionado a um incidente de segurança.

A **funcionalidade Obter estatísticas de rede** tem um fluxo de trabalho, Security Operations Integrations - Obter fluxo de trabalho de estatísticas de rede que aceita um ou mais ICs e tarefas. O

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

fluxo de trabalho itera em cada implementação e em cada IC e invoca novamente o fluxo de trabalho de implementação.

Nota:
Se não houver implementações disponíveis, as ações de recurso não serão exibidas nos menus do produto.

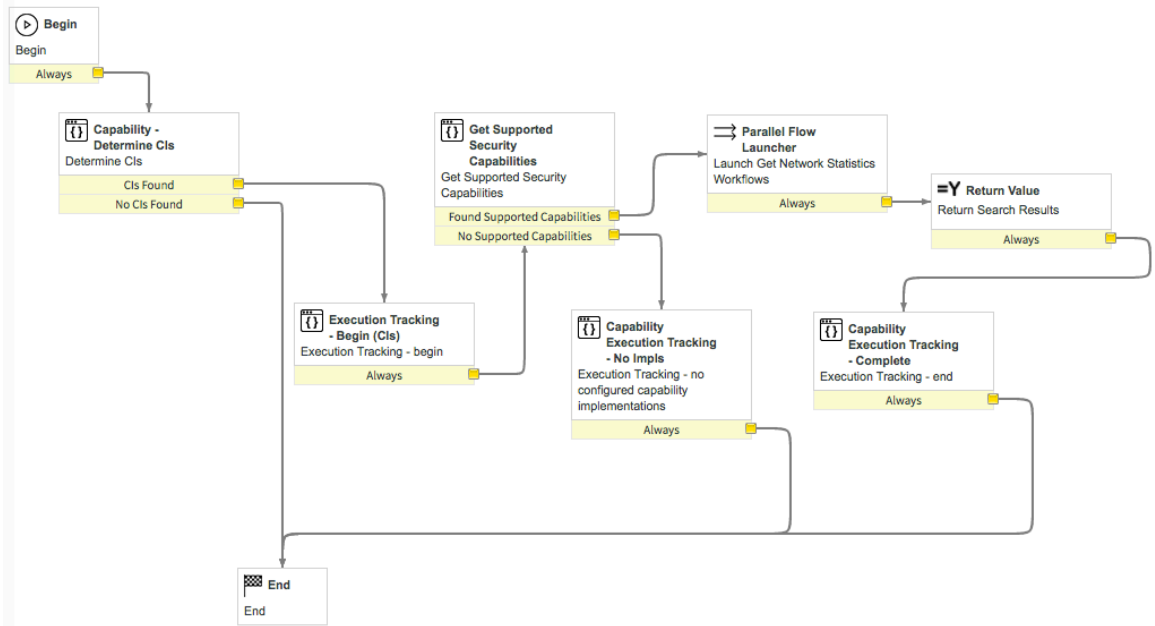
Security Operations Integrations - Obter fluxo de trabalho de estatísticas de rede

O fluxo de trabalho Integrações do Security Operations - Obter estatísticas de rede recupera uma lista de conexões de rede ativas de um host ou endpoint.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é executado automaticamente quando um item de configuração é adicionado a um incidente de segurança.

Obter Estatísticas de Rede



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Capacidade - Atividade Determinar ICs

A atividade de fluxo de trabalho Capacidade - Determinar ICs determina quais itens de configuração (ICs) serão incluídos no fluxo de trabalho.

A atividade Capacidade - Determinar ICs pode ser usada com qualquer fluxo de trabalho para determinar quais ICs serão incluídos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Itens de configuração encontrados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Falha	Nenhum IC encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
task_sys_id	Identificador de tarefa (mapeia o incidente de segurança para ICs).
cis_affected	Itens de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
cis_affected	ICs filtrados
task_sys_id	Identificador de tarefa (mapeia o incidente de segurança para ICs).

Acompanhamento de execução - Atividade de início (ICs)

A atividade de fluxo de trabalho **Acompanhamento de execução - Início (ICs)** inicia o processo de auditoria para um fluxo de trabalho de integração Security Operations que opera em itens de configuração (ICs).

A atividade **Acompanhamento de execução - Início (ICs)** pode ser usada com qualquer fluxo de trabalho de IC para começar a registrar o andamento do fluxo de trabalho em uma auditoria.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Um registro de auditoria é criado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityId	Identificador do sistema da capacidade de integração que está sendo executada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
isImpl	Sinalizador que especifica se a auditoria é feita para um fluxo de trabalho de capacidade de integração ou um fluxo de trabalho de implementação de capacidade de integração. Os valores possíveis são: • falso - denota auditoria em um fluxo de trabalho de capacidade de integração abstrato, como pesquisa de vistas. (padrão.) • verdadeiro: denota auditoria em um fluxo de trabalho de implementação de capacidade de integração. Por exemplo, Splunk ou Elasticsearch.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.

ListaC	Um ou mais itens de configuração (IC) para executar a ação desejada no seguinte formato:
	`["sysId", "sysId"]`
	ou
	`"sysId"`
	Usado como uma entrada de fluxo de trabalho.

workflowContextId	Identificador do sistema do registro de contexto de fluxo de trabalho associado. Fornecido pelo sistema.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.
parentCapabilityExcutionId	Identificador do sistema do registro de auditoria que iniciou o fluxo de trabalho de implementação. Necessário somente para fluxos de trabalho de implementação da capacidade de integração, como Splunk, Elasticsearch.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
capacidadeExecutionId	Identificador do sistema do registro de auditoria.

Atividade Obter capacidades de segurança compatíveis

A atividade de fluxo de trabalho Obter capacidades compatíveis recupera o nome e o número de integrações que estão ativas e oferecem suporte à funcionalidade solicitada.

A atividade Obter capacidades compatíveis pode ser usada com qualquer fluxo de trabalho para determinar quais recursos são compatíveis.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Integração que oferece suporte ao recurso encontrado.
Falha	Ocorreu um erro ao tentar encontrar uma integração ativa que ofereça suporte ao recurso. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityName	Nome da capacidade.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
domainId	Identificador do sistema para qualquer domínio associado ao fluxo de trabalho.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
SupportedCapabilities	Lista de integrações compatíveis com a funcionalidade.
capacidadeContagem	Número de integrações compatíveis com a funcionalidade.

Rastreamento de execução de capacidade - Nenhuma atividade de implementação

A atividade de fluxo de trabalho Rastreamento de execução de capacidade - sem implementações cria um registro de erro quando nenhuma implementação de capacidade de integração é encontrada.

A atividade Rastreamento de execução de capacidade - Sem Impls pode ser usada com qualquer fluxo de trabalho de capacidade de integração abstrata para lidar com a condição de erro quando nenhuma implementação de capacidade configurada estiver disponível.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de acompanhamento de execução é definido como **Erro** e uma mensagem indicando o erro é registrada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
capacidadeExecutionId	Identificador do sistema para o registro de auditoria. Saída da atividade usada para iniciar o acompanhamento de execução.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Variáveis de saída

Não há variáveis de saída.

Fluxo de trabalho do Security Incident Response - Obter estatísticas de rede

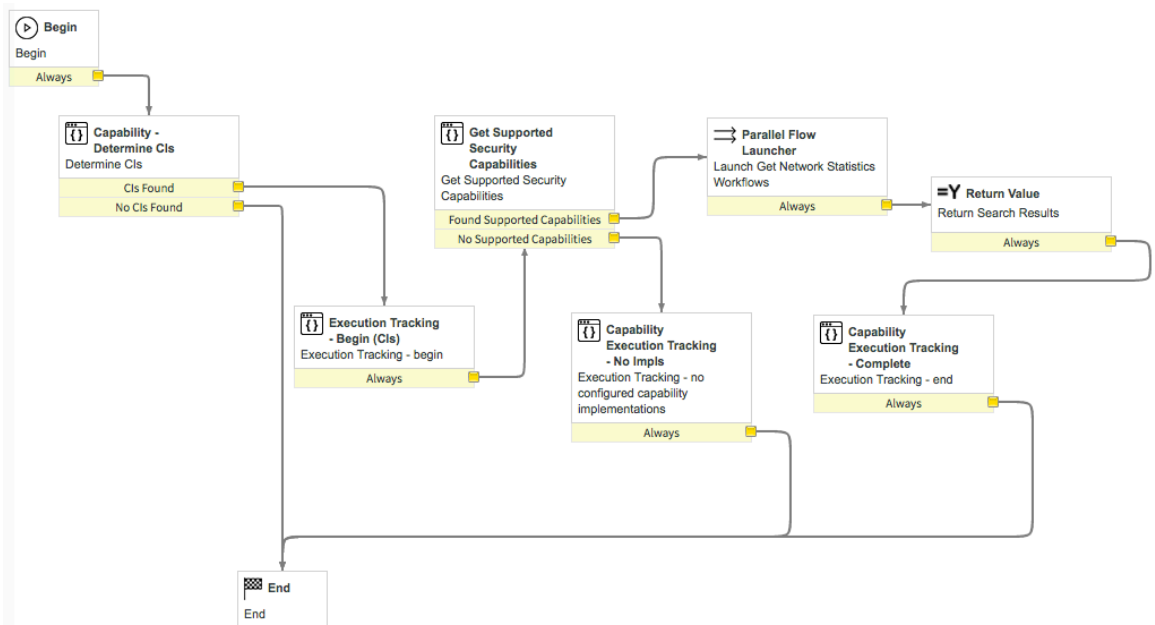
O **Security Incident Response** > **Obter Estatísticas de Rede** O fluxo de trabalho recupera as estatísticas de rede de um recurso baseado no Windows afetado quando adicionado a um incidente de segurança no estado **Análise**.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Para novos incidentes de segurança que contêm itens de configuração, o fluxo de trabalho é executado automaticamente quando o estado muda para **Análise**.

Os incidentes de segurança existentes são atualizados automaticamente quando você está no estado **Análise** e adiciona um novo item de configuração.

Obter Estatísticas de Rede



As atividades do processo de fluxo de trabalho incluem:

Atividade Obter FQDN do item de configuração

Determinar Shell Script por SO

Se a declaração for executada pelo PowerShell

Acompanhamento de execução - Iniciar atividade

Obter estatísticas de rede por meio da atividade netstat

Acompanhamento de execução de capacidade - Atividade com falha

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade Criar registros de dados de aprimoramento

Acompanhamento de execução de capacidade - Atividade com falha - Retorna o ID de aprimoramento.

Acompanhamento de execução de capacidade - Concluir atividade

Procedimento

1. Abra um incidente de segurança.
2. Atualize o **Estado** para **Análise**, se necessário.
3. Adicione um item de configuração (computador, servidor ou similar).
4. Clique em **Atualizar**.
   Orquestração de resposta de incidente de segurança fornece informações de estatísticas de rede no **Links relacionados** > **Aprimoramentos de incidente de segurança** guia. Para obter mais informações, consulte Security Operations mapeamento de dados de aprimoramento.

Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Atividade Obter FQDN do item de configuração

O **Orquestração do Security Common** > **Obter FQDN do item de configuração** A atividade de fluxo de trabalho recupera o nome de domínio totalmente qualificado (FQDN) de um item de configuração. Esta atividade pode acelerar o processo de investigação e correção.

A atividade Obter FQDN do item de configuração pode ser usada com qualquer fluxo de trabalho para recuperar o nome de domínio totalmente qualificado (FQDN) de um item de configuração.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
cmdb_ci.id [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
fqdn [cadeia de caracteres]	O nome de domínio totalmente qualificado (FQDN) do item de configuração.

Anotações Adicionais

O campo fqdn no item de configuração deve ser preenchido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Obter estatísticas de rede por meio da atividade netstat

A atividade de fluxo de trabalho Security Common Orchestration - Obter estatísticas de rede via netstat recupera as estatísticas de rede de um recurso afetado em um sistema baseado no Windows. Esta atividade pode acelerar o processo de investigação e correção.

A atividade Obter estatísticas de rede via netstat pode ser usada com qualquer fluxo de trabalho para recuperar estatísticas de rede de um sistema baseado no Windows. A máquina é consultada com o comando **netstat**, incluindo os parâmetros **-a** e **-o**. Para aprimorar os dados de saída, o comando **get-process** também é invocado.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	As estatísticas de rede foram recuperadas no formato JSON.
Falha	Ocorreu um erro ao tentar recuperar as estatísticas da rede. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

Variável	Descrição
destino [cadeia de caracteres]	O nome de domínio totalmente qualificado (FQDN) ou o endereço IP do sistema de destino.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta [cadeia de caracteres]	Uma cadeia de caracteres JSON que representa os processos em execução no momento na máquina de destino. Os dados JSON incluem: **PID** Identificador de processo **_port local** Porta local para a transação de rede **state** Status da conexão TCP. **Nota:** Este campo é nulo para conexões UDP. **local_address**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
	Nome de domínio totalmente qualificado (FQDN) local ou endereço IP **remote_address** Nome de domínio totalmente qualificado (FQDN) ou endereço IP remoto **protocolo** TCP ou UDP **remote_port** Porta remota da transação de rede **path** O caminho do arquivo do executável do processo **hash** O valor de hash do executável do processo. O hash está em SHA-256 para PowerShell V4 ou superior. Caso contrário, o hash estará em MD5.

Restrições

O MID Server deve oferecer suporte ao PowerShell.

O hash SHA-256 requer PowerShell V4.

Acompanhamento de execução de capacidade - Atividade com falha

A atividade de fluxo de trabalho Rastreamento de execução de capacidade - Falha registra uma falha no registro de auditoria.

A atividade Rastreamento de execução de capacidade - Falha pode ser usada com qualquer fluxo de trabalho para registrar uma condição de falha.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de auditoria é definido como **Erro** e uma mensagem indicando o erro é registrada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capacidadeExecutionId	Identificador do sistema para o registro de auditoria. Esta é a saída de qualquer uma das atividades Iniciar auditoria.
errorMessage	Mensagem indicando o motivo da falha.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Não há variáveis de saída.

Integração do Security Operations - Obter capacidade de processos em execução

A capacidade Obter processos em execução recupera uma lista de processos em execução em um item de configuração (IC) de um host ou endpoint. Essa capacidade é usada para aprimoramento de incidentes durante as investigações.

A funcionalidade Obter processos em execução tem três fluxos de trabalho de implementação :

- Fluxo de trabalho do Security Operations Carbon Black Integration - Obter processos em execução
- Fluxo de trabalho de integração de comandos do sistema de operações de segurança – Obter processos em execução
- Fluxo de trabalho do Security Operations Tanium Integration - Obter processos em execução

Nota:
Se não houver implementações disponíveis, as ações de recurso não serão exibidas nos menus do produto.

Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Security Operations - Obter fluxo de trabalho de processos em execução

O fluxo de trabalho Security Operations - Obter processos em execução é um fluxo de trabalho de alto nível independente de integrações. Ele recupera uma lista de processos em execução em um item de configuração (IC) de um host. Use-o para realizar uma integração, como Carbon Black, ou para um incidente de segurança baseado no Windows.

Antes de Iniciar
Função necessária: sn_si.analyst

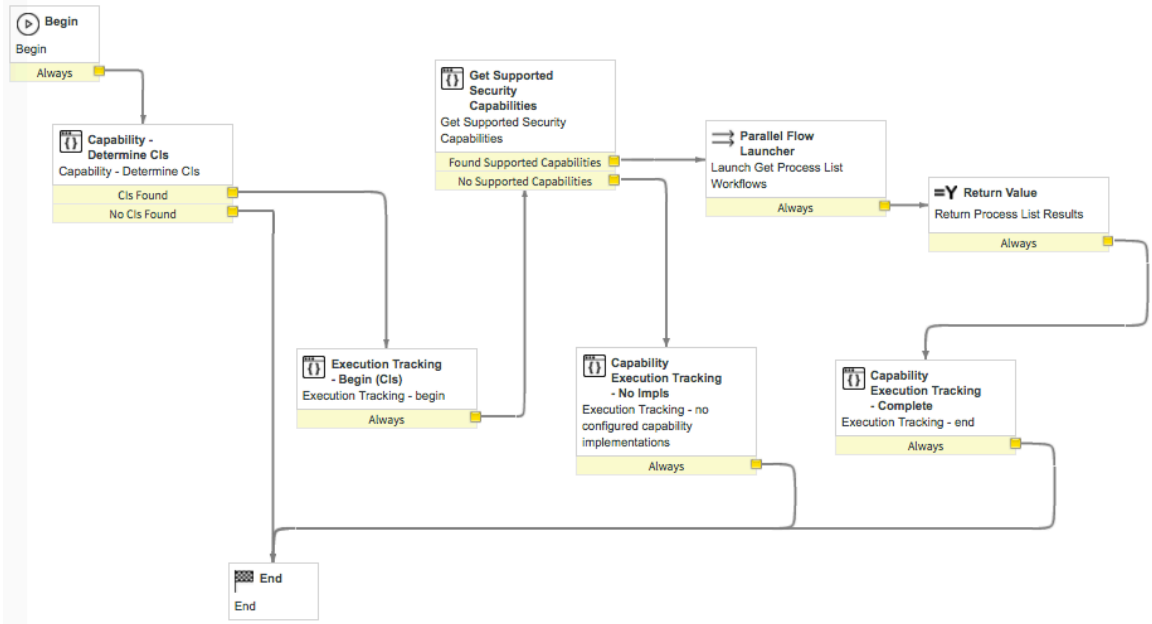
Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:

- Capacidade - Atividade Determinar ICs
- Acompanhamento de execução - Atividade de início (ICs)
- Atividade Obter capacidades de segurança compatíveis
- Rastreamento de execução de capacidade - Nenhuma atividade de implementação
- Inicializador de fluxo paralelo : retorna os resultados da pesquisa em uma matriz.
- Acompanhamento de execução de capacidade - Concluir atividade

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Obter Processos em Execução



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Capacidade - Atividade Determinar ICs

A atividade de fluxo de trabalho Capacidade - Determinar ICs determina quais itens de configuração (ICs) serão incluídos no fluxo de trabalho.

A atividade Capacidade - Determinar ICs pode ser usada com qualquer fluxo de trabalho para determinar quais ICs serão incluídos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Itens de configuração encontrados.
Falha	Nenhum IC encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
task_sys_id	Identificador de tarefa (mapeia o incidente de segurança para ICs).
cis_affected	Itens de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
cis_affected	ICs filtrados
task_sys_id	Identificador de tarefa (mapeia o incidente de segurança para ICs).

Atividade Obter capacidades de segurança compatíveis

A atividade de fluxo de trabalho Obter capacidades compatíveis recupera o nome e o número de integrações que estão ativas e oferecem suporte à funcionalidade solicitada.

A atividade Obter capacidades compatíveis pode ser usada com qualquer fluxo de trabalho para determinar quais recursos são compatíveis.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Integração que oferece suporte ao recurso encontrado.
Falha	Ocorreu um erro ao tentar encontrar uma integração ativa que ofereça suporte ao recurso. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityName	Nome da capacidade.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
domainId	Identificador do sistema para qualquer domínio associado ao fluxo de trabalho.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
SupportedCapabilities	Lista de integrações compatíveis com a funcionalidade.
capacidadeContagem	Número de integrações compatíveis com a funcionalidade.

Rastreamento de execução de capacidade - Nenhuma atividade de implementação

A atividade de fluxo de trabalho Rastreamento de execução de capacidade - sem implementações cria um registro de erro quando nenhuma implementação de capacidade de integração é encontrada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A atividade Rastreamento de execução de capacidade - Sem Impls pode ser usada com qualquer fluxo de trabalho de capacidade de integração abstrata para lidar com a condição de erro quando nenhuma implementação de capacidade configurada estiver disponível.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de acompanhamento de execução é definido como **Erro** e uma mensagem indicando o erro é registrada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capacidadeExecutionId	Identificador do sistema para o registro de auditoria. Saída da atividade usada para iniciar o acompanhamento de execução.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Variáveis de saída

Não há variáveis de saída.

Fluxo de trabalho do Security Operations Carbon Black Integration - Obter processos em execução

A Integração Carbon Black do Security Operations - Obter processos em execução é a implementação da integração Carbon Black iniciada pelo fluxo de trabalho Integração do Security Operations - Obter processo em execução.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:

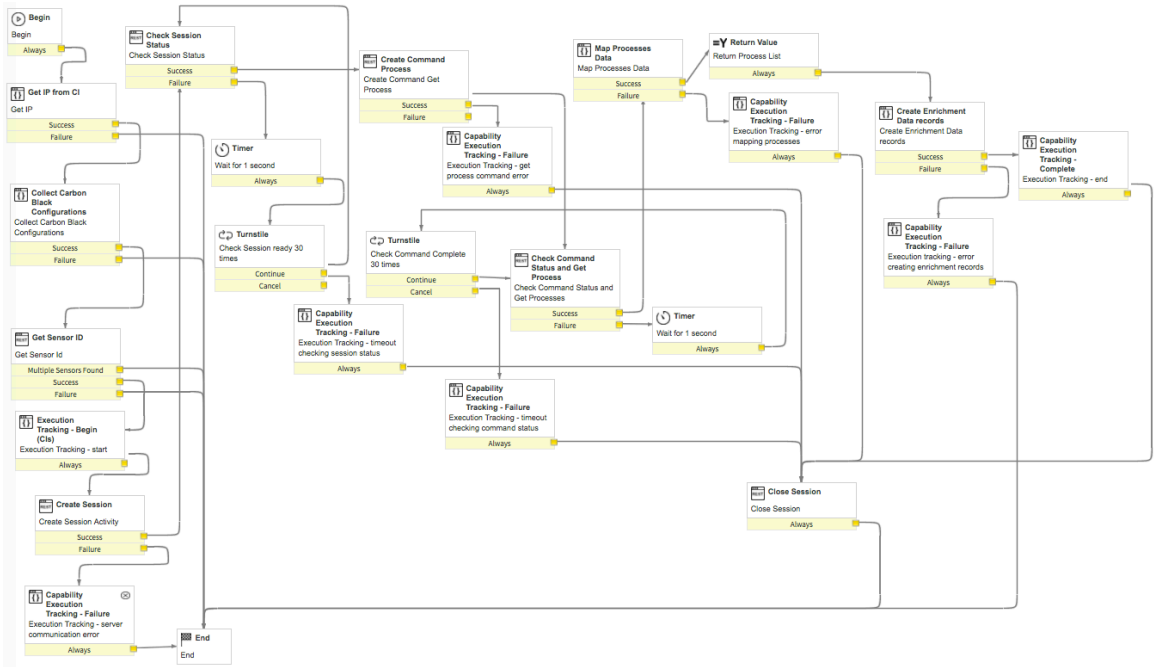
- Obter IP da atividade de IC
- Atividade Coletar configurações do Carbon Black
- Atividade Obter ID de sensor
- Acompanhamento de execução - Atividade de início (ICs)
- Criar Sessão
- Acompanhamento de execução de capacidade - Atividade com falha
- Atividade Verificar status da sessão
- Atividade de fluxo de trabalho Temporizador - Aguarda 1 segundo
- Atividade de fluxo de trabalho da catraca - Verificar se a sessão está pronta 30 vezes
- Atividade Criar processo de comando

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Atividade Verificar status do comando e obter processo
- Atividade Mapear dados de processos e retornam a lista de processos
- Atividade Criar registros de dados de aprimoramento
- Acompanhamento de execução de capacidade - Concluir atividade
- Atividade Fechar Sessão

Obter processos em execução do Carbon Black



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Obter IP da atividade de IC

A atividade de fluxo de trabalho Obter IP do IC coleta o endereço IP dos itens de configuração (ICs) para usar no fluxo de trabalho.

A atividade Obter IP do IC pode ser usada com qualquer fluxo de trabalho para coletar endereços IP de item de configuração (IC) para usar no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Endereços IP encontrados.
Falha	Nenhum endereço IP encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
ci_sys_id	Identificador do item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ip_addr	Endereços IP.

Atividade Coletar configurações do Carbon Black

A atividade de fluxo de trabalho Coletar configurações do Carbon Black reúne informações de configuração para usar no fluxo de trabalho.

A atividade Coletar configurações do Carbon Black coleta informações de configuração do Carbon Black para usar no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

Não há variáveis de entrada para esta atividade.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com Carbon Black ou não.
api_token	Chave de API de integração de terceiros.

Verificar status do MID Server

Determina se o MID Server identificado no campo **Host do MID Server** da configuração da integração está instalado e funcionando. Se o campo estiver definido como **Qualquer**, a atividade verificará se o MID Server está instalado e funcionando.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A atividade Verificar status do MID Server pode ser usada com qualquer fluxo de trabalho para verificar a presença de um MID Server em execução no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Status da sessão retornado.
Falha	Erro de status da sessão. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capacidadeExecutionId	O ID da capacidade que está sendo executada.
workflowName	O nome do fluxo de trabalho que está sendo executado.
mid_server_host	O MID Server identificado na configuração da integração i

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
mid_server_live	Identifica se o MID Server identificado no campo **Host do MID Server** da configuração da integração está instalado e funcionando. Se o campo estiver definido como **Qualquer**, a atividade verificará se o MID Server está instalado e funcionando.

Atividade Obter ID de sensor

A atividade de fluxo de trabalho Obter ID de sensor reúne identificadores de sensor para usar no fluxo de trabalho.

A atividade Obter ID do sensor pode ser usada com qualquer fluxo de trabalho para coletar informações do sensor para usar no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Identificadores de sensor encontrados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Falha	Nenhum sensor encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
api_token	Chave de API Carbon Black.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com Carbon Black ou não.
endpoint_base	URL base da API Carbon Black.
ci_ip_address	Endereço IP do item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
Tipo de elemento de matriz	Variáveis de API.
sensor_detail	Descrição do sensor Carbon Black no formato JSON.

Acompanhamento de execução - Iniciar atividade

A atividade de fluxo de trabalho Acompanhamento de execução - Iniciar inicia o processo de auditoria para um fluxo de trabalho de integração Security Operations que opera em observáveis.

A atividade Acompanhamento de execução - Início pode ser usada com qualquer fluxo de trabalho para começar a registrar o andamento do fluxo de trabalho em uma auditoria.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Um registro de auditoria é criado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityId	Identificador do sistema da capacidade de integração que está sendo executada.
isImpl	Sinalizador que especifica se a auditoria é feita para um fluxo de trabalho de capacidade de integração ou um fluxo de trabalho de implementação de capacidade de integração. Os valores possíveis são: • falso - denota auditoria em um fluxo de trabalho de capacidade de integração abstrato, como pesquisa de vistas. (padrão.) • verdadeiro: denota auditoria em um fluxo de trabalho de implementação de capacidade de integração. Por exemplo, Splunk ou Elasticsearch.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
observávelLista	Um ou mais SysIDs observáveis para executar a ação desejada. Usado como uma entrada de fluxo de trabalho.
workflowContextId	Identificador do sistema do registro de contexto de fluxo de trabalho associado. Fornecido pelo sistema.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.
parentCapabilityExcutionId	Identificador do sistema do registro de auditoria que iniciou o fluxo de trabalho de implementação. Necessário somente para fluxos de trabalho de implementação da capacidade de integração, como Splunk, Elasticsearch e VirusTotal.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
capacidadeExecutionId	Identificador do sistema do registro de auditoria.

Atividade Criar sessão

A atividade de fluxo de trabalho Criar sessão estabelece uma sessão Carbon Black para usar no fluxo de trabalho.

A atividade Criar sessão pode ser usada com qualquer fluxo de trabalho para criar uma sessão Carbon Black no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Sessão criada.
Falha	Sessão não criada. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
sensor_id	Identificador do sensor.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com Carbon Black ou não.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
saída	Variáveis de API

Atividade Verificar status da sessão

Determina o status de uma sessão Carbon Black no fluxo de trabalho.

A atividade Verificar status da sessão pode ser usada com qualquer fluxo de trabalho para verificar o status da sessão do Carbon Black no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Status da sessão retornado.
Falha	Erro de status da sessão. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
session_id	Identificador de sessão.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com Carbon Black ou não.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
saída	Informações sobre processos em execução do Carbon Black.

Atividade Criar processo de comando

A atividade de fluxo de trabalho Criar processo de comando cria um processo de comando Carbon Black para usar no fluxo de trabalho.

A atividade Criar processo de comando pode ser usada com qualquer fluxo de trabalho para criar um processo de comando Carbon Black no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Processo de comando criado.
Falha	Processo de comando não criado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
session_id	Identificador de sessão.
command_id	Identificador de comando.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com Carbon Black ou não.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
saída	Variáveis de API

Atividade Verificar status do comando e obter processo

Verifica o status do comando Carbon Black e recupera processos para usar no fluxo de trabalho.

A atividade Verificar status do comando e Obter processo pode ser usada com qualquer fluxo de trabalho para verificar o status de um comando Carbon Black e obter processos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Status do comando retornado e processos criados.
Falha	Status do comando ou erro de processo. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
session_id	Identificador de sessão.
command_id	Identificador de comando.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com Carbon Black ou não.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
saída	Variáveis de API

Atividade Mapear dados de processos

A atividade de fluxo de trabalho Mapear dados de processos mapeia dados de processo Carbon Black no fluxo de trabalho.

A atividade Mapear dados de processos pode ser usada com qualquer fluxo de trabalho para mapear processos do Carbon Black.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Processos mapeados
Falha	Processos não mapeados. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
afetado_ci	Item de configuração afetado.
Id_implementação	Identificador de implementação.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
saída	Dados de retorno formatados em processos em execução usados pelo fluxo de trabalho abstrato.
processos	Lista de processos em uma matriz.

Acompanhamento de execução de capacidade - Concluir atividade

A atividade de fluxo de trabalho Rastreamento de execução de capacidade - Concluir atualiza o registro de auditoria quando o fluxo de trabalho é concluído.

A atividade Rastreamento de execução de capacidade - Concluir pode ser usada com qualquer fluxo de trabalho para registrar a conclusão do fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
A matriz **Valor de Retorno** da atividade principal do **inicializador paralelo** contém uma matriz de resultados de todos os fluxos de trabalho de integração executados e solicita a conclusão bem-sucedida do acompanhamento da execução.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de auditoria é atualizado para **Concluído**.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capacidadeExecutionId	Identificador do sistema para o registro de auditoria. Este campo foi a saída de qualquer uma das atividades de auditoria Iniciar.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.
message	Mensagem de conclusão.

Variáveis de saída

Não há variáveis de saída.

Atividade Fechar Sessão

Fecha uma sessão Carbon Black no fluxo de trabalho.

A atividade Fechar sessão pode ser usada com qualquer fluxo de trabalho para fechar uma sessão Carbon Black.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Sessão encerrada.
Falha	Sessão não encerrada. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
api_token	Chave de API Carbon Black.
endpoint_base	URL base da API Carbon Black.
session_id	Identificador de sessão.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com Carbon Black ou não.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
saída	Variáveis de API

Fluxo de trabalho do Security Operations Tanium Integration - Obter processos em execução

A **integração do Tanium com o Security Operations - Obter processos em execução** é a implementação da integração do Tanium iniciada pelo fluxo de trabalho **Integração do Security Operations - Obter processo em execução**.

Antes de Iniciar
Função necessária: sn_si.analyst

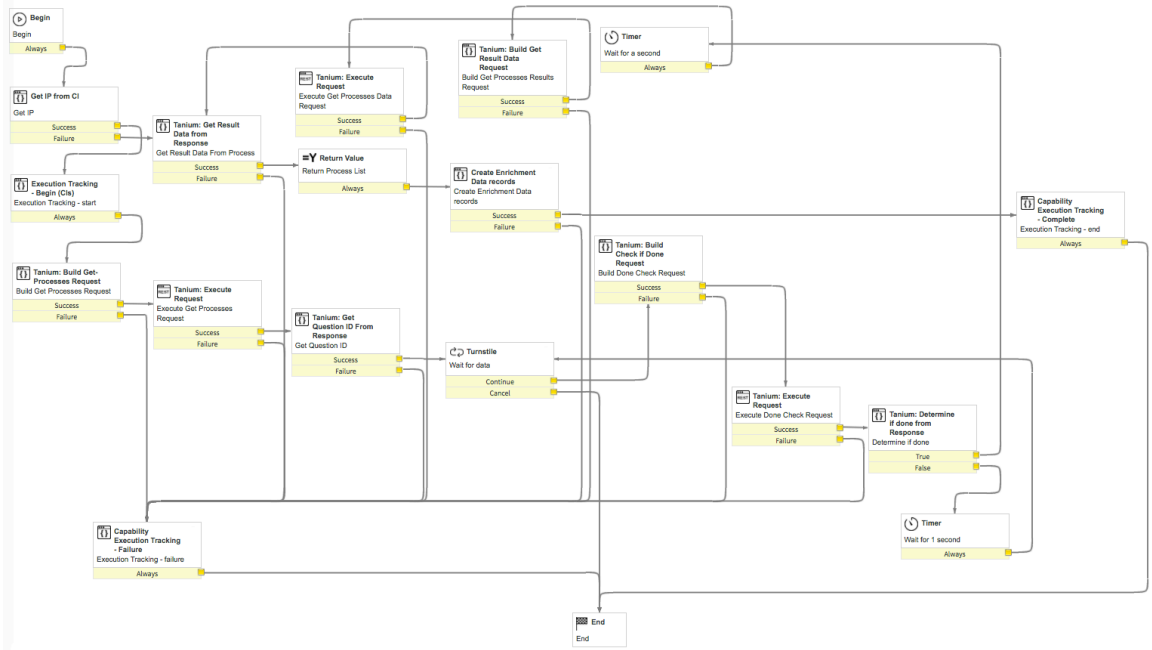
Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:

- Obter IP da atividade de IC
- Acompanhamento de execução de capacidade - Atividade com falha
- Tanium: executar atividade de solicitação
- Tanium: obter ID de pergunta da atividade de resposta
- Acompanhamento de execução - Atividade de início (ICs)
- Atividade de fluxo de trabalho da catraca - aguardar dados
- Tanium: Criar atividade de solicitação Verificar se concluído
- Tanium: determinar se foi concluído a partir da atividade de resposta
- Tanium: criar atividade de solicitação de dados de resultado
- Tanium: obter dados de resultado da atividade de resposta - retornar lista de processos
- Atividade Criar registros de dados de aprimoramento
- Atividade de fluxo de trabalho Temporizador - Aguarda 1 segundo
- Atividade Criar registros de dados de aprimoramento
- Acompanhamento de execução de capacidade - Concluir atividade

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Obter Processos em Execução



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Obter IP da atividade de IC

A atividade de fluxo de trabalho Obter IP do IC coleta o endereço IP dos itens de configuração (ICs) para usar no fluxo de trabalho.

A atividade Obter IP do IC pode ser usada com qualquer fluxo de trabalho para coletar endereços IP de item de configuração (IC) para usar no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Endereços IP encontrados.
Falha	Nenhum endereço IP encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
ci_sys_id	Identificador do item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
ip_addr	Endereços IP.

Tanium: criar atividade de solicitação de obtenção de processos

A atividade de fluxo de trabalho Tanium: obter dados de resultado da resposta cria uma solicitação de processos para usar no fluxo de trabalho.

A atividade Tanium: criar solicitação de obtenção de processos pode ser usada com qualquer fluxo de trabalho para criar uma solicitação de processo a ser usada no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Solicitação de processo criada.
Falha	Falha na solicitação de processo. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
ci_ip_address	Endereço IP do item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint	Especifica o endpoint SOAP criptografado a ser usado.
request_body	Conteúdo da solicitação SOAP criptografada.
http_timeout	Inteiro em segundos.
use_mid	Determina se o MID Server deve ser usado.

Tanium: executar atividade de solicitação

Esta atividade de fluxo de trabalho executa uma solicitação HTTP. As entradas definem o endpoint e o corpo da solicitação esperado. O próprio corpo da solicitação é o envelope SOAP criptografado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
request_body [Criptografado]	O corpo da solicitação SOAP. Este campo de entrada é obrigatório.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados. Este campo de entrada é obrigatório.
http_timeout [integer]	O valor do tempo limite de HTTP, em segundos.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code [integer]	Códigos de status HTTP padrão.
cabeçalho [cadeia de caracteres]	O cabeçalho SOAP.
corpo [cadeia de caracteres]	O corpo SOAP.
erro [cadeia de caracteres]	Quaisquer erros fornecidos pelo servidor.

Tanium: obter ID de pergunta da atividade de resposta

Esta atividade de fluxo de trabalho processa o corpo da resposta para obter o ID da pergunta.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
response_body [cadeia de caracteres]	O corpo da resposta SOAP.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
question_id [integer]	O ID da pergunta retornado do servidor Tanium.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tanium: Criar atividade de solicitação Verificar se concluído

Esta atividade de fluxo de trabalho cria uma solicitação do servidor Tanium para verificar se a coleta de dados para a pergunta foi concluída. Ele retorna a solicitação criptografada e outros componentes necessários para executar a solicitação.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
question_id [integer]	O ID da pergunta retornado do servidor Tanium.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados.
request_body [Criptografado]	O corpo da solicitação SOAP.
http_timeout [Inteiro]	O valor do tempo limite de HTTP, em segundos.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.

Tanium: executar atividade de solicitação

Esta atividade de fluxo de trabalho executa uma solicitação HTTP. As entradas definem o endpoint e o corpo da solicitação esperado. O próprio corpo da solicitação é o envelope SOAP criptografado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
request_body [Criptografado]	O corpo da solicitação SOAP. Este campo de entrada é obrigatório.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados. Este campo de entrada é obrigatório.
http_timeout [integer]	O valor do tempo limite de HTTP, em segundos.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
status_code [integer]	Códigos de status HTTP padrão.
cabeçalho [cadeia de caracteres]	O cabeçalho SOAP.
corpo [cadeia de caracteres]	O corpo SOAP.
erro [cadeia de caracteres]	Quaisquer erros fornecidos pelo servidor.

Tanium: determinar se foi concluído a partir da atividade de resposta

Esta atividade de fluxo de trabalho determina se uma solicitação foi concluída com base no corpo da resposta.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
response_body [cadeia de caracteres]	O corpo da solicitação SOAP retornado do Tanium.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
concluído [Booliano]	Retorna verdadeiro se o processamento da solicitação estiver concluído.

Tanium: criar atividade de solicitação de dados de resultado

Este fluxo de trabalho cria uma solicitação para coletar todos os dados retornados do Tanium em resposta a uma pergunta. Ele usa um ID de pergunta como entrada e fornece a saída para executar a solicitação, incluindo uma carga de envelope SOAP criptografada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
question_id [cadeia de caracteres]	O ID da pergunta apresentada ao Tanium.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados.
request_body [Criptografado]	O corpo da solicitação SOAP.
http_timeout [inteiro]	O valor do tempo limite de HTTP, em segundos.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.

Tanium: executar atividade de solicitação

Esta atividade de fluxo de trabalho executa uma solicitação HTTP. As entradas definem o endpoint e o corpo da solicitação esperado. O próprio corpo da solicitação é o envelope SOAP criptografado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
request_body [Criptografado]	O corpo da solicitação SOAP. Este campo de entrada é obrigatório.
use_mid [booliano]	Um sinalizador booliano que indica se o MID Server deve ser usado.
endpoint [cadeia de caracteres]	O endpoint criptografado do banco de dados. Este campo de entrada é obrigatório.
http_timeout [integer]	O valor do tempo limite de HTTP, em segundos.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code [integer]	Códigos de status HTTP padrão.
cabeçalho [cadeia de caracteres]	O cabeçalho SOAP.
corpo [cadeia de caracteres]	O corpo SOAP.
erro [cadeia de caracteres]	Quaisquer erros fornecidos pelo servidor.

Tanium: obter dados de resultado da atividade de resposta

A atividade de fluxo de trabalho Tanium: obter dados de resultado da resposta processa o corpo da resposta dos dados de resultado e gera uma matriz de objetos JSON que representa os resultados do Tanium.

A atividade Tanium: obter dados de resultado da resposta pode ser usada com qualquer fluxo de trabalho para recuperar dados de resultado a serem usados no fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Sucesso	Dados de resultado recuperados.
Falha	Nenhum dado recuperado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
response_body	Conteúdos de resposta SOAP criptografados
Id_implementação	Identificador de implementação.
afetado_ci	Item de configuração afetado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
data_resultado	Tipo de elemento de matriz de variáveis de API. Cada matriz contém pares de chave-valor compostos pela coluna e valores retornados do servidor. Se nenhum dado for recebido do servidor, a saída será uma matriz vazia.
saída	Dados de retorno formatados em processos em execução usados pelo fluxo de trabalho abstrato.

Fluxo de trabalho de integração de comandos do sistema de operações de segurança – Obter processos em execução

O fluxo de trabalho Integração de comandos do sistema de operações de segurança - Obter processos em execução recupera os processos em execução de um item de configuração quando adicionado ou atualizado para um incidente de segurança baseado em Windows ou Unix no estado de **análise**.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Para novos incidentes de segurança, o fluxo de trabalho é executado automaticamente quando você envia o incidente com um item de configuração selecionado, quando o estado muda automaticamente para **Análise**. Se permanecer no estado **Rascunho**, ele não será executado.

Tradução automática

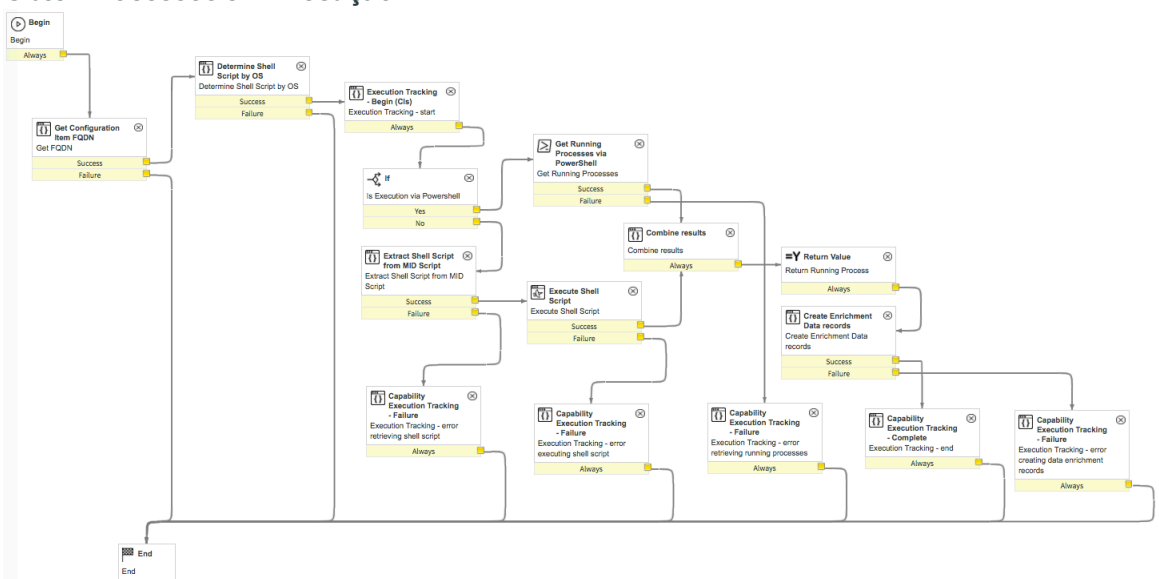
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Os incidentes de segurança existentes são atualizados automaticamente quando você está no estado **Análise** e adiciona um novo item de configuração.

As atividades do processo de fluxo de trabalho incluem:

- Atividade Obter FQDN do item de configuração
- Determinar Shell Script por atividade do SO
- Acompanhamento de execução - Iniciar atividade
- Obter processos em execução via PowerShell
- Atividade Executar script de shell
- Acompanhamento de execução de capacidade - Atividade com falha
- Atividade Extrair Shell Script do MID Script
- Combinar resultadose retornar valores em uma matriz
- Atividade Criar registros de dados de aprimoramento
- Acompanhamento de execução de capacidade - Concluir atividade

Obter Processos em Execução



Procedimento

1. Abra um incidente de segurança.
2. Atualize o **Estado** para **Análise**, se necessário.
3. Adicione um item de configuração (computador, servidor ou similar).
4. Clique em **Atualizar**.
   Orquestração de resposta de incidente de segurança fornece informações do processo em execução no **Link relacionados** > **Aprimoramentos de incidente de segurança**guia. Para obter mais informações, consulte Security Operations mapeamento de dados de aprimoramento.

   Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade Obter FQDN do item de configuração

O **Orquestração do Security Common** > **Obter FQDN do item de configuração** A atividade de fluxo de trabalho recupera o nome de domínio totalmente qualificado (FQDN) de um item de configuração. Esta atividade pode acelerar o processo de investigação e correção.

A atividade Obter FQDN do item de configuração pode ser usada com qualquer fluxo de trabalho para recuperar o nome de domínio totalmente qualificado (FQDN) de um item de configuração.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
cmdb_ci.id [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
fqdn [cadeia de caracteres]	O nome de domínio totalmente qualificado (FQDN) do item de configuração.

Anotações Adicionais

O campo fqdn no item de configuração deve ser preenchido.

Determinar Shell Script por atividade do SO

A atividade de fluxo de trabalho Determinar Shell Script por SO determina qual sistema operacional será usado no fluxo de trabalho

A atividade Determinar Shell Script por SO pode ser usada com qualquer fluxo de trabalho para determinar qual script de shell executar com base no sistema operacional em execução no sistema que contém o item de configuração.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Sistema operacional encontrado.
Falha	Nenhum sistema operacional encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
ciSysId	Identificador do sistema do item de configuração.
processType	Identificador interno que define qual script extrair da tabela.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
processScript	Agente de ECC que reúne o processo em execução.
executionTemplate	Determina se o script será executado por meio de um probe ou usando o PowerShell.
richmentMappingId	Identificador do sistema do mapeamento de aprimoramento usado para transformar os dados de resposta.

Obter processos em execução por meio da atividade do PowerShell

A atividade de fluxo de trabalho Obter ID do sensor reúne processos em execução usando o PowerShell para usar no fluxo de trabalho.

A atividade de fluxo de trabalho Obter processos em execução via PowerShell pode ser usada com qualquer fluxo de trabalho para recuperar processos a serem incluídos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Processos encontrados
Falha	Nenhum processo encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
destino	IP ou nome de domínio totalmente qualificado (FQDN) do IC de destino.
processScript	Script ECC executado em um sistema baseado em Windows.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Saída bruta. Dados de processos em execução.

Atividade Extrair Shell Script do MID Script

A atividade de fluxo de trabalho Extrair Shell Script do MID script extrai um script de shell do MID server para usar com no fluxo de trabalho.

A atividade Extrair Shell Script do MID Script pode ser usada com qualquer fluxo de trabalho para extrair um script de shell do MID server para incluir no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Shell script encontrado
Falha	Nenhum script de shell encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
sysId	Identificador do sistema

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
scriptValue	Script, como um valor de cadeia de caracteres, executado em um sistema Unix.

Atividade Executar script de shell

A atividade de fluxo de trabalho Executar Script de Shell executa um script de shell do MID server no fluxo de trabalho.

A atividade Executar Shell Script pode ser usada com qualquer fluxo de trabalho para executar um script de shell do MID server no fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Shell script encontrado
Falha	Nenhum script de shell encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
destino	IP ou nome de domínio totalmente qualificado (FQDN) do IC de destino.
scriptValue	Script, como um valor de cadeia de caracteres, executado em um sistema Unix.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Saída bruta. Dados de processos em execução.

Atividade Combinar resultados

A atividade de fluxo de trabalho Combinar resultados mescla os resultados de integrações de terceiros para usar no fluxo de trabalho.

A atividade Combinar resultados pode ser usada com qualquer fluxo de trabalho para executar um script de shell do MID server no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Resultados combinados.
Falha	Falha na combinação. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
entradaA	Conjunto de resultados A
entradaB	Conjunto de resultados B
Id_implementação	Identificador de implementação.
afetado_ci	Item de configuração

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado	Conjunto de resultados A ou conjunto de resultados B, dependendo de qual for preenchido.

Integração do Security Operations - Capacidade Isolar host

A funcionalidade **Isolar Host** restringe as conexões do sistema a outros dispositivos. Isolar host é executado em um item de configuração (IC).

A capacidade **Isolar Host** tem um fluxo de trabalho, Security Operations - Isolar fluxo de trabalho de host que aceita um ou mais ICs e, opcionalmente, uma implementação. Você pode especificar uma implementação a ser usada para isolar o host ou para o fluxo de trabalho tentar isolar o host usando todas as implementações.

Nota:
Embora não esteja integrado a um recurso, um fluxo de trabalho, Fluxo de trabalho Security Operations Carbon Black Integration - Remover isolamento de host está disponível para orquestração para restaurar a comunicação com um host isolado.

Nota:
Se não houver implementações disponíveis, as ações de recurso não serão exibidas nos menus do produto.

Executar Isolar Host

Isolar host restringe as conexões do sistema a outros dispositivos.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Nota:
Se não houver implementações disponíveis, as ações de recurso não serão exibidas nos menus do produto.

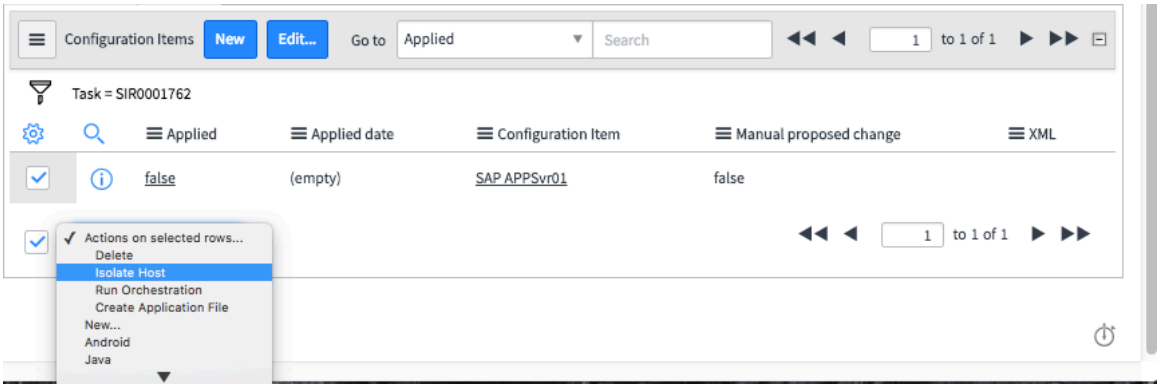
O fluxo de trabalho **Security Operations Integration - Isolar Host ou Endpoint**pode ser acionado a partir da lista relacionada em um incidente de segurança.

Procedimento

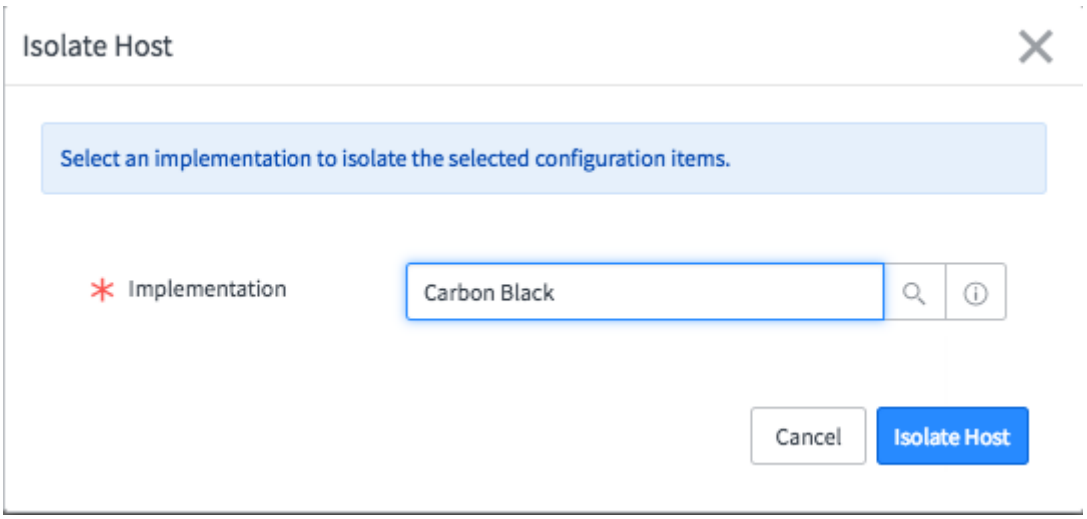
1. Navegue até um incidente de segurança.
2. Selecione **Itens de configuração** na guia **Lista relacionada**.
3. Clique em **Isolar host** no menu suspenso **Ações nas linhas selecionadas...**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A caixa de diálogo é exibida.



4. Escolha a implementação.
5. Clique **em Isolar host**.
   A auditoria de execução do fluxo de trabalho é exibida na seção de anotações de trabalho.

Security Operations - Isolar fluxo de trabalho de host

O fluxo de trabalho **Security Operations - Isolar host** é um fluxo de trabalho de alto nível independente de integrações. Ele usa as consultas configuradas para pesquisar um conjunto de itens de configuração. Use-o para realizar uma integração, como Carbon Black.

Antes de Iniciar

Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

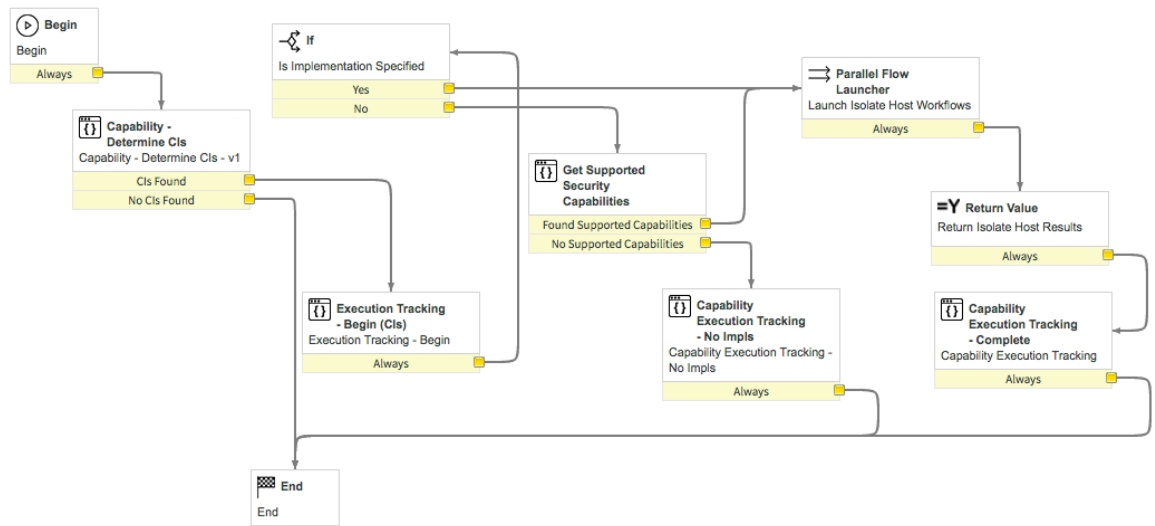
Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho é acionado na guia **Itens de configuração** em uma lista relacionada de incidente de segurança.

As atividades do processo de fluxo de trabalho incluem:

- Capacidade - Atividade Determinar ICs
- Acompanhamento de execução - Atividade de início (ICs)
- Atividade Obter capacidades de segurança compatíveis
- Inicializador de fluxo paralelo : inicia o fluxo de trabalho apropriado. Armazene os resultados em uma matriz.
- Rastreamento de execução de capacidade - Nenhuma atividade de implementação
- Acompanhamento de execução de capacidade - Atividade com falha

Isolar Host



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Capacidade - Atividade Determinar ICs

A atividade de fluxo de trabalho Capacidade - Determinar ICs determina quais itens de configuração (ICs) serão incluídos no fluxo de trabalho.

A atividade Capacidade - Determinar ICs pode ser usada com qualquer fluxo de trabalho para determinar quais ICs serão incluídos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Itens de configuração encontrados.
Falha	Nenhum IC encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
task_sys_id	Identificador de tarefa (mapeia o incidente de segurança para ICs).
cis_affected	Itens de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
cis_affected	ICs filtrados
task_sys_id	Identificador de tarefa (mapeia o incidente de segurança para ICs).

Atividade Obter capacidades de segurança compatíveis

A atividade de fluxo de trabalho Obter capacidades compatíveis recupera o nome e o número de integrações que estão ativas e oferecem suporte à funcionalidade solicitada.

A atividade Obter capacidades compatíveis pode ser usada com qualquer fluxo de trabalho para determinar quais recursos são compatíveis.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Integração que oferece suporte ao recurso encontrado.
Falha	Ocorreu um erro ao tentar encontrar uma integração ativa que ofereça suporte ao recurso. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityName	Nome da capacidade.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
domainId	Identificador do sistema para qualquer domínio associado ao fluxo de trabalho.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
SupportedCapabilities	Lista de integrações compatíveis com a funcionalidade.
capacidadeContagem	Número de integrações compatíveis com a funcionalidade.

Rastreamento de execução de capacidade - Nenhuma atividade de implementação

A atividade de fluxo de trabalho Rastreamento de execução de capacidade - sem implementações cria um registro de erro quando nenhuma implementação de capacidade de integração é encontrada.

A atividade Rastreamento de execução de capacidade - Sem Impls pode ser usada com qualquer fluxo de trabalho de capacidade de integração abstrata para lidar com a condição de erro quando nenhuma implementação de capacidade configurada estiver disponível.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de acompanhamento de execução é definido como **Erro** e uma mensagem indicando o erro é registrada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capacidadeExecutionId	Identificador do sistema para o registro de auditoria. Saída da atividade usada para iniciar o acompanhamento de execução.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Variáveis de saída

Não há variáveis de saída.

Security Operations Carbon Black Integration - Isolar fluxo de trabalho de host

A Integração Carbon Black do Security Operations - Isolar Host é a implementação da integração Carbon Black iniciada pelo fluxo de trabalho Integração do Security Operations - Isolar Host.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:

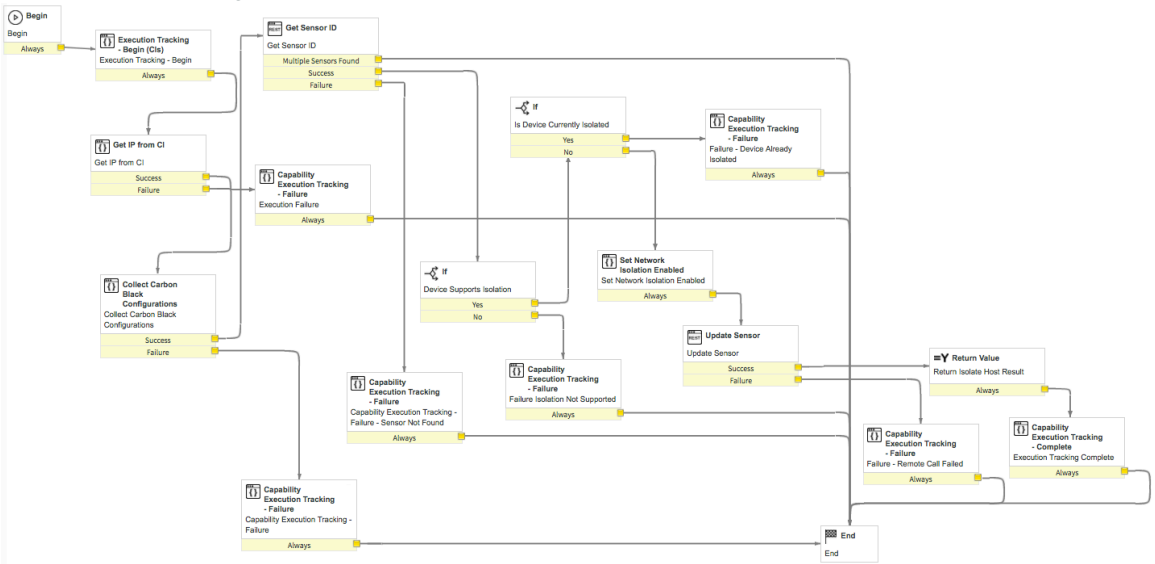
- Acompanhamento de execução - Atividade de início (ICs)
- Obter IP do IC

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Coletar configurações do Carbon Black
- Acompanhamento de execução de capacidade - Atividade com falha
- Obter Identificador de Sensor
- Definir o isolamento de rede como habilitado
- Atualizar sensor : retorna o resultado de Isolar host.
- Acompanhamento de execução de capacidade - Concluir atividade

Carbon Black Integration - Isolar host



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Obter IP da atividade de IC

A atividade de fluxo de trabalho Obter IP do IC coleta o endereço IP dos itens de configuração (ICs) para usar no fluxo de trabalho.

A atividade Obter IP do IC pode ser usada com qualquer fluxo de trabalho para coletar endereços IP de item de configuração (IC) para usar no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Endereços IP encontrados.
Falha	Nenhum endereço IP encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Tradução automática

Variável	Descrição
ci_sys_id	Identificador do item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ip_addr	Endereços IP.

Atividade Coletar configurações do Carbon Black

A atividade de fluxo de trabalho Coletar configurações do Carbon Black reúne informações de configuração para usar no fluxo de trabalho.

A atividade Coletar configurações do Carbon Black coleta informações de configuração do Carbon Black para usar no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

Não há variáveis de entrada para esta atividade.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com Carbon Black ou não.
api_token	Chave de API de integração de terceiros.

Atividade Obter ID de sensor

A atividade de fluxo de trabalho Obter ID de sensor reúne identificadores de sensor para usar no fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A atividade Obter ID do sensor pode ser usada com qualquer fluxo de trabalho para coletar informações do sensor para usar no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Identificadores de sensor encontrados.
Falha	Nenhum sensor encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
api_token	Chave de API Carbon Black.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com Carbon Black ou não.
endpoint_base	URL base da API Carbon Black.
ci_ip_address	Endereço IP do item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
Tipo de elemento de matriz	Variáveis de API.
sensor_detail	Descrição do sensor Carbon Black no formato JSON.

Atividade Definir isolamento de rede habilitado

A atividade de fluxo de trabalho Definir isolamento de rede habilitado permite o isolamento de rede.

A atividade Definir isolamento de rede habilitado pode ser usada com qualquer fluxo de trabalho para habilitar o isolamento de rede.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Isolamento de rede habilitado.
Falha	O isolamento de rede não pode ser habilitado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
sensor_detail	Descrição do sensor Carbon Black no formato JSON.
desativar	Determina se o host está isolado ou remove o isolamento do host. Verdadeiro = desabilitar isolamento Falso = o isolamento permanece habilitado

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
sensor_detail	Descrição do sensor Carbon Black no formato JSON.

Atualizar atividade do sensor

A atividade de fluxo de trabalho Atualizar sensor atualiza o sensor para isolar hosts ou endpoints.

A atividade Atualizar sensor pode ser usada com qualquer fluxo de trabalho para isolar hosts ou endpoints.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Sensor atualizado.
Falha	Não é possível atualizar o sensor. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
api_token	Chave de API Carbon Black.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com Carbon Black ou não.
endpoint_base	URL base da API Carbon Black.
sensor_id	Identificador do sensor.
sensor_detail	Descrição do sensor Carbon Black no formato JSON.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.

Fluxo de trabalho Security Operations Carbon Black Integration - Remover isolamento de host

O fluxo de trabalho **Security Operations Carbon Black Integration - Remove Host Isolation** desbloqueia a comunicação com um host ou endpoint especificado em um sistema Carbon Black.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho não faz parte de uma funcionalidade e precisa de uma orquestração personalizada para ser executado.

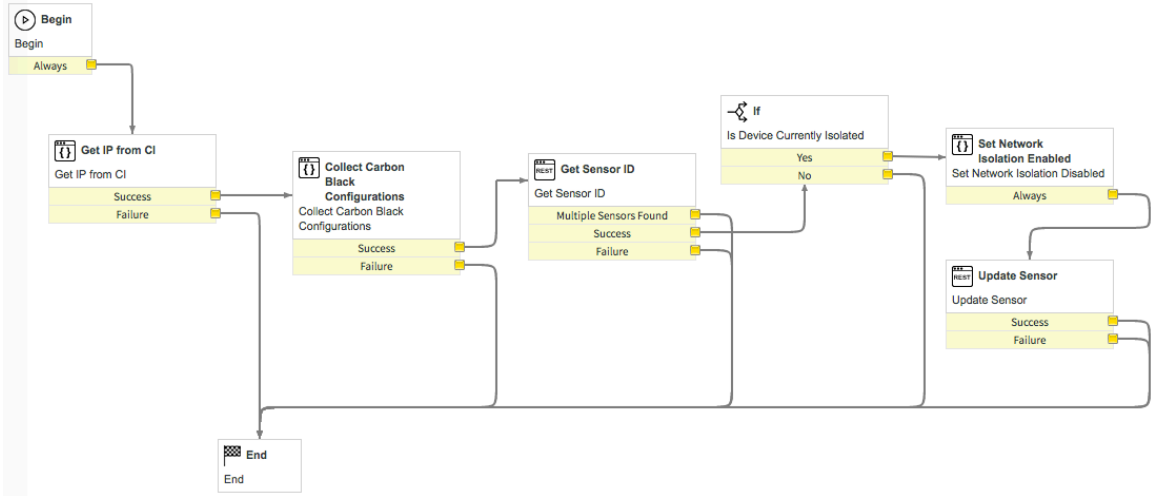
As atividades do processo de fluxo de trabalho incluem:

- Obter IP do IC
- Em caso de sucesso - Coletar configurações Carbon Black
- Obter Identificador de Sensor
- Se - O dispositivo oferecer suporte ao isolamento - e o dispositivo não estiver isolado:defina o Isolamento de rede habilitado como desabilitado.
- Atualizar sensor : retorna o resultado de Isolar host.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Carbon Black Integration - Remover isolamento de host



Obter IP da atividade de IC

A atividade de fluxo de trabalho Obter IP do IC coleta o endereço IP dos itens de configuração (ICs) para usar no fluxo de trabalho.

A atividade Obter IP do IC pode ser usada com qualquer fluxo de trabalho para coletar endereços IP de item de configuração (IC) para usar no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Endereços IP encontrados.
Falha	Nenhum endereço IP encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
ci_sys_id	Identificador do item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ip_addr	Endereços IP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade Coletar configurações do Carbon Black

A atividade de fluxo de trabalho Coletar configurações do Carbon Black reúne informações de configuração para usar no fluxo de trabalho.

A atividade Coletar configurações do Carbon Black coleta informações de configuração do Carbon Black para usar no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

Não há variáveis de entrada para esta atividade.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com Carbon Black ou não.
api_token	Chave de API de integração de terceiros.

Atividade Obter ID de sensor

A atividade de fluxo de trabalho Obter ID de sensor reúne identificadores de sensor para usar no fluxo de trabalho.

A atividade Obter ID do sensor pode ser usada com qualquer fluxo de trabalho para coletar informações do sensor para usar no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Identificadores de sensor encontrados.
Falha	Nenhum sensor encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
api_token	Chave de API Carbon Black.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com Carbon Black ou não.
endpoint_base	URL base da API Carbon Black.
ci_ip_address	Endereço IP do item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.
Tipo de elemento de matriz	Variáveis de API.
sensor_detail	Descrição do sensor Carbon Black no formato JSON.

Atividade Definir isolamento de rede habilitado

A atividade de fluxo de trabalho Definir isolamento de rede habilitado permite o isolamento de rede.

A atividade Definir isolamento de rede habilitado pode ser usada com qualquer fluxo de trabalho para habilitar o isolamento de rede.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Isolamento de rede habilitado.
Falha	O isolamento de rede não pode ser habilitado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
sensor_detail	Descrição do sensor Carbon Black no formato JSON.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
desativar	Determina se o host está isolado ou remove o isolamento do host. Verdadeiro = desabilitar isolamento Falso = o isolamento permanece habilitado

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
sensor_detail	Descrição do sensor Carbon Black no formato JSON.

Atualizar atividade do sensor

A atividade de fluxo de trabalho Atualizar sensor atualiza o sensor para isolar hosts ou endpoints.

A atividade Atualizar sensor pode ser usada com qualquer fluxo de trabalho para isolar hosts ou endpoints.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Sensor atualizado.
Falha	Não é possível atualizar o sensor. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
api_token	Chave de API Carbon Black.
use_mid_server	Determina se a atividade REST usa o MID server para interagir com Carbon Black ou não.
endpoint_base	URL base da API Carbon Black.
sensor_id	Identificador do sensor.
sensor_detail	Descrição do sensor Carbon Black no formato JSON.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
status_code	Determina se a solicitação foi bem-sucedida. Caso contrário, exibirá um código de erro HTTP e uma mensagem.

Integração do Security Operations - Capacidade de publicar na lista de observação

A funcionalidade Publicar na lista de observação adiciona observáveis e indicadores associados a um incidente de segurança a uma lista de observação de terceiros que monitora eventos de segurança e gera alertas. Essa capacidade é usada como parte da resposta do incidente durante as investigações.

Nota:
Se não houver implementações disponíveis, as ações de recurso não serão exibidas nos menus do produto.

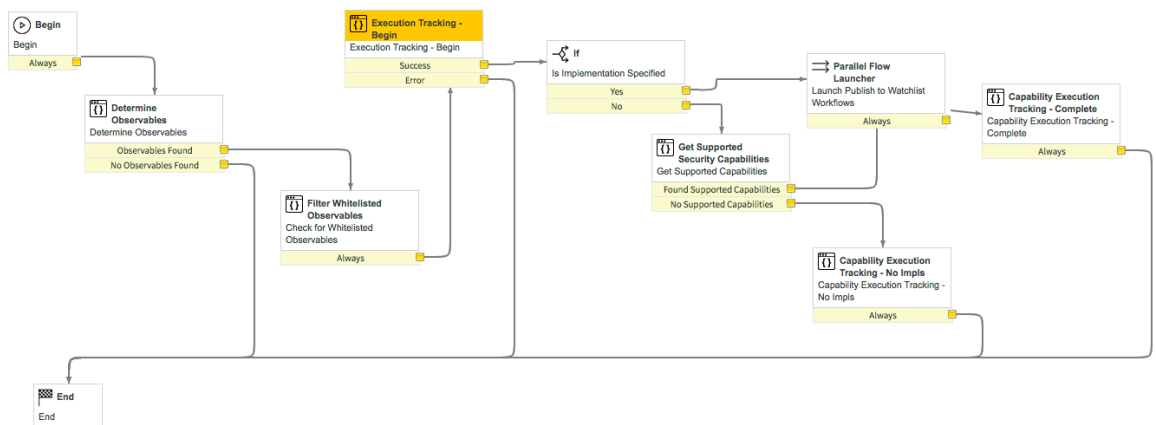
Integração do Security Operations - Fluxo de trabalho Publicar na lista de observação

O fluxo de trabalho **Integrações do Security Operations - Publicar na lista de** observação é um fluxo de trabalho de alto nível independente de integrações. Ele adiciona observáveis a listas de observação de terceiros que oferecem suporte ao recurso. Use-o para realizar uma integração.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é visível e é executado somente quando uma integração está disponível. Ele é acionado na guia **Observáveis** ou **Indicadores associados** em um incidente de segurança.

Publicar na Watchlist



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Atividade Determinar observáveis

A atividade de fluxo de trabalho **Determinar observáveis** determina qual observável incluir no fluxo de trabalho

A atividade **Determinar observáveis** pode ser usada com qualquer fluxo de trabalho para determinar quais observáveis serão incluídos no fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Observáveis encontrados
Falha	Nenhum observável encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
task_sys_id	Identificador de tarefa (mapeia o incidente de segurança para observáveis).
observáveis	Endereços IP, hash, URLs, nomes de domínio.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
observáveis	Observáveis filtrados

Atividade Filtrar observáveis na lista de permissões

A atividade de fluxo de trabalho Observáveis na lista de permissões filtrados remove observáveis que podem ser ignorados da lista de observáveis. Esta atividade pode acelerar o processo de investigação e correção.

A atividade Filtrar observáveis na lista de permissões pode ser usada com qualquer fluxo de trabalho para filtrar observáveis antes de executar qualquer ação.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Lista de filtros criada.
Falha	Ocorreu um erro ao tentar filtrar os observáveis. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
observáveis	Lista de observáveis disponíveis.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
observáveis filtrados	Observáveis filtrados.

Atividade Obter capacidades de segurança compatíveis

A atividade de fluxo de trabalho Obter capacidades compatíveis recupera o nome e o número de integrações que estão ativas e oferecem suporte à funcionalidade solicitada.

A atividade Obter capacidades compatíveis pode ser usada com qualquer fluxo de trabalho para determinar quais recursos são compatíveis.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Integração que oferece suporte ao recurso encontrado.
Falha	Ocorreu um erro ao tentar encontrar uma integração ativa que ofereça suporte ao recurso. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityName	Nome da capacidade.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
domainId	Identificador do sistema para qualquer domínio associado ao fluxo de trabalho.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
SupportedCapabilities	Lista de integrações compatíveis com a funcionalidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
capacidadeContagem	Número de integrações compatíveis com a funcionalidade.

Rastreamento de execução de capacidade - Nenhuma atividade de implementação

A atividade de fluxo de trabalho Rastreamento de execução de capacidade - sem implementações cria um registro de erro quando nenhuma implementação de capacidade de integração é encontrada.

A atividade Rastreamento de execução de capacidade - Sem Impls pode ser usada com qualquer fluxo de trabalho de capacidade de integração abstrata para lidar com a condição de erro quando nenhuma implementação de capacidade configurada estiver disponível.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de acompanhamento de execução é definido como **Erro** e uma mensagem indicando o erro é registrada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capacidadeExecutionId	Identificador do sistema para o registro de auditoria. Saída da atividade usada para iniciar o acompanhamento de execução.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Variáveis de saída

Não há variáveis de saída.

Integração do Security Operations com o recurso Pesquisa de detecções

A **funcionalidade Pesquisa** de vistas aceita um conjunto de observáveis, encontra todas as integrações que oferecem suporte a uma pesquisa de vistas e executa essas pesquisas.

A capacidade Pesquisa de vistas tem um fluxo de trabalho, Integração do Security Operations - Fluxo de trabalho de pesquisa de detecções, que executa a pesquisa de vistas. Este fluxo de trabalho aceita uma lista de observáveis, encontra todos os recursos de implementação, cria as consultas com base nas configurações de pesquisa de vistas e executa as pesquisas com base no fluxo de trabalho configurado. Quando a pesquisa estiver concluída, uma anotação será adicionada às Anotações de trabalho do incidente, incluindo se alguma vista foi encontrada e, em caso afirmativo, quantos.

Para exibir as Configurações de pesquisa de vistas, navegue até **Security Operations** > **Integrações** > **Configurações de Pesquisa de Vistas**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Se não houver implementações disponíveis, as ações de recurso não serão exibidas nos menus do produto.

Criar registros de configuração de pesquisa de vistas

Crie vários registros de configuração de pesquisa de vistas e use-os ao consultar vários armazenamentos de log ou variar os parâmetros de pesquisa.

Antes de Iniciar

Função necessária: sn_si.admin

- O complemento CIM deve ser instalado na instância do Splunk.
- Pesquisas salvas e consultas no local são compatíveis somente com a integração do Splunk.

Por Que e Quando Desempenhar Esta Tarefa

Você também pode criar registros de configuração de pesquisa de vistas para invocar pesquisas salvas no armazenamento de log do Splunk Enterprise.

Nota:
As consultas de configuração de pesquisa dependem dos dados de log do Splunk para serem compatíveis com o Splunk Common Information Model (CIM).

Com as configurações de pesquisa salvas, você pode:

- Crie pesquisas personalizadas que combinam vários registros de evento.
- Pesquisas eficazes e com design eficiente.
- Use entradas parametrizadas na pesquisa salva do Splunk.

O sistema de base inclui as configurações de amostra, conforme mostrado nesta imagem:

Configurações de pesquisa salvas

		Name	Observable type	Search	Is saved search
		Search	Search	Search	Search
☐	ⓘ	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
☐	ⓘ	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
☐	ⓘ	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

A pesquisa salva e as consultas de configuração Inplace são consultas de exemplo e podem ser substituídas por parâmetros apropriados para o seu ambiente. Crie configurações adicionais de pesquisa salva conforme necessário. Ao definir uma configuração de pesquisa salva, o nome e os parâmetros na consulta de pesquisa devem corresponder à configuração salva definida na sua instância do Splunk. Se o nome e os parâmetros não forem os mesmos, talvez você não veja resultados precisos ao executar uma pesquisa de vistas.

Nota:
Na sua instância do Splunk, navegue até a página Pesquisas, relatórios e alertas e localize sua consulta de pesquisa salva. Clique no link **Permissões** para navegar até a página Permissões. Selecione o botão de opção **Todos os aplicativos** e habilite a opção **Permissão de leitura** para **Todos**. Isso mudará o valor da coluna Compartilhamento de Privado para Aplicação para sua consulta de pesquisa salva. Se isso não estiver definido, a consulta de pesquisa salva pode não retornar resultados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

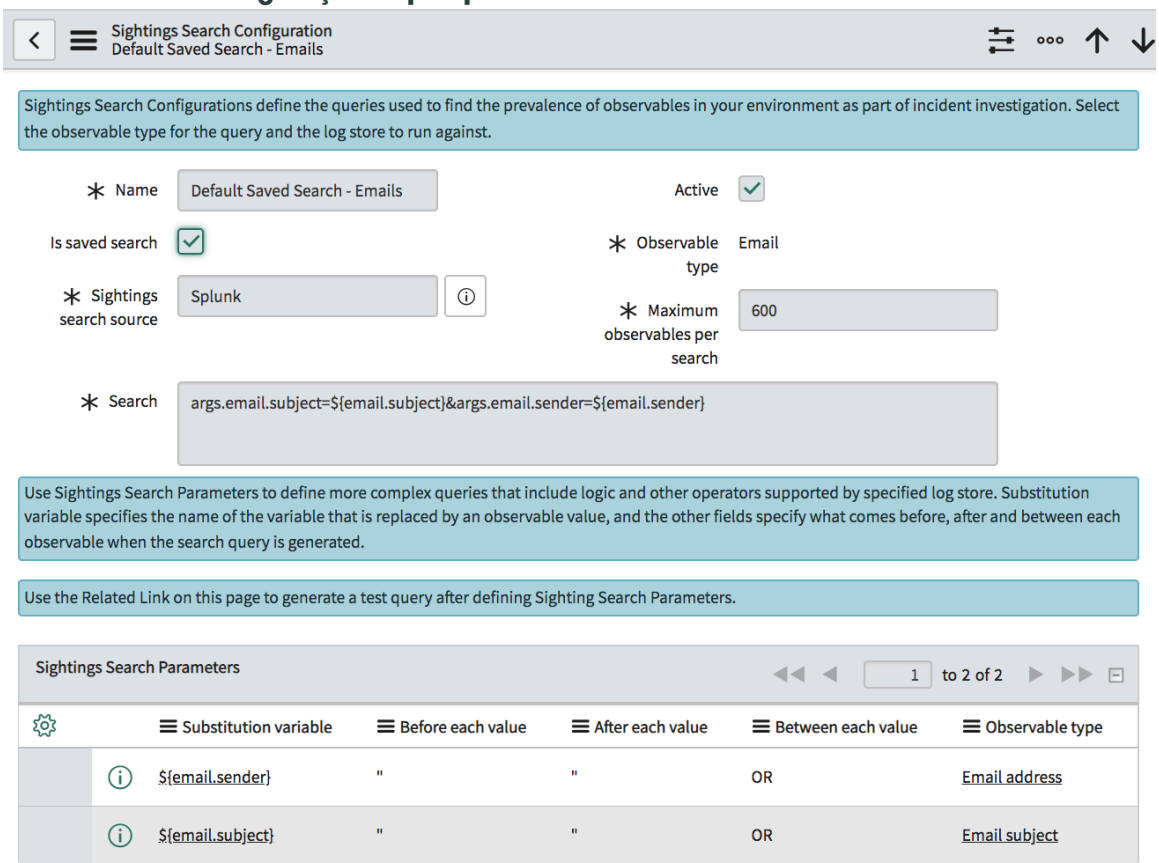
Para verificar se a configuração de pesquisa salva corresponde à configuração definida na sua instância do Splunk:

1. Navegar até **Configurações** > **Pesquisas, relatórios e alertas**.
2. Altere o **Contexto da aplicação** para **Todos**.

   Uma lista de relatórios de pesquisa será exibida.
3. Confirme se a consulta de pesquisa salva está presente na lista.

Por exemplo, o formulário Configuração de pesquisa de vistas contém o endereço de e-mail e o remetente do e-mail como parâmetros de pesquisa:

Formulário de Configuração de pesquisa de vistas



Na instância do Splunk, defina a pesquisa salva com o mesmo nome, Pesquisa salva padrão - e-mails e os mesmos parâmetros de pesquisa para o endereço e o assunto do e-mail. Se o nome e os parâmetros de pesquisa não forem iguais, a pesquisa de vistas não gerará um resultado preciso.

Procedimento

1. Navegar até **Security Operations** > **Integrações** > **Configuração de Pesquisa de Vistas** e crie um novo registro (consulte a tabela para obter as descrições dos campos).

Formulário de Configuração de pesquisa de vistas

Campo	Descrição
Nome	Nome da configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Pesquisa salva	A configuração de pesquisa salva será criada se você selecionar esta opção.
Origem de pesquisa de vistas	A origem da pesquisa de vistas. Selecione o armazenamento de log do Splunk como a origem.
Ativo	Opção para o status de pesquisa salvo. Somente configurações de pesquisa ativas podem ser usadas para executar uma pesquisa de vistas.
Tipo de observável	O tipo de observável pode ser qualquer tipo de observável, como IP, valor de hash, URL, nome de domínio e assim por diante.
Máximo de observáveis por pesquisa	Número máximo de observáveis a serem retornados da pesquisa.
Pesquisar	A cadeia de caracteres de pesquisa padrão é `$(observable)`, mas você pode definir sua própria consulta de pesquisa especificando parâmetros que são compatíveis com o armazenamento de log do Splunk.

2. Clique em **Enviar**.

Resultado
Você criou um registro de configuração de pesquisa de vistas.

O que Fazer Depois
Depois de definir a consulta de pesquisa, clique em **Gerar consulta de teste de pesquisa de detecções**e especifique uma lista de valores observáveis para gerar uma consulta de teste com base nesta configuração de pesquisa salva.

Executar uma pesquisa de vistas

Determine a predominância de uma ameaça ao longo do tempo ou teste os esforços de correção ou erradicação. Você pode selecionar observáveis individuais ou vários e o intervalo de datas para sua pesquisa de um incidente de segurança. Os resultados são incluídos na lista relacionada **de observáveis de incidente de segurança**.

Antes de Iniciar
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa
A capacidade Pesquisa de vistas tem um fluxo de trabalho, Integração do Security Operations - Fluxo de trabalho de pesquisa de detecções, que executa a pesquisa de vistas. Este fluxo de trabalho aceita uma lista de observáveis, encontra todos os recursos de implementação, cria as consultas com base nas configurações de pesquisa de vistas e executa as pesquisas com base no fluxo de trabalho configurado.

Nota:
Uma implementação ativa deve ser configurada. O Sightings Search oferece suporte ao aprimoramento de incidentes do Elasticsearch, Splunk, McAfee ESM, HPE ArcSight Logger e QRadar. Se não houver implementações disponíveis, as ações de recurso, como **Executar pesquisa**de vistas, não serão exibidas nos menus do produto.

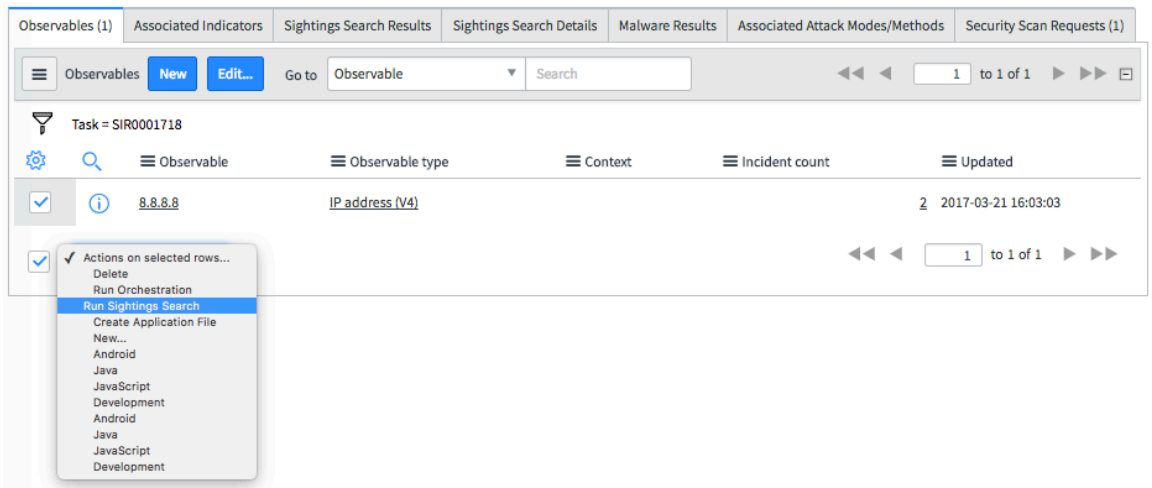
Procedimento

1. Navegue até um incidente de segurança.
2. Clique no link relacionado **Mostrar IoC**.
3. Selecione **Observáveis** na guia Lista relacionada.

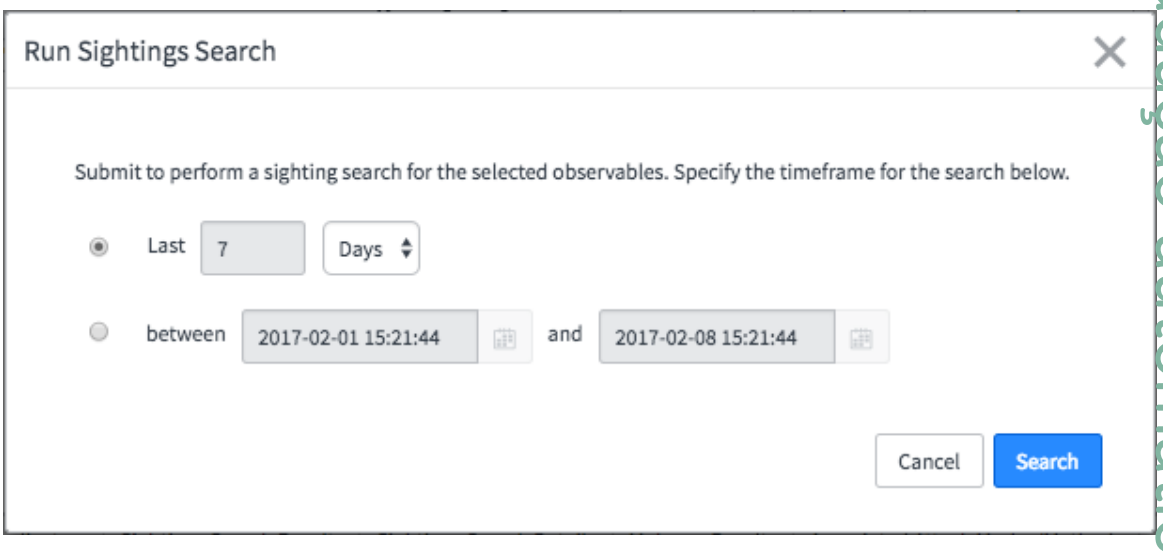
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Selecione os observáveis nos quais você deseja executar uma pesquisa de vistas.
5. Clique em **Executar pesquisa** de vistas no menu suspenso **Ações nas linhas selecionadas...**



A caixa de diálogo Executar pesquisa de vistas é aberta.



Nota:
Os valores inseridos na caixa de diálogo substituem os valores de configuração de recurso para esta execução.

6. Escolha o número de dias ou um intervalo de datas para pesquisar dados.

Opção	Descrição
Último	O número de horas ou dias anteriores à criação do incidente a ser pesquisado. O padrão é 7 dias. O limite é de 99 horas ou dias.
entre	Intervalo de datas para pesquisa. As datas padrão são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	A data e a hora em que o incidente foi aberto. A data e a hora sete dias antes da abertura do incidente.

Nota:
O **último** é o número de horas ou dias anteriores à criação do incidente a ser pesquisado. O padrão é 7 dias. O limite é de 99 horas ou dias.

7. Clique em **Pesquisar**.
Um registro de pesquisa de detecções é criado. Os dados agregados e de vistas associadas são exibidos no incidente de segurança nas guias **Resultados** da pesquisa de vistas e **Detalhes da pesquisa** de vistas.

Nota:
Os dados dos resultados da pesquisa de detecções podem ser compartilhados com Trusted Security Circle, com exceção dos dados brutos no caso de implementações configuradas para incluir dados brutos.

Resultados da pesquisa de detecções

Resultado	Descrição
Número	O identificador da pesquisa de vistas.
Contagem de observáveis	Número de observáveis pesquisados por consulta.
Vistas internas	Contagem de vistas internas.
Vistas externas	Contagem de avistamentos externos. (Recebido do compartilhamento de ameaças.)
Itens de configuração correspondentes	Contagem de itens de configuração que corresponderam a um registro existente no seu cmdb para cada observável encontrado em seu ambiente.
Intervalo de datas de início	Hora de começar a procurar vistas.
Intervalo de datas de término	Hora de parar de procurar vistas.
Atualizado em:	Data e hora da última modificação.

Observação: se a implementação usada para a pesquisa de vistas estiver configurada para incluir dados brutos e pelo menos uma vista for encontrada, um anexo contendo amostras de dados brutos aparecerá na parte superior do incidente de segurança.

Detalhes da pesquisa de detecções

Detalhe	Descrição
Pesquisa de vista	O identificador da pesquisa de vistas.
Observável	Observável pesquisado por consulta.
Tipo de observável	Tipo de observável pesquisado por consulta.
Vistas internas	Contagem agregada de vistas internas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhe	Descrição
Vistas externas	Contagem agregada de avistamentos externos. (Recebido do compartilhamento de ameaças.)
Atualizado em:	Data e hora da última modificação.

Integração do Security Operations - Fluxo de trabalho de pesquisa de detecções

O fluxo de trabalho**Security Operations Integration - Sightings Search** é um fluxo de trabalho de alto nível independente de integrações. Ele usa as consultas configuradas para pesquisar um conjunto de observáveis com base nas integrações configuradas que oferecem suporte ao recurso. Use-o para realizar uma integração como Splunk ou Elasticsearch.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

Se um incidente de segurança tiver um observável anexado a ele, este fluxo de trabalho será acionado quando você clicar em **Executar pesquisa de detecções** no menu suspenso **Ações em linhas selecionadas...** na guia **Observáveis de incidente de segurança**.

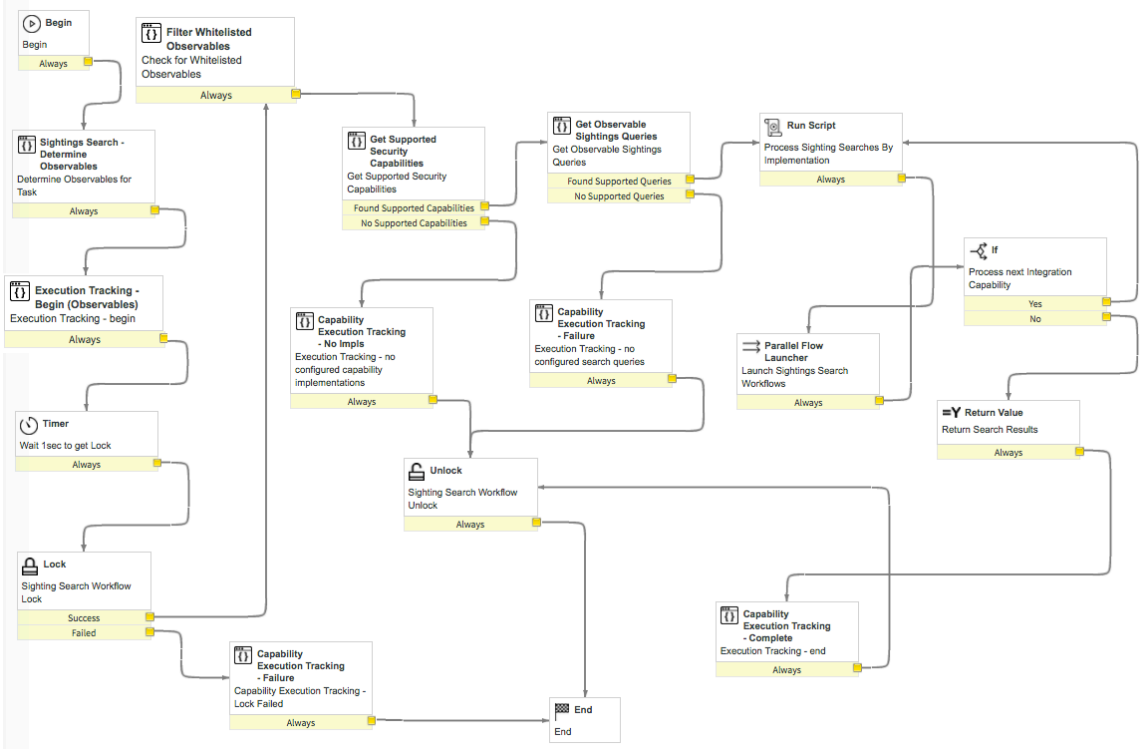
As atividades do processo de fluxo de trabalho incluem:

- Atividade Determinar observáveis
- Acompanhamento de execução - Iniciar atividade
- Atividade de fluxo de trabalho Temporizador : aguarda um segundo para obter um bloqueio.
- Bloquear atividade de fluxo de trabalho
- Filtrar observáveis listados como permitidos
- Atividade Obter capacidades de segurança compatíveis
- Rastreamento de execução de capacidade - Nenhuma atividade de implementação
- Desbloquear fluxo de trabalho atividade
- Atividade Obter consultas de vistas de observável
- Acompanhamento de execução de capacidade - Atividade com falha
- Executar script fluxo de trabalho atividade
- Inicializador de Fluxo paralelo
- Se a atividade do fluxo de trabalho Se a atividade do fluxo de trabalho : iterar até que todos os fluxos de trabalho apropriados tenham sido executados e armazenar os resultados em uma matriz.
- Acompanhamento de execução de capacidade - Concluir atividade

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de Vistas



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Pesquisa de vistas - Atividade Determinar observáveis

A atividade de fluxo de trabalho **Pesquisa de vistas - Determinar observáveis** determina quais observáveis serão incluídos no fluxo de trabalho.

A atividade **Pesquisa de vistas - Determinar observáveis** pode ser usada com qualquer fluxo de trabalho para determinar quais observáveis serão incluídos no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Observáveis encontrados
Falha	Nenhum observável encontrado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
task_sys_id	Identificador de tarefa (mapeia o incidente de segurança para observáveis).
observáveis	Endereços IP, hash, URLs, nomes de domínio.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
workflow_current_sys_id	Identificador do sistema do registro atual. (Usado somente se `task_sys_id`, entradas observáveis não estão disponíveis.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
observáveis	Observáveis filtrados

Atividade Filtrar observáveis na lista de permissões

A atividade de fluxo de trabalho Observáveis na lista de permissões filtrados remove observáveis que podem ser ignorados da lista de observáveis. Esta atividade pode acelerar o processo de investigação e correção.

A atividade Filtrar observáveis na lista de permissões pode ser usada com qualquer fluxo de trabalho para filtrar observáveis antes de executar qualquer ação.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Lista de filtros criada.
Falha	Ocorreu um erro ao tentar filtrar os observáveis. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
observáveis	Lista de observáveis disponíveis.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
observáveis filtrados	Observáveis filtrados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade Obter capacidades de segurança compatíveis

A atividade de fluxo de trabalho Obter capacidades compatíveis recupera o nome e o número de integrações que estão ativas e oferecem suporte à funcionalidade solicitada.

A atividade Obter capacidades compatíveis pode ser usada com qualquer fluxo de trabalho para determinar quais recursos são compatíveis.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Integração que oferece suporte ao recurso encontrado.
Falha	Ocorreu um erro ao tentar encontrar uma integração ativa que ofereça suporte ao recurso. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityName	Nome da capacidade.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
domainId	Identificador do sistema para qualquer domínio associado ao fluxo de trabalho.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
SupportedCapabilities	Lista de integrações compatíveis com a funcionalidade.
capacidadeContagem	Número de integrações compatíveis com a funcionalidade.

Rastreamento de execução de capacidade - Nenhuma atividade de implementação

A atividade de fluxo de trabalho Rastreamento de execução de capacidade - sem implementações cria um registro de erro quando nenhuma implementação de capacidade de integração é encontrada.

A atividade Rastreamento de execução de capacidade - Sem Impls pode ser usada com qualquer fluxo de trabalho de capacidade de integração abstrata para lidar com a condição de erro quando nenhuma implementação de capacidade configurada estiver disponível.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	O estado do registro de acompanhamento de execução é definido como **Erro** e uma mensagem indicando o erro é registrada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capacidadeExecutionId	Identificador do sistema para o registro de auditoria. Saída da atividade usada para iniciar o acompanhamento de execução.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Variáveis de saída

Não há variáveis de saída.

Atividade Obter consultas de vistas de observável

A atividade de fluxo de trabalho **Obter consultas de vistas de observável** recupera consultas da configuração de integração.

A atividade **Obter consultas de vistas de observável** pode ser usada com qualquer fluxo de trabalho para obter consultas a serem enviadas para a implementação especificada usando o inicializador de **fluxo paralelo**.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Consultas encontradas.
Falha	Ocorreu um erro ao tentar obter consultas. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
observáveis	Lista de observáveis filtrados.
Capacidades	Lista de capacidades compatíveis.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
consultas	Cadeia de caracteres de pesquisa.
queryCount	Número de consultas a serem executadas.

Security Operations - Fluxo de trabalho de pesquisa de detecções do agente de log do Arcsight

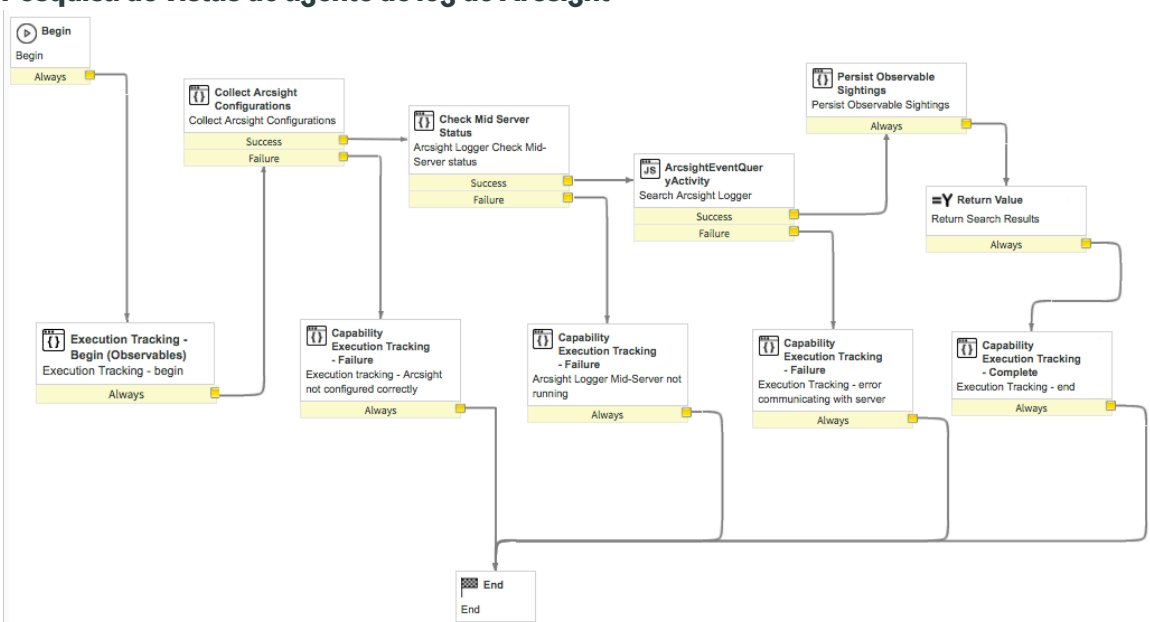
O fluxo de trabalho**Security Operations - ArcSight Logger Sightings Search** é a implementação da integração do Splunk iniciada pelo **fluxo de trabalho Security Operations Integration - Sightings Search**.

Antes de Iniciar
Função necessária: sn_si_analyst

Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:

- Acompanhamento de execução - Iniciar atividade
- Atividade Coletar configurações do ArcSight
- Acompanhamento de execução de capacidade - Atividade com falha
- Atividade de consulta de evento do ArcSight
- Verifica se o MID Server está sendo executado ou não.
- Atividade de consulta de evento do ArcSight
- Atividade de vistas de observável persistente - retorna resultados de pesquisa em uma matriz.
- Acompanhamento de execução de capacidade - Concluir atividade

Pesquisa de vistas do agente de log do Arcsight



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Atividade Coletar configurações do ArcSight

A atividade de fluxo de trabalho **Coletar configurações do ArcSight** coleta informações de configuração para usar no fluxo de trabalho.

A atividade **Coletar configurações do ArcSight** pode ser usada com qualquer fluxo de trabalho para coletar as definições de configuração do Agente de Log do HPE Security ArcSight.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
observáveis	A lista de observáveis de Trusted Security Circle ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
link_endpoint_base	Link para uma interface de pesquisa do ArcSight Logger, quando disponível.
use_default_workflows	Determina o uso do fluxo de trabalho que foi instalado com o plug-in. Os valores possíveis são: • verdadeiro - usa o fluxo de trabalho • falso - não usa o fluxo de trabalho

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
arcsight_username	Nome de usuário do agente de log HPE Security ArcSight
arcsight_password	Senha do agente de segurança HPE ArcSight
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros. .
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.
all_peers	Determina se todos os outros agentes conectados à rede devem ser pesquisados.

Atividade de consulta de evento do ArcSight

A atividade de fluxo de trabalho **Consulta de evento** do ArcSight pesquisa os logs de eventos do ArcSight em busca de indicadores mal-intencionados.

A atividade **de consulta de evento do ArcSight** pode ser usada com qualquer fluxo de trabalho para pesquisar os logs de eventos do HPE Security ArcSight Logger.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Consulta bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a consulta. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
usuário	Nome de usuário do sistema HPE Security ArcSight Logger.
password	Senha para o sistema HPE Security ArcSight Logger.
observáveis	A lista de observáveis de Trusted Security Circles ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
base_url	URL base da API de integração de terceiros.
link_base_URL	Link para uma interface de pesquisa do ArcSight Logger, quando disponível.
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.
all_peers	Determina se todos os outros agentes conectados à rede devem ser pesquisados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
saída	Saída da consulta no formato JSON.

Atividade de vistas de observável persistente

A atividade de fluxo de trabalho **Observações de observáveis persistentes** recupera observáveis da integração de terceiros.

A atividade **Observações de observáveis persistentes** pode ser usada com qualquer fluxo de trabalho para registrar observáveis encontrados na integração de terceiros.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Observáveis recuperados.
Falha	Ocorreu um erro ao tentar coletar observáveis. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
avistamentosResposta	
taskId	Identificador de tarefa.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
resposta	

Security Operations - Fluxo de trabalho de pesquisa de detecções do Elasticsearch

O fluxo de trabalho**Security Operations - Elasticsearch Sightings Search** é a implementação do Elasticsearch iniciada pelo fluxo de trabalho **Security Operations Integration - Sightings Search**.

Antes de Iniciar

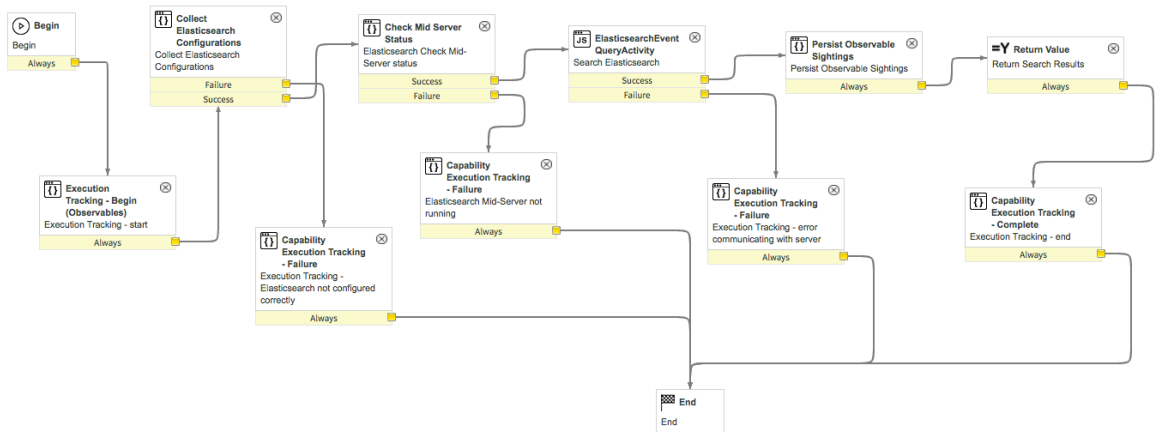
Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

As atividades do processo de fluxo de trabalho incluem:

- Acompanhamento de execução - Iniciar atividade
- Atividade Coletar configurações do Elasticsearch
- Verifica se o MID Server está sendo executado ou não.
- Acompanhamento de execução de capacidade - Atividade com falha
- Consulta de evento do ElasticsearchAtividade de atividade
- Atividade de vistas de observável persistente - retorna resultados de pesquisa em uma matriz.
- Acompanhamento de execução de capacidade - Concluir atividade

Pesquisa de detecções do Elasticsearch



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Atividade Coletar configurações do Elasticsearch

A atividade de fluxo de trabalho **Coletar configurações do Elasticsearch** coleta informações de configuração para usar no fluxo de trabalho.

A atividade **Coletar configurações do Elasticsearch** pode ser usada com qualquer fluxo de trabalho para coletar as definições de configuração do Elasticsearch.

Resultados

Os resultados possíveis para esta atividade são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida. .
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
observáveis	A lista de observáveis de Trusted Security Circles ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
link_endpoint_base	[Opcional] Link para uma instância do Kibana, quando disponível.
use_default_workflows	Determina o uso do fluxo de trabalho que foi instalado com o plug-in. Os valores possíveis são: • verdadeiro - usa o fluxo de trabalho • falso - não usa o fluxo de trabalho
Elastic_username	Nome de usuário do Elasticsearch
elastic_password	Senha do Elasticsearch
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros. .
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Rastreamento de execução de capacidade - Nenhuma atividade de implementação

A atividade de fluxo de trabalho Rastreamento de execução de capacidade - sem implementações cria um registro de erro quando nenhuma implementação de capacidade de integração é encontrada.

A atividade Rastreamento de execução de capacidade - Sem Impls pode ser usada com qualquer fluxo de trabalho de capacidade de integração abstrata para lidar com a condição de erro quando nenhuma implementação de capacidade configurada estiver disponível.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de acompanhamento de execução é definido como **Erro** e uma mensagem indicando o erro é registrada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capacidadeExecutionId	Identificador do sistema para o registro de auditoria. Saída da atividade usada para iniciar o acompanhamento de execução.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Variáveis de saída

Não há variáveis de saída.

Consulta de evento do ElasticsearchAtividade de atividade

A atividade de fluxo de trabalho **Elasticsearch Event Query** pesquisa os logs de eventos do Elasticsearch em busca de indicadores maliciosos.

A atividade **Elasticsearch Event QueryActivity** pode ser usada com qualquer fluxo de trabalho para pesquisar os logs de eventos do Elasticsearch.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Consulta bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a consulta. Mais informações de erro estão disponíveis no erro de saída da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
usuário	Nome de usuário do sistema Elasticsearch.
password	Senha para o sistema Elasticsearch.
observáveis	A lista de observáveis de Trusted Security Circles ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
base_url	URL base da API de integração de terceiros.
link_base_URL	[Opcional] Link para uma instância do Kibana, quando disponível.
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
saída	Saída da consulta no formato JSON.

Atividade de vistas de observável persistente

A atividade de fluxo de trabalho **Observações de observáveis persistentes** recupera observáveis da integração de terceiros.

A atividade **Observações de observáveis persistentes** pode ser usada com qualquer fluxo de trabalho para registrar observáveis encontrados na integração de terceiros.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Observáveis recuperados.
Falha	Ocorreu um erro ao tentar coletar observáveis. Mais informações de erro estão disponíveis no erro de saída da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
avistamentosResposta	
taskId	Identificador de tarefa.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	

Security Operations - Fluxo de trabalho de pesquisa de detecções do McAfee ESM

O fluxo de trabalho**Security Operations - McAfee ESM Sightings Search** é a implementação da integração Splunk iniciada pelo **fluxo de trabalho Security Operations Integration - Sightings Search**.

Antes de Iniciar
Função necessária: sn_si_analyst

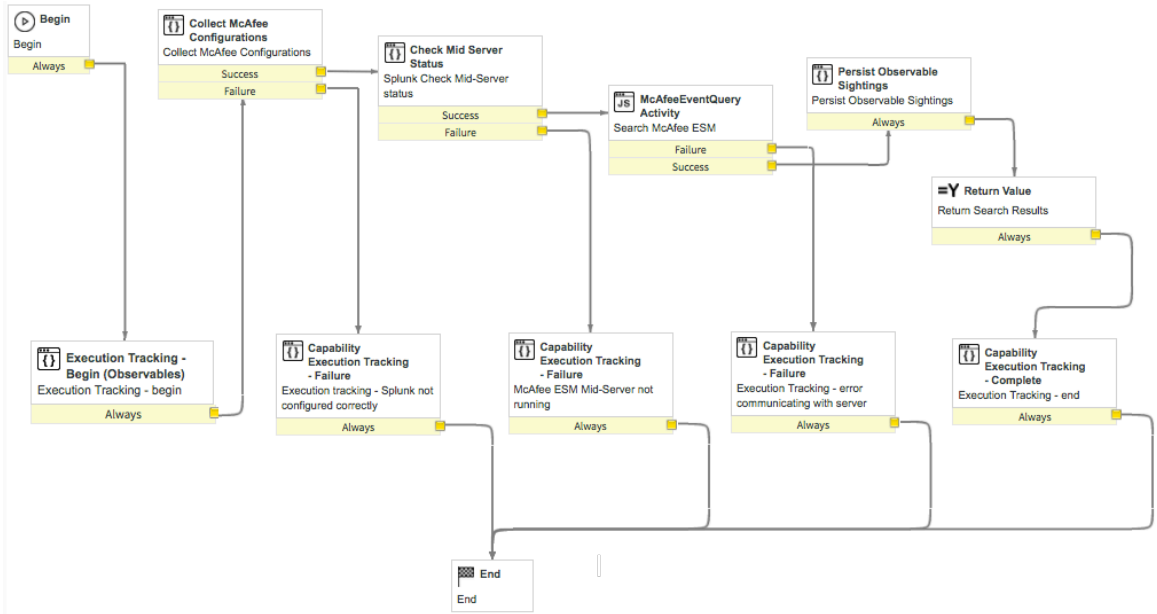
Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:

- Acompanhamento de execução - Iniciar atividade
- Atividade Coletar configurações do McAfee
- Acompanhamento de execução de capacidade - Atividade com falha
- Atividade de consulta de evento do McAfee ESM
- Verifica se o MID Server está em execução.
- Atividade de vistas de observável persistente - retorna resultados de pesquisa em uma matriz.
- Acompanhamento de execução de capacidade - Concluir atividade

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de detecções do McAfee ESM



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Atividade Coletar configurações do McAfee

A atividade de fluxo de trabalho **Coletar configurações do McAfee** coleta informações de configuração para usar no fluxo de trabalho.

A atividade **Coletar configurações do McAfee** pode ser usada com qualquer fluxo de trabalho para coletar as definições de configuração do McAfee ESM.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida. .
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
observáveis	A lista de observáveis de Trusted Security Circles ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
link_endpoint_base	Link para uma interface web da McAfee, quando disponível.
use_default_workflows	Determina o uso do fluxo de trabalho que foi instalado com o plug-in. Os valores possíveis são: • verdadeiro - usa o fluxo de trabalho • falso - não usa o fluxo de trabalho
Elastic_username	Nome de usuário da McAfee
elastic_password	Senha da McAfee
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros. .
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Atividade de consulta de evento do McAfee ESM

A atividade de fluxo de trabalho **Consulta de evento** do McAfee ESM pesquisa os logs de eventos do McAfee ESM em busca de indicadores maliciosos.

A atividade **de consulta de evento do McAfee ESM** pode ser usada com qualquer fluxo de trabalho para pesquisar os logs de eventos do HPE Security ArcSight Logger.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Consulta bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a consulta. Mais informações de erro estão disponíveis no erro de saída da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
usuário	Nome de usuário do sistema McAfee ESM.
password	Senha para o sistema McAfee ESM.
observáveis	Sintaxe de pesquisa. `$(observable)` é o padrão.
base_url	URL base da API de integração de terceiros.
link_base_URL	Link para uma interface web da McAfee, quando disponível.
observáveis	A lista de observáveis de Trusted Security Circles ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
saída	Saída da consulta no formato JSON.

Atividade de vistas de observável persistente

A atividade de fluxo de trabalho **Observações de observáveis persistentes** recupera observáveis da integração de terceiros.

A atividade **Observações de observáveis persistentes** pode ser usada com qualquer fluxo de trabalho para registrar observáveis encontrados na integração de terceiros.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Observáveis recuperados.
Falha	Ocorreu um erro ao tentar coletar observáveis. Mais informações de erro estão disponíveis no erro de saída da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
avistamentosResposta	
taskId	Identificador de tarefa.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	

Security Operations - Fluxo de trabalho de pesquisa de detecções do QRadar

O fluxo de trabalho**Security Operations - QRadar Sightings Search** é a implementação da integração do IBM QRadar iniciada pelo **fluxo de trabalho Security Operations Integration - Sightings Search**.

Antes de Iniciar
Função necessária: sn_si_analyst

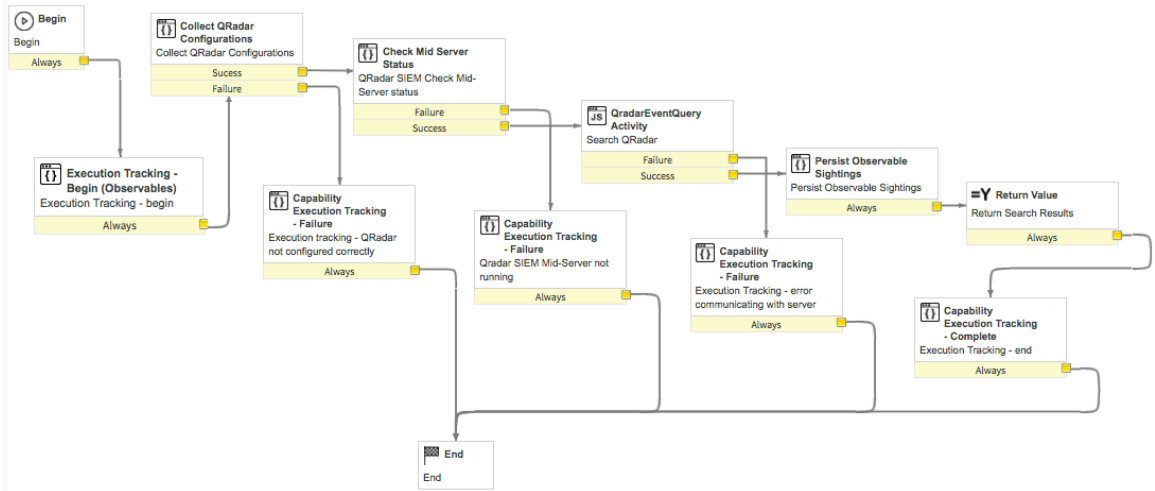
Por Que e Quando Desempenhar Esta Tarefa
As atividades do processo de fluxo de trabalho incluem:

- Acompanhamento de execução - Iniciar atividade
- Atividade Coletar configurações do QRadar
- Acompanhamento de execução de capacidade - Atividade com falha
- Verifica se o MID Server está em execução.
- QRadar Event QueryActivity atividade
- Atividade de vistas de observável persistente - retorna resultados de pesquisa em uma matriz.
- Acompanhamento de execução de capacidade - Concluir atividade

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Pesquisa de detecções do QRadar



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Atividade Coletar configurações do QRadar

A atividade de fluxo de trabalho **Coletar configurações do QRadar** reúne informações de configuração para usar no fluxo de trabalho.

A atividade **Coletar configurações do QRadar** pode ser usada com qualquer fluxo de trabalho para coletar as definições de configuração do IBM QRadar.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida. .
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
observáveis	A lista de observáveis de Trusted Security Circles ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
link_endpoint_base	Link para uma instância IBM QRadar, quando disponível.
use_default_workflows	Determina se o fluxo de trabalho que foi instalado com o plug-in deve ser usado ou não. Os valores possíveis são verdadeiro e falso..
Elastic_username	Nome de usuário do QRadar
elastic_password	Senha do QRadar
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros. .
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

QRadar Event QueryActivity atividade

A atividade de fluxo de trabalho **Consulta de evento** do QRadar pesquisa os logs de eventos do QRadar em busca de indicadores maliciosos.

A atividade **QRadar Event QueryActivity** pode ser usada com qualquer fluxo de trabalho para pesquisar os logs de eventos do Elasticsearch.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Consulta bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a consulta. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
usuário	Nome de usuário do sistema QRadar.
password	Senha para o sistema QRadar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
observáveis	A lista de observáveis de Trusted Security Circles ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
base_url	URL base da API de integração de terceiros.
link_base_URL	Link para uma instância IBM QRadar, quando disponível.
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
saída	Saída da consulta no formato JSON.

Atividade de vistas de observável persistente

A atividade de fluxo de trabalho **Observações de observáveis persistentes** recupera observáveis da integração de terceiros.

A atividade **Observações de observáveis persistentes** pode ser usada com qualquer fluxo de trabalho para registrar observáveis encontrados na integração de terceiros.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Observáveis recuperados.
Falha	Ocorreu um erro ao tentar coletar observáveis. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
avistamentosResposta	
taskId	Identificador de tarefa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	

Fluxo de trabalho do Security Operations Integration - Splunk Sightings Search

O fluxo de trabalho**Security Operations - Splunk Sightings Search** é a implementação da integração Splunk iniciada pelo **fluxo de trabalho Security Operations Integration - Sightings Search**.

Antes de Iniciar

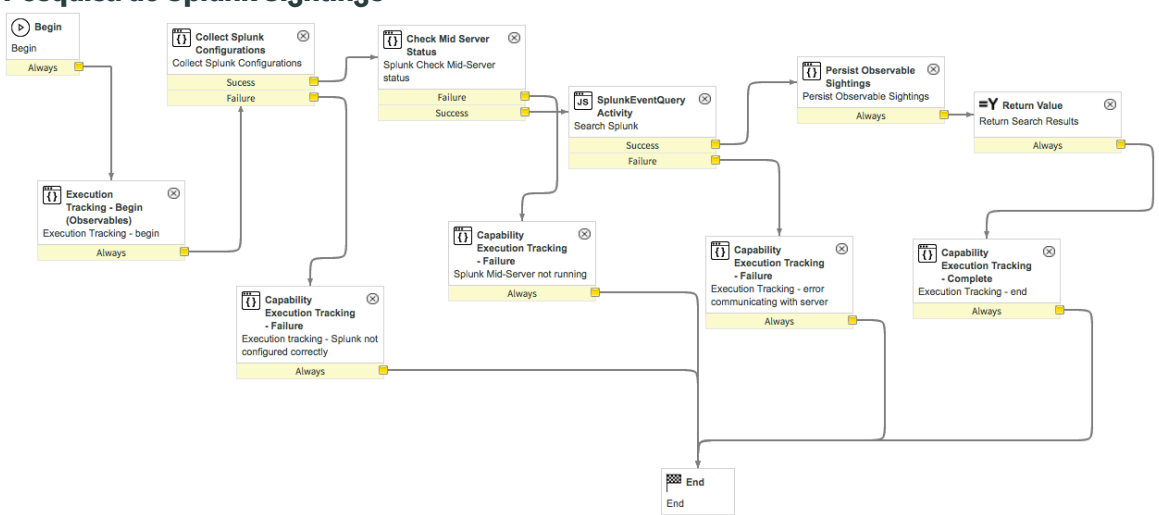
Função necessária: sn_si_analyst

Por Que e Quando Desempenhar Esta Tarefa

As atividades do processo de fluxo de trabalho incluem:

- Acompanhamento de execução - Iniciar atividade
- Atividade Coletar configurações do Splunk
- Acompanhamento de execução de capacidade - Atividade com falha
- Verifica se o MID Server está sendo executado ou não.
- Atividade de consulta de evento do Splunk
- Atividade de vistas de observável persistente - retorna resultados de pesquisa em uma matriz.
- Acompanhamento de execução de capacidade - Concluir atividade

Pesquisa do Splunk Sightings



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Atividade Coletar configurações do Splunk

A atividade de fluxo de trabalho **Coletar configurações do Splunk** coleta informações de configuração para usar no fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A atividade **Coletar configuração do Splunk** pode ser usada com qualquer fluxo de trabalho para coletar as definições de configuração do Splunk.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Configuração bem-sucedida.
Falha	Ocorreu um erro ao tentar verificar a configuração. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
observáveis	A lista de observáveis de Trusted Security Circle ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
endpoint_base	URL base da API de integração de terceiros.
link_endpoint_base	Links para a interface da Web Splunk, quando disponível.
use_default_workflows	Determina o uso do fluxo de trabalho que foi instalado com o plug-in. Os valores possíveis são: • verdadeiro - usa o fluxo de trabalho • falso - não usa o fluxo de trabalho
Elastic_username	Nome de usuário do Splunk.
elastic_password	Senha do Splunk.
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Atividade de consulta de evento do Splunk

A atividade de fluxo de trabalho **Splunk Event Query** pesquisa os logs de eventos do Splunk em busca de indicadores mal-intencionados.

A atividade **Splunk Event QueryActivity** pode ser usada com qualquer fluxo de trabalho para pesquisar os logs de eventos do Splunk.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Splunk
Falha	Ocorreu um erro ao tentar verificar a consulta do Splunk. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
usuário	Nome de usuário do sistema Splunk.
password	Senha para o sistema Splunk.
observáveis	A lista de observáveis de Trusted Security Circle ou a tarefa de incidente de segurança a ser pesquisada. Retornado no formato JSON.
base_url	URL do endpoint de integração do Splunk.
link_base_URL	Link para a interface da Web Splunk, quando disponível.
fonte	Origem da solicitação para executar o fluxo de trabalho. As entradas compatíveis são: Trusted Security Circles ou tarefa de incidente de segurança.
max_rows	Máximo de linhas a serem retornadas da consulta. O limite depende da integração de terceiros.
days_to_search	Dias para pesquisar a partir do dia atual para trás. O padrão é 7.
consulta	Sintaxe de pesquisa. `$(observable)` é o padrão.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
saída	Saída da consulta no formato JSON.

Atividade de vistas de observável persistente

A atividade de fluxo de trabalho **Observações de observáveis persistentes** recupera observáveis da integração de terceiros.

A atividade **Observações de observáveis persistentes** pode ser usada com qualquer fluxo de trabalho para registrar observáveis encontrados na integração de terceiros.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Observáveis recuperados.
Falha	Ocorreu um erro ao tentar coletar observáveis. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
avistamentosResposta	
taskId	Identificador de tarefa.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	

Exibir Resultados da Pesquisa de Vistas

Você pode revisar os Resultados da pesquisa de detecções para indicadores maliciosos internos e externos.

Antes de Iniciar
Função necessária: sn_si.analyst

Tradução automática

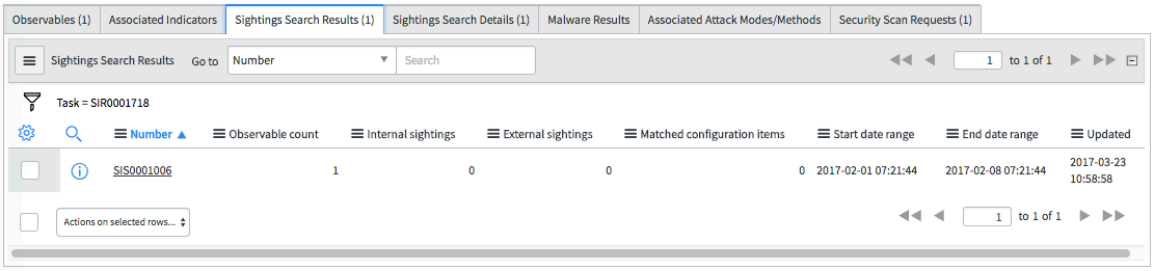
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

.

Procedimento

1. Navegue até um incidente de segurança.
2. Selecione a guia **Resultados** da pesquisa de vistas no grupo **Mostrar lista relacionada de IoC** para exibir a lista de pesquisas de vistas.



Nota:
Esses dados podem ser compartilhados com Trusted Security Circle.

Resultados da pesquisa de detecções

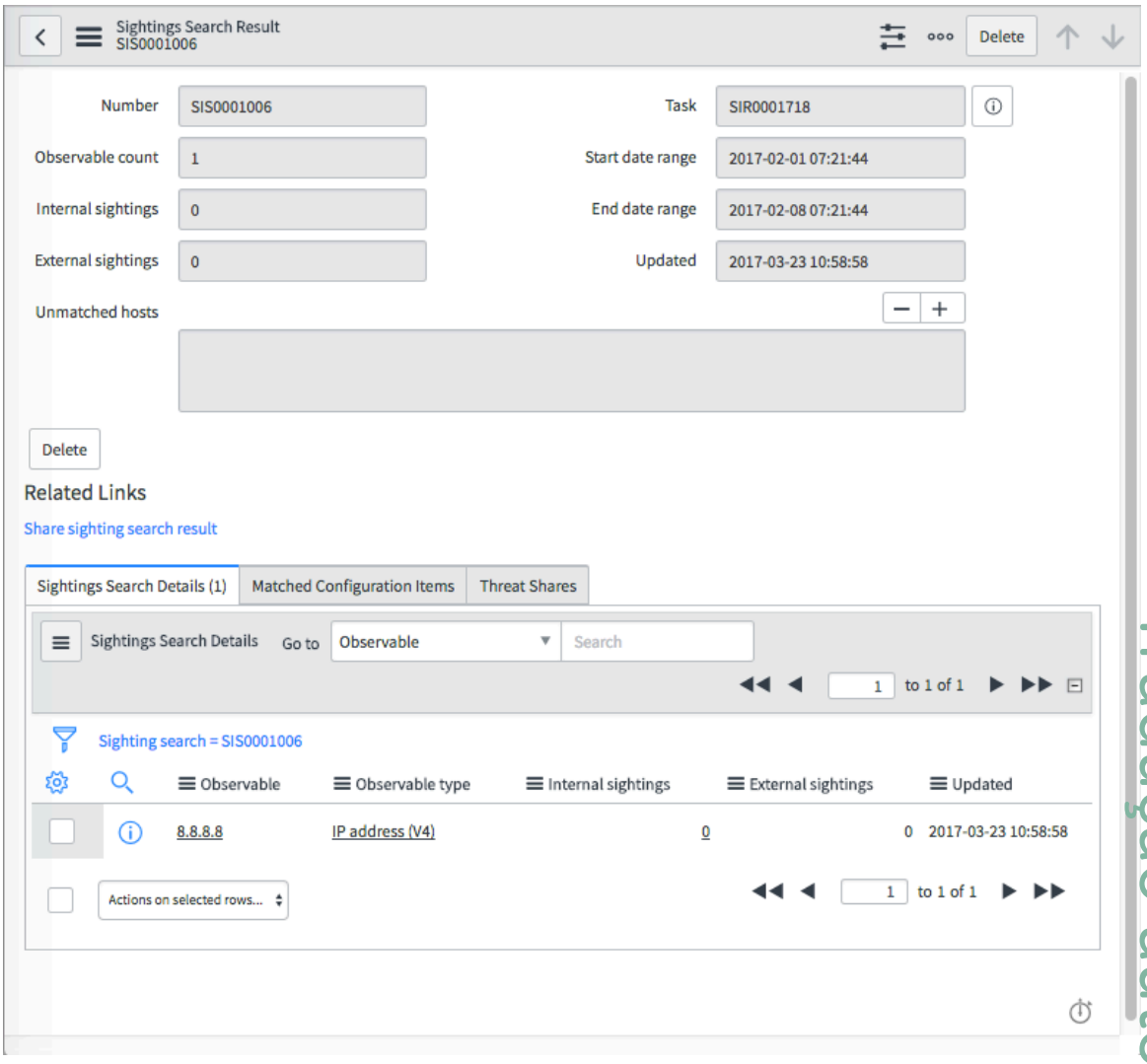
Resultado	Descrição
Número	Identificador de pesquisa de detecções.
Contagem de observáveis	Número de observáveis pesquisados.
Vistas Internas	Contagem agregada de vistas internas.
Vistas Externas	Contagem agregada de avistamentos externos. (Recebido do compartilhamento de ameaças.)
Itens de configuração correspondentes	Contagem agregada de itens de configuração que corresponderam a um registro existente no seu `cmdb`.
Intervalo de datas de início	Hora de começar a procurar vistas.
Intervalo de datas de término	Hora de parar de procurar vistas.
Atualizado em:	Data e hora da última modificação.

Para exibir os detalhes de uma única pesquisa:

3. Clique em uma pesquisa de vistas na lista **Resultados** da pesquisa de vistas.
O formulário Resultado da pesquisa de detecções é exibido.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



Formulário Resultados da pesquisa de detecções

Detalhe	Descrição
Número	Identificador interno da Pesquisa de vistas.
Contagem de observáveis	Contagem de observáveis pesquisados por esta consulta.
Vistas internas	Contagem de vistas internas para esta pesquisa.
Vistas externas	Contagem de avistamentos externos para esta pesquisa. (Recebido de Trusted Security Circle.)
Hosts incompatíveis	Lista de possíveis itens de configuração para esta pesquisa que não foram correspondidos a nenhum registro no seu `cmdb`.
Tarefa	Identificador de tarefa de incidente de segurança.
Intervalo de datas de início	Hora de início da pesquisa de vistas.
Intervalo de datas de término	Hora em que a pesquisa de vistas parou.
Atualizado em:	Data e hora da última modificação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Detalhe	Descrição
Detalhes de Pesquisa de detecções	Tipo, número de vistas e data da modificação.
Itens de configuração correspondentes	Contagem de itens de configuração que corresponderam a um registro existente no seu `cmdb`. Lista o IC e a vista.
Compartilhamentos de ameaças	Lista de ameaças compartilhadas com Trusted Security Circle.

Compartilhar resultados da pesquisa de detecções

Você pode compartilhar detalhes de vistas locais ou resultados que estão associados a uma pesquisa específica com seu Trusted Security Circle.

Antes de Iniciar

Função necessária: sn_si.analyst

Por Que e Quando Desempenhar Esta Tarefa

O compartilhamento pode ser automatizado usando as seguintes **propriedades**do Security Incident Response.

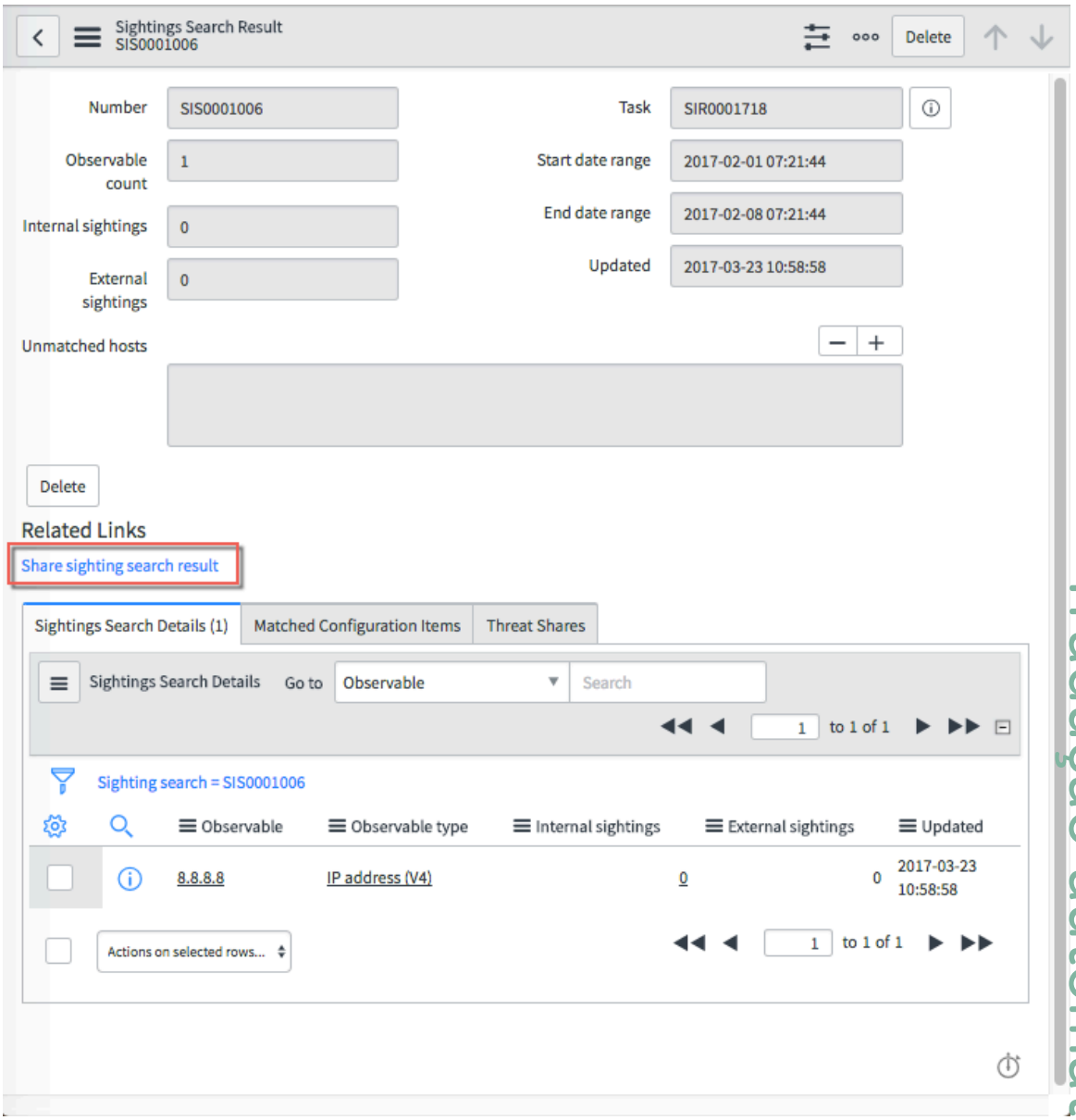
- Compartilhe automaticamente os resultados de uma pesquisa de vistas com o círculo confiável padrão da ServiceNow
- Incluir observáveis sem vistas locais ao compartilhar automaticamente os resultados da pesquisa de vistas
- Responder com vistas locais sempre que um compartilhamento de ameaça for recebido de um círculo confiável

Procedimento

1. Navegue até um incidente de segurança.
2. Clique na lista relacionada **Mostrar IoC** e selecione a guia **Resultados** da pesquisa de vistas para exibir a lista de pesquisas de vistas.
3. Clique em um resultado de pesquisa de vistas.

Tradução automática

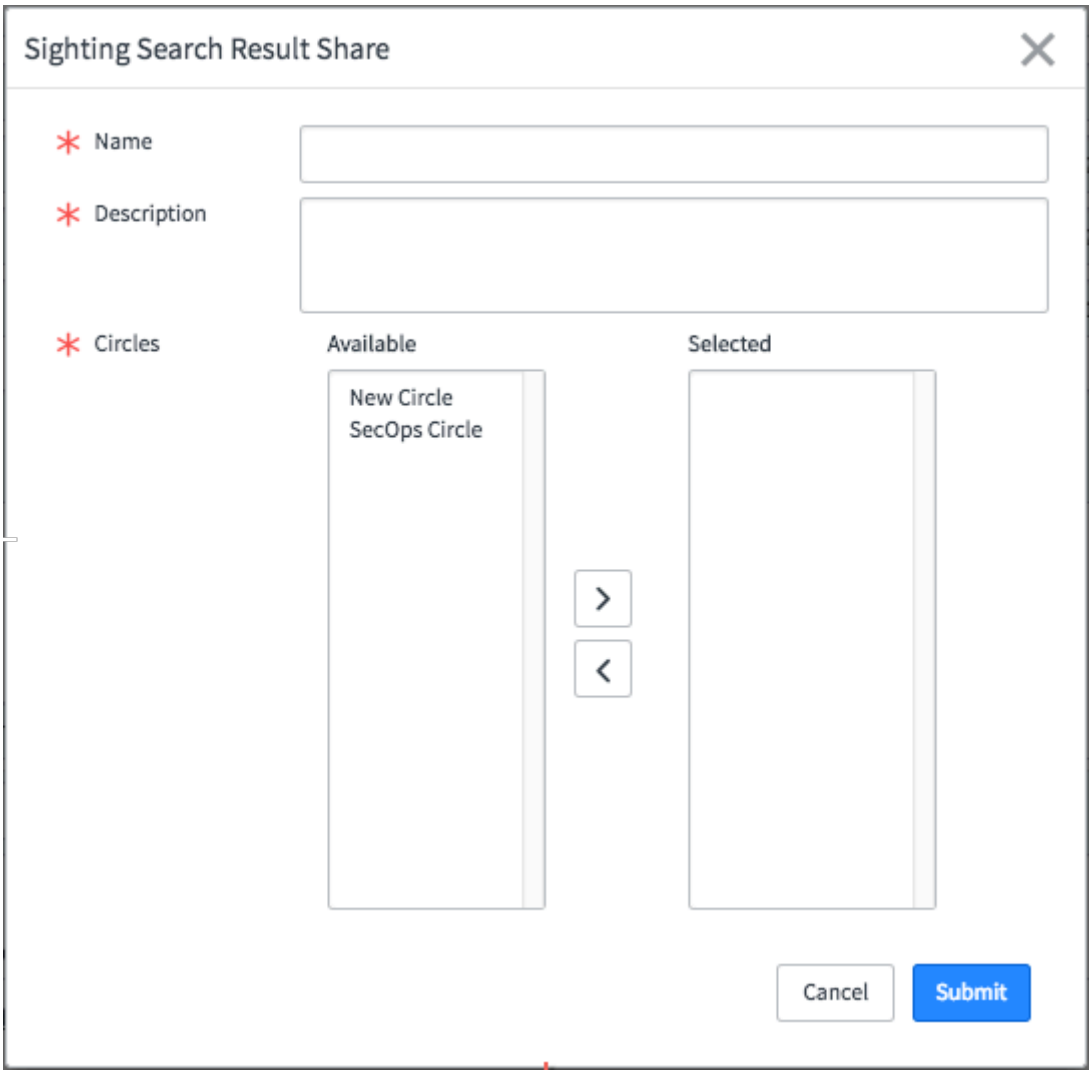
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. No formulário **Resultado**da pesquisa de detecções, clique no link relacionado **Compartilhar resultado da pesquisa de detecções**.
   A caixa de diálogo Compartilhamento do resultado da pesquisa de detecções é exibida.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Insira um **Nome** para este registro de compartilhamento observável.
6. Insira uma **Descrição**dos observáveis a serem compartilhados.
7. Escolha **Círculos** para compartilhar os observáveis.
8. Clique em **Enviar**.
   O(s) observável(is) é(são) compartilhado(s) com o Círculo Confiável especificado.

Compartilhar observáveis de um incidente de segurança

Os observáveis podem ser compartilhados de um incidente de segurança em Security Incident Response para membros em seu círculo confiável.

Antes de Iniciar

Função necessária: sn_si.analyst

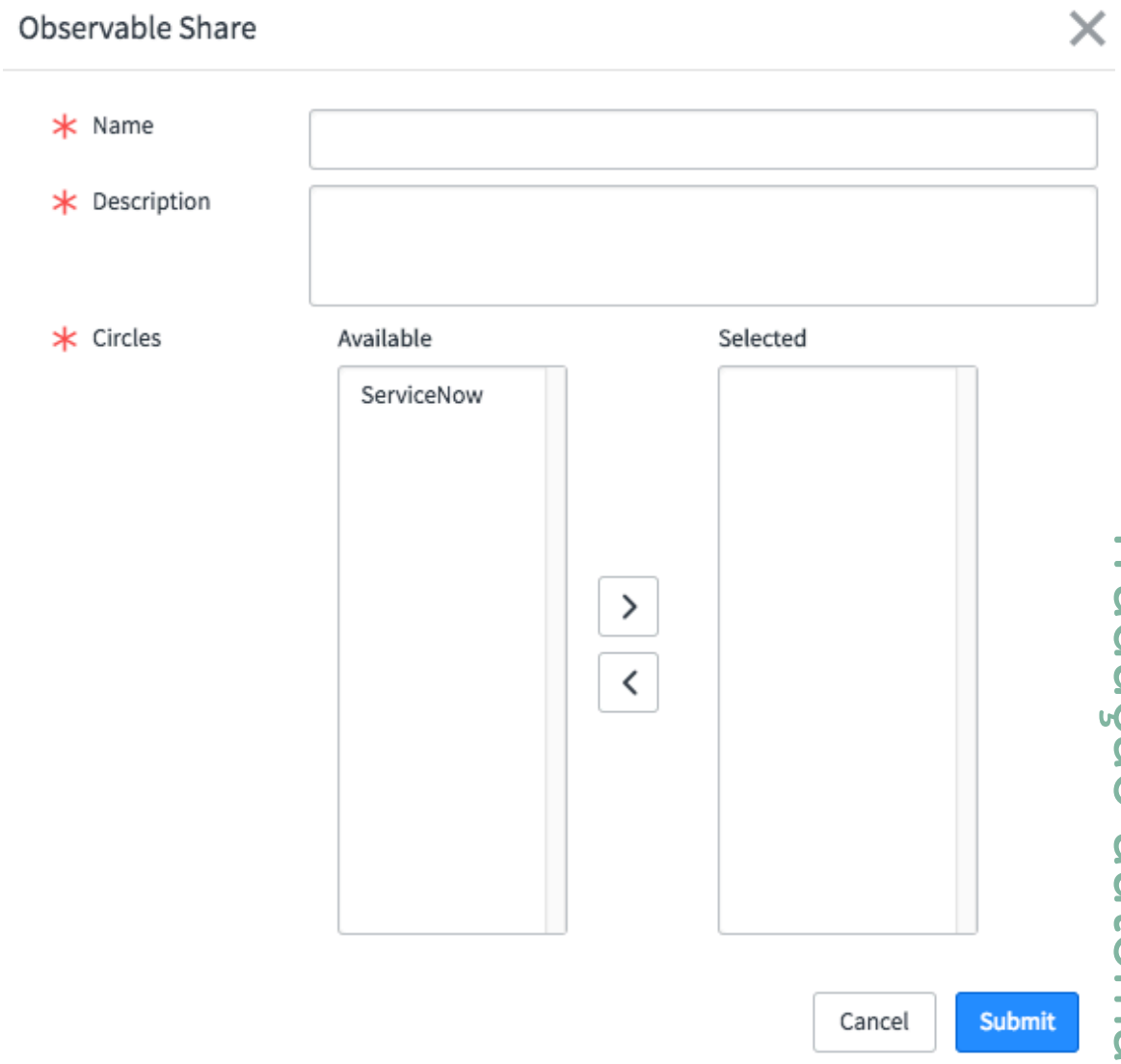
Procedimento

1. Navegue até um incidente de segurança.
2. Selecione a guia **Observáveis** no grupo **Mostrar lista relacionada de IoC**.
3. Clique em um observável.
4. No formulário **Observável**, clique no link relacionado **Compartilhar observável**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A caixa de diálogo Compartilhamento do observável é exibida.



5. Insira um **Nome** para este registro de compartilhamento de ameaça.
6. Insira uma **Descrição**dos observáveis selecionados.
7. Escolha **Círculos** para compartilhar os observáveis.
8. Clique em **Enviar**.
   O(s) observável(is) é(são) compartilhado(s) com o Círculo Confiável especificado.
9. Você pode exibir os registros de compartilhamento de ameaças clicando na guia **Compartilhamentos** de ameaças.
10. Se algum dos observáveis compartilhados contiver vistas, as vistas também serão compartilhadas e poderão ser exibidas clicando na guia **Vistas**.

Exibir detalhes da pesquisa de detecções

Revise os detalhes agregados de todas as pesquisas de vista.

Antes de Iniciar
Função necessária: sn_si.analyst

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

.

Procedimento

1. Navegue até um incidente de segurança.
2. Selecione a guia **Detalhes da pesquisa** de vistas no grupo **Mostrar lista relacionada de IoC** para exibir a lista de pesquisas de vistas.

Nota:
Esses dados podem ser compartilhados com Trusted Security Circle.

Detalhes de Pesquisa de detecções

Detalhe	Descrição
Observável	Lista de todos os observáveis pesquisados por consulta.
Tipo de observável	
Vistas internas	Contagem de vistas internas para todas as pesquisas.
Vistas externas	Contagem de avistamentos externos para todas as pesquisas. (Recebido do compartilhamento de ameaças.)
Pesquisa de vista	Identificador de pesquisa de detecções.
Atualizado em:	Data e hora da última modificação.

Integração do Security Operations - Pesquisa de ameaças

A funcionalidade Pesquisas de **ameaças** executa pesquisas de inteligência contra ameaças para determinar se um ou mais observáveis estão associados a ameaças de segurança conhecidas.

A funcionalidade Pesquisas de **ameaças** tem um fluxo de trabalho, Integração do Security Operations - Fluxo de trabalho de pesquisa de ameaças. Quando o fluxo de trabalho do recurso é executado, ele executa fluxos de trabalho adicionais para as implementações ativadas. Você pode especificar uma implementação a ser usada para executar uma pesquisa nos observáveis selecionados ou pode executar a pesquisa usando todas as implementações.

Nota:
Se não houver implementações disponíveis, as ações de recurso não serão exibidas nos menus do produto.

Integração do Security Operations - Fluxo de trabalho de pesquisa de ameaças

O fluxo de trabalho do recurso **Security Operations Integration - Pesquisa de ameaças** acessa as implementações de pesquisa de ameaças disponíveis e executa os fluxos de trabalho de implementação associados a cada um para executar pesquisas de ameaça de observáveis selecionados.

Antes de Iniciar

Função necessária: sn_ti.write

Por Que e Quando Desempenhar Esta Tarefa

Este fluxo de trabalho pode ser acionado dessas maneiras.

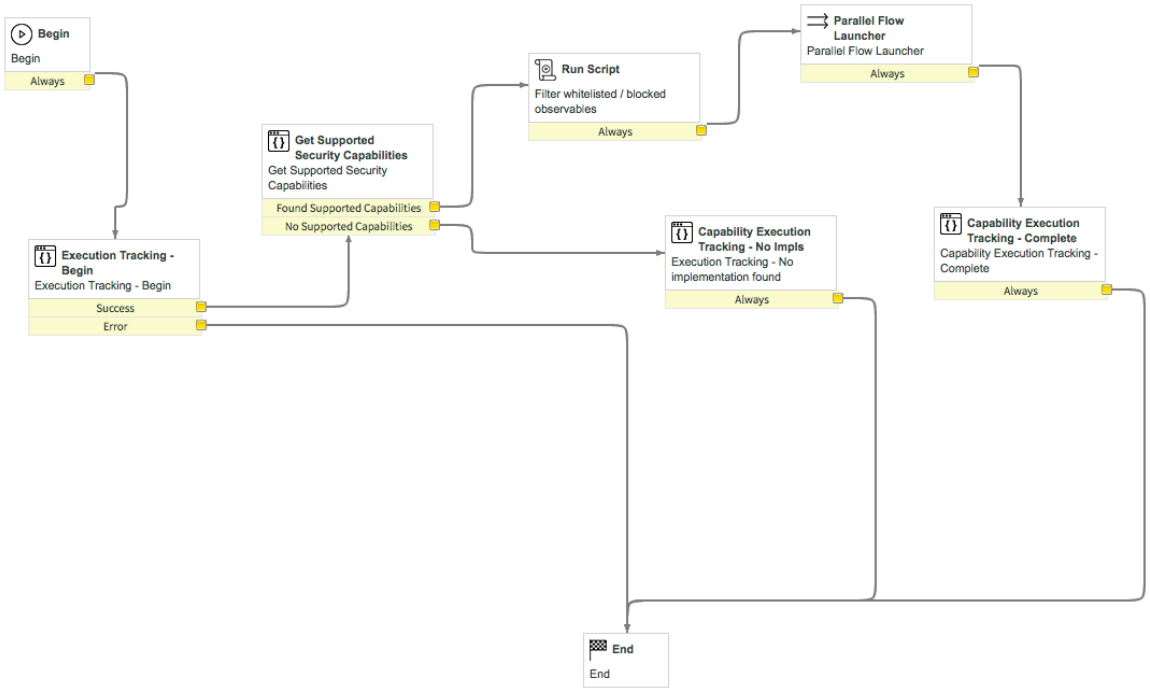
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- selecionando um ou mais observáveis na lista Observáveis e selecionando **Executar pesquisa de ameaça** na lista de seleção **Ações nas linhas selecionadas**.
- abrindo um registro observável e clicando no link relacionado **Executar pesquisa de ameaça**.
- Na lista relacionada Observáveis em um incidente de segurança.

Cada método permite especificar quais implementações de pesquisa serão usadas para verificar os observáveis selecionados. Os fluxos de trabalho de implementação associados são executados para realizar as pesquisas.

Pesquisa de ameaças



Atividades específicas para este fluxo de trabalho são descritas aqui. Para obter mais informações sobre outras atividades, consulte Atividades de fluxo de trabalho de integração comuns.

Atividade Obter capacidades de segurança compatíveis

A atividade de fluxo de trabalho Obter capacidades compatíveis recupera o nome e o número de integrações que estão ativas e oferecem suporte à funcionalidade solicitada.

A atividade Obter capacidades compatíveis pode ser usada com qualquer fluxo de trabalho para determinar quais recursos são compatíveis.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Integração que oferece suporte ao recurso encontrado.
Falha	Ocorreu um erro ao tentar encontrar uma integração ativa que ofereça suporte ao recurso. Mais informações de erro estão disponíveis no erro de saída da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityName	Nome da capacidade.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
domainId	Identificador do sistema para qualquer domínio associado ao fluxo de trabalho.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
SupportedCapabilities	Lista de integrações compatíveis com a funcionalidade.
capacidadeContagem	Número de integrações compatíveis com a funcionalidade.

Rastreamento de execução de capacidade - Nenhuma atividade de implementação

A atividade de fluxo de trabalho Rastreamento de execução de capacidade - sem implementações cria um registro de erro quando nenhuma implementação de capacidade de integração é encontrada.

A atividade Rastreamento de execução de capacidade - Sem Impls pode ser usada com qualquer fluxo de trabalho de capacidade de integração abstrata para lidar com a condição de erro quando nenhuma implementação de capacidade configurada estiver disponível.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de acompanhamento de execução é definido como **Erro** e uma mensagem indicando o erro é registrada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capacidadeExecutionId	Identificador do sistema para o registro de auditoria. Saída da atividade usada para iniciar o acompanhamento de execução.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Não há variáveis de saída.

Alterar a ordem de execução do fluxo de trabalho

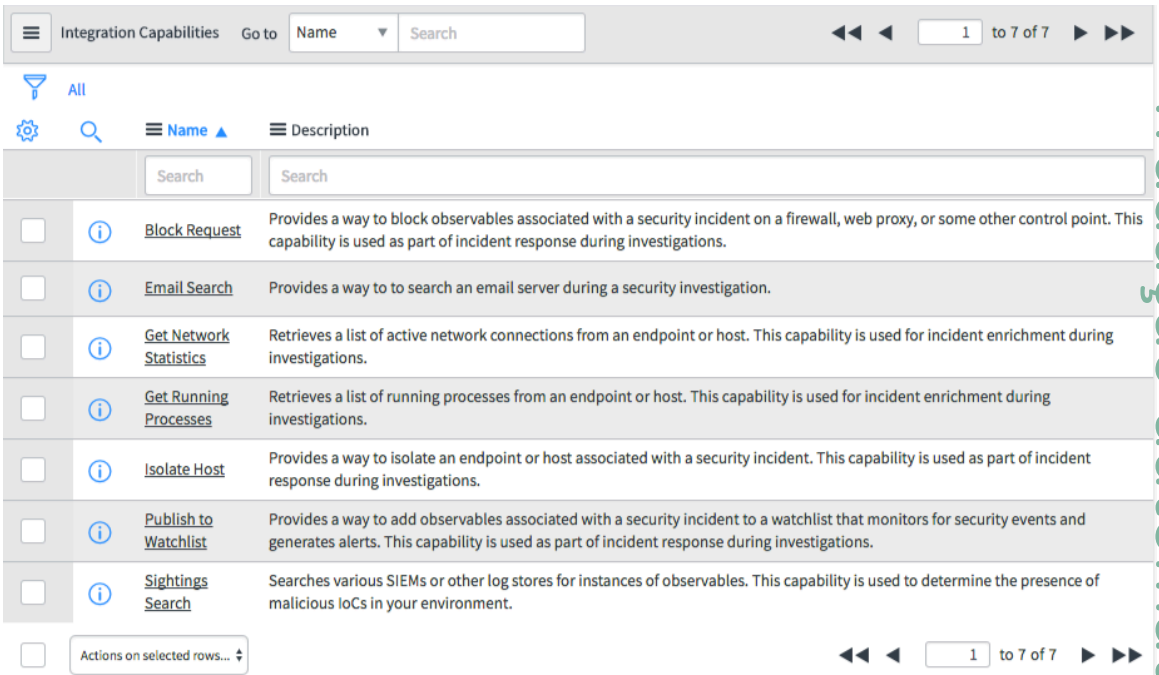
As implementações de capacidade de integração especificam o fluxo de trabalho a ser executado. No sistema de base, os fluxos de trabalho são executados sequencialmente, na ordem especificada na implementação. Você pode mudar a ordem conforme necessário.

Antes de Iniciar

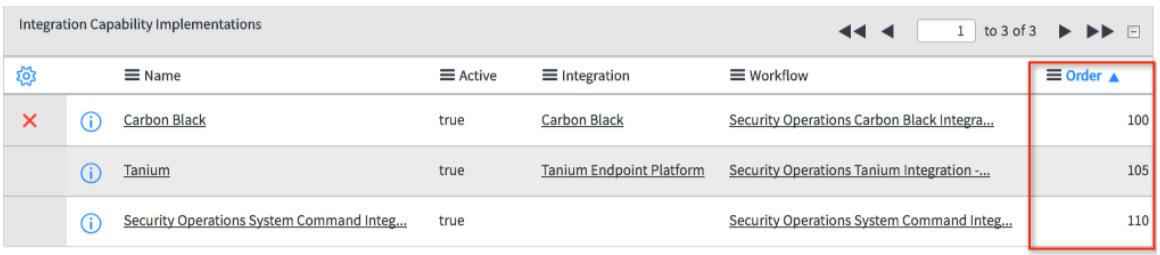
Função necessária: sn_sec_cmn.write

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Integrações** > **Capacidades de integração**.



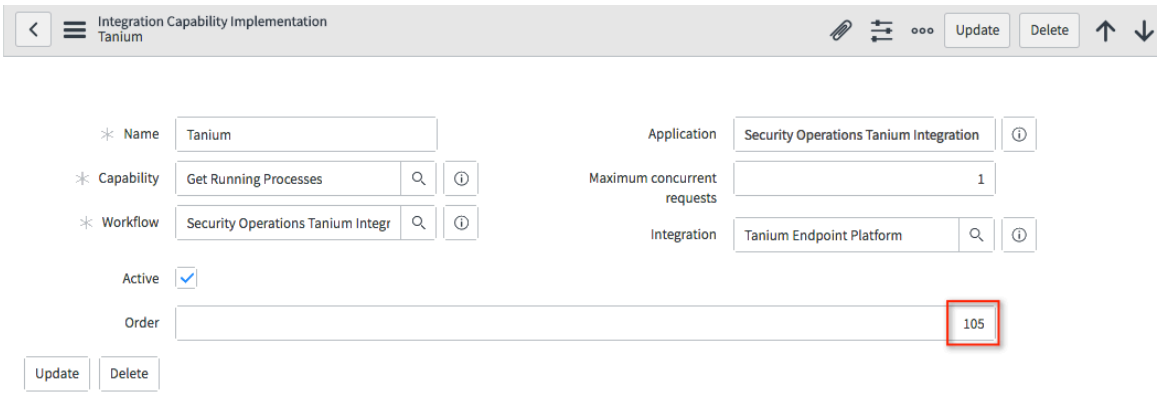
2. Selecione a capacidade de integração para a qual você deseja mudar a ordem de execução.



3. Selecione a implementação que você deseja modificar.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



4. Altere a **Ordem** para um número maior ou menor.
   Números mais baixos têm uma prioridade de execução mais alta.
5. Clique em **Enviar**.

Atividades de fluxo de trabalho de integração comuns

Muitos dos fluxos de trabalho associados a integrações de terceiros incluem as mesmas atividades. Por exemplo, atividades para iniciar e concluir o processamento.

Acompanhamento de execução - Iniciar atividade

A atividade de fluxo de trabalho Acompanhamento de execução - Iniciar inicia o processo de auditoria para um fluxo de trabalho de integração Security Operations que opera em observáveis.

A atividade Acompanhamento de execução - Início pode ser usada com qualquer fluxo de trabalho para começar a registrar o andamento do fluxo de trabalho em uma auditoria.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Um registro de auditoria é criado.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capabilityId	Identificador do sistema da capacidade de integração que está sendo executada.
isImpl	Sinalizador que especifica se a auditoria é feita para um fluxo de trabalho de capacidade de integração ou um fluxo de trabalho de implementação de capacidade de integração. Os valores possíveis são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
	• falso - denota auditoria em um fluxo de trabalho de capacidade de integração abstrato, como pesquisa de vistas. (padrão.) • verdadeiro: denota auditoria em um fluxo de trabalho de implementação de capacidade de integração. Por exemplo, Splunk ou Elasticsearch.
taskId	Identificador do sistema para qualquer tarefa associada ao fluxo de trabalho.
observávelLista	Um ou mais SysIDs observáveis para executar a ação desejada. Usado como uma entrada de fluxo de trabalho.
workflowContextId	Identificador do sistema do registro de contexto de fluxo de trabalho associado. Fornecido pelo sistema.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.
parentCapabilityExcutionId	Identificador do sistema do registro de auditoria que iniciou o fluxo de trabalho de implementação. Necessário somente para fluxos de trabalho de implementação da capacidade de integração, como Splunk, Elasticsearch e VirusTotal.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
capacidadeExecutionId	Identificador do sistema do registro de auditoria.

Acompanhamento de execução de capacidade - Concluir atividade

A atividade de fluxo de trabalho Rastreamento de execução de capacidade - Concluir atualiza o registro de auditoria quando o fluxo de trabalho é concluído.

A atividade Rastreamento de execução de capacidade - Concluir pode ser usada com qualquer fluxo de trabalho para registrar a conclusão do fluxo de trabalho.

Nota:
A matriz **Valor de Retorno** da atividade principal do **inicializador paralelo** contém uma matriz de resultados de todos os fluxos de trabalho de integração executados e solicita a conclusão bem-sucedida do acompanhamento da execução.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de auditoria é atualizado para **Concluído**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capacidadeExecutionId	Identificador do sistema para o registro de auditoria. Este campo foi a saída de qualquer uma das atividades de auditoria Iniciar.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.
message	Mensagem de conclusão.

Variáveis de saída

Não há variáveis de saída.

Acompanhamento de execução de capacidade - Atividade com falha

A atividade de fluxo de trabalho Rastreamento de execução de capacidade - Falha registra uma falha no registro de auditoria.

A atividade Rastreamento de execução de capacidade - Falha pode ser usada com qualquer fluxo de trabalho para registrar uma condição de falha.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	O estado do registro de auditoria é definido como **Erro** e uma mensagem indicando o erro é registrada.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
capacidadeExecutionId	Identificador do sistema para o registro de auditoria. Esta é a saída de qualquer uma das atividades Iniciar auditoria.
errorMessage	Mensagem indicando o motivo da falha.
workflowName	Nome do fluxo de trabalho. Fornecido pelo sistema.

Variáveis de saída

Não há variáveis de saída.

Atividade Criar registros de dados de aprimoramento

A atividade de fluxo de trabalho **Criar registros de dados de** aprimoramento cria ou atualiza registros de aprimoramento para uso no fluxo de trabalho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A atividade **Criar registros de dados de aprimoramento** pode ser usada com qualquer fluxo de trabalho para atualizar registros de aprimoramento no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Registro de aprimoramento atualizado.
Falha	Registro de aprimoramento não atualizado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
task_id	Identificador de tarefa.
conteúdo	Conteúdo bruto (dados de processos em execução).
richment_mapping_id	Identificador de mapeamento de aprimoramento.
ci_id	Identificador do item de configuração.
valor_referência	Não utilizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado	GlideRecords criado usando o script richmentUtils.

Tradução automática

Security Operations gatilhos de fluxo de trabalho

Security Operations Os gatilhos de fluxo de trabalho contêm uma condição em uma tabela. Todos os fluxos de trabalho anexados ao registro do gatilho de fluxo de trabalho são executados quando a condição é atendida.

Criar gatilhos de fluxo de trabalho Security Operations

Crie um gatilho de fluxo de trabalho que contenha uma condição em uma tabela.

Antes de Iniciar

Security Operations contém vários gatilhos de fluxo de trabalho no sistema de base:

Mudanças de item de configuração em um incidente de segurança ativo

Usa a integração para aprimorar os dados relacionados ao IC conforme os itens de configuração mudam.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verificar novamente o grupo vulnerável

Verifica novamente um grupo vulnerável, usando o Fluxo de trabalho de vulnerabilidade de verificação, quando você **Fecha/Ignora** o grupo.

Verificar novamente o item vulnerável

Verifica novamente um item vulnerável, usando Fluxo de trabalho do item de vulnerabilidade de verificação ao **fechar/ignorar** o item.

Funções necessárias:

- Para ler: sn_sec_cmn.read
- Para criar ou atualizar: sn_sec_cmn.write
- Para excluir: sn_sec_cmn.admin

Procedimento

1. Navegar até **Todos** > **Security Operations** > **Utilitários** > **Gatilhos de Fluxo de Trabalho**.
2. Clique em **Nova**.
3. Preencha os campos no formulário, conforme apropriado.

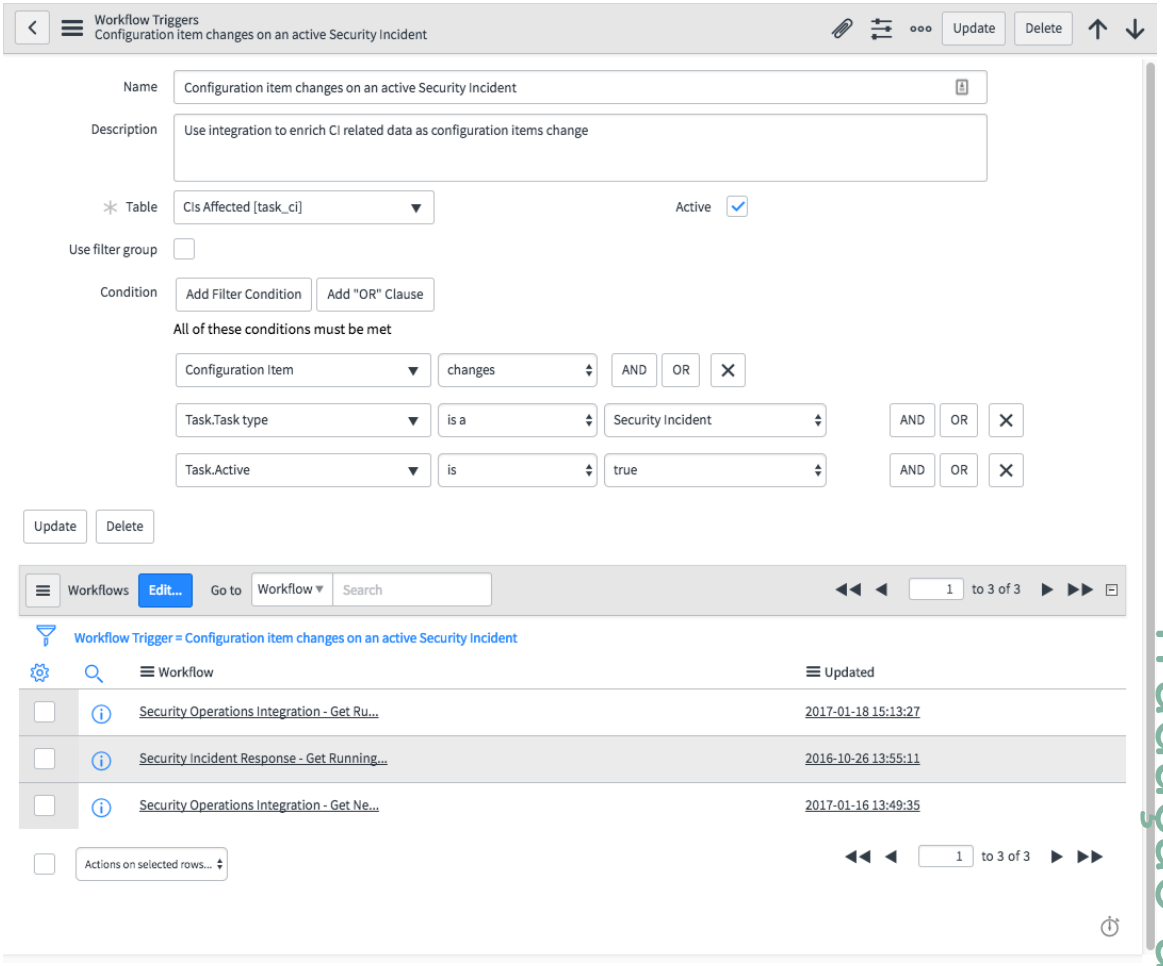
Gatilhos de Fluxo de Trabalho

Campo	Descrição
Nome	O nome do gatilho de fluxo de trabalho.
Descrição	Insira uma descrição para o gatilho de fluxo de trabalho.
Tabela	A tabela que contém o gatilho de fluxo de trabalho. Se você marcou a caixa de seleção **Usar grupo de filtros** e selecionou um grupo de filtros, este campo será padronizado para a tabela associada ao grupo de filtros selecionado.
Condição	Use o Construtor de condição para definir os critérios do gatilho de fluxo de trabalho. Se você marcou a caixa de seleção **Usar grupo de filtros** e selecionou um grupo de filtros, os campos **Condição** não serão exibidos.
Ativo	Marque esta caixa de seleção para ativar o gatilho de fluxo de trabalho.
Usar grupo de filtros	Marque esta caixa de seleção para usar um grupo de filtros predefinido ou criar um novo grupo de filtros para definir os critérios do gatilho de fluxo de trabalho.
Grupo de filtros	Selecione o grupo de filtros a ser usado para definir gatilhos de fluxo de trabalho. Este campo aparecerá somente se a caixa de seleção **Usar grupos de filtros** estiver marcada.

4. Ao concluir suas entradas, clique com o botão direito do mouse no cabeçalho do formulário e selecione **Salvar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



A guia **Fluxos** de trabalho é exibida. Ele contém fluxos de trabalho que são executados quando todas as condições de filtro ou condições de grupo de filtros são atendidas.

5. Para adicionar fluxos de trabalho, siga estas etapas.
   a. Na guia **Fluxos** de trabalho, clique em **Editar**.
   b. Use o construtor de condição, se necessário, para localizar os fluxos de trabalho que deseja selecionar ou use a interface de caixa de listagem dupla para selecionar fluxos de trabalho e movê-los para a Lista de fluxos de trabalho.
   c. Clique em **Salvar**.
   Os fluxos de trabalho selecionados são adicionados.
6. Clique em **Atualizar**.

Orquestração do Security Operations

Os usuários podem interagir e recuperar dados de sistemas e ambientes baseados no Windows ou no UNIX usando pacotes de atividades e fluxos de trabalho em Security Operations Orchestration.

Security Operations Orchestration economiza tempo eliminando processos manuais e obtendo informações contextuais para corrigir incidentes. Os produtos Security Operations têm pacotes de atividades padrão e fluxos de trabalho que estão incluídos e ativados em cada um dos plug-ins.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para criar e acessar atividades de orquestração adicionais que não estão disponíveis com a oferta padrão de produtos Security Operations, adquira uma licença de orquestração completa.

- Orquestração de resposta de incidente de segurança fluxos de trabalho:
  - Fluxo de trabalho do Security Incident Response - Obter estatísticas de rede
  - Fluxo de trabalho de integração de comandos do sistema de operações de segurança – Obter processos em execução
  - Criar solicitação de pesquisa para fluxo de trabalho de mudanças de IoC
  - Integração do Security Operations - Fluxo de trabalho de pesquisa e exclusão de e-mails
- Orquestração de inteligência contra ameaças fluxos de trabalho:
  - Inteligência contra ameaças - Executar fluxo de trabalho de pesquisa de IoC
  - Atualizar incidente de segurança com fluxo de trabalho de resultados de pesquisa
- Orquestração do Vulnerability Response fluxos de trabalho:
  - Fluxo de trabalho de vulnerabilidade de verificação
  - Fluxo de trabalho do item de vulnerabilidade de verificação

Fluxos de trabalho de orquestração do Security Operations

Vários fluxos de trabalho estão incluídos com Security Operations.

Fluxo de trabalho de vulnerabilidade de verificação

O **Vulnerability Response** > **Vulnerabilidade de verificação** O fluxo de trabalho verifica novamente uma tarefa de correção.

Antes de Iniciar
Função necessária: none

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado pela nova verificação do **grupo vulnerável** durante uma ação **Fechar/Ignorar**.

As atividades do processo de fluxo de trabalho incluem:

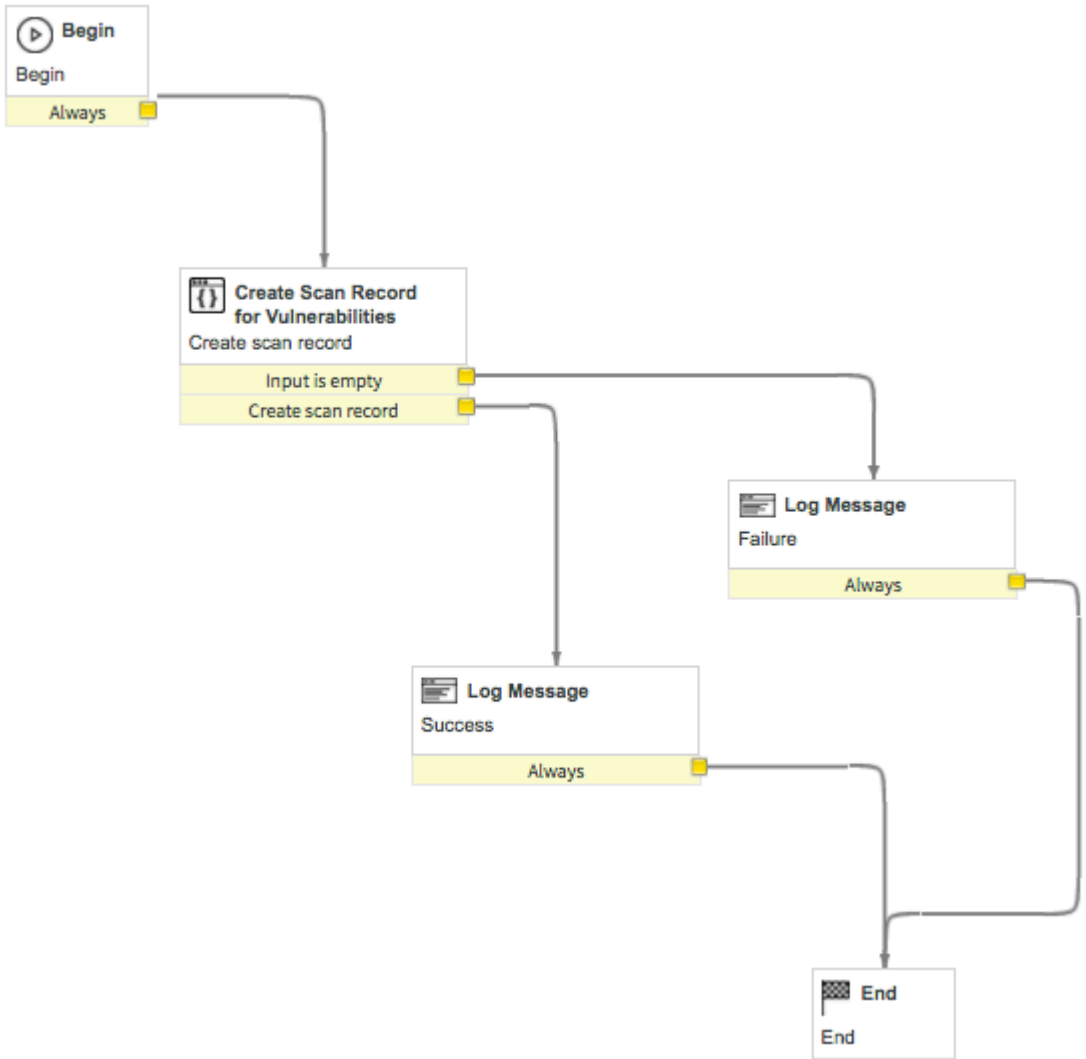
Variáveis para a atividade Criar registro de verificação para vulnerabilidades

Mensagem de log

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de verificação de vulnerabilidade



Tradução automática

Procedimento

1. Navegar até **Todos** > **Vulnerability Response** > **Tarefas de correção**.
2. Abra um registro de tarefa (VUL).
3. Clique em **Fechar**.
4. Escolha **Encerrado** para o **Estado desejado**.
5. Escolha **Fixo** para o **Subestado**.
6. Escolha **Aguardar confirmação da próxima verificação** para **Fechar agora?**
   Para a tarefa de correção e os itens vulneráveis, o **Estado** muda para **Confirmação pendente**, o **Subestado** muda para **Fixo**e uma nova verificação é executada.

Variáveis para a atividade Criar registro de verificação para vulnerabilidades

As verificações de vulnerabilidade para um ou vários itens vulneráveis podem ser executadas usando a atividade de fluxo de trabalho **Criar registro de verificação para vulnerabilidades** incluída no sistema de base. Quando a entrada é passada para a atividade, ela cria um registro de verificação.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
taskids [cadeia de caracteres]	Uma cadeia de caracteres de sysIds separados por vírgulas que define as entradas esperadas. Este campo é obrigatório.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado da verificação [booliano]	Retorna Verdadeiro se a entrada não estiver vazia. Um registro de verificação é criado para os taskIds.

Fluxo de trabalho do item de vulnerabilidade de verificação

O**Resposta vulnerável** > **Item de vulnerabilidade de verificação** O fluxo de trabalho verifica novamente um item vulnerável.

Antes de Iniciar
Função necessária: none

Por Que e Quando Desempenhar Esta Tarefa
Este fluxo de trabalho é acionado pela **vulnerabilidade**de nova verificação durante uma ação **Fechar/Ignorar**.

As atividades do processo de fluxo de trabalho incluem:

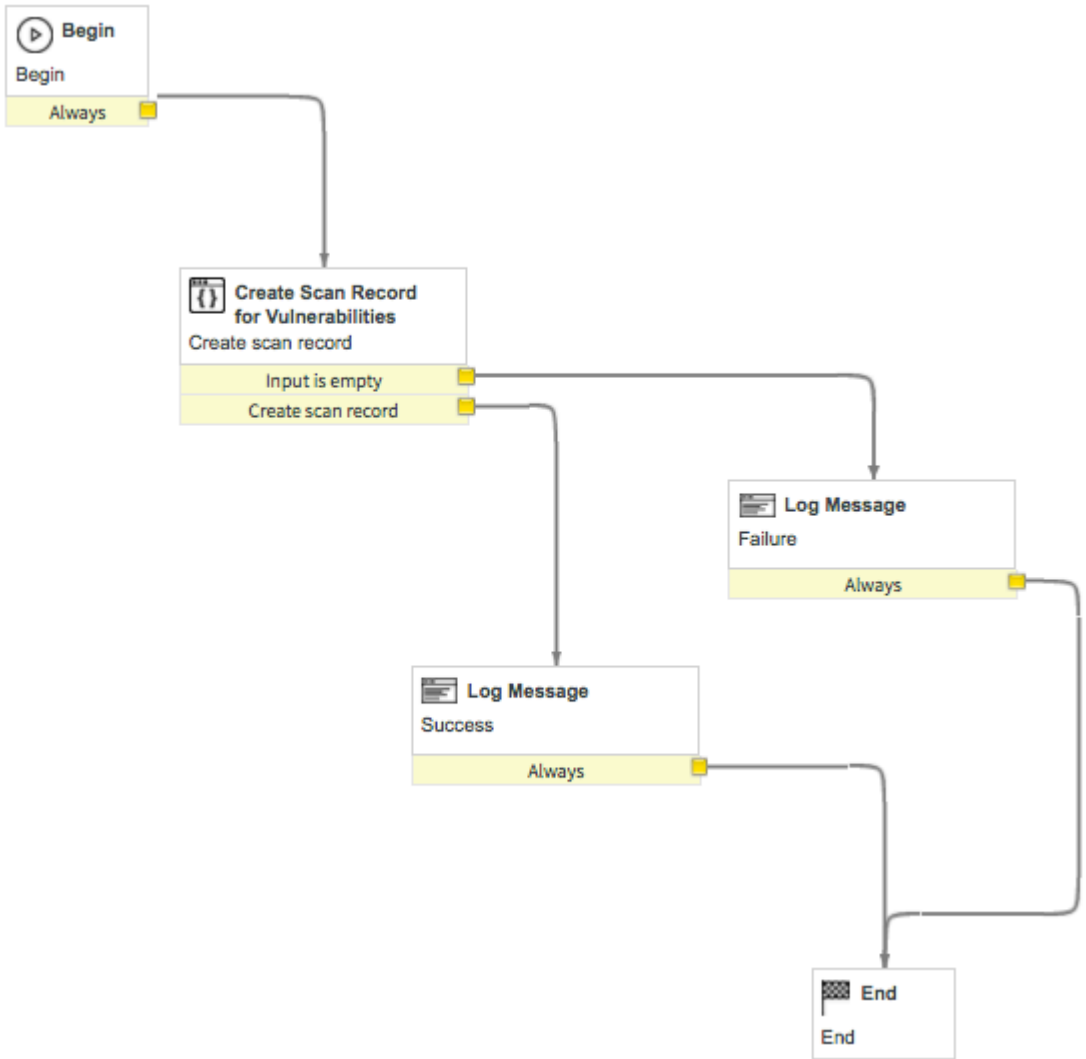
Variáveis para a atividade Criar registro de verificação para vulnerabilidades

Mensagem de log

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Fluxo de trabalho de verificação de vulnerabilidade



Tradução automática

Procedimento

1. Navegar até **Vulnerabilidade** > **Vulnerabilidades** > **Itens vulneráveis**.
2. Abra um item de vulnerabilidade.
3. Clique **em Fechar/Ignorar**.
4. Escolha **Encerrado**para o **Estado desejado**.
5. Escolha **Fixo** para o **Subestado**.
   O **Estado** do grupo muda para **Confirmação pendente**, o **Subestado** muda para **Fixo**e uma nova verificação é executada.

Atualizar incidente de segurança com fluxo de trabalho de resultados de pesquisa

O fluxo de trabalho Atualizar **incidente de segurança com resultados de pesquisa** atualiza os incidentes de segurança existentes com resultados de pesquisa.

Antes de Iniciar

Função necessária: sn_si.basic

Por Que e Quando Desempenhar Esta Tarefa

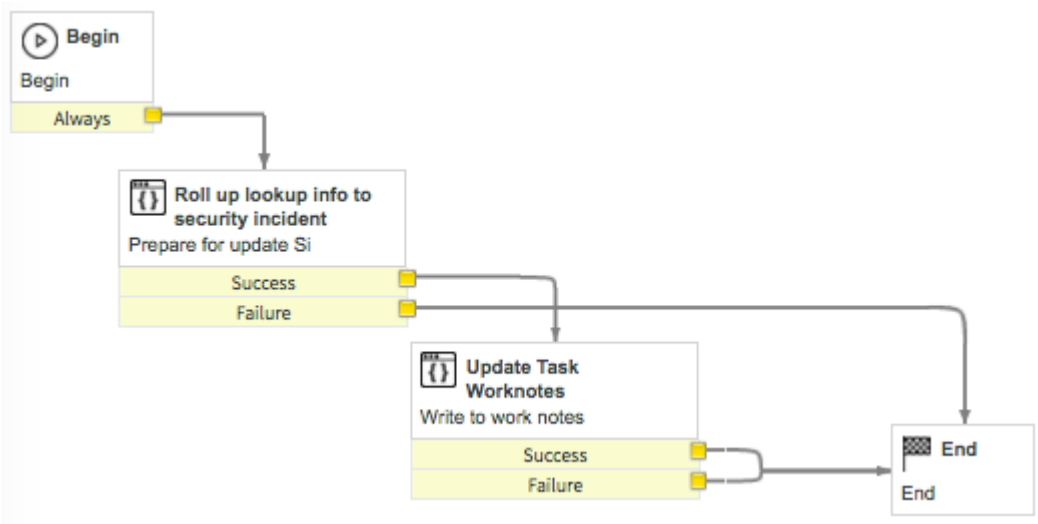
Este fluxo de trabalho é acionado por uma regra de negócios na tabela de pesquisa que monitora quando o campo **Resultado** muda para Falha.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

As atividades do processo de fluxo de trabalho incluem:

Acumular informações de pesquisa para atividade de incidente de segurança

Atividade Atualizar anotações de trabalho da tarefa



Atividades de orquestração do Security Operations

Muitas atividades estão incluídas com Security Operations para uso em fluxos de trabalho.

Atividade Criar registros de dados de aprimoramento

A atividade de fluxo de trabalho **Criar registros de dados de** aprimoramento cria ou atualiza registros de aprimoramento para uso no fluxo de trabalho.

A atividade **Criar registros de dados de aprimoramento** pode ser usada com qualquer fluxo de trabalho para atualizar registros de aprimoramento no fluxo de trabalho.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Registro de aprimoramento atualizado.
Falha	Registro de aprimoramento não atualizado. Mais informações de erro estão disponíveis no erro de saída da atividade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
task_id	Identificador de tarefa.
conteúdo	Conteúdo bruto (dados de processos em execução).
richment_mapping_id	Identificador de mapeamento de aprimoramento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variável	Descrição
ci_id	Identificador do item de configuração.
valor_referência	Não utilizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado	GlideRecords criado usando o script richmentUtils.

Atividade Obter FQDN do item de configuração

O **Orquestração do Security Common** > **Obter FQDN do item de configuração** A atividade de fluxo de trabalho recupera o nome de domínio totalmente qualificado (FQDN) de um item de configuração. Esta atividade pode acelerar o processo de investigação e correção.

A atividade Obter FQDN do item de configuração pode ser usada com qualquer fluxo de trabalho para recuperar o nome de domínio totalmente qualificado (FQDN) de um item de configuração.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
cmdb_ci.id [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de item de configuração.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
fqdn [cadeia de caracteres]	O nome de domínio totalmente qualificado (FQDN) do item de configuração.

Anotações Adicionais

O campo fqdn no item de configuração deve ser preenchido.

Criar atividade de pesquisa de conformidade

A atividade Criar pesquisa de conformidade cria uma pesquisa de conformidade para e-mails no(s) servidor(es) do Exchange designado(s) usando as consultas de pesquisa definidas e retorna o nome da pesquisa de conformidade criada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
search_query	Consulta de pesquisa obrigatória usada para encontrar e-mails no Exchange Server em todas as caixas de correio.
Exchange Local	Campo de local obrigatório usado para pesquisar no local definido. Os valores são: • Todos • Nome da caixa de correio específica
targetId	Campo de identificador de host de destino obrigatório onde o Exchange Server está localizado.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Nome da pesquisa de conformidade criada.

Condições de Saída

As possíveis condições de saída para esta atividade são:

Condições de Saída

Variável	Descrição
Falha na criação da pesquisa	Quando a criação da pesquisa falha devido a uma exceção no Exchange Server.
Pesquisa criada com sucesso	Quando a criação da pesquisa é bem-sucedida.
Falha na criação da pesquisa devido a um erro de análise	Quando a criação da pesquisa falha devido a um problema de análise.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Obter IP da atividade de IC

Esta atividade de fluxo de trabalho determina o endereço IPV4 associado a um item de configuração (IC).

A atividade **Obter IP do IC** pode ser usada com qualquer fluxo de trabalho para recuperar o endereço IPv4 de um IC.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
ci_sys_id [cadeia de caracteres]	Identificador do sistema do item de configuração

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
ip_addr [cadeia de caracteres]	Endereço IPv4. Se o endereço IP não puder ser determinado, este valor ficará em branco.

Condições de Saída

Os resultados possíveis para esta atividade são:

Condições

Condição	Descrição
Êxito	Um endereço IPv4 foi retornado.
Falha	Não foi possível determinar um endereço IPv4.

Obter estatísticas de rede por meio da atividade netstat

A atividade de fluxo de trabalho Security Common Orchestration - Obter estatísticas de rede via netstat recupera as estatísticas de rede de um recurso afetado em um sistema baseado no Windows. Esta atividade pode acelerar o processo de investigação e correção.

A atividade Obter estatísticas de rede via netstat pode ser usada com qualquer fluxo de trabalho para recuperar estatísticas de rede de um sistema baseado no Windows. A máquina é consultada com o comando **netstat**, incluindo os parâmetros **-a** e **-o**. Para aprimorar os dados de saída, o comando **get-process** também é invocado.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	As estatísticas de rede foram recuperadas no formato JSON.
Falha	Ocorreu um erro ao tentar recuperar as estatísticas da rede. Mais informações de erro estão disponíveis no erro de saída da atividade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de entrada

Variável	Descrição
destino [cadeia de caracteres]	O nome de domínio totalmente qualificado (FQDN) ou o endereço IP do sistema de destino.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta [cadeia de caracteres]	Uma cadeia de caracteres JSON que representa os processos em execução no momento na máquina de destino. Os dados JSON incluem: **PID** Identificador de processo **_port local** Porta local para a transação de rede **state** Status da conexão TCP. **Nota:** Este campo é nulo para conexões UDP. **local_address** Nome de domínio totalmente qualificado (FQDN) local ou endereço IP **remote_address** Nome de domínio totalmente qualificado (FQDN) ou endereço IP remoto **protocolo** TCP ou UDP **remote_port** Porta remota da transação de rede **path** O caminho do arquivo do executável do processo **hash** O valor de hash do executável do processo. O hash está em SHA-256 para PowerShell V4 ou superior. Caso contrário, o hash estará em MD5.

Restrições

O MID Server deve oferecer suporte ao PowerShell.

O hash SHA-256 requer PowerShell V4.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Obter processos em execução por meio de atividade WMI

A atividade de fluxo de trabalho**Obter processos em execução** recupera os processos em execução de um item de configuração em um sistema baseado no Windows. Esta atividade pode acelerar o processo de investigação e correção.

A atividade **Obter processos em execução via WMI** pode ser usada com qualquer fluxo de trabalho para recuperar processos em execução em um sistema baseado no Windows.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
destino [cadeia de caracteres]	O nome de domínio totalmente qualificado (FQDN) ou o endereço IP do sistema de destino.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta [cadeia de caracteres]	Uma cadeia de caracteres JSON que representa os processos em execução no sistema de destino. Os dados JSON incluem: **PID** O identificador do processo **nome** O nome do processo Além disso, se disponível: **Responsável** O nome do proprietário do processo **owner_sid** O identificador do sistema do responsável pelo processo **owner_domain** O domínio do proprietário do processo **path** O caminho do arquivo do executável do processo **hash** O valor de hash do executável do processo. O hash está em SHA-256 para PowerShell V4 ou superior. Caso contrário, o hash estará em MD5.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Restrições

O MID Server deve oferecer suporte ao **PowerShell**.

O hash SHA-256 requer PowerShell V4.

Verificar atividade de status de pesquisa de conformidade

A atividade Verificar status de pesquisa de conformidade verifica o status da pesquisa de conformidade criada no Exchange Server e, se o status for concluído, retorna as informações sobre a pesquisa de e-mail encontrada para a pesquisa de conformidade.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variável	Descrição
targetId	Campo de identificador de host de destino obrigatório onde o Exchange Server está localizado.
searchName	Nome obrigatório da pesquisa de conformidade criada no Exchange Server.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resposta	Contém o status da pesquisa de conformidade e o número de e-mails encontrados no servidor de troca para a pesquisa de conformidade.

Condições de Saída

As possíveis condições de saída para esta atividade são:

Condições de Saída

Variável	Descrição
Pesquisa em andamento	Quando o status da pesquisa de conformidade está em andamento.
Pesquisa concluída - Nenhum e-mail de ameaça encontrado	Quando o status da pesquisa de conformidade é concluído e nenhum e-mail é encontrado como parte da pesquisa de conformidade.
Pesquisa concluída - E-mails de ameaça encontrados	Quando o status da pesquisa de conformidade é concluído, e os e-mails são encontrados como parte da pesquisa de conformidade.
Erro ao verificar status	Quando a verificação de status falha devido a uma exceção no Exchange Server.
Erro	Quando ocorre uma exceção na atividade de fluxo de trabalho.

Atividade Atualizar anotações de trabalho da tarefa

A atividade de fluxo de trabalho **Security Common Orchestration - Atualizar anotações de trabalho de tarefa** atualiza a seção **Atividade** (anotações de trabalho) de um registro de tarefa. Isso é útil para registrar informações.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A atividade **Atualizar** anotações de trabalho da tarefa pode ser usada com qualquer fluxo de trabalho para atualizar as anotações de trabalho de qualquer registro de tarefa.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
task_id [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de tarefa.
conteúdo [cadeia de caracteres]	Os dados gravados nas anotações de trabalho de uma tarefa.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	Indica se a atualização foi bem-sucedida.

Acumular informações de pesquisa para atividade de incidente de segurança

A atividade **Acumular informações de pesquisa para incidente de segurança** pode ser usada com qualquer fluxo de trabalho para coletar informações de uma pesquisa de ameaça e gerar um resumo do conteúdo, bem como o ID do incidente de segurança de origem nas anotações de trabalho da tarefa.

Resultados

Os resultados possíveis para esta atividade são:

Resultados

Resultado	Descrição
Êxito	Resumo do relatório de pesquisa acumulado para incidente de segurança.
Falha	A tarefa de origem e o relatório resumido de pesquisa estão vazios.

Variáveis de entrada

Variável	Descrição
scanID[cadeia de caracteres]	Identificador de pesquisa.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Variáveis de saída

Variável	Descrição
siId[cadeia de caracteres]	Identificador de incidente de segurança.
resposta [cadeia de caracteres]	Resumo dos resultados da pesquisa, incluindo: valor de IoC, resultado, motivo da falha, referência de pesquisa e assim por diante.

Gravar conteúdo para registro como atividade de anexo

Esta atividade grava o conteúdo passado de uma entrada e cria um anexo designado para um determinado registro.

A atividade **Gravar conteúdo para registro como anexo** pode ser usada com qualquer fluxo de trabalho para gravar conteúdo e anexá-lo a um registro.

Variáveis de entrada

As variáveis de entrada determinam o comportamento inicial da atividade.

Variáveis de entrada

Variável	Descrição
nome da tabela [cadeia de caracteres]	O nome da tabela para o registro. Este campo de entrada é obrigatório.
sysid [cadeia de caracteres]	O identificador do sistema (sys_id) de um registro de tarefa. Este campo de entrada é obrigatório.
carga	O conteúdo de texto sem formatação a ser gravado como anexo. Este campo de entrada é obrigatório.
nome do arquivo	O nome do arquivo do anexo.

Variáveis de saída

As variáveis de saída contêm dados que podem ser usados em atividades subsequentes.

Variáveis de saída

Variável	Descrição
resultado [cadeia de caracteres]	Indica se a atualização foi bem-sucedida.

Data Loss Prevention Incident Response

A aplicação Data Loss Prevention Incident Response (DLP IR) permite revisar e gerenciar o fluxo de trabalho de correção de incidentes DLP de várias fontes, como endpoint, rede, e-mail e nuvem.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Data Loss Prevention Incident Response

Explorar Saiba mais sobre como analistas e administradores usam o DLP Incident Response	**Instalar e configurar** Instalar e configurar a aplicação DLP Incident Response	**Administrar** Tarefas de administração sobre como gerenciar os incidentes do DLP na Now Platform
Usar Atualize e gerencie incidentes aproveitando o DLP End User Portal, o DLP Ops Portal e o DLP Dashboard.	**Integrar** Estenda as capacidades do DLP integrando-as a aplicações de terceiros	

Explorar o Data Loss Prevention Incident Response

Explore a aplicação Data Loss Prevention Incident Response para saber como gerenciar informações confidenciais de seus clientes, como dados financeiros e proprietários, registros de saúde ou números de previdência social.

A perda de dados ocorre quando informações confidenciais ou confidenciais saem da rede corporativa como resultado de comunicação não autorizada. Com a aplicação DLP, você pode identificar, responder e proteger seus canais de perda de dados.

Ao usar a aplicação Data Loss Prevention Incident Response, sua organização tem os seguintes benefícios principais:

- Integre a várias soluções DLP de terceiros para obter uma exibição unificada dos incidentes no Now Platform.
- Monitore e atribua incidentes aos usuários finais para simplificar a gestão de incidentes do DLP.
- Treine seus funcionários por meio de modelos de e-mail personalizados e notificações que são enviadas para cada incidente, bem como na forma de um resumo.
- Escale os incidentes DLP atrasados dos usuários finais para os gerentes.
- Exiba relatórios resumidos de incidentes em aberto por política, severidade, principais infratores e assim por diante.
- Rastreie tendências de incidentes do DLP, tendências de falsos positivos e tendências de correção.

Use esta seção para saber mais sobre os principais recursos e várias funções envolvidas no trabalho com incidentes do DLP.

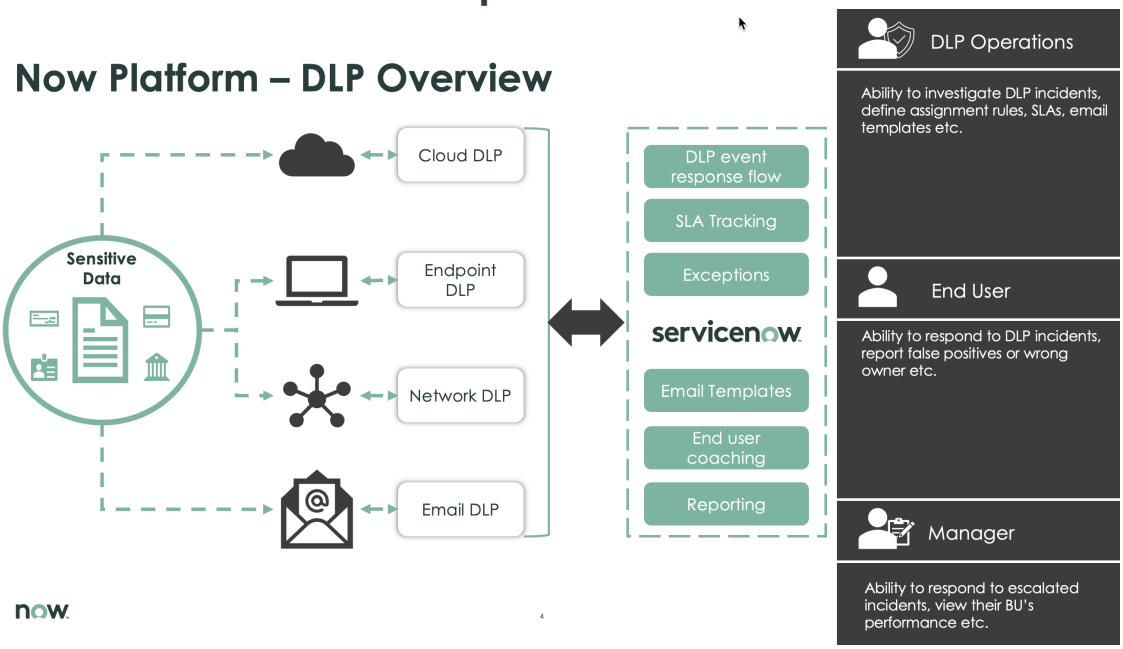
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral do Incident Response do DLP

Saiba como você pode usar a aplicação Now Platform e Data Loss Prevention Incident Response (DLP IR). Gerencie informações confidenciais de seus clientes, como dados financeiros e proprietários, registros de saúde ou números de previdência social. Automatize os fluxos de trabalho de correção com a aplicação DLP Incident Response.

Data Loss Prevention Incident Response e o Now Platform



A aplicação Data Loss Prevention Incident Response inclui os seguintes recursos:

- Um espaço de usuário final no qual os usuários finais ou funcionários podem revisar e responder aos incidentes atribuídos ao DLP.
- Um espaço para gerentes em que um gerente pode revisar os incidentes do DLP escalonados e agir sobre eles de forma apropriada.
- Um espaço unificado onde sua equipe de operações do DLP pode rastrear as tendências dos incidentes em aberto, principais infratores, incidentes por origem de verificação e pode exibir, editar, atribuir e fechar os incidentes do DLP em várias origens (endpoints, redes e e-mail).
- Controles administrativos que definem os modelos de e-mail para coaching e comunicação do usuário final, regras de atribuição para atribuição automática de incidentes, regras de escalação automática e delegação para respostas a incidentes.

Introdução ao DLP Incident Response

Revise as informações a seguir antes de iniciar a configuração da aplicação Data Loss Prevention Incident Response (DLP IR).

Check-list

Configuração de tarefa	Descrição
Verifique se você atribuiu as funções Now Platform e DLP necessárias.	O DLP Incident Response é compatível com as seguintes funções:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
	• O administrador (admin) instala as aplicações do ServiceNow Store e atribui o administrador do DLP (sn_dlir.admin). • sn_dlir.admin • sn_dlir.analista
Verifique se as aplicações principais ServiceNow que são necessárias para oferecer suporte à aplicação Data Loss Prevention Incident Response estão instaladas e ativadas.	O plug-in Data Loss Prevention Incident Response (com.snc.data_loss_incident) é necessário para oferecer suporte ao produto Data Loss Prevention Incident Response. Verifique se as seguintes Security Operations aplicações estão instaladas e ativadas a partir de ServiceNow Store. Se não estiverem instalados, instale e ative um aplicativo de cada vez na seguinte ordem para garantir uma instalação sem problemas: • Data Loss Prevention Incident Response (com.snc.data_loss_incident) • Security Support Common Para obter mais informações sobre como configurar sua instância Now Platform para a integração, consulte Obter direito de um produto ou aplicação do Security Operations ou Ativar uma aplicação da ServiceNow Store.
Separação de Domínio	Verifique o tópico Domain Separation e DLP Incident Response se você pretende separar dados, processos e tarefas administrativas.

Tradução automática

Instalando e configurando o DLP IR Incident Response

Baixe a aplicação Data Loss Prevention Incident Response (DLP IR) de ServiceNow Store e instale-a em sua instância.

Antes de invocar os fluxos de trabalho para a integração, instale e configure a aplicação Data Loss Prevention Incident Response do ServiceNow Store na sua instância Now Platform.

Instalar e configurar a aplicação DLP Incident Response

Gerencie informações confidenciais e automatize os fluxos de trabalho de correção usando a aplicação Data Loss Prevention Incident Response (DLP IR) em sua instância Now Platform.

Antes de Iniciar
Antes de concluir as etapas de configuração, você deve baixar a aplicação do ServiceNow Store e instalá-lo em sua instância.

Funções necessárias: admin e sn_dlir.admin

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Siga as instruções para baixar um aplicativo da ServiceNow Store.
2. Depois de baixar a aplicação **DLP Incident Response** e todas as suas aplicações dependentes, navegue até **Todos** > **Administração do DLP** > **Configuração padrão** para concluir o restante da configuração da aplicação.

Domain Separation e DLP Incident Response

Você pode usar a separação de domínio com o DLP Incident Response para separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte: Padrão

- Inclui nível de suporte **Básico**.
- Lógica de negócios: o provedor de serviço (SP) cria ou modifica processos por cliente. Os casos de uso refletem o uso adequado do aplicativo por vários clientes de SP em uma única instância.
- O proprietário da instância deve configurar a lógica de negócios do produto minimamente viável (MVP) e os parâmetros de dados por locatário conforme esperado para o aplicativo específico.

Exemplo de caso de uso: um administrador deve ser capaz de fazer os comentários necessários quando um registro é encerrado para um locatário, mas não para outro.

Para obter mais informações sobre os níveis de suporte, consulte Suporte de aplicação para separação de domínio .

Como a separação de domínio funciona com o DLP Incident Response

- Crie um usuário com as funções sn_dlir.admin e sn_dlir.analyst no respectivo domínio.
- Execute as configurações do DLP Incident Response no domínio apropriado.

DLP Incident Response Administration

Você pode configurar e atribuir regras, configurar regras de data de vencimento, usar modelos de e-mail, configurar ações de resposta do usuário final e muito mais para gerenciar os incidentes Data Loss Prevention Incident Response (DLP IR) no Now Platform.

A aplicação Data Loss Prevention Incident Response permite que você execute as configurações a seguir.

Definições de configuração padrão do DLP

Defina as configurações padrão para incidentes Data Loss Prevention Incident Response (DLP IR) para identificar e configurar a notificação de incidente e as preferências de atribuição de incidente para os usuários finais.

Antes de Iniciar

Função necessária:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

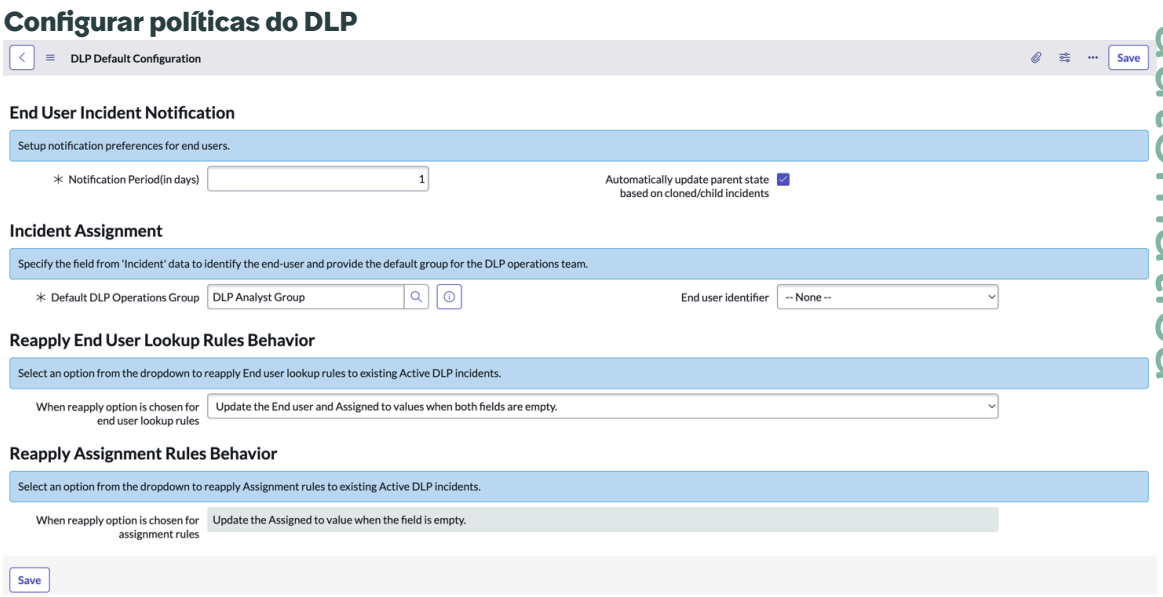
Você pode usar este módulo para definir as configurações padrão quando as regras de atribuição principais e as regras de identificador estiverem esgotadas e não puderem corresponder a uma condição ou usuário. Você também pode definir e reaplicar as regras de pesquisa de usuário final e as regras de atribuição a incidentes ativos do DLP existentes.

A notificação de incidente do usuário final permite que você especifique a frequência com que as notificações por e-mail são enviadas aos usuários finais. Por exemplo, você pode configurar preferências de notificação para acumular incidentes e enviar um resumo por e-mail uma vez por semana. Ao atribuir um incidente, você pode especificar a qual grupo você atribui inicialmente os incidentes do DLP. Você também pode especificar como os usuários finais serão identificados pela equipe de operações do DLP.

Por exemplo, digamos que um usuário tenha armazenado informações de cartão de crédito em um arquivo em uma rede. Quando o produto de integração DLP de terceiros cria um incidente para uma violação de política de dados confidenciais, os dados do incidente que o Now Platform DLP ingere contêm informações sobre o usuário final. Você poderá atribuir o incidente ao usuário final correto.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Configuração padrão**.



2. No formulário, preencha os campos.

Formulário Configuração padrão do DLP

Nome da configuração	Campo	Descrição
Notificação de incidente do usuário final	Período de notificação (dias)	Defina o número de dias após o qual uma notificação por e-mail deve ser enviada ao usuário final. O número de dias deve estar entre 1 e 60 dias.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da configuração	Campo	Descrição
	Atualiza automaticamente o estado primário com base em incidentes clonados/ secundários	Opção para atualizar automaticamente o incidente de estado primário com base nos incidentes clonados ou secundários.
Atribuição de incidente	Grupo de operações DLP padrão	Grupo padrão ao qual todos os incidentes do DLP são atribuídos. **Nota:** Você só pode exibir e selecionar grupos que foram atribuídos à função sn_dlir.analyst.
	Identificador de usuário final	Especifique o campo a ser usado nos dados de incidente para identificar o usuário final. Os valores possíveis são os seguintes: ○ **E-mail do proprietário dos dados** ○ **Destino** ○ **Arquivo criado por** ○ **Arquivo modificado por** ○ **Proprietário do arquivo** ○ **Nome de usuário do FTP** ○ **Remetente**
Reaplicar comportamento das regras de pesquisa de usuário final	Quando a opção de reaplicação é escolhida para regras de pesquisa de usuário final	Opção para reaplicar as regras de pesquisa de usuário final aos incidentes ativos do DLP existentes. Você pode selecionar uma das seguintes opções para reaplicar: ○ **Atualizar o valor do usuário final quando o campo estiver vazio**: atualiza o valor do usuário final dos incidentes DLP ativos existentes se o campo estiver vazio. ○ **Atualizar o valor do usuário final**: atualiza o valor do usuário final dos incidentes DLP ativos existentes. ○ **Atualizar os valores de Usuário final e Atribuído a quando ambos os campos estiverem vazios**: atualiza os valores de Usuário final e Atribuído a dos incidentes DLP ativos existentes se ambos os campos estiverem vazios.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nome da configuração	Campo	Descrição
		Nota: Se esta opção for selecionada, a opção **Atualizar o valor Atribuído a quando o campo estiver vazio** será desabilitada automaticamente na seção Reaplicar comportamento das regras de atribuição, pois é aplicável a ambos. ○ **Atualizar os valores de Usuário final e Atribuído a de todos os incidentes DLP ativos**: atualiza os valores de Usuário final e Atribuído a de todos os incidentes DLP ativos. **Nota:** Se esta opção for selecionada, a opção **Atualizar o valor atribuído a todos os incidentes DLP ativos** será desabilitada automaticamente na seção Reaplicar comportamento das regras de atribuição, pois é aplicável a ambos.
Reaplicar comportamento das regras de atribuição	Quando a opção de reaplicação é escolhida para regras de atribuição	Opção para reaplicar regras de atribuição a incidentes DLP ativos existentes. Você pode selecionar uma das seguintes opções para reaplicar: ○ **Atualize o valor Atribuído a quando o campo estiver vazio.** ○ **Atualize o valor Atribuído a para todos os incidentes DLP ativos.**

3. Clique em **Salvar**.

Configurar regras de pesquisa de usuário final

Você pode criar e configurar regras de pesquisa de usuário final e atribuir os incidentes do DLP aos respectivos usuários finais com base nessas regras.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

O administrador do DLP define essas regras de pesquisa de usuário final para atribuir automaticamente os usuários finais a incidentes do DLP usando somente o campo de usuário final. A regra de pesquisa de usuário final do DLP permite que você atribua o usuário final em incidentes do DLP com base no identificador do usuário final, nos atributos personalizados ou no script.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Regras de pesquisa de usuário final do DLP**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de pesquisa de usuário final do DLP

Campo	Descrição
Nome	Nome da regra de pesquisa de usuário final.
Ativo	Opção para indicar se a regra de pesquisa de usuário final está ativa.
Ordem de execução	A prioridade da regra de pesquisa do usuário final. Este campo indica a ordem na qual as regras de pesquisa de usuário final são executadas quando duas ou mais regras compartilham as condições de acionamento. A regra de pesquisa de usuário final com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.
Descrição	Descrição exclusiva da regra de pesquisa de usuário final.
Condição	Condições no construtor de condição. Essas condições são baseadas na tabela de incidentes do DLP. Para criar uma condição para a regra de pesquisa de usuário final, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**. ○ Se **AND** for selecionado, todas as condições deverão ser correspondidas. ○ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. Por exemplo, você pode definir as condições para esta regra de pesquisa de usuário final selecionando a condição como **Origem de integração**, **contém**, **Symantec**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: As condições no construtor de condição fazem distinção entre maiúsculas e minúsculas.
Pesquisar usuário final usando	Opção para pesquisar usuário final usando o **campo Incidente** ou **Script**.
Identificador de usuário final	O identificador de usuário final do incidente do DLP. Este campo aparece quando o **campo Incidente** é selecionado no campo **Pesquisar usuário final usando**. Você pode selecionar um identificador de usuário final a partir do seguinte: ○ **E-mail do proprietário dos dados** ○ **Destino** ○ **Arquivo criado por** ○ **Arquivo modificado por** ○ **Proprietário do arquivo** ○ **Nome de usuário do FTP** ○ **Remetente** ○ **Usuário personalizado do incidente**
Atributo personalizado	Opção para especificar um atributo personalizado do incidente que tem a referência a um usuário. Este campo é exibido somente quando **Usuário personalizado do incidente** é selecionado no campo **Identificador do usuário final**.
Script	Você pode usar o editor de script para personalizar e formatar os valores de campo durante a criação da regra de pesquisa do usuário final. Por exemplo, você pode usar o campo de endereço de e-mail para identificar o usuário final.

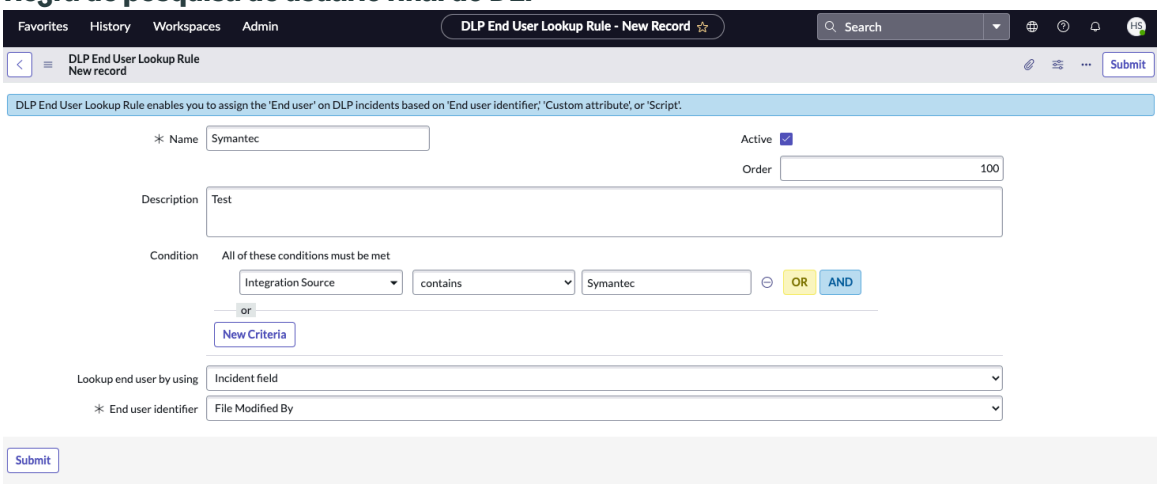
Tradução automática

Example

O exemplo a seguir mostra uma regra de pesquisa de usuário final com o nome "Symantec". O construtor de condição requer que a "Origem da integração" seja "Symantec". A opção **Pesquisar usuário final usando** está definida como "Campo de incidente" e a opção **Identificador de usuário final** está definida como "Arquivo modificado por".

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regra de pesquisa de usuário final do DLP



4. Clique em **Enviar**.
   Você também tem a opção de selecionar uma ou mais regras de pesquisa de usuário final e reaplicá-las em todos os incidentes do DLP existentes.
5. Para reaplicar uma regra de pesquisa de usuário final em todos os incidentes do DLP existentes, clique em **Reaplicar**.

Criar uma regra de atribuição para seus Data Loss Prevention Incident Response incidentes

Crie e ative as regras de atribuição. Em seguida, atribua os incidentes Data Loss Prevention Incident Response (IR do DLP) a grupos de usuários, usuários finais, gerentes ou usuário do incidente.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar regras de atribuição para atribuir incidentes de IR do DLP a grupos de usuários, usuários finais ou gerentes. A atribuição dos incidentes do DLP ocorre quando as condições na regra de atribuição são atendidas.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Regras de atribuição**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de atribuição do DLP

Campo	Descrição
Nome	Nome da regra de atribuição.
Ativo	Opção para indicar se a regra de atribuição está ativa.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Ordem de execução	A prioridade da regra de atribuição. Este campo indica a ordem na qual as regras de atribuição são executadas quando duas ou mais regras compartilham as condições do gatilho. A regra de atribuição com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.
Descrição	Descrição exclusiva desta regra de atribuição.
Condição	Condições no construtor de condição. Essas condições são baseadas na tabela de incidentes do DLP. Para criar uma condição para a regra de atribuição, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**. ○ Se **AND** for selecionado, todas as condições deverão ser correspondidas. ○ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. Por exemplo, suponha que você crie uma regra de atribuição DLP para um endpoint. Você pode especificar que a origem da verificação de condição é um sistema de arquivos de endpoint que deve ser atendido antes de atribuir um incidente. **Nota:** As condições no construtor de condição fazem distinção entre maiúsculas e minúsculas.
Atribuir a	Atribuição a um dos seguintes: ○ Grupo de usuários ○ Usuário final ○ Gerente ○ Usuário do incidente A atribuição ocorre quando as condições no construtor de condição são atendidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Grupo de usuários	Opção para pesquisar e selecionar um grupo de usuários ao qual atribuir os incidentes do DLP. Este campo aparece quando **o Grupo de usuários** é selecionado no campo **Atribuir a**. **Nota:** Você só pode exibir e selecionar grupos que foram atribuídos à função sn_dlir.analyst.
Usuário final	Opção para atribuir o incidente DLP ao usuário final. A atribuição ocorre quando as condições no construtor de condição são atendidas.
Atribuir usando campos de gerente	Gerente do usuário final. Este campo aparece quando **Gerente** é selecionado no campo **Atribuir a**. Você pode atribuir os incidentes do DLP a um gerente específico selecionando um dos campos do gerente, como Sobrenome, E-mail, Cidade, Número do funcionário.
Identificador de usuário	O identificador de usuário do incidente. Este campo aparece quando **Usuário do incidente** é selecionado no campo **Atribuir a**. Você pode selecionar um identificador de usuário a partir do seguinte: ○ **E-mail do proprietário dos dados** ○ **Destino** ○ **Arquivo criado por** ○ **Arquivo modificado por** ○ **Proprietário do arquivo** ○ **Nome de usuário do FTP** ○ **Remetente** ○ **Usuário personalizado do incidente**
Atributo personalizado	Opção para especificar um atributo personalizado do incidente que tem a referência a um usuário. Este campo é exibido somente quando o **Usuário personalizado do Incidente** é selecionado no campo **Identificador do usuário**.
Anexar avaliação	Opção para indicar se você deseja anexar uma avaliação ao incidente.
Estado da resposta da pré-avaliação	Opção para selecionar o estado em que o incidente deve estar antes que o usuário final responda. Também pode ser um estado personalizado. O valor padrão é Avaliação pendente.

Tradução automática

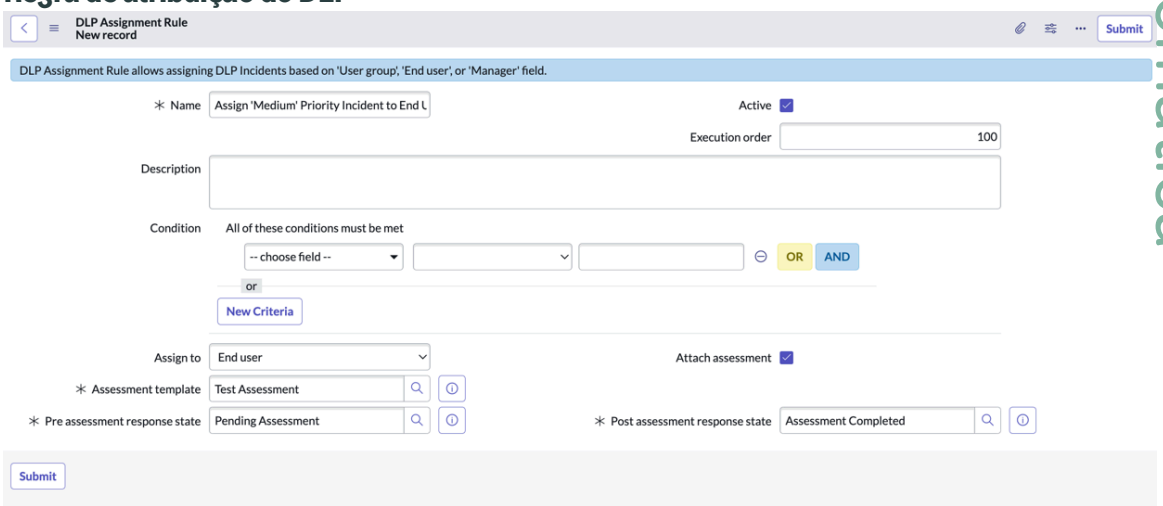
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Estado da resposta pós-avaliação	Opção para selecionar em que estado o incidente DLP deve estar depois que o usuário responder. O valor padrão é Avaliação concluída.
Avançado	Opção avançada para identificar o usuário final. Este campo é exibido somente quando o **Usuário personalizado do Incidente** é selecionado no campo **Identificador do usuário**. Você pode usar o editor de script para personalizar e formatar os valores de campo durante a criação da regra de atribuição para identificar o usuário final. Em seguida, você escolhe a quem deseja atribuir o incidente DLP, que pode ser um usuário final ou o gerente do usuário final. Por exemplo, você pode usar o campo de endereço de e-mail para identificar o usuário final.

Example

O exemplo a seguir mostra uma regra de atribuição com o nome Atribuir incidente de prioridade "média" ao usuário final. O construtor de condição requer que a Origem de verificação seja Atribuir incidente de prioridade "média" ao usuário finale que o campo Atribuir a esteja definido como Usuário final. Em seguida, você pode pesquisar o "E-mail" do usuário final.

Regra de atribuição do DLP



4. Clique em **Enviar**.
   Você também tem a opção de selecionar uma ou mais regras de atribuição e reaplicá-las em todos os incidentes do DLP existentes.
5. Para reaplicar uma regra de atribuição em todos os incidentes do DLP existentes, clique em **Reaplicar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configure regras de consolidação de incidentes para consolidar seus incidentes DLP

Configure a regra de consolidação de incidentes para consolidar vários incidentes de natureza semelhante em um incidente primário.

Antes de Iniciar

Função necessária:

- sn_dlir.admin - criar, editar e excluir
- sn_dlir.analyst e sn_dlir.analyst_read - Exibir (somente leitura)

Por Que e Quando Desempenhar Esta Tarefa

O administrador do DLP define essas regras de consolidação de incidentes para consolidar automaticamente os incidentes do DLP da mesma natureza em um incidente primário. A regra de consolidação de incidentes DLP permite consolidar os incidentes DLP com base na configuração fornecida para Duração da consolidação e Identificação de consolidação.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Regras de consolidação de incidentes do DLP**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de atribuição do DLP

Campo	Descrição
Nome	Nome da regra de consolidação do incidente.
Ativo	Opção para indicar se a regra de consolidação do incidente está ativa.
Ordem de execução	A prioridade da regra de consolidação de incidentes. Este campo indica a ordem na qual as regras de consolidação de incidentes são executadas quando duas ou mais regras compartilham as condições de acionamento. A regra de consolidação de incidente com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.
Descrição	Descrição exclusiva da regra de consolidação do incidente.
Condição	Condições no construtor de condição. Essas condições são baseadas na tabela de incidentes do DLP. Para criar uma condição para a regra de consolidação de incidente, selecione qualquer um dos campos de incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**. ○ Se **AND** for selecionado, todas as condições deverão ser correspondidas. ○ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. Por exemplo, você pode definir as condições para esta regra de consolidação de incidente selecionando a condição como **Origem de integração**, **contém**, **Symantec**. **Nota:** As condições no construtor de condição fazem distinção entre maiúsculas e minúsculas.
Duração da consolidação	Opção para definir a duração da consolidação do incidente. Os incidentes neste período com os mesmos valores para os campos selecionados serão consolidados no primeiro incidente. O primeiro incidente correspondente a esta regra será o incidente primário e o restante dos incidentes serão incidentes secundários.
Consolidar incidentes por	Selecione o campo de incidente DLP para consolidar os incidentes quando tiverem o mesmo valor no campo selecionado para incidentes diferentes. Selecione pelo menos um campo. Selecione pelo menos um campo.

O exemplo a seguir mostra uma regra de consolidação de incidentes com o nome Consolidar incidentes para integração da Symantec. O construtor de condição requer que a Origem de integração seja Symantec. A opção **Duração da condição** é definida como 1 hora e a opção Nome da política é selecionada para **Consolidar incidente em**.

No momento da ingestão do incidente do Symantec DLP, esta regra será executada e, quando vários incidentes tiverem o mesmo nome de política, o incidente será consolidado no primeiro incidente ingerido correspondente a esta regra.

4. Clique em **Enviar**.
   Os incidentes consolidados com base na regra de consolidação estarão disponíveis na lista Incidentes secundários no DLP Analyst Workspace.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar as regras de data de vencimento da resposta para seus incidentes do DLP

Configure as regras de prazo da resposta para determinar o tempo que você deseja conceder aos usuários finais para responder aos incidentes atribuídos Data Loss Prevention Incident Response (IR do DLP).

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Você pode usar este módulo para definir as regras de data de vencimento da resposta para os diferentes tipos de incidentes do DLP e as regras para iniciar a contagem da data de vencimento. Depois que a data de vencimento expirar, os usuários serão notificados sobre o incidente atrasado. Você também tem a opção de escalonar o incidente atrasado para um dos seguintes:

- Gerente
- Usuário personalizado do incidente
- Grupo de usuários

Por exemplo, quando você escala o incidente atrasado para um gerente e especificou no máximo três níveis de escalação. O primeiro nível de gerente é notificado primeiro. Se o incidente estiver atrasado novamente, o segundo nível de gerente será notificado, seguido pelo terceiro nível se o incidente ainda estiver atrasado. Se o gerente tiver um delegado, ele terá a opção de atribuir a escalação ou o incidente atrasado ao delegado.

Você também tem a capacidade de criar várias regras de prazo de resposta.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Regras do prazo da resposta**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra do prazo da resposta

Campo	Descrição
Nome	Nome da regra de prazo da resposta.
Ativo	Opção para indicar se a regra de prazo da resposta está ativa.
Vencimento em (dias)	Número de dias de vencimento.
Data de vencimento contada a partir de	Data de início usada para calcular a data de vencimento. A data de vencimento pode ser calculada a partir da primeira vez em que o usuário foi notificado sobre o incidente ou a partir da data de atribuição do incidente.
Notificar antes do prazo	Opção para notificar o usuário final sobre o incidente do DLP antes da data de vencimento.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Notificar em (dias antes do prazo)	Número de dias antes do prazo em que a regra aciona uma notificação para o usuário final.
Descrição	Descrição exclusiva para esta regra de data de vencimento da resposta.
Condição	Condições no construtor de condição. Essas condições são baseadas na tabela de incidentes do DLP. Para criar uma condição para a regra de prazo da resposta, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**. ○ Se **AND** for selecionado, todas as condições deverão ser correspondidas. ○ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. **Nota:** As condições no construtor de condição fazem distinção entre maiúsculas e minúsculas.
Escalar	Opção para escalonar o incidente DLP para alguém se a data de vencimento da resposta tiver sido violada. Para obter mais informações, consulte Adicionar vários usuários para acessar incidentes do DLP
Escalar incidente atrasado para	Opção para especificar se o incidente deve ser escalonado para um gerente, um usuário personalizado ou um grupo de usuários. Este campo é exibido somente quando a opção **Escalar** está habilitada.
Atribuir usando	Especifique como um gerente deve ser identificado. Este campo é exibido somente quando **Gerente** é selecionado no campo **Escalar incidente atrasado para**.
Níveis máximos de escalação	Opção para definir o número máximo de níveis de escalação para um gerente e um usuário personalizado. Como gerente ou usuário personalizado, você pode definir qualquer número de

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	níveis de escalação. Por padrão, são fornecidos três níveis de escalação. ○ Como gerente, você pode definir qualquer número de níveis de escalação atualizando o valor neste campo. ○ Como usuário personalizado, você pode usar o ícone + para definir qualquer número de níveis de escalação.
Atributo personalizado	Opção para especificar um atributo personalizado do incidente que tem a referência a um usuário. Este campo é exibido somente quando **Usuário personalizado do incidente** é selecionado no campo **Escalar incidente atrasado para**.
Grupo de usuários	Opção para pesquisar e selecionar um grupo de usuários para o qual escalar incidentes do DLP. Este campo é exibido somente quando **o grupo de usuários** é selecionado no campo **Escalar incidente atrasado para**. **Nota:** Você só pode exibir e selecionar grupos que foram atribuídos à função sn_dlir.analyst.

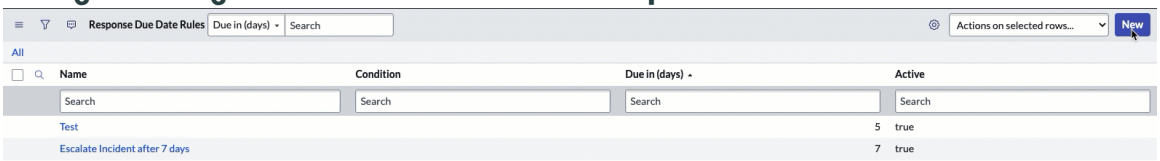
Example

O exemplo a seguir mostra a regra de prazo da resposta para determinar quanto tempo você deseja conceder aos usuários finais para responder aos incidentes Data Loss Prevention Incident Response (DLP) atribuídos. Depois que o usuário final for notificado pela primeira vez, o prazo da resposta será em dois dias. O construtor de condições mostra que a origem da verificação deve corresponder ao sistema de arquivos do endpoint para prosseguir com a criação da data de vencimento da resposta. A opção de escalação está selecionada. O incidente é escalado para o gerente se a data de vencimento da resposta for violada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar as regras de data de vencimento da resposta



4. Clique em **Enviar**.

Adicionar vários usuários para acessar incidentes do DLP

Use o recurso de cadeia de escalação para permitir que todos os respectivos usuários envolvidos no incidente acessem os incidentes do DLP na exibição de lista, embora o incidente seja atribuído a um usuário diferente.

Antes de Iniciar

Função necessária:

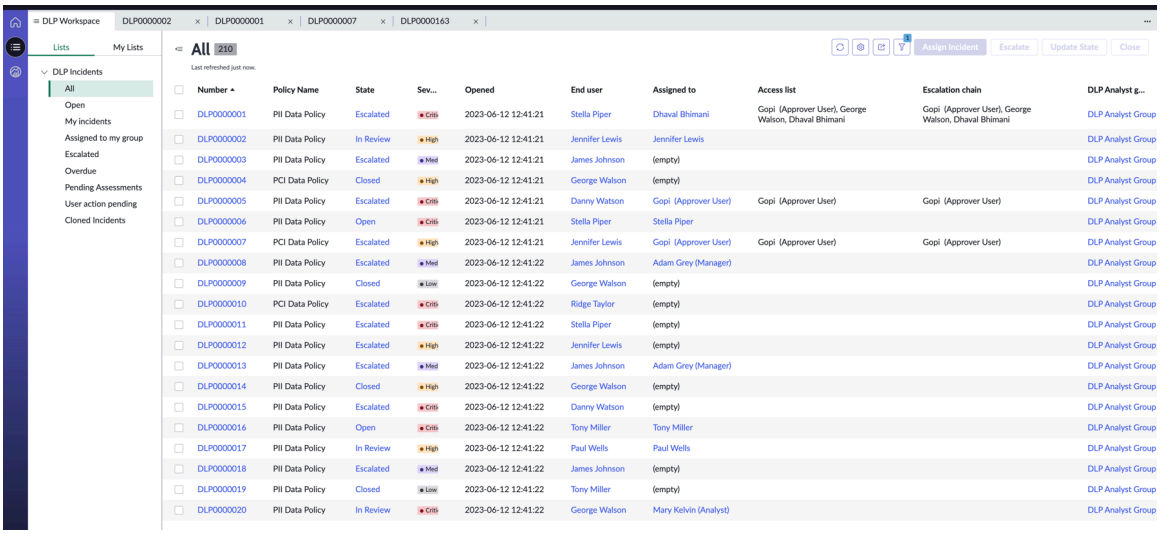
- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.read, sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Procedimento

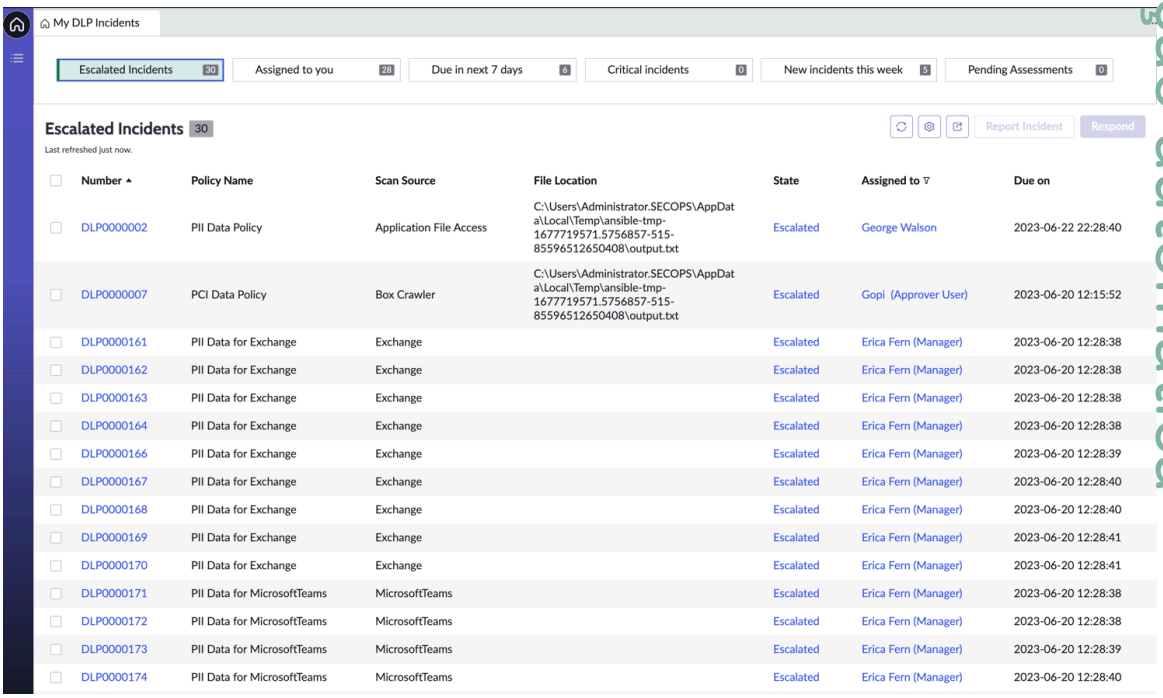
1. Navegar até **DLP** > **Espaço do analista do DLP**.
   Na exibição de lista, os usuários e seus delegados devem ser capazes de exibir o incidente DLP na guia Incidentes **escalonados** no portal do usuário final.
2. Abra qualquer incidente.
3. Clique no botão **Escalar** para escalar um incidente.
4. Selecione o usuário ou grupo de usuários na lista suspensa.
   Você pode adicionar vários usuários à cadeia de escalação. Todos os usuários com acesso são listados na seção Detalhes da exibição de formulário e também na guia **Todos os** incidentes. A cadeia de escalação é exibida com base nas definições de configuração. Para obter mais informações, consulte Definir configurações avançadas para Data Loss Prevention Incident Response

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Enviar**.
   Depois de enviar, o incidente será atribuído a um gerente, mas o usuário final ainda poderá exibir o incidente.
6. Para verificar isso, navegue até o **Espaço do usuário do DLP** como um usuário final.
   Todos os incidentes atribuídos ao usuário final são exibidos.
7. Exiba a lista de incidentes **escalonados na seção Incidentes escalonados**.



Você também pode exibir a lista de acesso dos usuários na coluna **Cadeia de escalação**na exibição de lista.

8. Abra qualquer incidente.
9. Clique no botão **Responder** para enviar a resposta do incidente.
10. Selecione a resposta na lista suspensa.
11. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar regras de aprovação

Configure regras de aprovação para obter aprovação de vários níveis de usuários aprovadores sempre que um tipo avançado de opção de resposta for selecionado.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

O administrador do DLP define essas regras de aprovação para conceder consentimento em solicitações feitas por usuários finais para a aprovação do tipo avançado de opção de resposta. O administrador do DLP também pode definir vários níveis de aprovação aqui.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Regras de aprovação do DLP**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regra de atribuição do DLP

Campo	Descrição
Nome	Nome da regra de aprovação.
Ativo	Opção para indicar se a regra de aprovação está ativa.
Ordem de execução	A prioridade da regra de aprovação. Este campo indica a ordem na qual as regras de aprovação são executadas quando duas ou mais regras compartilham as condições do gatilho. A regra de aprovação com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.
Descrição	Descrição exclusiva da regra de aprovação.
Condição	Condições no construtor de condição. Essas condições são baseadas na tabela de incidentes do DLP. Para criar uma condição para a regra de aprovação, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Para adicionar mais condições, clique em **E** ou **OU**. ○ Se **AND** for selecionado, todas as condições deverão ser correspondidas. ○ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. Por exemplo, você pode definir as condições para esta regra de consolidação de incidente selecionando a condição como **Origem de integração**, **contém**, **Microsoft**.
Aplicável para opções de resposta	Opção para selecionar a opção de resposta do tipo avançado. Você pode selecionar várias opções de resposta.
Aprovador	Selecione o tipo de usuário aprovador que você deseja definir. ○ **Tabela de usuários**: selecione esta opção se quiser selecionar o usuário aprovador na tabela Usuários (sys_user). ○ **Lista de aprovação personalizada**: selecione esta opção se quiser configurar vários níveis de aprovador personalizado para uma única solicitação
Identificador do aprovador	Este campo aparecerá quando **Tabela de usuários** for selecionada para a opção **Aprovador**. Selecione o campo para identificar o aprovador da tabela Usuários (sys_user).
Número de níveis	Este campo aparecerá quando **Tabela de usuários** for selecionada para a opção **Aprovador**. Número final neste campo para definir os níveis de aprovação. Por exemplo, se 3 for adicionado no campo Número de níveis e Gerente for selecionado no campo Identificador do aprovador, a solicitação de aprovação percorrerá três níveis de aprovação.

O exemplo a seguir mostra a regra de aprovação criada para uma das opções de resposta antecipadas. A condição requer que o nome da origem de integração contenha a palavra-chave Microsoft que aciona esta configuração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

4. Para a opção **Aprovador**, selecione **Lista de aprovações personalizadas**.
5. Clique em **Enviar**.
6. A lista relacionada de**Níveis de aprovação** será preenchida na exibição do formulário.
7. Na seção **Níveis de aprovação**, clique em **Novo**.
8. No formulário, preencha os campos.

Formulário de Nível de aprovação

Campo	Descrição
Nome	Nome do nível de aprovação.
Ativo	Opção para indicar se o nível de aprovação está ativo.
nível	O nível da regra de aprovação. Este campo indica a ordem na qual os níveis de aprovação são executados quando dois ou mais níveis são configurados. O nível de aprovação com o número mais baixo tem a prioridade mais alta. Para definir o nível de operação, insira um valor. Por exemplo, 100, 200, 300 e assim por diante. O valor padrão é 100.
Regra de aprovação	Regra de aprovação para a qual você deseja definir esta configuração. Este será um campo somente leitura.
Descrição	Descrição exclusiva da regra de aprovação.
Aprovações necessárias	Selecione a opção para definir se a aprovação de todos os usuários/grupos configurados é necessária ou somente de um usuário.
Aprovadores	Opção para selecionar os aprovadores. **a.** Usuários e Grupos: **i. Usuários**: clique no para adicionar um usuário específico da lista. Você também pode adicionar um usuário usando o endereço de e-mail ou a opção de pesquisa. Para adicionar a si mesmo como o usuário ao qual as condições do DLP são aplicáveis, clique no . **ii. Grupos**: clique no botão<add_icon> ícone para adicionar um grupo

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	específico da lista. Você também pode adicionar um grupo usando a opção de pesquisa. **b. Localizar usando script**: você pode usar o editor de script para personalizar e formatar os valores de campo durante a criação do nível de aprovação. Por exemplo, você pode usar o campo de endereço de e-mail para identificar o usuário aprovador.

9. Clique em **Enviar**.

Criar e gerenciar modelo de instruções do usuário para incidentes do DLP

Crie e gerencie o modelo de instruções do usuário para incidentes do DLP para ajudar os usuários a entender as instruções envolvidas na resolução de incidentes e as próximas etapas envolvidas no processo de resolução.

Antes de Iniciar

O modelo de cartão de instruções do usuário exibe dois cabeçalhos diferentes que fornecem mais informações sobre um incidente específico na exibição do formulário.

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Quando um incidente é atribuído ao usuário final, pode ser necessário que o usuário saiba as instruções adicionais sobre como responder aos incidentes, apresentar aos usuários a terminologia e fornecer informações adicionais sobre o incidente. Esses modelos podem orientar os usuários a fornecer a resposta precisa aos incidentes do DLP.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Modelos de instruções do usuário**.

2. Clique em **Nova**.

3. No formulário, preencha os campos.

Avaliação de incidentes do DLP

Campo	Descrição
Nome	Nome do modelo de instrução do usuário.
Descrição resumida	Descrição exclusiva deste modelo de instrução do usuário.
Ativo	Opção para indicar se o modelo de instrução do usuário está ativo.
Ordem de execução	Prioridade do modelo de instrução do usuário do incidente. Este campo indica a ordem na qual

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	a ordem é executada para avaliar o modelo de instrução do usuário quando um incidente é criado. A opção com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O padrão é 100.
Condição de correspondência de incidentes	Os incidentes que correspondem às condições definidas no construtor de condição serão exibidos. Essas condições são baseadas nos dados de incidentes do DLP. Para criar uma condição para uma instrução do usuário, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em E ou OU: Se AND for selecionado, todas as condições deverão ser correspondidas. Se OU for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. **Nota:** As condições no construtor de condição fazem distinção entre maiúsculas e minúsculas.
Aplica-se a	Selecione o usuário ou grupos de usuários para os quais o modelo é aplicável. As outras opções disponíveis são: ○ **Todos os usuários finais**: marque esta caixa de seleção se o modelo de instruções se aplicar a todos os usuários. ○ **Todos os revisores de incidentes escalonados**: marque esta caixa de seleção se o modelo se aplicar a todos os revisores dos incidentes escalonados. ○ **Usuários específicos**: clique no ícone para adicionar um usuário específico da lista ao qual as condições de incidente do DLP são aplicáveis. Você também pode adicionar um usuário usando o endereço de e-mail ou a opção de pesquisa. Por exemplo, Gerente jurídico.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Para adicionar a si mesmo como o usuário ao qual as condições do DLP são aplicáveis, clique no ícone **Adicionar-me**. ○ **Grupos de usuários específicos**: clique no ícone para adicionar um grupo específico da lista ao qual as condições de incidente do DLP são aplicáveis. Você também pode adicionar um grupo usando a opção de pesquisa. Por exemplo, Criadores de pesquisa.
Modelo de instruções: instruções	Adicione instruções no editor de rich text com variáveis disponíveis em um nível de incidente.

4. Faça uma busca detalhada na seção **Modelo de instruções**, insira a instrução do modelo e adicione informações de nível de incidente nesta seção, se necessário.
5. Arraste e solte as variáveis necessárias para exibir determinados campos dinamicamente.
6. Clique em **Enviar**.
   Os modelos de instruções do usuário agora foram criados e você pode clicar em qualquer cabeçalho de instrução do usuário para saber os detalhes adicionais de um incidente do DLP.

   Para obter mais informações, consulte Data Loss Prevention Incident Response Espaço do usuário.

Configurar instruções do usuário da IU do DLP

Configure as mensagens de IU do sistema para adicionar cabeçalhos detalhados de instruções do usuário, conforme necessário.

Antes de Iniciar
Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **IU do Sistema** > **Mensagens**.
2. Pesquise por **user_instrution_card_heading**.

   Por padrão, user_instruction_card_heading e user_instruction_modal_window_heading são as duas configurações de mensagem de IU provisionadas para os usuários.
3. Clique em qualquer uma das instruções do usuário para atualizar ou modificar.

Criar e gerenciar modelos de e-mail para seus incidentes do DLP

Crie e gerencie os modelos de e-mail pré-configurados para enviar notificações aos usuários finais, grupos de usuários ou gerentes. Com esses modelos, você pode treinar e se comunicar com os usuários finais sobre os incidentes Data Loss Prevention Incident Response (DLP IR).

Antes de Iniciar
Função necessária:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Importante:
Para que os analistas exibam as comunicações por e-mail de um incidente do DLP no fluxo de atividades, você deve adicionar ou anexar a função "sn_dlir.analyst" à propriedade do sistema global glide.ui.activity.email_roles.

Por Que e Quando Desempenhar Esta Tarefa

As notificações por e-mail são categorizadas pelas notificações de incidente que são enviadas aos usuários finais, pelas notificações de escalação que são enviadas aos gerentes ou pelas notificações de data de vencimento. Você pode enviar notificações por e-mail sobre os prazos dos incidentes do DLP ou até mesmo treinar os usuários finais sobre o que fazer quando determinadas condições forem atendidas no filtro de condições de e-mail.

Os modelos de e-mail do DLP permitem que você envie a notificação por e-mail para usuários finais, gerentes e analistas. Você pode configurar os modelos a serem enviados por incidente ou como um resumo. O assunto e o corpo do e-mail podem conter variáveis para que você possa reutilizar o conteúdo existente.

O DLP fornece os seguintes modelos de e-mail pré-configurados com base nas categorias:

- **Modelo de e-mail do DLP – Notificação de aprovação por incidente: notifique** os usuários sobre a aprovação de suas solicitações.
- **Modelo de e-mail do DLP – Notificação de escalação:** envie notificações de escalação para os gerentes na forma de resumos.
- **Modelo de e-mail do DLP – Notificação de aprovação pendente: notifique** os aprovadores sobre itens pendentes.
- **Modelo de e-mail do DLP – Notificação de cancelamento da solicitação de aprovação por incidente: notifique**os usuários sobre uma solicitação de aprovação que foi cancelada pela equipe de analistas do DLP.
- **Modelo de e-mail do DLP – Notificação de conclusão de resposta do usuário: notifique** a equipe de analistas do DLP sobre a resposta enviada pelos usuários.
- **Modelo de e-mail do DLP – Notificação de incidente do usuário:**este é um modelo padrão para notificação de resumo do usuário. Envie notificações de incidentes para os usuários finais na forma de resumos a cada poucos dias, mesmo se não houver novos incidentes, para informar os usuários sobre o número total de incidentes no nome do usuário específico. Você também pode enviar notificações de resumo para notificar os usuários sobre as datas de vencimento mais próximas dos incidentes do DLP com a severidade crítica, alta, média ou baixa.
- **Modelo de e-mail do DLP - notificação de aprovação pendente por incidente**: notifica os aprovadores sobre aprovações pendentes.
- **Modelo de e-mail do DLP - notificação de rejeição:** envie uma notificação de rejeição ao solicitante.
- **Modelo de e-mail do DLP – Notificação de data de vencimento:** envie uma notificação de data de vencimento do incidente. Se um incidente do DLP for atribuído ao usuário final e o usuário final não tiver realizado nenhuma ação antes da data de vencimento, uma notificação por e-mail será enviada ao usuário final. Você também tem a opção de escalar o incidente DLP para um gerente, um usuário personalizado ou um grupo de usuários se a data de vencimento da resposta tiver sido violada.

Nota:
As notificações de data de vencimento devem estar na forma de resumos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- **Modelo de e-mail do DLP – Notificação de resposta do usuário por incidente: notifique** os analistas sobre a resposta enviada aos usuários por incidente.
- **Modelo de e-mail do DLP –** Notificação de escalação por incidente: notifique os gerentes sobre escalações por incidente.
- **Modelo de e-mail do DLP: notificação de usuário por incidente:** notifica os usuários sobre a atribuição por incidente.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Modelos de e-mail**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de modelo de e-mail do DLP

Campo	Descrição
Nome	Nome do modelo de e-mail.
Ativo	Opção para indicar se o modelo de e-mail do DLP está ativo. Se esta opção não estiver habilitada, as notificações não serão enviadas para este modelo de e-mail.
Categoria	Categoria de notificação por e-mail. O DLP oferece suporte às seguintes opções: ○ **Notificação de incidente para usuários finais**: enviada quando os incidentes são atribuídos aos usuários finais. ○ **Notificação de escalação para gerentes**: enviada quando a data de vencimento da resposta é violada ou atribuída manualmente ao gerente por meio do portal de operações do DLP. ○ **Notificação de prazo**: enviada quando o prazo da resposta é violado. ○ **Notificação de resposta do usuário para analistas**: enviada quando o usuário final executa qualquer ação no incidente do DLP. ○ Notificação de**aprovações pendentes**: notifica os aprovadores sobre itens pendentes. ○ **Notificação de aprovação para o solicitante**: notifica os usuários sobre a aprovação de suas solicitações. ○ **Rejeitar notificação ao solicitante**: notifica os usuários sobre a rejeição de suas solicitações. ○ **Cancelar notificação ao solicitante**: notifica os usuários sobre o cancelamento de suas solicitações.
Tipo	Opção para indicar se o e-mail é enviado por incidente ou como um resumo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Se você selecionou **notificação de data de vencimento** no campo **Categoria**, poderá usar somente resumos. Selecione esta opção.
Descrição	Descrição exclusiva deste modelo de e-mail.
Ordem de execução	Prioridade do modelo de e-mail. Este campo indica a ordem na qual os modelos de e-mail são executados quando dois ou mais modelos de e-mail compartilham as condições de acionamento. O modelo de e-mail com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O valor padrão é 100.
Condição do modelo	Opções nas condições do modelo que são baseadas na tabela de incidentes do DLP. Você pode selecionar qualquer um dos campos de incidente para criar a condição do gatilho do modelo de e-mail. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**. ○ Se **AND** for selecionado, todas as condições deverão ser correspondidas. ○ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. **Nota:** As condições no construtor de condição fazem distinção entre maiúsculas e minúsculas.
Usuários de Meta	Usuários de destino para o modelo quando as condições forem atendidas. Os usuários de destino podem ser um dos seguintes: ○ **Todos os destinatários**: envie o e-mail para os usuários de destino. ○ **Destinatários no grupo:** envie o e-mail somente para destinatários em um grupo específico usando a opção de filtro. ○ **Destinatários que correspondem aos critérios**: envie o e-mail para usuários de destino que correspondam aos critérios. Você pode usar o filtro para fazer uma busca detalhada nos usuários de destino com base nas condições. Por exemplo, cidade.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição

Modelo de e-mail	Modelo de e-mail que você pode selecionar. Você pode definir as variáveis para reutilizar o conteúdo existente e adicionar à notificação por e-mail.
	
	Os campos **Categoria** e **Tipo** determinam as variáveis que estão disponíveis para seleção. Por exemplo, digamos que a categoria de e-mail esteja definida como notificação de incidente e que o tipo de e-mail seja um resumo. As variáveis para seleção são campos de resumo para acomodar o acúmulo de vários incidentes do DLP.
	
	Aqui está um exemplo de HTML do corpo do e-mail de cada modelo de e-mail:
	○ **Modelo padrão para notificação de aprovação por incidente**:
	`Dear ${respondent.first_name},`
	`Your request "${end_user_response}" on the incident ${number} has been approved.`
	`- Date protection team`
	○ **Notificação de cancelamento da solicitação de aprovação por incidente**
	`Dear ${respondent.first_name},`
	`Your request "${end_user_response}" on the DLP incident ${number} has been cancelled.`
	`No action is required from you at this point. Data protection team will contact you for any further information required.`
	`- Data protection team`
	○ **Modelo padrão para notificação de data de vencimento**:
	`Dear ${target_user.name},`
	`Following incidents require your response.`
	`${due_days_table}`
	`- Data protection team`
	○ **Modelo padrão para notificação de usuário por incidente**:
	`Dear ${assigned_to.name},`
	`DLP Incident ${number} is assigned to you.`

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Please review and submit your response. - Data protection team
	○ **Modelo padrão para notificação de incidente do usuário**: Hello ${target_user.name}, You have ${total_number_of_incidents} incidents assigned to you currently that require your response. ${new_incidents_in_period} new incidents got assigned to you since the last email communication. Nearest upcoming due date for responding to a critical incident is ${nearest_due_date_for_critical_severity_incidents}. Please log in to the ${link_to_dlp_portal} and submit your response. - Data protection team
	○ **Modelo padrão para escalação - Resumo**: Hi ${target_user.name}, The following data security incidents have been escalated to you due to lack of response from the assignees. Please login to the incident response workspace to review the incidents and submit your response. ${overdue_table} - Data protection team
	○ **Modelo padrão para escalação - por incidente**: Dear ${assigned_to.name}, Data security incident ${number} has been escalated to you. Please review and submit your response or assign the incident back to the user. - Data protection team
	○ **Modelo padrão para notificação de aprovação pendente**: Dear ${approver.first_name},

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Your approval is required for a few requests on data security incidents. Please login to the workspace here and review the requests. - Data protection team
	○ **Modelo padrão para notificação de aprovação pendente Por incidente**: Dear ${Approver}, Your approval is required for the incident ${number} requested by the user ${respondent.first_name} ${respondent.last_name}. Please visit this here to approve or reject the request. - Data Protection Team
	○ **Modelo padrão para notificação de rejeição por incidente**: Dear ${respondent.first_name} ${respondent.last_name}, This is to inform you that your request "${end_user_response}" for the DLP incident ${number} has been rejected. Please review the incident here. - Data protection team
	○ **Modelo padrão para notificação de resposta do usuário por incidente**: Hi ${assigned_to.name}, This is to inform you that a response has been submitted for the DLP Incident ${number}.
	○ **Modelo padrão para notificação de conclusão de resposta do usuário**: Hello ${target_user.name}, This email is to inform you that users have submitted their response for ${new_incidents_in_period_user_response_completed} new incidents since the last email communication. Please review the response for these incidents ${link_to_incidents_in_period_user_response_completed}.

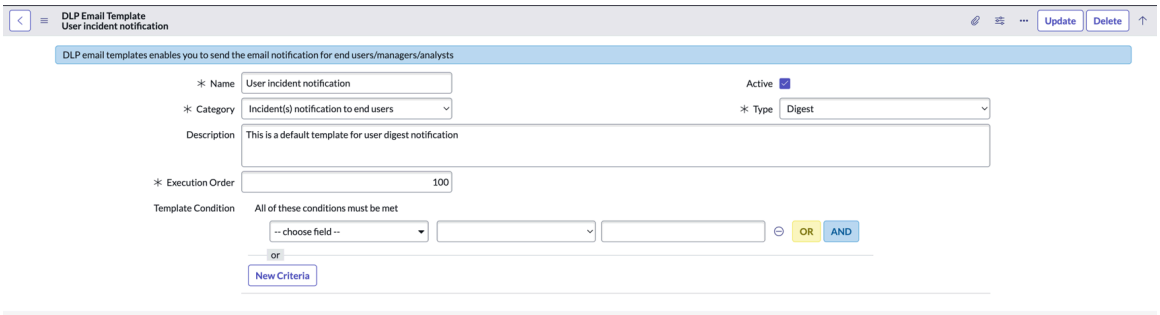
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição

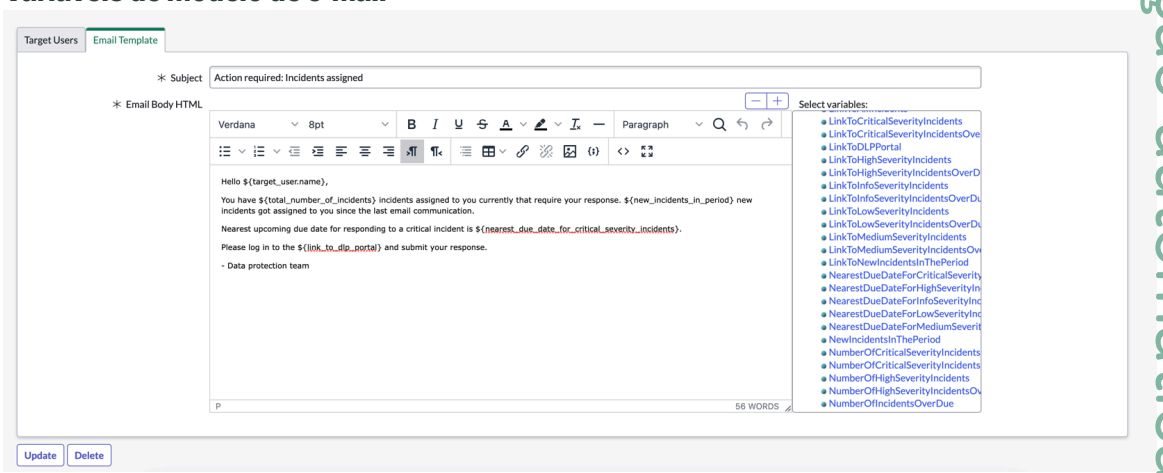
Example
O exemplo a seguir mostra o modelo de e-mail do DLP com os usuários de destino definidos como todos os destinatários.

Modelo de e-mail



O exemplo a seguir mostra um modelo de e-mail com o assunto "Notificação de incidente do usuário" e uma variável *new_incidents_in_period*. O corpo do e-mail contém várias variáveis que são adicionadas da coluna Selecionar variáveis.

Variáveis de modelo de e-mail



4. Clique em **Enviar**.

Resultado
O usuário final recebe um e-mail de notificação de resumo com todos os campos de variáveis selecionados no modelo.

Criar e gerenciar avaliações para incidentes do DLP

Crie e gerencie avaliações para permitir que os usuários finais respondam a incidentes do DLP. Você pode usar as avaliações para coletar informações sobre os dados confidenciais expostos ou vazados dos incidentes do DLP.

Criar e gerenciar avaliações para incidentes do DLP

Antes de Iniciar
Função necessária:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

As avaliações de incidentes do DLP ajudam a identificar possíveis ameaças e vulnerabilidades aos seus dados com base na resposta do usuário final. Você pode usar essas informações para determinar as lacunas, preocupações e expectativas existentes dos usuários finais.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Avaliações**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Avaliação de incidentes do DLP

Campo	Descrição
Nome	Nome da avaliação de incidente do DLP.
Ativo	Opção para indicar se a avaliação de incidente do DLP está ativa.
Descrição	Descrição exclusiva para esta avaliação de incidente do DLP.
Introdução da avaliação	Forneça uma introdução ou contexto para sua avaliação. Você também pode usar variáveis da seção Selecionar variáveis para exibir determinados campos dinamicamente.

4. Clique em **Enviar**.
5. Depois de criar uma avaliação, abra a avaliação e clique em **Designer de avaliações**.
6. Na seção Nova avaliação, selecione um tipo de pergunta de avaliação na seção Controles.
7. Arraste e solte o tipo de pergunta de avaliação necessária na seção Nova avaliação.
   Por exemplo, você pode arrastar e soltar o controle de **Opção** na seção Nova Avaliação ou Nova Categoria.
8. Para adicionar mais categorias à avaliação, clique no .
9. Para modificar uma categoria existente, clique no .
10. Depois de criar as diferentes perguntas de avaliação pela primeira vez, clique em **Salvar**e em **Publicar**.

Configurar regras de opção de resposta do incidente para seus incidentes do DLP

Configure as regras de opção de resposta do incidente que o usuário final ou analista pode usar ao responder a um incidente.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

Você pode configurar o tipo de resposta que um usuário final deve executar com base no tipo de incidente do DLP. A aplicação DLP Incident Response do sistema básico fornece as seguintes opções de resposta para os usuários:

- Avaliação concluída
- Conteúdo excluído
- Arquivo excluído
- Arquivo criptografado
- Conteúdo Mascarado
- Relatar falso-positivo
- Denunciar proprietário incorreto
- Necessário para Processo de negócios
- Direitos revisados

Por exemplo, digamos que um usuário final relate um incidente DLP como um falso positivo. O estado deste incidente é marcado automaticamente como fechado porque o estado de destino configurado por você é fechado.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Regras de opção de resposta do incidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Regras de opção de resposta do incidente

Campo	Descrição
Nome	Nome da opção de resposta do incidente.
Ativo	Opção para indicar se a opção de resposta do incidente está ativa.
Ordem de execução	Prioridade da opção de resposta do incidente. Este campo indica a ordem na qual as opções de resposta do incidente são executadas quando duas ou mais opções de resposta do incidente compartilham as condições de acionamento. A opção de resposta do incidente com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O padrão é 100.
Descrição	Descrição exclusiva para esta opção de resposta do incidente.
Estado de destino padrão	O estado de destino padrão que você configurou.

Tradução automática

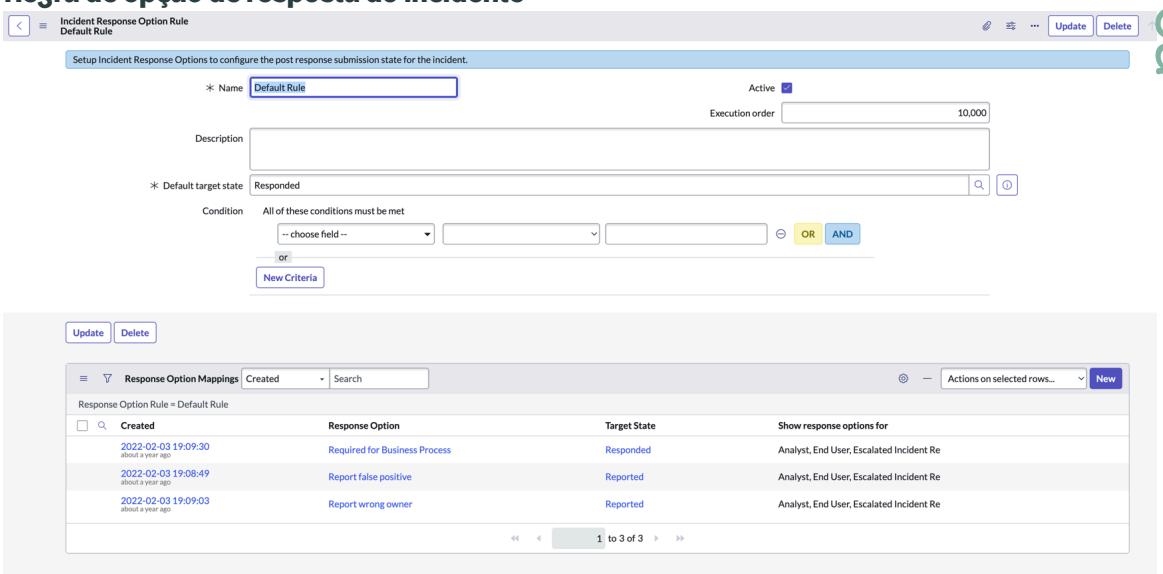
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Condição	Condições no construtor de condição. Essas condições são baseadas na tabela de incidentes do DLP. Para criar uma condição para as opções de resposta do incidente, selecione qualquer um dos campos de incidente. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**: ○ Se **AND** for selecionado, todas as condições deverão ser correspondidas. ○ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. **Nota:** As condições no construtor de condição fazem distinção entre maiúsculas e minúsculas.

Example

O exemplo a seguir mostra a configuração de ação do usuário final para um endpoint. A condição requer que a origem da verificação seja um sistema de arquivos de endpoint que aciona esta configuração de ação do usuário final. O mapeamento mostra que o proprietário incorreto do relatório, o relatório de falso-positivo e o arquivo excluído são as opções de resposta disponíveis para o usuário final.

Regra de opção de resposta do incidente



4. Na seção **Mapeamentos de opção de resposta**, clique em **Novo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

5. No formulário, preencha os campos.

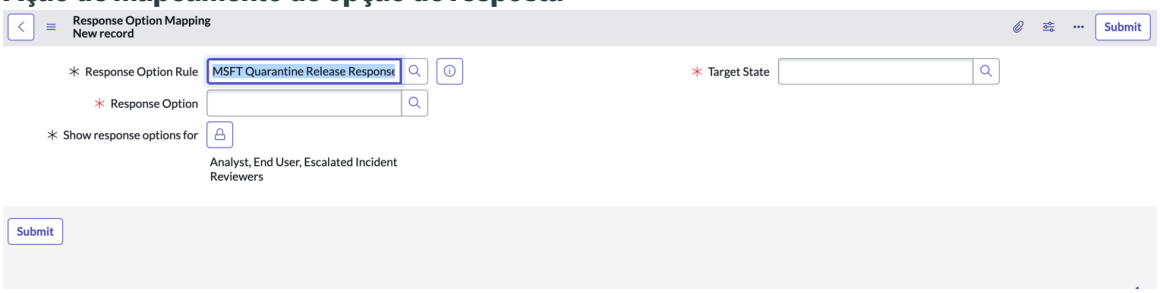
Formulário Mapeamento de opção de resposta

Regra de opção de resposta	Nome da regra de opção de resposta do incidente. Por exemplo, o SharePoint implica que a origem da verificação é o SharePoint. Você pode inserir o nome da resposta do incidente ou pesquisar usando a pesquisa.
Opção de resposta	Opção para selecionar a opção de resposta. Você pode inserir a opção de resposta ou pesquisar usando a pesquisa.
Estado de destino	O estado de destino do incidente DLP depois que o usuário final seleciona a ação apropriada. **Nota:** a. O campo **Estado do destino** aparecerá somente quando você selecionar a **Opção de resposta** que é do **Tipo: Básica**. Para obter mais informações sobre como os tipos de estado de destino são configurados, consulte Configure a opção de resposta para seus incidentes do DLP. b. Quando uma Opção de resposta que é do **Tipo: Avançado** é selecionada, você não poderá definir o Estado de destino e ficará oculto. O Estado de destino será atribuído com base no estado personalizado configurado no subfluxo do Flow Designer.
Mostrar opções de resposta para	Opção para determinar as funções do usuário para as quais as opções de resposta serão mostradas. Você pode escolher entre **Analista**, **Usuário final** e **Revisor de analista escalonado** usando a opção de desbloqueio. Você tem permissão para escolher uma ou todas as funções.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Ação de mapeamento de opção de resposta



6. Clique em **Enviar**.

Configure a opção de resposta para seus incidentes do DLP

Use este recurso para configurar o tipo de resposta que um usuário final ou analista deve executar.

Antes de Iniciar

A aplicação DLP Incident Response do sistema básico fornece as seguintes opções de resposta:

1. Avaliação concluída
2. Conteúdo excluído
3. Arquivo excluído
4. Arquivo criptografado
5. Conteúdo Mascarado
6. Relatar falso-positivo
7. Denunciar proprietário incorreto
8. Solicitar liberação de e-mail da quarentena

> **Nota:**
> Esta opção está disponível para os registros DLP do Microsoft Exchange.

9. Necessário para Processo de negócios
10. Direitos revisados

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Opções de resposta**.

   Por padrão, o sistema de base fornece dois tipos de opção de resposta:

   a. **Básico**: uma opção de resposta manual enviada pelo usuário.

   b. **Avançado**: uma opção de resposta automatizada aciona um subfluxo do Flow Designer quando o usuário envia a opção de resposta.

2. Clique em **Nova**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. No formulário, preencha os campos.

Formulário Opção de resposta do tipo: básica

Campo	Descrição
Nome	Insira o nome da opção de resposta do incidente.
Tipo	Opção para selecionar o tipo de opção de resposta.

Formulário Opção de resposta do tipo: Avançado

Campo	Descrição
Nome	Insira o nome da opção de resposta do incidente.
Tipo	Opção para selecionar a opção de resposta. Por padrão, este campo exibe os dois tipos de opções a seguir: ○ **Básico**: ao selecionar esta opção ao criar uma nova opção de resposta, talvez seja necessário adicionar um nome de opção de resposta e o tipo. ○ **Avançado**: quando você seleciona esta opção, os seguintes campos ficam disponíveis para você selecionar: ▪ **Fluxo**: selecione o subfluxo do Flow Designer. ▪ **Requer MID Server**: marque esta caixa de seleção se o fluxo selecionado usar o MID Server.
Fluxo	Selecione o fluxo do Flow Designer necessário para ativar a aplicação MID e a capacidade MID. Ao criar um subfluxo para a opção de resposta, adicione as seguintes entradas de subfluxo: **a. Nome**: ▪ dlp_incident ▪ mid_server_capability ▪ mid_server_application **b. Tipo**: ▪ Referência (para tabela de incidentes do DLP) ▪ SYS ID da aplicação do MID Server e da capacidade do MID Server
Requer MID Server	Opção para determinar essa configuração do MID Server. Ao habilitar a caixa de seleção **Requer MIDServer Aplicativo** do **MID Server e Recursos** do MID Server, você pode configurar o aplicativo MID e o recurso do MID.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

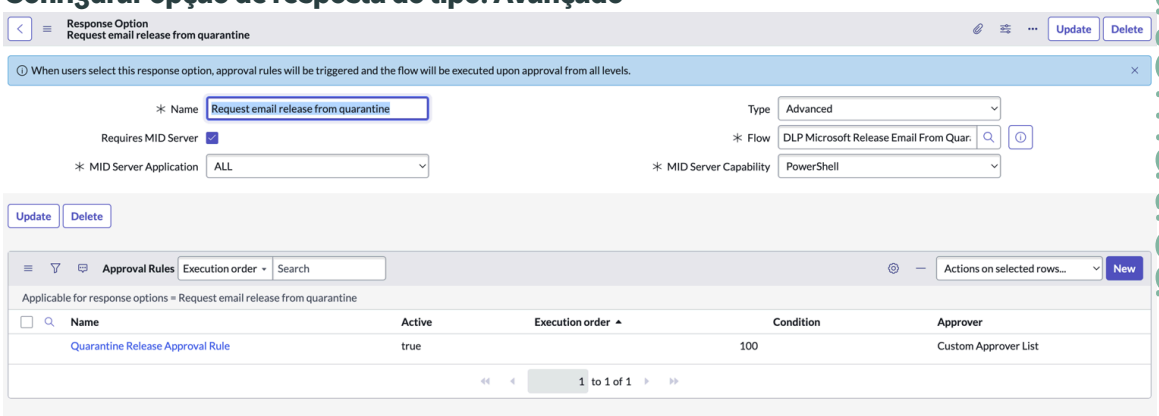
Campo	Descrição
	Nota: Com base na configuração da aplicação do MID Server e do recurso do MID Server, e se algum MID estiver instalado e em execução, somente a opção de resposta ficará visível no espaço.
Aplicação do MID Server	Selecione a aplicação do MID Server necessária na lista suspensa.
Capacidade do MID Server	Selecione o recurso do MID Server necessário na lista suspensa.

Nota:
Se não houver nenhum MID Server disponível para o recurso do MID Server selecionado, a opção de resposta não ficará visível. Se você quiser um MID Server específico da lista, será necessário configurar o app MID e torná-lo visível na lista e, em seguida, pelo menos um MID Server configurado deve estar instalado e funcionando a partir dos aplicativos MID selecionados e deve ter o Recurso do MID Server selecionado.

4. Clique em **Enviar**.

Nota:
Se você estiver criando um tipo **Avançado** de opção de resposta, a lista relacionada **Regras de aprovação** será preenchida para você configurar a regra de aprovação para essa nova opção de resposta. Para obter mais informações, consulte Configurar regras de aprovação.

Configurar opção de resposta do tipo: Avançado



Configure o gráfico de idade para seus incidentes do DLP

Configure o gráfico de idade que aparece no portal de operações Data Loss Prevention Incident Response (DLP IR). Este gráfico mostra a contagem de incidentes em aberto pelo número de dias.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Configuração da Tabela de Idade**.
2. Revise as entradas do gráfico de idade na tabela a seguir e personalize as entradas para o seu ambiente.

Formulário Configurações do gráfico de idade do DLP

Nome	Condição
0 a 30 dias	Idade do incidente em aberto que está entre 0 e 30 dias.
31 a 60 dias	Idade do incidente em aberto que está entre 31 e 60 dias.
61 a 90 dias	Idade do incidente em aberto que está entre 61 e 90 dias.
Mais de 90 dias	Idade do incidente em aberto que é superior a 90 dias.

3. Adicione uma nova configuração de gráfico de idade clicando em **Novo**.
4. No campo Nome, insira um **Nome** para a configuração do gráfico de idade do DLP.
5. Defina as condições para a configuração do gráfico de idade do DLP.
   a. Para adicionar condições, clique em **E** ou **OU**.
      - Se **AND** for selecionado, todas as condições deverão ser correspondidas.
      - Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida.

      Nota:
      As condições no construtor de condição fazem distinção entre maiúsculas e minúsculas.

   b. Para definir uma segunda condição de filtro, clique em **Novos critérios**.
6. Clique em **Enviar**.

Configurar como as ações do usuário final são delegadas

Impeça que determinados executivos da organização recebam notificações sobre os incidentes atribuídos ou escalonados a eles.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Considere um cenário em que o executivo é um usuário que pertence a uma liderança ou grupo executivo. O executivo não deve receber e-mails sobre atribuição de incidente ou escalação. Um usuário delegado pode tomar as medidas necessárias em nome do executivo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Depois que um usuário tiver atribuído uma pessoa específica, Henry, como um delegado, outro usuário não poderá atribuir Henry como um delegado novamente. Da mesma forma, um delegado não pode atribuir outro usuário como delegado.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Delegar configuração**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário Configuração de delegado

Campo	Descrição
Usuário	Nome do usuário que precisa de um delegado para incidentes do DLP.
Delegado	Nome do usuário que pode responder ao incidente do DLP em nome do usuário final original.

4. Clique em **Enviar**.

Configurar regras de identificação de reincidentes

Configure as regras de identificação de reincidentes para identificar usuários que repetem o mesmo problema várias vezes.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Você pode identificar os reincidentes usando determinadas regras ou critérios. Data Loss Prevention Incident Response fornece campos que você pode usar para identificar infratores reincidentes.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Regras de identificação de infrator reincidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de regras de identificação de infrator reincidente

Campo	Descrição
Nome	Nome da regra de identificação do infrator reincidente.
Ordem de execução	Prioridade das regras de identificação de reincidentes. Este campo indica a ordem na qual as regras de identificação do infrator reincidente são executadas quando duas ou mais regras compartilham as condições-gatilho.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

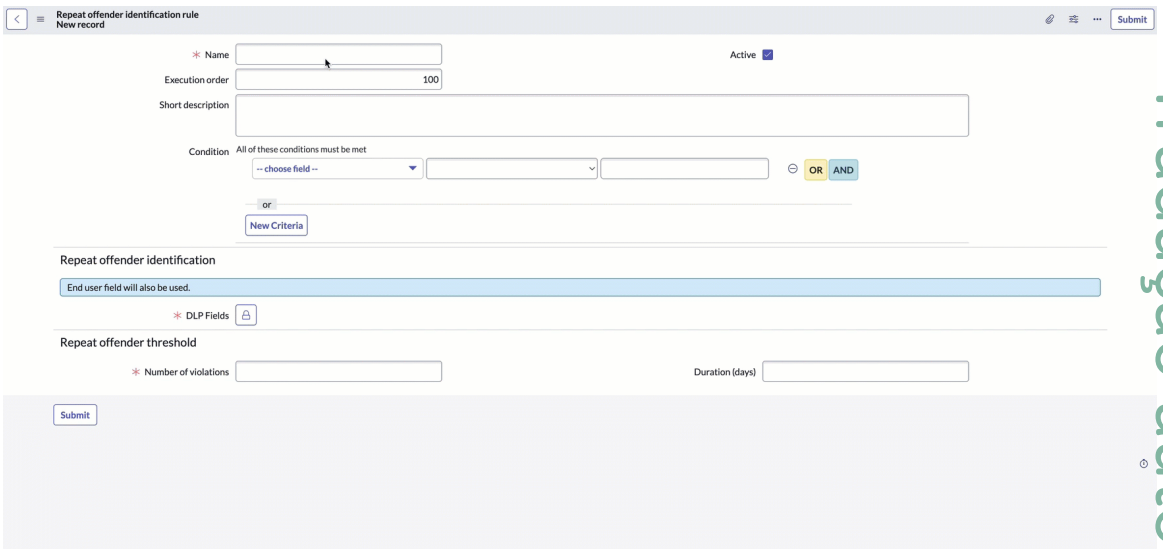
Campo	Descrição
	A regra de identificação do infrator reincidente com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O valor padrão é 100.
Descrição resumida	Descrição exclusiva desta regra de identificação de infrator reincidente.
Condição	Condições no construtor de condição que são baseadas na tabela de incidentes do DLP. Você pode selecionar qualquer um dos campos de incidente para criar a condição do gatilho para a regra de identificação de infrator reincidente. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**: ○ Se **AND** for selecionado, todas as condições deverão ser correspondidas. ○ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. **Nota:** As condições no construtor de condição fazem distinção entre maiúsculas e minúsculas.
Campos do DLP	Identifique os reincidentes com base nos campos DLP obrigatórios. Clique no ao lado dos Campos do DLP para exibir a lista de campos do DLP disponíveis. Selecione os campos do DLP que você deseja usar na coluna Disponível e mova-os para a coluna Selecionado. Por exemplo, você pode selecionar os campos**Nome do arquivo** e **Proprietário** do arquivo na coluna Disponível e movê-los para a coluna Selecionado. Em seguida, você pode identificar os infratores reincidentes com base nos campos **Nome do arquivo** e **Proprietário do arquivo**. Portanto, se um usuário violar o limite do reincidente (número de violações e duração) e se o mesmo usuário

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	corresponder aos campos do DLP, esse usuário específico será identificado como reincidente.
Número de violações	Defina o valor limite do infrator reincidente. Depois que o usuário repete as mesmas ações e viola o número especificado de violações, o usuário é identificado como reincidente.
Duração (em dias)	Defina o limite do infrator reincidente na forma de dias. Depois que o usuário repete as mesmas ações e viola a duração do limite, o usuário é identificado como um infrator reincidente.

Identificar infratores reincidentes



4. Clique em **Enviar**.

Criar estados personalizados para seus incidentes do DLP

Crie e configure seus próprios estados personalizados para os DLP IR incidentes.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Por padrão, a aplicação Data Loss Prevention Incident Response fornece os seguintes estados:

- Encerrado
- Em aberto
- Em Revisão
- Escalado
- Atrasado

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Respondido
- Rascunho
- Relatado

Você pode selecionar um dos estados padrão ou seus estados personalizados com base nos incidentes do DLP.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Estados personalizados**.
2. Para criar um estado personalizado, clique em **Novo**.
3. No campo **Estado**, insira um nome para o estado personalizado.
4. Clique em **Enviar**.

Criar campos personalizados para seus incidentes do DLP

Crie e configure seus campos personalizados para os incidentes do DLP. Você pode criar diferentes tipos de campos personalizados, como cadeia de caracteres, número, caixa de seleção, opção, data e hora, e usá-los nos formulários de incidente do DLP.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Importante:
Campos personalizados para incidentes do DLP são compatíveis somente com a versão San Diego ou posterior.

Por Que e Quando Desempenhar Esta Tarefa

Os campos personalizados estão associados a restrições de nível de campo. Portanto, se houver alguma restrição de nível de campo, ela se aplicará aos campos personalizados no portal de operações do DLP e no portal do usuário final.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Campos personalizados**.
2. Crie um campo personalizado clicando em **Novo**.
3. No formulário, preencha os campos.

Formulário Campo personalizado do DLP

Campo	Descrição
Nome	Nome do campo personalizado.
Tipo	Opção para selecionar o tipo de campo personalizado. Você pode escolher um dos seguintes tipos: ○ **Cadeia de caracteres** ○ **Número** ○ **Caixa de seleção**

Tradução automática

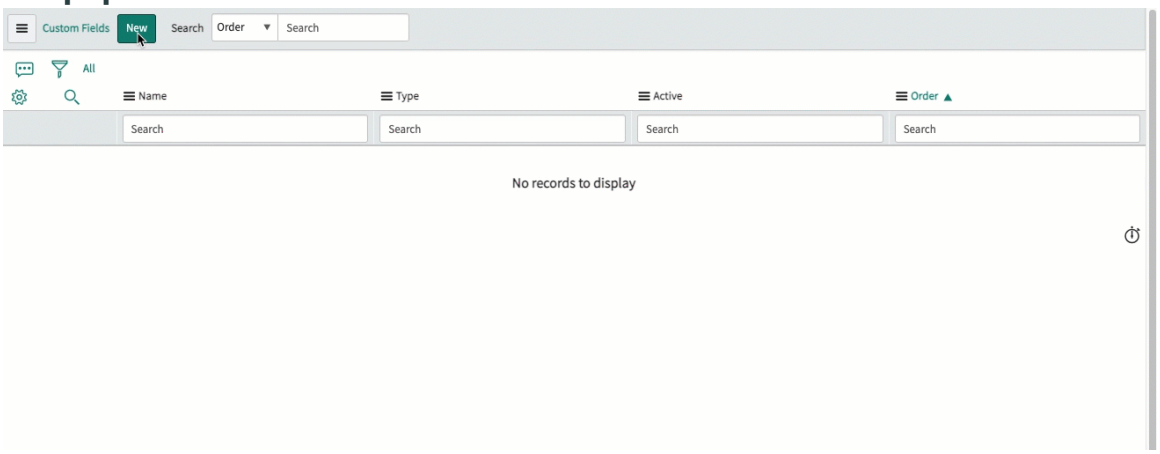
© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ **Escolha** Se você selecionar o tipo de campo personalizado como **Opção**, depois de criar o campo personalizado, poderá definir as opções de escolha do campo personalizado. Para criar uma opção de escolha de campo personalizado: **a.** Abra o campo personalizado obrigatório. **b.** Na seção Opções de campo de escolha personalizada, clique em **Novo**. **c.** No campo Nome da opção, defina o nome da opção necessária. **d.** Clique em **Enviar**. ○ **Data** ○ **Data/Hora** **Nota:** Depois de selecionar um tipo para o novo campo personalizado, você não terá permissão para modificá-lo. Se você quiser modificar o tipo, será necessário criar um novo campo personalizado novamente com o tipo necessário.
Ordem	Opção para escolher a ordem na qual os campos personalizados devem ser exibidos. Você pode definir o valor do pedido para cada campo personalizado. Os campos personalizados são classificados com base nos valores de ordem que você define. Por padrão, os campos personalizados são classificados em ordem crescente. Você pode classificar os campos personalizados em ordem decrescente clicando na coluna **Ordem**.
Ativo	Opção para indicar se o campo personalizado está ativo.
Descrição	Descrição do campo personalizado que você criou.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo personalizado do DLP



4. Clique em **Enviar**.

Definir configurações avançadas para Data Loss Prevention Incident Response

Defina as configurações avançadas para que você possa determinar os campos no Incidente para identificar os usuários finais, entre outros recursos.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

Definir configurações avançadas no Data Loss Prevention Incident Response é opcional. Algumas configurações avançadas incluem o seguinte:

- Defina o número máximo de incidentes que podem ser enviados em um e-mail de resumo.
- Habilite o modo rápido para enviar e-mails mais rapidamente.
- Determine o detalhamento do log da aplicação.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Configurações Avançadas**.
2. No formulário, preencha os campos.

Formulário Configurações avançadas

Campo	Descrição
Os dados confidenciais que causaram a violação devem ser exibidos no incidente?	Opção para escolher se você deseja exibir os dados confidenciais que causaram a violação no incidente do DLP. Por padrão, esta opção está habilitada.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Os dados confidenciais que causaram a violação também devem ser exibidos nos incidentes secundários?	Opção para escolher se você deseja exibir os dados confidenciais que causaram a violação no incidente secundário do DLP também. Por padrão, esta opção está desativada.
Lista de campos no incidente que são usados para identificar o usuário final	A lista de campos no incidente do módulo Regra de atribuição que são usados para identificar o usuário final. Você também pode especificar seus próprios atributos personalizados para identificar o usuário final.
Número máximo de incidentes em um e-mail de resumo	O número máximo de incidentes que podem ser enviados em um e-mail de resumo. Por padrão, o valor é 100.
Duração máxima da reincidência (em dias)	A duração máxima para identificar um infrator reincidente. Por padrão, o valor é 90 dias.
Modo rápido para enviar e-mails	Opção para validar e-mails e identificar problemas. Você pode executar a validação habilitando a opção **Sim**. Por padrão, esta opção está habilitada.
Esta propriedade é usada para definir o detalhamento do log da aplicação	O nível de detalhamento do log da aplicação, ou seja, o nome do tipo de informação. Você também pode atualizar o valor para as seguintes opções: ○ **error** ○ **aviso** ○ **informações** ○ **depurar** Por padrão, o valor é **info**.
Excluir incidentes secundários e clonados de relatórios	Opção para excluir os incidentes clonados e secundários dos relatórios. Por padrão, esta opção é **Sim**.
Dia(s) de espera para excluir o conteúdo correspondente no armazenamento em nuvem após o incidente ser encerrado	Opção para escolher o número de dias de espera para limpar o conteúdo de correspondência dos incidentes que estão inativos por um período de tempo específico. Por padrão, o valor é 90. Após 90 dias, se o incidente DLP estiver inativo, o conteúdo de correspondência será limpo do armazenamento em nuvem.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Atribuir incidente ao grupo de analistas DLP após o último nível de escalação	Marque esta caixa de seleção para atribuir o incidente ao analista após o último nível de escalação.
Permitir que os usuários acessem os incidentes após a escalação	Marque esta caixa de seleção para permitir que os usuários atribuídos acessem o(s) incidente(s) após a escalação. Ao selecionar esta opção, todos os usuários que foram adicionados à lista da cadeia de escalação poderão acessar o(s) incidente(s).
Permitir que o analista edite a avaliação concluída	Marque esta caixa de seleção para permitir que o analista edite a avaliação concluída. Quando você seleciona esta opção, os analistas podem editar as Avaliações. Quando essa opção está desmarcada, você pode exibir as avaliações no modo Somente leitura.

3. Clique em **Salvar**.

Monitorar o processo de execução da integração do DLP da Microsoft

Rastreie e monitore o processo de ingestão em andamento. Os processos de execução de integração contêm as estatísticas sobre a quantidade de dados que foi processada e o status da integração.

Função necessária: sn_dlir.admin.

O processo de execução da integração lista os detalhes sobre quantos registros foram ingeridos. Por exemplo:

1. No Symantec, o processo contém execuções de integração secundária e primária. O registro primário indica os dados de ingestão e o registro secundário indica as chamadas de aprimoramento e os registros de atributo personalizado.
2. Na Microsoft, há apenas o processo de ingestão de registro primário a ser executado.

Processos de execução de integração do DLP: exibe as entradas da fila, o status das entradas da fila e os registros obtidos.

A execução de integração contém a origem para a qual o perfil de integração e o registro de execução de integração são criados, intervalos de pesquisa de perfil, estados e subestados de ingestão, contagem de incidentes que indica o número de registros ingeridos.

1. Navegar até **Administração do DLP** > **Execuções de Integração**.
2. Selecione a execução de integração na lista.
3. Navegue até **DLP Integration Run Process**.
4. Exibir o status de entrada da fila do registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Restrições de acesso a incidentes do DLP

Gerencie a visibilidade de um incidente DLP específico que contém informações confidenciais. Você pode usar restrições de acesso a incidentes para definir quem pode acessar um incidente DLP específico e restringir o acesso de usuários ou grupos específicos a esse incidente.

Configurar restrições de nível de campo para seus incidentes do DLP

Defina restrições de nível de campo em incidentes do DLP para proteger informações confidenciais contra exposição. Você pode usar restrições de nível de campo para controlar os usuários ou grupos que podem acessar campos específicos nos incidentes do DLP.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

As restrições de nível de campo permitem que você exiba somente determinados campos para usuários ou grupos específicos, fornecendo uma maneira mais granular de controlar os dados que um usuário pode acessar. Você pode criar uma restrição de nível de campo definindo as condições de correspondência de incidente DLP, selecionando os usuários ou grupos aos quais essas condições se aplicam e, em seguida, escolhendo os campos DLP que esses usuários ou grupos podem exibir.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Restrições de acesso a incidentes** > **Restrições de nível de campo**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de restrição de nível de campo do DLP

Campo	Descrição
Nome	Nome da restrição de nível de campo.
Ativo	Opção para indicar se a restrição de nível de campo está ativa.
Ordem de execução	Prioridade das restrições de nível de campo. Este campo indica a ordem na qual as restrições de nível de campo são executadas quando duas ou mais restrições de nível de campo compartilham as condições de acionamento. A restrição de nível de campo com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O valor padrão é 100.
Descrição resumida	Descrição exclusiva para esta restrição de nível de campo.
Condição de correspondência de incidente	Opções no incidente que correspondem às condições definidas. Você pode selecionar qualquer um dos campos de incidente para definir a condição do gatilho para as restrições de nível de campo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

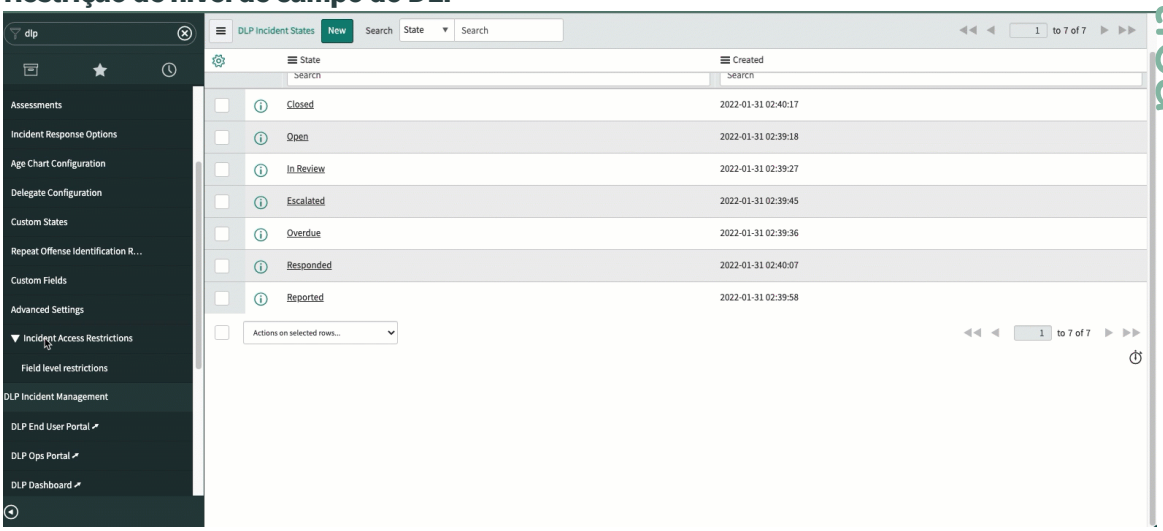
Campo	Descrição
	Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**: ○ Se **AND** for selecionado, todas as condições deverão ser correspondidas. ○ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. Por exemplo, você pode selecionar o campo como Nome da políticae definir a condição como eme Nome da política. **Nota:** As condições no construtor de condição fazem distinção entre maiúsculas e minúsculas.
Aplica-se a	Opção para aplicar as condições de correspondência de incidentes a usuários ou grupos específicos. Você pode aplicar as condições ao seguinte: ○ **Todos os usuários finais**: opção para selecionar todos os usuários finais aos quais as condições de incidente do DLP são aplicáveis. ○ **Todos os revisores de incidentes escalonados**: opção para selecionar todos os revisores de incidentes escalonados aos quais as condições de incidente do DLP são aplicáveis. Isso se refere a todos os incidentes do DLP escalonados para o gerente. ○ **Usuários**: clique no para adicionar um usuário específico da lista ao qual as condições de incidente do DLP são aplicáveis. Você também pode adicionar um usuário usando o endereço de e-mail ou a opção de pesquisa. Por exemplo, Gerente jurídico. Para adicionar a si mesmo como o usuário ao qual as condições do DLP são aplicáveis, clique no ○ **Grupos**: clique no ícone de para adicionar um grupo específico da lista ao qual as condições de incidente do DLP são aplicáveis. Você também pode adicionar um grupo usando a opção de pesquisa. Por exemplo, Criadores de pesquisa.
Permitir acesso somente aos seguintes campos	○ **Campos do DLP**: opção para definir os campos do DLP que você deseja permitir o acesso aos usuários ou grupos selecionados. Selecione os campos do DLP aos quais você deseja permitir o acesso na coluna Disponível e mova-os para a coluna Selecionado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: Os usuários ou grupos selecionados poderão acessar somente os campos do DLP selecionados. Por exemplo, você pode selecionar os campos**Atribuído a** e **Aberto** na coluna Disponível e movê-los para a coluna Selecionado. Em seguida, os usuários ou grupos selecionados têm acesso somente aos campos Atribuído a e Aberto. ○ **Carregar anexos**: opção para indicar se você deseja permitir que os usuários ou grupos selecionados carreguem anexos. ○ **Campos personalizados**: opção para definir os campos personalizados que você deseja permitir o acesso aos usuários ou grupos selecionados. Você pode exibir os campos personalizados que criou na coluna Disponível. Selecione os campos personalizados que você deseja permitir o acesso na coluna Disponível e mova-os para a coluna Selecionado. **Importante:** ▪ Campos personalizados para incidentes do DLP são compatíveis somente com a versão San Diego ou posterior. ▪ Os usuários ou grupos selecionados poderão acessar somente os campos personalizados selecionados.

Restrição de nível de campo do DLP



4. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar restrições de nível de registro para seus incidentes do DLP

Defina restrições de nível de registro em incidentes do DLP para proteger registros confidenciais contra exposição. Você pode usar restrições de nível de registro para controlar os usuários ou grupos que podem acessar registros específicos nos incidentes do DLP.

Antes de Iniciar

Função necessária:

- sn_dlir.admin — Criar, editar e excluir.
- sn_dlir.analyst e sn_dlir.analyst_read — Exibir (somente leitura).

Por Que e Quando Desempenhar Esta Tarefa

As restrições de nível de registro permitem que você forneça acesso a registros somente para usuários ou grupos específicos, fornecendo uma maneira mais granular de controlar os registros que um usuário pode acessar. Você pode criar uma restrição de nível de registro definindo as condições de correspondência de incidente DLP, selecionando os usuários ou grupos aos quais essas condições se aplicam e, em seguida, escolhendo os registros DLP que esses usuários ou grupos podem exibir.

Procedimento

1. Navegar até **Todos** > **Administração do DLP** > **Restrições de acesso a incidentes** > **Restrições de nível de registro**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Formulário de restrição de nível de registro do DLP

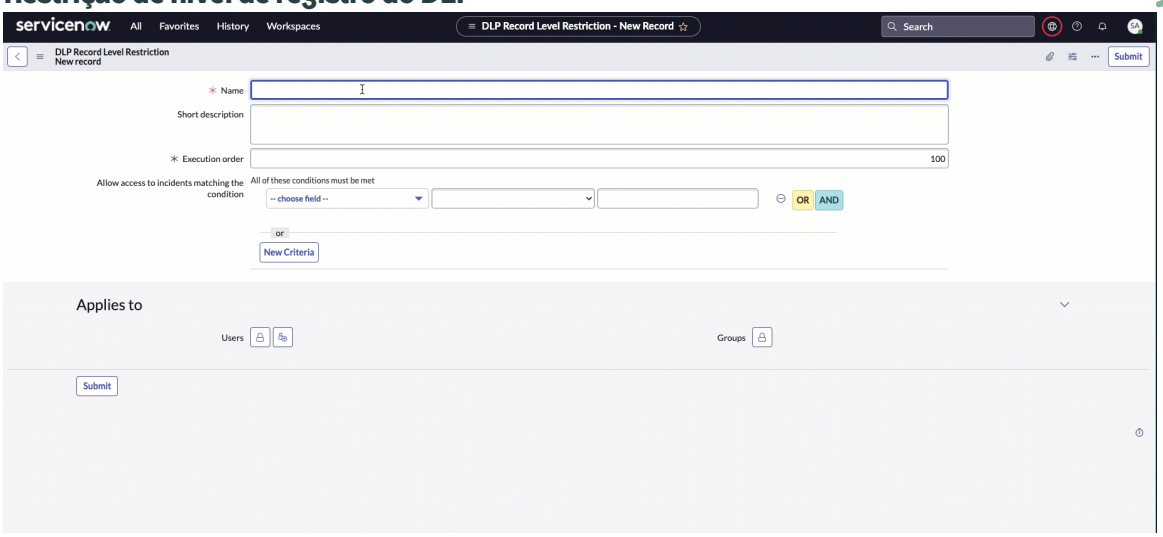
Campo	Descrição
Nome	Nome da restrição de nível de registro.
Descrição resumida	Descrição exclusiva para esta restrição de nível de registro.
Ordem de execução	Prioridade das restrições de nível de registro. Este campo indica a ordem na qual as restrições de nível de registro são executadas quando duas ou mais restrições de nível de registro compartilham as condições de acionamento. A restrição de nível de registro com o número mais baixo tem a prioridade mais alta. Para definir a ordem de operação, insira um valor. Por exemplo, 100, 200 ou qualquer outro número. O valor padrão é 100.
Permitir acesso a incidentes que correspondam à condição	As opções permitem o acesso aos incidentes que correspondem às condições definidas. Você pode selecionar qualquer um dos campos de incidente para definir a condição do gatilho para as restrições de nível de registro. Use as listas e os campos do construtor de condições para definir os filtros da primeira linha. Para adicionar mais condições, clique em **E** ou **OU**:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Se **AND** for selecionado, todas as condições deverão ser correspondidas. ○ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. Para definir uma segunda condição de filtro, clique em **Novos critérios**. **Nota:** As condições no construtor de condição fazem distinção entre maiúsculas e minúsculas. Por exemplo, você pode selecionar o campo como Ativoe definir a condição como ée verdadeiro.
Aplica-se a	Opção para aplicar restrições de nível de registro a usuários ou grupos específicos. Você pode aplicar as condições da seguinte forma: ○ **Usuários**: clique no para adicionar um usuário específico da lista ao qual o registro selecionado é aplicável. Você também pode adicionar um usuário usando o endereço de e-mail ou a opção de pesquisa. Por exemplo, Gerente jurídico. Para adicionar a si mesmo como o usuário ao qual o registro é aplicável, clique no . Por exemplo, administrador do sistema. ○ **Grupos**: clique no para adicionar um grupo específico da lista ao qual o registro selecionado é aplicável. Você também pode adicionar um grupo usando a opção de pesquisa. Por exemplo, Criadores de pesquisa.

Restrição de nível de registro do DLP



4. Clique em **Enviar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Arquivamento de incidentes do DLP

O Data Loss Prevention Incident Response é provisionado com uma regra de arquivamento no sistema de base para a tabela de incidentes do DLP. Os registros relacionados também são adicionados no sistema de base à regra de arquivamento de incidentes do DLP.

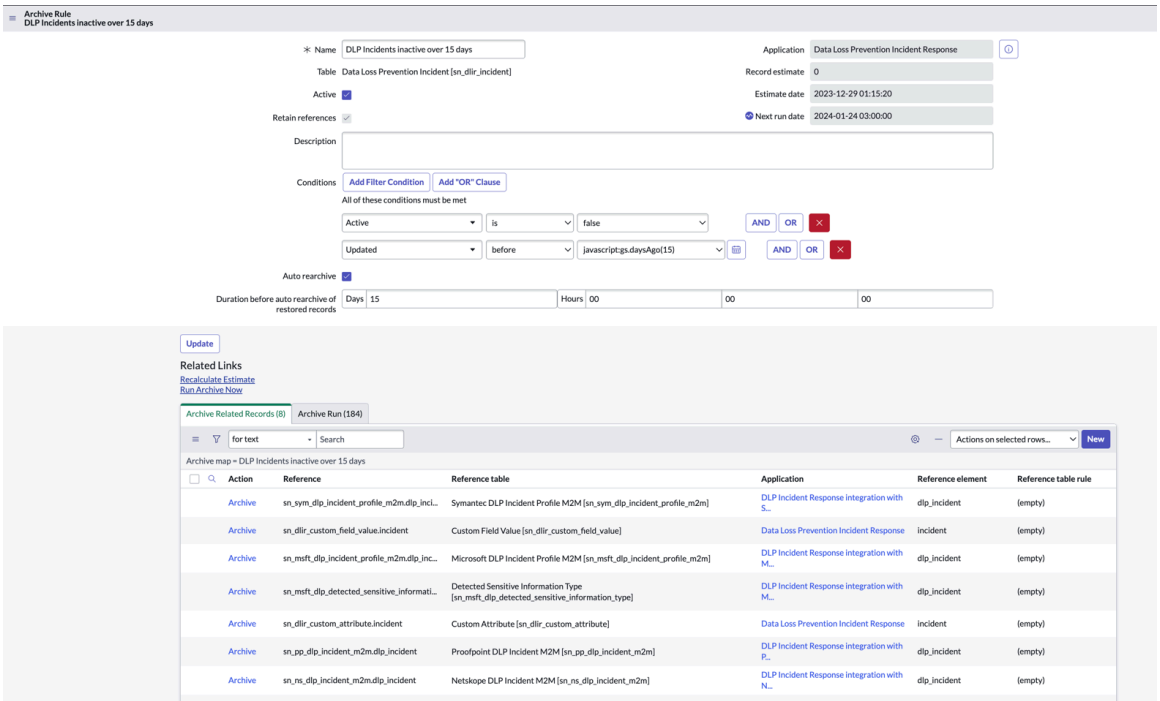
Antes de Iniciar

Função necessária: administrador

Procedimento

1. Navegar até **Todos** > **Arquivamento do Sistema** > **Regras de Arquivamento**.
   As regras de arquivamento do sistema que estão no sistema de base são exibidas.
2. Exiba a regra de arquivamento do DLP.

Nota:
Incidentes DLP inativos por mais de 15 dias é a regra de arquivamento do sistema de base padrão para incidentes DLP. Você pode modificar a regra de arquivamento, se necessário. Esta regra significa que os incidentes que estão inativos acima de 15 dias serão arquivados automaticamente.



Nota:
Para obter informações sobre como as regras de arquivamento são criadas, consulte Criar uma regra de arquivamento .

3. **Atualize** a regra, se necessário.

Arquivar registros relacionados ao DLP

Use a lista relacionada Arquivar registros relacionados para incidentes do DLP para adicionar os registros relacionados à regra de arquivamento.

Antes de Iniciar

Função necessária: administrador

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Arquivamento do Sistema** > **Regras de Arquivamento**.
2. Selecione a regra de arquivamento **Incidentes DLP inativos em mais de 15 dias**.
3. Vá para a lista relacionada **Arquivar registros** relacionados.
4. Exiba os registros relacionados ao DLP.

Aplicação	Tabela de Referência
DLP Incident Response integration with Symantec	Perfil de incidente do Symantec DLP M2M [sn_sym_dlp_incident_profile_m2m]
Data Loss Prevention Incident Response	Valor do campo personalizado [sn_dlir_custom_field_value]
DLP Incident Response integration with Microsoft	Perfil de incidente do Microsoft DLP M2M [sn_msft_dlp_incident_profile_m2m]
DLP Incident Response integration with Microsoft	Tipo de informação confidencial detectada [sn_msft_dlp_detected_sensitive_information_type]
Data Loss Prevention Incident Response	Atributo personalizado [sn_dlir_custom_attribute]
DLP Incident Response integration with Proofpoint	Incidente com DLP da Proofpoint M2M [sn_pp_dlp_incident_m2m]
DLP Incident Response integration with Netskope	Netskope DLP Incident M2M [sn_ns_dlp_incident_m2m]
DLP Incident Response integration with Symantec	Tipo de informação confidencial detectada [sn_sym_dlp_detected_sensitive_information_type]

Nota:
Todas as tabelas do sistema, como e-mails, avaliações e anexos, serão direcionadas automaticamente para o registro DLP arquivado.

5. Selecione a regra de registro relacionada ao arquivamento que você deseja arquivar.

Nota:
Para obter mais informações sobre como adicionar mais registros relacionados, consulte Arquivar registros relacionados ao DLP em Now Platform.

Data Loss Prevention Incident Response Gestão de incidentes

Use o Data Loss Prevention Incident Response Incident Management para atualizar e gerenciar incidentes aproveitando o DLP User Workspace, o DLP Analyst Workspace e o DLP Dashboard.

Data Loss Prevention Incident Response Espaço do usuário

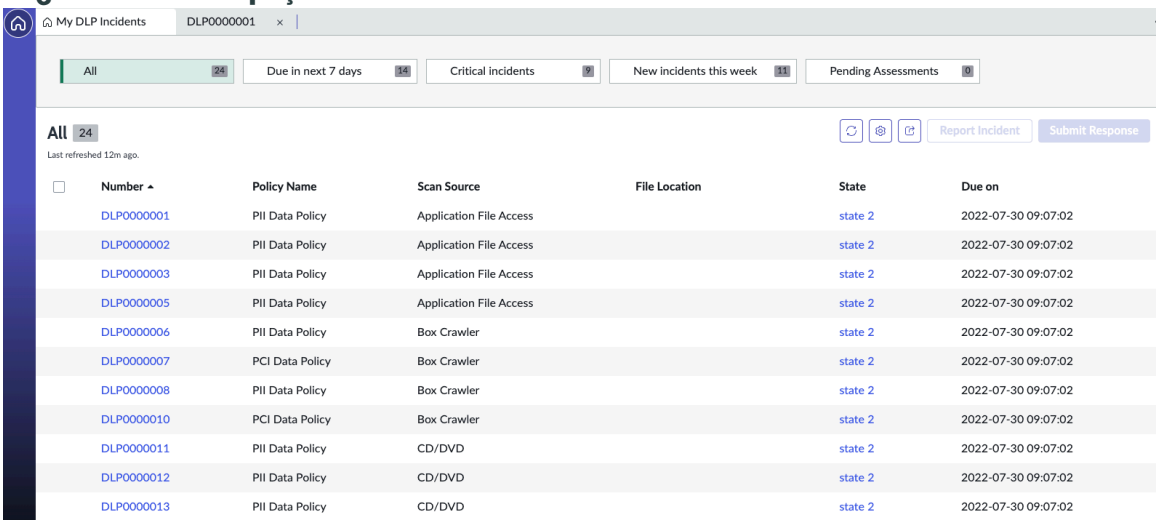
O espaço do usuário Data Loss Prevention Incident Response (DLP IR) é um espaço onde os usuários finais, gerentes e aprovadores podem responder aos incidentes do DLP atribuídos. Os usuários finais, gerentes e aprovadores podem responder aos incidentes especificando as ações corretas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Você também pode criar e gerenciar avaliações para permitir que os usuários finais respondam a incidentes do DLP. O espaço consiste em uma página principal e exibições de lista que permitem ver os incidentes do DLP atribuídos.

Página inicial do espaço do usuário do DLP



Relatar ou responder a incidentes do DLP

Acesse o espaço do usuário Data Loss Prevention Incident Response (DLP), revise os incidentes DLP atribuídos e relate ou responda aos incidentes.

Antes de Iniciar

Função necessária:

- Qualquer usuário/funcionário válido

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes do DLP** > **Espaço do usuário do DLP**.
   A página Meus incidentes DLP é aberta em uma nova guia.
2. Clique em uma exibição de lista para revisar os incidentes atribuídos a você.

Exibição em lista	Descrição
Todos	Exibir todos os incidentes atribuídos.
Vencimento nos próximos 7 dias	Exibir todos os incidentes que vencem nos próximos 7 dias.
Incidentes críticos	Exiba todos os incidentes com o rótulo de severidade crítica.
Novos incidentes nesta semana	Exiba todos os incidentes atribuídos esta semana.
Avaliações pendentes	Exiba todas as avaliações que ainda estão pendentes.

3. Você pode revisar os incidentes do DLP de duas maneiras:

   a. A primeira maneira é localizar e selecionar um ou mais incidentes do DLP que você deseja revisar e clicar na caixa de seleção ao lado dos incidentes.

   b. Escolha a opção apropriada para você.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

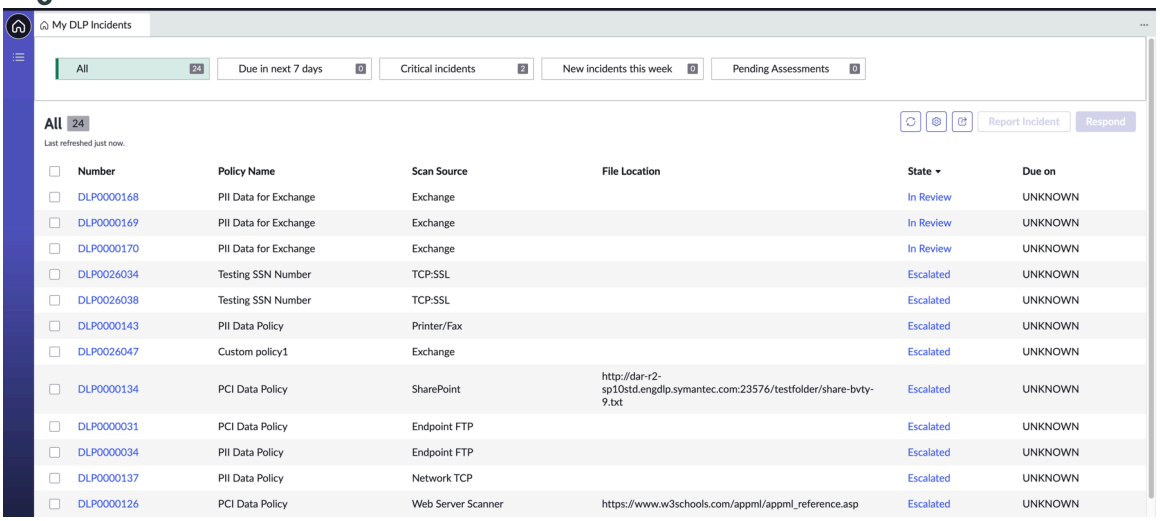
Página inicial do portal do usuário final do DLP

Opção	Descrição
Atualizar lista	Opção para atualizar a lista de incidentes do DLP se você fez uma atualização.
Ações de Lista	Lista de ações que você pode executar. Estas são as opções: ▪ **Salvar como** ▪ **Editar colunas** ▪ **Redefinir larguras** **Nota:** Quando você tiver sua própria lista personalizada criada na seção **Minhas listas** configurada para o seu espaço, também poderá executar as ações de lista adicionais abaixo: ▪ **Renomear** ▪ **Salvar** ▪ **Excluir**
Copiar URL para Todos	Opção para copiar os URLs de todos os incidentes do DLP.
Relatar incidente	Ação para relatar o incidente como falso positivo ou proprietário incorreto. Por exemplo, você pode relatar um proprietário incorreto e sugerir outro proprietário ou relatar o incidente como um falso positivo.
Responder	Responda a um incidente selecionando uma opção de resposta do incidente. Por exemplo, se o usuário excluir um arquivo que viola uma política DLP, o usuário pode escolher a opção **Arquivo excluído** para enviar a confirmação manual de que o arquivo foi excluído e fornecer comentários. Aqui, você também pode selecionar opções de resposta avançadas. Por exemplo, **Solicitar liberação de e-mail da quarentena**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Página inicial do Portal do usuário do DLP



c. A segunda maneira é clicar em um incidente DLP específico para abri-lo.
A guia **Detalhes** exibe as seguintes seções:

- Detalhes: você pode exibir os detalhes do incidente DLP, como número do incidente, severidade e nome do arquivo.
- Redigir: para adicionar comentários sobre o incidente do DLP que fiquem visíveis para todos, insira os comentários na guia Comentários. Para adicionar comentários que são visíveis para determinadas pessoas, insira os comentários na guia Anotações de trabalho (privadas).
- Atividade: você pode exibir os detalhes das diferentes atividades no incidente do DLP.
- Anexos: se você tiver anexos relacionados ao incidente do DLP, clique em **Procurar** e selecione o anexo na sua unidade local.

  A guia **Detalhes adicionais** exibe todas as informações adicionais sobre o incidente do DLP, incluindo campos personalizados.

  Importante:
  - Campos personalizados para incidentes do DLP são compatíveis somente com a versão San Diego ou posterior.
  - Se houver dados de campos personalizados disponíveis para um incidente DLP específico, você poderá exibi-los na guia **Detalhes adicionais**. Se não houver campos personalizados para o incidente DLP, você verá uma página em branco.

- **Tipo de**informação confidencial detectada : exibe as informações confidenciais detectadas do incidente.

  Nota:
  Essa lista relacionada fica visível somente para os incidentes do DLP criados para integrações da Microsoft ou da Symantec. No registro de incidente da Microsoft ou da Symantec, sempre que o usuário acessar o registro de tipo de informação confidencial detectado, o conteúdo de correspondência realçado em relação a essa integração será exibido.

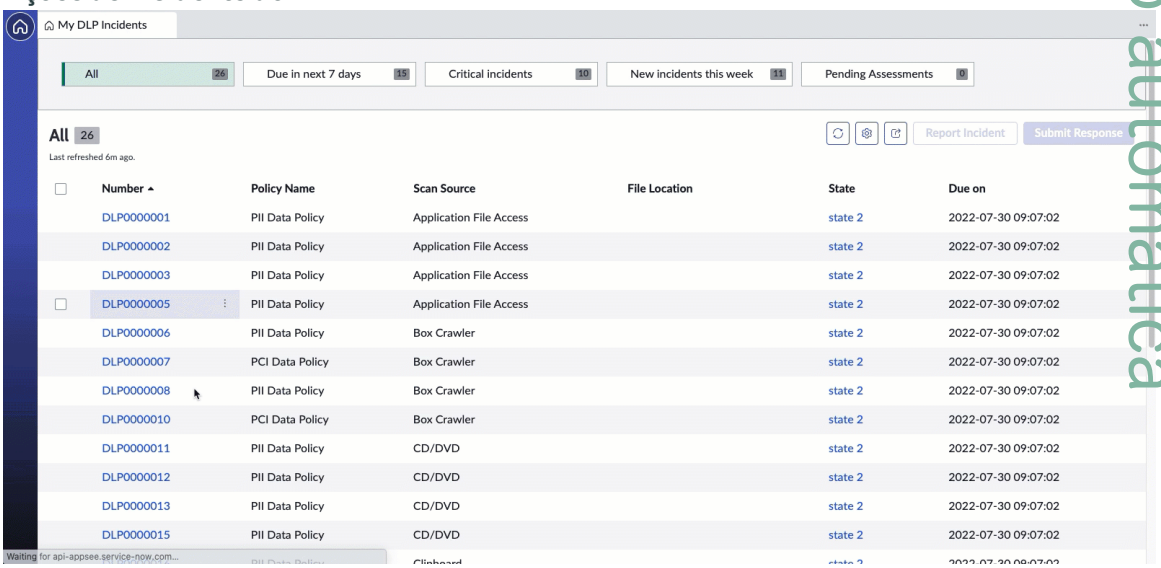
d. Escolha a opção apropriada para você.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Relatar falso-positivo	Ação para relatar que o incidente DLP foi acionado ou criado incorretamente. Você pode mencionar os detalhes do motivo pelo qual marcou o incidente como falso positivo no campo Comentários.
Relatar proprietário incorreto	Ação para relatar que o incidente DLP foi atribuído ao usuário incorreto. Se você souber o proprietário correto do incidente, poderá selecionar o nome do proprietário no campo Proprietário sugerido. Para adicionar detalhes adicionais, use o campo Comentários.
Responder	Responda a um incidente selecionando uma opção de resposta do incidente. Por exemplo, se o usuário excluir um arquivo que viola uma política DLP, o usuário pode escolher a opção **Arquivo excluído** para enviar a confirmação manual de que o arquivo foi excluído e fornecer comentários. Aqui, você também pode selecionar opções de resposta avançadas. Por exemplo, **Solicitar liberação de e-mail da quarentena**.

Ações de incidente do DLP



4. Para fazer avaliações, selecione a exibição de lista **Avaliações pendentes**.

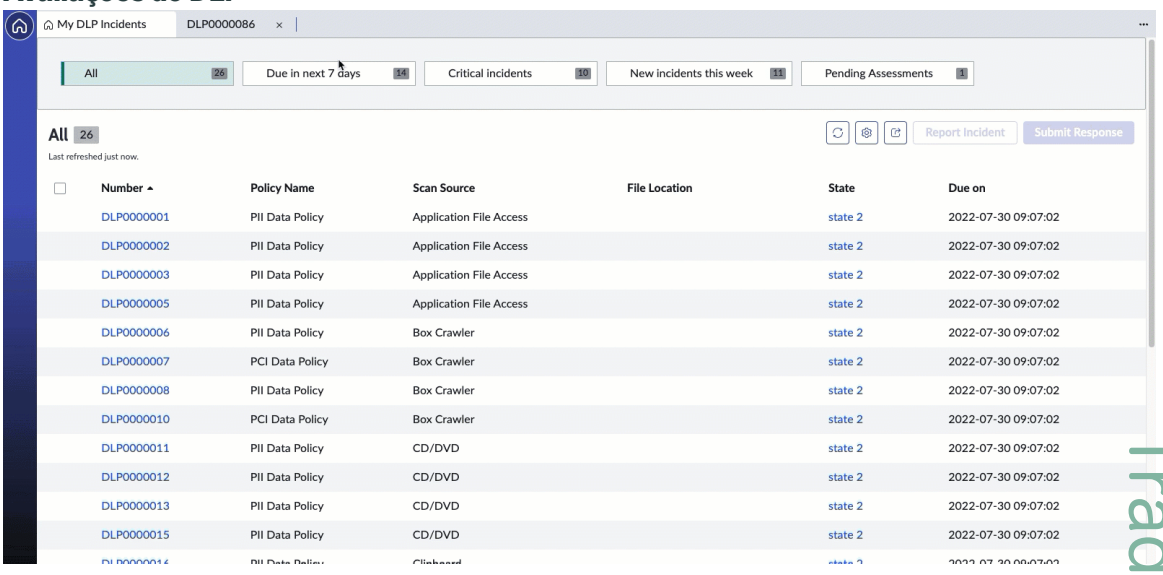
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

a. Clique em um número de avaliação específico para abri-lo.

b. Responda às perguntas de avaliação e clique em **Salvar** ou **Enviar** com base em seus requisitos.

Avaliações do DLP



5. Clique na seção do cartão **Instruções** que é exibida na parte superior de todos os campos na exibição do formulário de incidente do DLP para exibir as informações adicionais sobre um incidente específico.

Nota:
Esta seção no espaço orienta os usuários sobre as informações do incidente, o que ajuda a entender as próximas etapas da resolução do incidente.

O cartão de instruções do usuário exibe dois cabeçalhos diferentes que fornecem mais informações sobre um incidente específico na exibição do formulário. Clique em qualquer cabeçalho de instrução do usuário para saber os detalhes adicionais.

Para obter mais informações, consulte Criar e gerenciar modelo de instruções do usuário para incidentes do DLP e Configurar instruções do usuário da IU do DLP.

Como trabalhar com o módulo Minhas aprovações

O módulo Minhas aprovações estará disponível no Espaço de usuários do DLP para os usuários conectados. Os usuários podem aprovar ou rejeitar as solicitações de aprovação de atribuição aqui.

Antes de Iniciar

Função necessária:

- Usuário final
- Gerente
- Aprovador

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes do DLP** > **Espaço do usuário do DLP**.
   A página **Meus incidentes DLP** será exibida em uma nova guia.
2. Clique no módulo **Minhas aprovações**, presente no módulo **Meus incidentes de DLP**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

A exibição da lista Minhas aprovações será exibida.

O aprovador pode aprovar ou rejeitar as solicitações na exibição de lista da página **Minhas aprovações**. É possível aprovar ou rejeitar várias solicitações da exibição de lista.

O aprovador pode exibir os detalhes da solicitação atribuída na exibição do formulário. Ao clicar na ação **Aprovar** ou **Rejeitar** na exibição do formulário, é possível aprovar ou rejeitar a solicitação individual.

Nota:

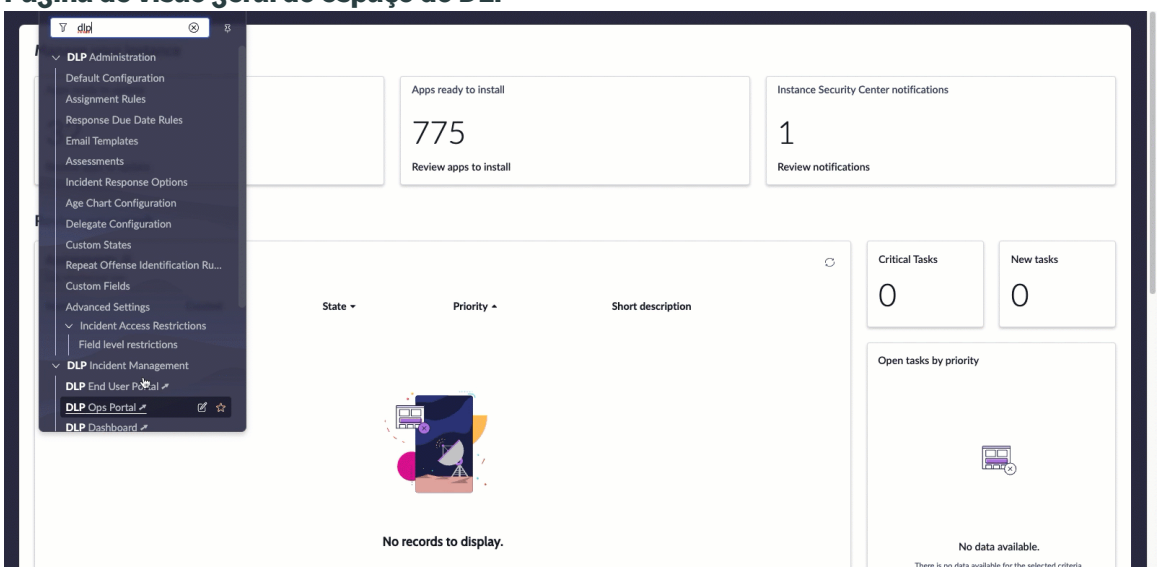
Para exibir os detalhes do incidente do DLP, clique no disponível no campo **Aprovar**.

Data Loss Prevention Incident Response Espaço do analista

Use o espaço do analista Data Loss Prevention Incident Response (DLP IR) para exibir os incidentes do DLP. Atribua os incidentes aos usuários finais para resolução e muito mais.

O espaço do DLP consiste em uma página inicial com painéis, exibições de lista e exibições de formulário que permitem monitorar incidentes do DLP.

Página de visão geral do espaço do DLP



Revisar e atribuir seus incidentes do DLP

Acesse o Espaço do analista Data Loss Prevention Incident Response (DLP IR) para revisar os incidentes do DLP e atribuí-los ou resolvê-los. Você pode rastrear tendências de incidentes por severidade, principais infratores, incidentes por origem de verificação e incidentes por política.

Página inicial inicial do DLP Workspace

Visão geral Visão geral do espaço do DLP

Antes de Iniciar

Função necessária:

- sn_dlir.analyst — Edite e exiba incidentes do DLP.
- sn_dlir.analyst_read e sn_dlir.read — Exibir incidentes do DLP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes do DLP** > **Espaço do analista do DLP**.
   A página da lista de operações Meus incidentes do espaço do DLP é aberta em uma nova guia.
2. Clique no ícone inicial do **espaço do DLP** para exibir a página inicial do espaço.
3. Analise os widgets do painel para identificar tendências por incidentes por gravidade, principais infratores, incidentes por origem de verificação e incidentes por política.
4. Clique nos filtros apropriados na página inicial para exibir os widgets por suas várias categorias.

Filtros	Descrição
Incidentes abertos	Exibir todos os incidentes em aberto.
Incidentes críticos atrasados	Exiba os incidentes que têm o rótulo de severidade crítica e que estão atrasados.
Incidentes atribuídos a usuários finais	Exiba os incidentes atribuídos aos usuários finais.

5. Você pode revisar e atribuir os incidentes do DLP de duas maneiras:

   a. A primeira maneira é localizar e selecionar um ou mais incidentes do DLP que você deseja revisar e clicar na caixa de seleção ao lado dos incidentes.

   b. Escolha a opção apropriada para você.

Opção	Descrição
Atualizar lista	Opção para atualizar a lista de incidentes do DLP ao fazer uma atualização.
Ações de Lista	Lista de ações que você pode executar. Estas são as opções: ▪ **Salvar como** ▪ **Editar colunas** ▪ **Redefinir larguras** **Nota:** Quando você tiver sua própria lista personalizada criada na seção **Minhas listas** configurada para o seu espaço, também poderá executar as ações de lista adicionais abaixo: ▪ **Renomear** ▪ **Salvar** ▪ **Excluir**
Copiar URL para Todos	Opção para copiar os URLs de todos os incidentes do DLP.
Mostrar painel de filtros	Opção para detalhar os incidentes necessários usando a opção de filtro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	i. Clique no filtro na parte superior esquerda da página e selecione **Exibição avançada**. **ii.** Use um filtro existente ou crie o seu próprio adicionando condições que contenham um campo, operador e valores. **iii.** Para adicionar mais condições, clique em **E** ou **OU**: ▪ Se **AND** for selecionado, todas as condições deverão ser correspondidas. ▪ Se **OU** for selecionado, qualquer uma das condições poderá ser correspondida. **iv.** Clique em **Atualizar**.
Atribuir Incidente	Ação para determinar a quem atribuir o incidente DLP. Estas são as opções: ▪ **Atribuir incidente a**: opção para atribuir o incidente a um analista, usuário final ou outra pessoa. ▪ **Usuário**: opção para determinar a qual usuário o incidente deve ser atribuído. ▪ **Resposta pré-usuário do**estado do incidente : opção para determinar em que estado o incidente deve estar antes que o usuário responda. Também pode ser um estado personalizado. ▪ **Anexar avaliação**: opção para indicar se você deseja anexar uma avaliação ao incidente. Se habilitada, as opções abaixo estarão disponíveis: ▪ **Modelo de avaliação**: opção para selecionar um modelo de avaliação para o incidente do DLP. ▪ **Estado do incidente após a resposta do usuário** Opção para selecionar o estado em que o incidente do DLP deve estar depois que o usuário responder.
Responder	Responda a um incidente selecionando uma opção de resposta do incidente. Por exemplo, se o usuário excluir um arquivo que viola uma política DLP, o usuário pode escolher a opção **Arquivo excluído** para enviar a confirmação manual de que o arquivo foi excluído e fornecer comentários.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	Aqui, você também pode selecionar opções de resposta avançadas. Por exemplo, **Solicitar liberação de e-mail da quarentena**.
Escalar	Ação para escalar o incidente. Você pode escalar o incidente selecionando o usuário para o qual deseja escaloná-lo. Você também pode obter informações adicionais no campo Comentários.
Atualizar Estado	Ação para atualizar o estado do incidente. Você pode atualizar o estado do incidente selecionando um dos estados nas opções suspensas. Também pode ser um estado personalizado.
Fechar	Ação para fechar o incidente. Você também pode adicionar comentários adicionais antes de fechar o incidente.

c. A segunda maneira é clicar em um incidente DLP específico para abri-lo.

- Guia**Detalhes** : exibe as seguintes seções:
  - **Detalhes**: você pode exibir os detalhes do incidente do DLP, como número do incidente, gravidade, nome do arquivo e assim por diante. Você também pode modificar os campos Severidade, Estado, Usuário final e Grupo de analistas do DLP, respectivamente, e salvá-los.
  - **Redigir**: para adicionar comentários sobre o incidente do DLP que fiquem visíveis para todos, insira os comentários na guia Comentários. Para adicionar comentários que são visíveis para determinadas pessoas, insira os comentários na guia Anotações de trabalho (privadas).
  - **Atividade**: você pode exibir os detalhes das diferentes atividades no incidente do DLP.
  - **Anexos**: se você tiver anexos relacionados ao incidente do DLP, clique em **Procurar** e selecione o anexo na sua unidade local.
- Guia**Detalhes adicionais** : exibe todas as informações adicionais sobre o incidente do DLP, incluindo campos personalizados.

  Importante:
  - Campos personalizados para incidentes do DLP são compatíveis somente com a versão San Diego ou posterior.
  - Você pode usar a guia **Detalhes adicionais** para ver se algum campo personalizado foi criado para um incidente DLP específico ou não.

- Guia**Atributos personalizados** : exibe a lista de atributos personalizados relacionados ao incidente do DLP.
- **Outros incidentes do usuário final**: exibe o incidente do mesmo usuário final. É possível consolidar incidentes executando a ação **Adicionar como incidente** secundário desta lista relacionada.
- **Tipo de**informação confidencial detectada : exibe as informações confidenciais detectadas do incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Essa lista relacionada fica visível somente para os incidentes do DLP criados para integrações da Microsoft ou da Symantec. No registro de incidente da Microsoft ou da Symantec, sempre que o usuário acessar o registro de tipo de informação confidencial detectado, o conteúdo de correspondência realçado em relação a essa integração será exibido.

- **Incidentes secundários**: exibe os incidentes secundários criados manualmente (executando a ação "Adicionar como incidente secundário") ou a partir das regras de consolidação do DLP. É possível desvincular o incidente secundário executando "Desvincular incidente secundário" nesta lista relacionada.
- **Incidentes clonados**: exibe os incidentes clonados do incidente primário. Ao clicar na ação **Clonar incidente** da exibição do formulário, você pode criar um novo incidente clonado.
- Guia**Avaliações** : exibe a lista de avaliações atribuídas ao incidente do DLP.

d. Escolha a opção apropriada para você.

Opção	Descrição
Atribuir Incidente	Ação para determinar a quem atribuir o incidente DLP. Estas são as opções: ▪ **Atribuir incidente a**: opção para atribuir o incidente a um analista, usuário final ou outra pessoa. ▪ **Usuário**: opção para selecionar o usuário ao qual o incidente deve ser atribuído. ▪ **Resposta pré-usuário do**estado do incidente : opção para selecionar o estado em que o incidente deve estar antes que o usuário responda. Também pode ser um estado personalizado. ▪ **Anexar avaliação**: opção para indicar se você deseja anexar uma avaliação ao incidente. Se habilitada, as opções abaixo estarão disponíveis: ▪ **Modelo de avaliação**: opção para selecionar um modelo de avaliação para o incidente do DLP. ▪ **Estado do incidente após a resposta do usuário**: opção para selecionar o estado em que o incidente DLP deve estar depois que o usuário responder.
Cancelar aprovação	Ação para cancelar a solicitação de aprovação. Esta ação ficará visível para os analistas na exibição do formulário somente quando o incidente do DLP estiver no estado **Aprovação pendente**. As opções disponíveis são:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
	▪ **Atribuir incidente a**: opção para atribuir o incidente a ninguém, a um analista ou a outra pessoa. ▪ **Usuário**: opção para selecionar o usuário ao qual o incidente deve ser atribuído. ▪ **Estado pós-cancelamento do incidente**: opção para selecionar o estado em que o incidente deve estar após o cancelamento da solicitação. ▪ **Comentários**: para fornecer detalhes adicionais para o cancelamento.
Designar Avaliação	Ação para anexar uma avaliação ao atribuir o incidente. As opções são as seguintes: ▪ **Modelo de avaliação**: opção para selecionar um modelo de avaliação para o incidente do DLP. ▪ **Estado do incidente após a resposta do usuário**: opção para selecionar o estado em que o incidente DLP deve estar depois que o usuário responder.
Baixar arquivo	Ação para baixar o arquivo ou e-mail que tem o conteúdo violador. Esta ação pode ser realizada para incidentes criados para Microsoft OneDrive, SharePoint Online ou Exchange Online.
Salvar	Ação para salvar as mudanças feitas. Você tem a opção de modificar os campos Severidade, Estado e Usuário final do incidente DLP e salvá-los.
Responder	Responda a um incidente selecionando uma opção de resposta do incidente. Por exemplo, se o usuário excluir um arquivo que viola uma política DLP, o usuário pode escolher a opção **Arquivo excluído** para enviar a confirmação manual de que o arquivo foi excluído e fornecer comentários. Aqui, você também pode selecionar as opções de resposta avançadas. **Por exemplo: Solicitar liberação de e-mail da quarentena**.
Escalar	Ação para escalar o incidente. Você pode escalar o incidente selecionando o usuário para o qual deseja escaloná-lo. Você também pode obter informações adicionais no campo Comentários.
Clonar incidente	Ação para criar um incidente de clone se o registro do incidente afetar vários usuários. Você pode atribuir os incidentes clonados a várias partes interessadas, como jurídico/TI.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

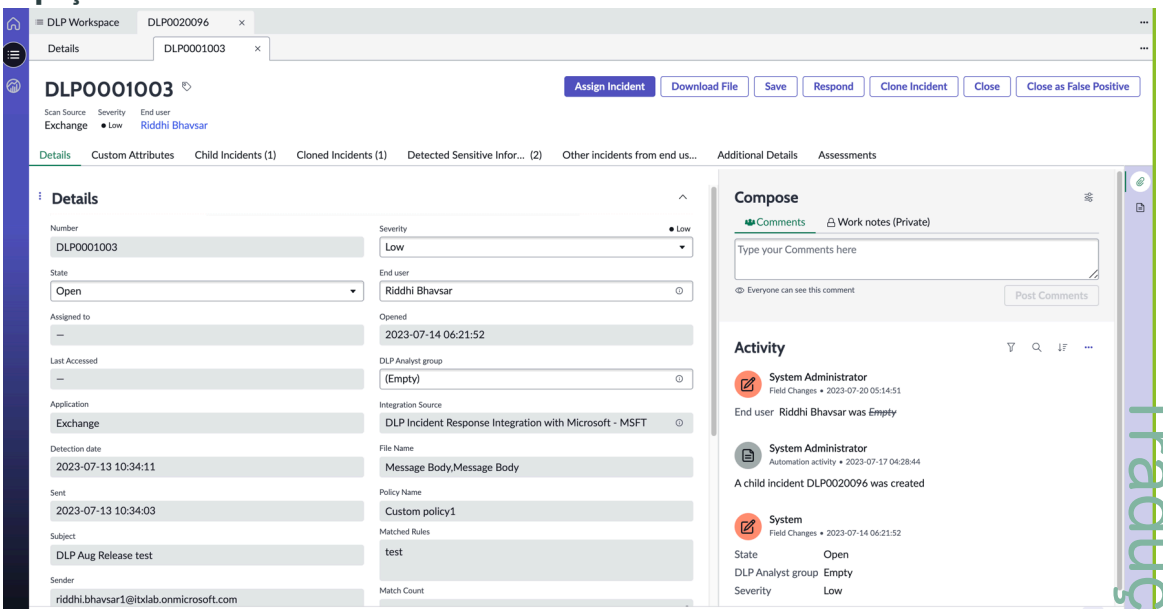
Opção	Descrição
	Depois de criar um registro de incidente de clone, uma nova guia **Incidentes clonados** é criada no incidente DLP primário e todos os incidentes clonados são listados nesta exibição. **Nota:** ▪ Se o registro de incidente do DLP primário for fechado, todos os registros de incidentes clonados serão fechados automaticamente. ▪ Se um registro de incidente do DLP contiver um incidente clonado, ele não poderá ser atribuído aos usuários finais. Os registros de incidentes do DLP primário podem ser gerenciados somente por usuários com a função de analista. ▪ Você também tem a opção de atualizar automaticamente o estado primário com base no estado dos incidentes clonados no módulo Configuração padrão. Por exemplo, se todos os incidentes clonados forem movidos para o estado Escalado, o incidente primário também será movido para o estado Escalado.
Fechar	Ação para fechar o incidente. Você também pode adicionar comentários adicionais antes de fechar o incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Opção	Descrição
Fechar como falso positivo	Ação para fechar o incidente como falso-positivo. Você também pode adicionar comentários adicionais antes de fechar o incidente.

Espaço do analista do DLP



6. Você pode ver a exibição de lista na página inicial, indo para o canto superior esquerdo da página e clicando na guia **Listas**.
   A categoria Listas consiste nas páginas de lista padrão e personalizadas para incidentes do DLP.
   - Guia **Listas**: listas padrão para incidentes do DLP. Estas são as listas padrão:
     - Todos
     - Em aberto
     - Meus Incidentes
     - Atribuído ao meu grupo
     - Escalado
     - Atrasado
     - Avaliações pendentes
     - Ação do usuário pendente
     - Incidentes clonados
     - Incidentes arquivados
   - Guia **Minhas listas**: exibe todas as listas que você renomeou e todas as que você criou.

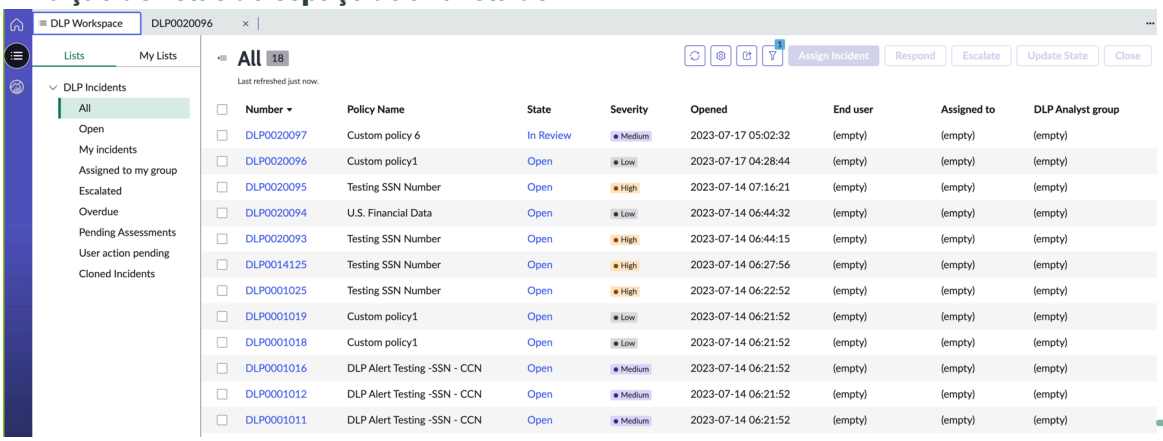
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Example

O exemplo a seguir mostra o espaço do DLP com as categorias de exibição de lista. A opção de exibição de lista **Todos** é selecionada.

Exibição de listas do espaço do analista do DLP



Exibir incidentes DLP arquivados

Use o espaço do analista do DLP para exibir os incidentes do DLP arquivados

Antes de Iniciar

Função necessária:

- sn_dlir.analyst — Edite e exiba incidentes do DLP.
- sn_dlir.analyst_read e sn_dlir.read — Exibir incidentes do DLP.

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes do DLP** > **Espaço do analista do DLP**.
   Por padrão, a seção Meus incidentes é exibida.
2. Clique **em Incidentes arquivados**.
   A lista de incidentes DLP arquivados é exibida.
3. Clique no botão **Mostrar contagem de incidentes** para exibir a contagem de incidentes arquivados.

Nota:

- Por padrão, a contagem de incidentes arquivados está oculta para melhorar o tempo de carregamento da lista. Você deve clicar no botão **Mostrar contagem de incidentes** para exibir a contagem de incidentes. Além disso, é exibida uma mensagem informativa que mostra a contagem de incidentes.
- A propriedade do sistema glide.ui.list.seismic.omit.count está habilitada no sistema de base para os incidentes arquivados para ocultar a contagem da lista de incidentes.

4. Selecione um ou mais incidentes do DLP que você deseja exibir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O incidente do DLP exibe a seção de detalhes do incidente.

Nota:

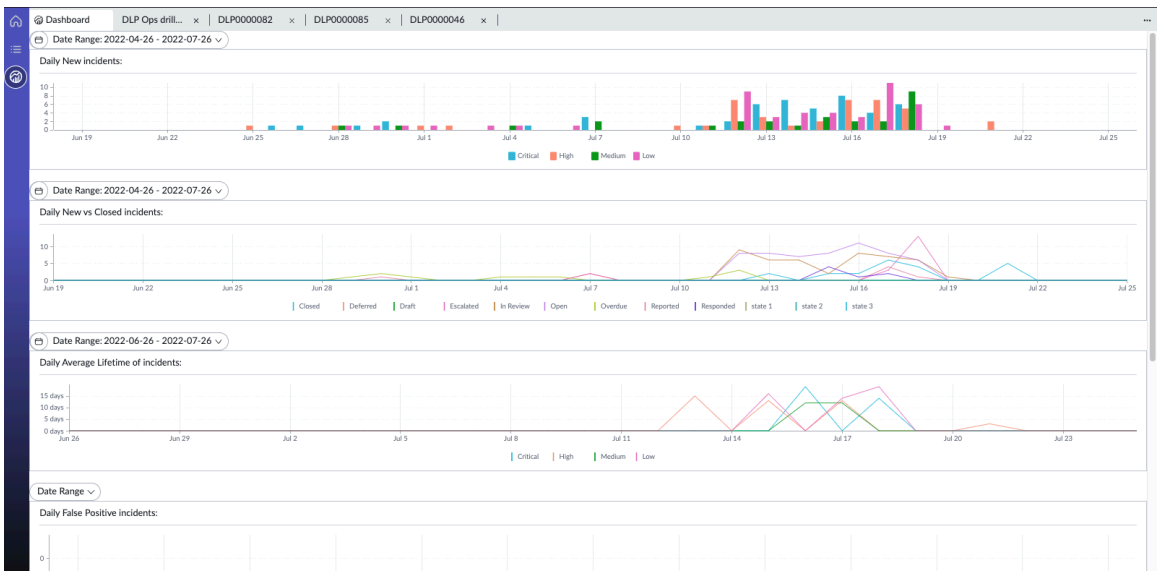
- A guia **Outros incidentes de usuários finais** também incluirá os incidentes arquivados.
- **Corresponder conteúdo** é compatível com todos os incidentes arquivados (que também serão compatíveis com todas as integrações), mas **o download do arquivo** é compatível somente com integrações da Microsoft.

Painel Data Loss Prevention Incident Response

O painel Data Loss Prevention Incident Response (DLP IR) fornece uma visão geral de alto nível de seus incidentes DLP e tendências de incidentes diários em sua instância na forma de gráficos. Esses gráficos ajudam a exibir, gerenciar e corrigir com eficácia os incidentes do DLP.

O painel Data Loss Prevention Incident Response fornece informações importantes sobre seus incidentes DLP diariamente. Você pode configurar indicadores e coletar regularmente snapshots de dados dos incidentes que correspondam às condições nas propriedades do indicador. Os dados coletados são visualizados usando widgets no painel. Para analisar os incidentes do DLP em diferentes intervalos de tempo, você pode aplicar diferentes intervalos de datas.

Painel do DLP



Analise as tendências de incidentes diários em seus incidentes do DLP

Acesse o painel Data Loss Prevention Incident Response (IR do DLP) para analisar as tendências diárias em seus incidentes do DLP e corrigi-los com eficácia.

Antes de Iniciar

Função necessária:

- sn_dlir.analyst — Edite e exiba incidentes do DLP.
- sn_dlir.analyst_read e sn_dlir.read — Exibir incidentes do DLP.

Por Que e Quando Desempenhar Esta Tarefa

Você pode visualizar as tendências diárias usando widgets no painel do DLP. Os dados ou estatísticas das tendências diárias dos incidentes do DLP são coletados das propriedades

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

do indicador de incidentes diários que são definidas pela sua organização. Você pode obter informações importantes aplicando diferentes intervalos de dados para analisar os incidentes do DLP em diferentes intervalos de tempo para os seguintes gráficos:

- **Novos incidentes diários**: dados dos incidentes gerais do DLP criados diariamente, independentemente do estado dos incidentes. Os incidentes do DLP são categorizados com base nas gravidades, incluindo Médio, Crítico, Alto e Baixo. Cada severidade de incidente do DLP é representada por uma cor específica no gráfico.
- **Incidentes diários novos versus encerrados**: os diferentes estados dos incidentes do DLP e uma comparação entre os novos incidentes diários e os incidentes encerrados diariamente. A categoria Novo diário inclui todos os incidentes do DLP nos estados Aberto, Rascunho, Escalado, Em revisão, Atrasado, Relatado, Respondido ou Personalizado (se houver). A categoria de incidente Encerrado inclui os incidentes DLP encerrados. Cada estado de incidente do DLP é representado por uma cor específica no gráfico.
- **Tempo de vida médio diário dos incidentes**: o tempo de vida de um incidente é o período entre a abertura e o fechamento de um incidente DLP específico. O tempo de vida médio diário é calculado somente para os incidentes DLP encerrados.
- **Incidentes falso-positivos diários**: dados de todos os incidentes do DLP relatados como falso-positivos diários. Os incidentes falso-positivos diários são categorizados com base nas gravidades, incluindo Média, Crítica, Alta e Baixa. Cada gravidade de incidente falso-positivo diário é representada por uma cor específica no gráfico.
- **Idade versus gravidade dos incidentes**: comparação de dados de todos os incidentes do DLP, categorizados pela idade e configurados com a gravidade dos incidentes do DLP. A categoria Idade inclui todos os incidentes do DLP abaixo da idade que sua organização define. Para obter mais informações sobre gráficos de idade, consulte Configure o gráfico de idade para seus incidentes do DLP. A Severidade dos incidentes inclui todos os incidentes do DLP na categoria Alta ou Baixa. Cada severidade é representada por uma cor específica no gráfico.
- **Incidentes escalonados diariamente**: dados de todos os incidentes do DLP escalonados diariamente. Os incidentes escalonados diariamente são categorizados com base nas gravidades, incluindo Média, Crítica, Alta e Baixa. Cada severidade de incidente escalonada diariamente é representada por uma cor específica no gráfico.

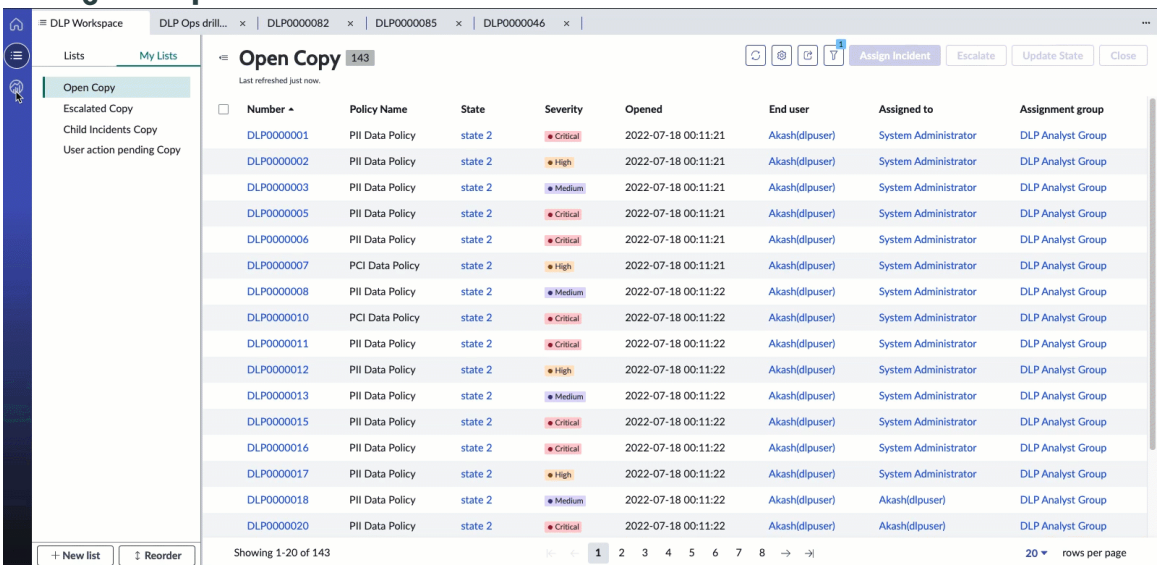
Procedimento

1. Navegar até **Todos** > **Gestão de incidentes do DLP** > **Painel do DLP**.
   A página Meu painel DLP é exibida em uma nova guia do navegador.
2. Selecione um widget de painel para o qual você deseja executar uma análise de tendência diária.
   Por exemplo, o gráfico de Novos incidentes diários.
3. Revise os widgets do painel para identificar tendências.
4. Clique **em Intervalo de datas**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Visão geral do painel do DLP



5. Selecione um intervalo de datas no calendário e clique em **Aplicar**.

Example
Por exemplo, o gráfico Novos incidentes diários é atualizado para o intervalo de dados selecionado.

6. Use os filtros abaixo do gráfico para fazer uma busca detalhada e realizar uma análise mais detalhada.

Integração de entrada para Data Loss Prevention Incident Response

Crie um ou vários incidentes do DLP usando a REST API de entrada.

Criar um único incidente DLP

Função necessária: sn_dlir.api_integration_user.

Para criar um único incidente DLP, defina os seguintes parâmetros conforme necessário:

Campo	Descrição
Método HTTP	`POST`
URL	https://{instance}/api/now/import/sn_dlir_incident_import
Cabeçalho de solicitação	**Aceitar:** `application/json` **Tipo de conteúdo:** `application/json`
Carga de amostra	`{ "application_window_title": "<value>", "assigned_to": "<value>", "attachments": "<value>", "data_owner_email": "<value>", "destination": "<value>", "dest_ip": "<value>",`

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	"dest_ip_port": "<value>", "detection_date": "<value>", "endpoint_on_corporate_net": "<value>", "files": "", "file_created": "", "file_created_by": "", "file_location": "", "file_modified_by": "", "file_name": "", "file_owner": "", "file_permissions": "", "ftp_user_name": "", "last_modified": "", "machine_ip": "", "machine_name": "", "match_count": "", "policy_id": "", "policy_name": "", "printer_name": "", "printer_type": "", "print_job_name": "", "recipients": "", "scanned_machine": "", "scan_source": "", "seen_before": "", "sender":"", "source":"", "source_file":"", "source_ip":"", "source_ip_port":"", "subject":"", "url":"", "user_justification":"" }

Exemplo de resposta	{
	"import_set": "ISET0010003",
	"staging_table": "sn_dlir_incident_import",
	"result": [
	{
	"transform_map": "",
	"table": "sn_dlir_incident",
	"display_name": "number",
	"display_value": "DLP0001012",
	"record_link":
	"https://{instance}/api/now/table/sn_dlir_incident/7cda322297c2411056a43d1e6253af1f",
	"status": "inserted",
	"sys_id": "7cda322297c2411056a43d1e6253af1f"
	}
	]
	}

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar vários incidentes do DLP

Função necessária: sn_dlir.api_integration_user.

Para criar vários incidentes do DLP a partir da mesma solicitação, defina os seguintes parâmetros conforme necessário:

Campo	Descrição
Método HTTP	`POST`
URL	https://{instance}/api/now/import/sn_dlir_incident_import/insertMultiple
Cabeçalho de solicitação	**Aceitar:** `application/json` **Tipo de conteúdo:** `application/json`

Carga de amostra	<pre>{
	"records": [
	{
	"file_name": "<value>",
	"file_modified_by": "<value>",
	"work_notes": "<value>",
	"url": "<value>",
	"scan_source": "<value>",
	"data_owner_email": "<value>",
	"file_created_by": "<value>",
	"file_owner": "<value>",
	"policy_name": "<value>"
	},
	{
	"dest_ip": "<value>",
	"dest_ip_port": "<value>",
	"detection_date": "<value>",
	"endpoint_on_corporate_net": "<value>",
	"files": "<value>",
	"file_created": "<value>",
	"file_created_by": "<value>",
	"file_location": "<value>",
	"file_modified_by": "<value>",
	"file_name": "<value>",
	"file_owner": "<value>",
	}
	]
	}</pre>

Exemplo de resposta	<pre>{
	"import_set_id": "a38f69229734dd1056a43d1e6253af75",
	"multi_import_set_id":
	"e78f69229734dd1056a43d1e6253af75"
	}</pre>

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Por padrão, a transformação é assíncrona. Para definir a transformação síncrona, crie um novo registro na tabela Inserir vários REST [sys_rest_insert_multiple], selecione a tabela de origem como **sn_dlir_incident_import**e defina a transformação como **síncrona**.

Integrações do DLP

O sistema base Data Loss Prevention Incident Response inclui integrações a pacotes de software de prevenção de perda de dados de terceiros.

Esta seção fornece instruções para ativar os plug-ins e configurar ServiceNow e integrações de terceiros. Também estão incluídas algumas diretrizes básicas para desenvolver suas próprias integrações, bem como detalhes sobre integrações específicas incluídas no sistema básico.

Configurações de Integração

O sistema básico inclui uma série de cartões para cada uma das implementações de integração que você pode ativar e usar. Além disso, os cartões são exibidos para todas as integrações publicadas na ServiceNow Store que têm dependências nos plug-ins Security Operations. Os cartões de integração podem ser exibidos selecionando **Security Operations** > **Configurações de Integração**.

Data Loss Prevention Incident Response O é compatível com os seguintes pacotes de software de prevenção de perda de dados de terceiros:

Symantec Integração para Data Loss Prevention Incident Response

A integração do DLP Symantec oferece suporte à ingestão de Data Loss Prevention Incident Response incidentes criados na implantação Symantec Data Loss Prevention Incident Response. Após a ingestão, você pode usar as funcionalidades de gerenciamento de incidentes para corrigir os incidentes do DLP.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral e principais recursos

A integração do DLP Symantec ajuda as empresas a rastrear o uso e a movimentação de dados confidenciais em várias plataformas.

Esta integração inclui os seguintes recursos principais:

- Capacidade de criar vários perfis de integração para diferentes Symantec endpoints de API.
- Ingestão programada de incidentes DLP de Symantec em sua instância ServiceNow.
- Capacidade de aplicar filtros de API para recuperar os incidentes que correspondem aos critérios de filtro e também especificar o filtro para Symantec incidentes do DLP que precisam ser importados.
- Mapeando os estados de incidentes do DLP em sua instância ServiceNow para os estados de incidentes do DLP em Symantec.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Atualize automaticamente o status do incidente em Symantec quando o estado mudar em sua instância ServiceNow.
- Capacidade de personalizar e definir o mapeamento de severidade entre incidentes do Symantec DLP com incidentes da ServiceNow.

Para saber mais sobre a integração, consulte a documentação do produto Symantec .

Introdução à integração de DLP Symantec para Prevenção de perda de dados

Antes de usar a integração, você deve baixá-la do ServiceNow® Store.

Check-list

Revise as informações a seguir antes de começar a configurar sua integração DLP Symantec para prevenção de perda de dados.

Check-list

Campo	Descrição
Verifique se você atribuiu as funções de aplicativo Now Platform, Aplicação de prevenção de perda de dados, MID.	As funções a seguir são usadas na integração do DLP Symantec no Now Platform: • O administrador (admin) instala as aplicações do ServiceNow® Store e atribui o administrador de prevenção de perda de dados (sn_dlir.admin). • O usuário com a função sn_dlir.admin pode configurar a integração e configurar os perfis de incidente. • Os usuários com a função sn_dlir.analyst terão funções de leitura na integração.
Atribua as funções de usuário DLP Symantec necessárias.	Analise as Symantec funções e permissões de integração do DLP.
Verifique se você está usando Symantec DLP 15.8	A integração do DLP Symantec para Prevenção de perda de dados foi testada com a versão 15.8 do Symantec Prevenção de perda de dados. **Nota:** Verifique se você está usando Symantec DLP 15.8
Verifique se a aplicação principal ServiceNow® necessária para oferecer suporte à integração DLP Symantec está instalada e ativada.	Verifique se as seguintes aplicações DLP e aplicações comuns de suporte de segurança estão instaladas e ativadas na ServiceNow Store. Se não estiver instalado, instale e ative na aplicação. • Security Support Common • Data Loss Prevention Incident Response

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Instalar e configurar a integração DLP Symantec para Prevenção de perda de dados

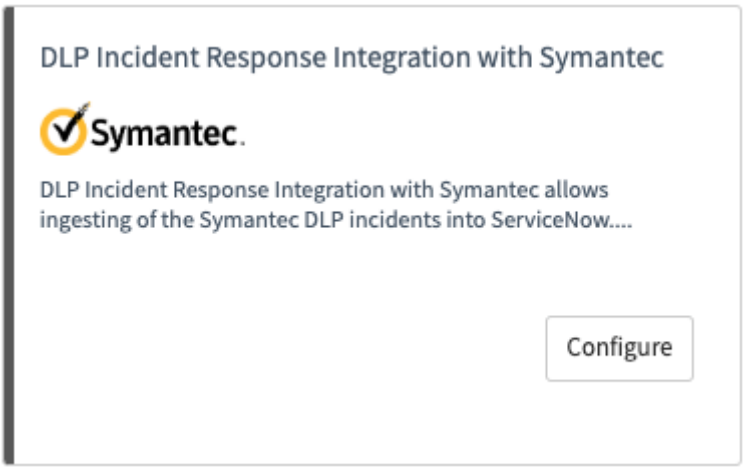
Instale e configure a integração DLP [Symantec do ServiceNow® Store na sua instância Now Platform. Comece a investigar incidentes do DLP usando os dados de incidentes do DLP Symantec.

Antes de Iniciar

Função necessária: sn_dlir.admin

Procedimento

1. Baixe a integração DLP [Symantec do ServiceNow® Store e instale-a.
2. Navegar até **Security Operations** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco DLP Incident Response Integration with Symantec e clique em **Configurar**.



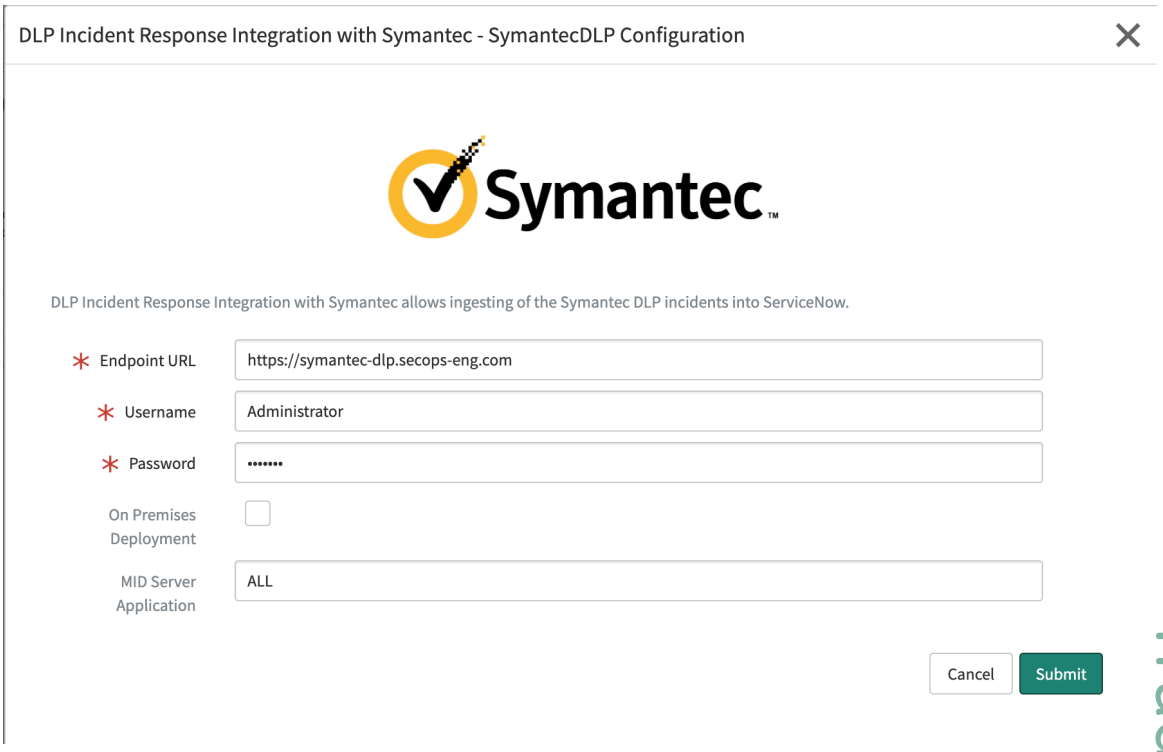
4. No formulário, preencha os campos.

Formulário de configuração de integração do DLP da Symantec

Campo	Descrição
Nome	Nome da configuração de integração do DLP Symantec.
URL de endpoint	Symantec Endpoint da REST API.
Nome do usuário	Symantec nome da conta. Para obter informações sobre as funções e permissões necessárias, consulte Funções e permissões .
Senha	Symantec senha da conta.
Implantação no local	Opção que você pode selecionar se o seu Symantec for implantado em uma instância no local. Ao selecionar esta opção, você deve usar o MID Server para se conectar à Symantec.
Aplicação do MID Server	O nome da aplicação MID que é usado para se comunicar com Symantec. Este campo é necessário ao selecionar a opção **Implantação no** local.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



5. Clique em **Enviar**.

Resultado
Depois de validar e enviar a configuração com sucesso, a Symantec Integração DLP é salva na página Integrações de segurança como um bloco.

Criar um perfil para integração DLP Symantec

Crie um perfil de incidente na sua instância Now Platform. Determine os Symantec incidentes DLP que são adequados para criar incidentes DLP.

Antes de Iniciar
Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa
Configure o Now Platform® para buscar os incidentes DLP do endpoint Symantec. Armazene esses incidentes em sua instância ServiceNow® como incidentes do DLP.

Procedimento

1. Navegar até **Integração do Symantec DLP** > **Perfil do incidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos na seção Nome.

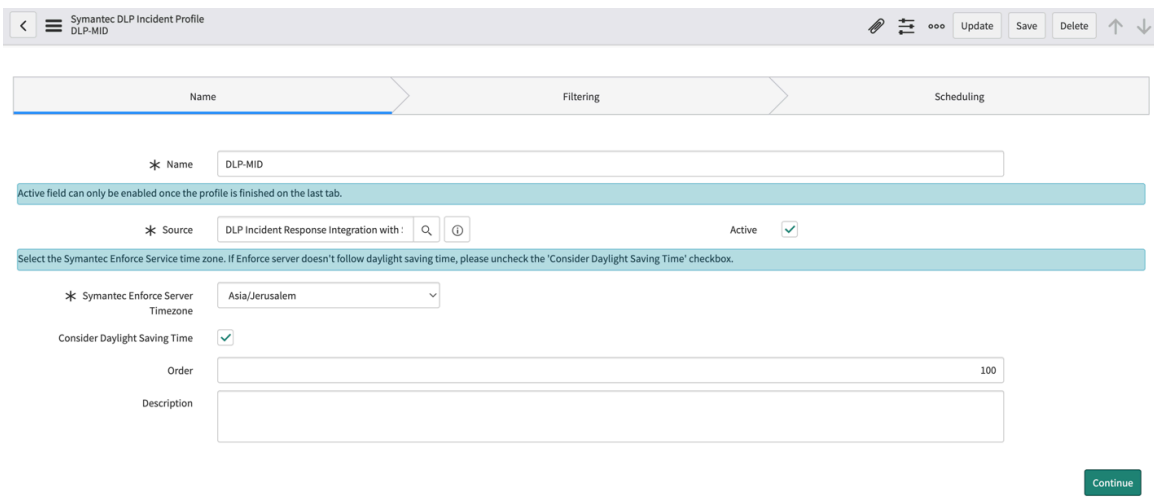
Criar um perfil

Campo	Descrição
Nome	Nome do perfil. Este campo ajuda a identificar o perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: O nome deve ser exclusivo para cada perfil.
Origem	Symantec Instância do DLP que você configurou para ingerir incidentes. Se você tiver várias instâncias configuradas, selecione a instância apropriada para os tipos de incidentes que você planeja ingerir para o perfil.
Ativo	Opção para indicar se o perfil está ativo. Este campo só pode ser habilitado depois de clicar em **Concluir** na seção Programação. Quando o perfil está ativo, isso implica que o Now Platform está pesquisando ativamente Symantec incidentes do DLP. Os incidentes correspondentes do DLP são criados no DLP quando as condições de filtragem são correspondidas com base nos parâmetros de programação fornecidos.
Fuso horário do servidor do Symantec Enforce	Selecione o fuso horário do servidor de aplicação da Symantec no perfil para que os incidentes não sejam perdidos devido a problemas de fuso horário.
Considerar o horário de verão	Marque esta caixa de seleção se o servidor de imposição seguir o horário de verão.
Ordem	Ordem de execução do perfil. O perfil com a ordem mais baixa considerada como a prioridade mais alta. Por padrão, o valor é 100.
Descrição	Descrição exclusiva para este perfil.



Tradução automática

O que Fazer Depois

Para mover para a seção Filtragem, clique em **Continuar**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir filtros a serem aplicados na criação do Incidente

Defina e defina condições de filtro para detalhar os incidentes do DLP de entrada Symantec. Determine os incidentes que devem ser criados como incidentes DLP em ServiceNow®.

Antes de Iniciar

Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa

A filtragem ajuda a isolar incidentes DLP e a limitar o número de incidentes DLP que você cria. Se critérios de filtragem adicionais forem definidos, somente os incidentes que corresponderem às condições serão criados.

Procedimento

1. Marque a caixa de seleção **Filtro baseado em API para ingestão de incidentes** para aplicar os filtros de API e recuperar os incidentes que correspondem aos critérios do filtro.
2. Adicione os filtros de API.
   A seguir está um exemplo que mostra os filtros de API.

```
{
            "operandOne": {
               "name": "incidentStatusName"
            },
            "filterType": "string",
            "operator": "EQ",
            "operandTwoValues": [
               "incident.status.New"
            ]
         }
```

Nota:
Para obter mais informações sobre os filtros de API na integração da Symantec, consulte Listas de incidentes: parâmetros - Detalhes do objeto de solicitação .

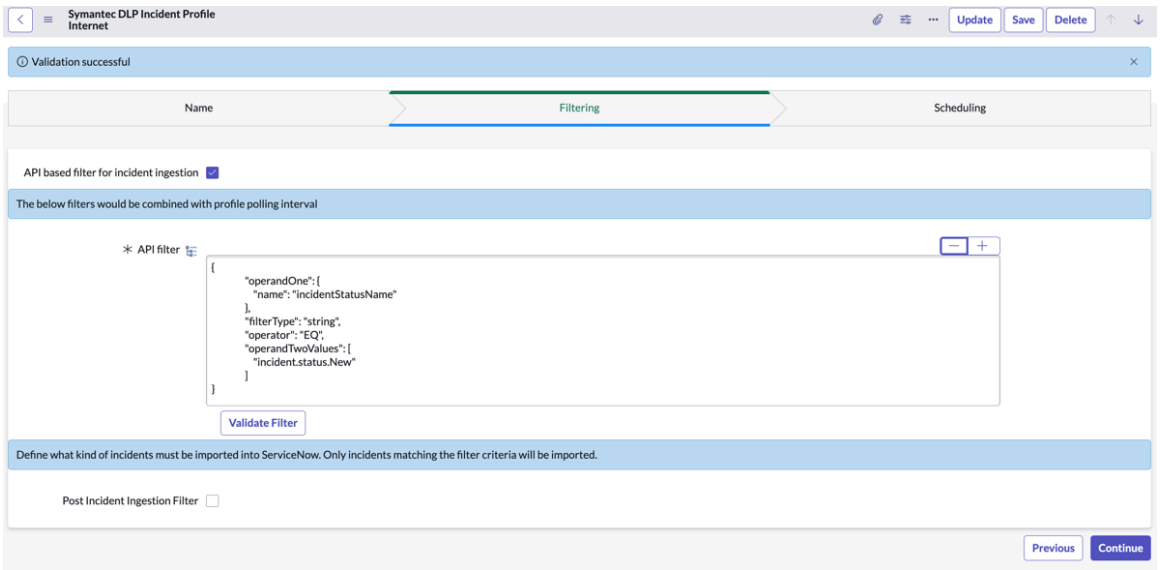
3. Clique em **Validar filtro** depois de aplicar os filtros de API.

Nota:
Se a validação for malsucedida, será exibida uma mensagem de erro informando que a validação falhou e isso acontece quando os filtros não são inseridos corretamente de acordo com as APIs da Symantec.

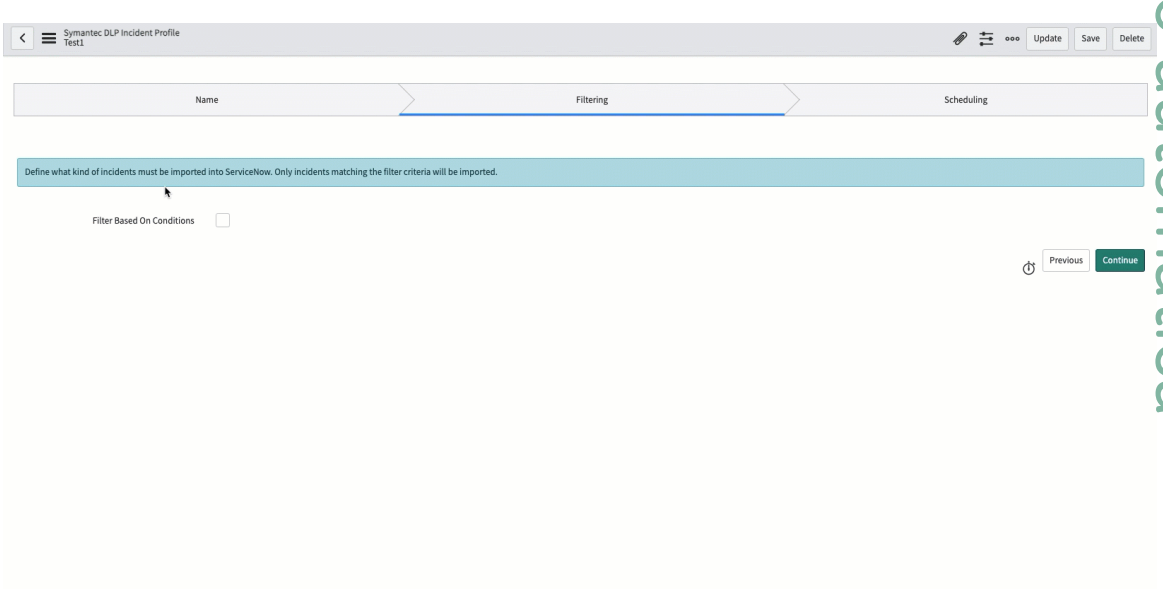
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Como adicionar filtros de API



4. Marque a caixa de seleção **Filtro de ingestão pós-incidente** para definir os critérios que um incidente DLP da Symantec deve satisfazer para que um incidente DLP seja criado.
   As opções no primeiro campo nas Condições do filtro correspondem aos campos disponíveis no incidente do DLP. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas. Verifique se os critérios definidos correspondem aos valores do incidente.
5. No construtor de condição, defina os filtros no campo **Condições do filtro**.



6. Para adicionar mais condições, clique em **E**ou **OU**.
   - Se **AND**for selecionado, todas as condições deverão ser correspondidas.
   - Se **OU**for selecionado, qualquer uma das condições poderá ser correspondida.

O que Fazer Depois

Para configurar a programação, clique em **Continuar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Programar a Symantec recuperação de incidente do DLP

Defina uma programação para recuperar os dados do incidente e ingerir Symantec incidentes DLP que correspondam aos critérios no perfil. Configure a programação para definir como e quando você extrai incidentes de Symantec.

Antes de Iniciar

Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa

Você pode planejar a frequência com que pesquisará incidentes futuros que correspondam à configuração do perfil de incidente. Para habilitar a ingestão automatizada de incidentes, você deve configurar a programação e a recuperação de incidentes antes de ativar o perfil. O perfil pode ser configurado para fazer uma recuperação única usando a caixa de seleção **Recuperação única**. A data histórica pode ser até os últimos três meses a partir da data atual.

O intervalo de pesquisa é configurado para cada perfil individualmente. Os diferentes intervalos de pesquisa podem afetar o desempenho da integração de incidentes do DLP Symantec. Ao programar, planeje equilibrar a carga do sistema em relação à urgência de um incidente.

Procedimento

1. Defina uma programação para recuperar dados e incluir incidentes que correspondam aos critérios no perfil.
2. No formulário, preencha os campos.

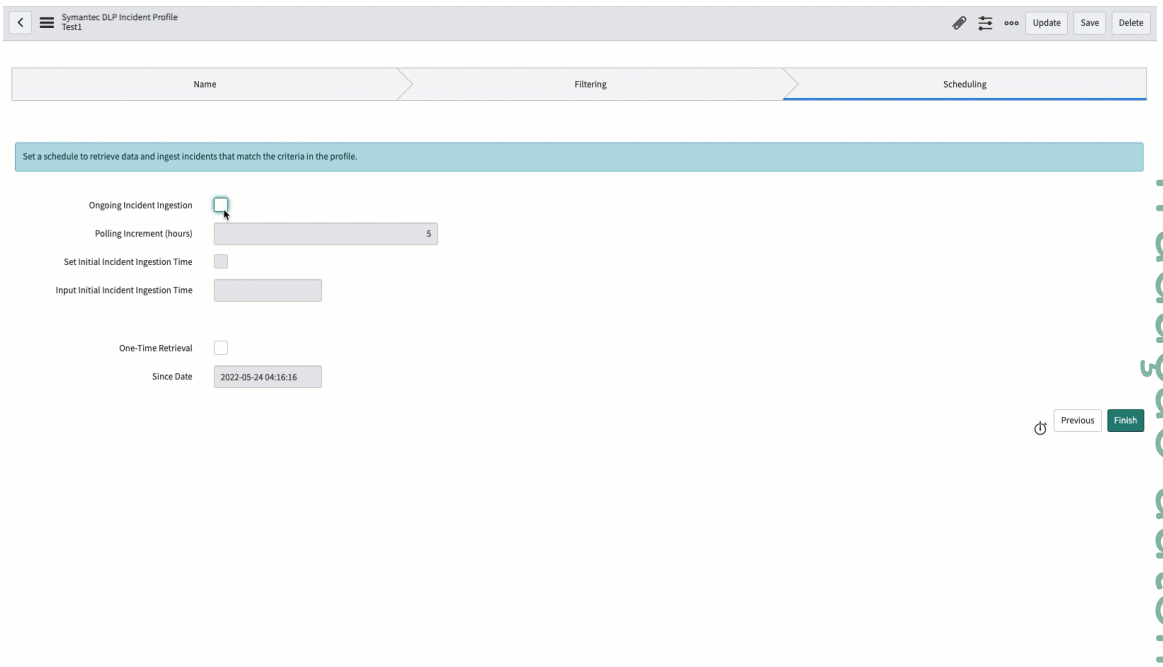
Programação do incidente do DLP

Campo	Descrição
Adição de incidentes em andamento	A ingestão de incidentes em andamento que a instância Now Platform extrai do Symantec para novos incidentes. Os incidentes do DLP serão criados se forem encontrados incidentes acionados e os critérios de filtragem de geração de incidentes corresponderem.
Incrementos de pesquisa (minutos)	A frequência de pesquisa que é definida em minutos. Este campo é definido automaticamente como 300 minutos.
Definir horário de adição do incidente inicial	Opção para definir uma data e hora para a ingestão inicial. As adições subsequentes são baseadas no período de intervalo de pesquisa.
Horário de entrada de adição do incidente inicial	Data e hora que você especifica para a ingestão de incidentes.
Horário de adição do incidente inicial	Primeira vez em que os dados são ingeridos. Você pode ver que os valores começam a aparecer quando o tempo de ingestão do incidente inicial é definido.
Horário de adição do próximo incidente (estimado)	Próximo período para uma ingestão de incidente estimada.
Recuperação Única	Opção para habilitar a extração única de dados históricos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Se este campo for selecionado, os dados históricos serão extraídos do Symantec DLP de acordo com a data adicionada ao campo **Desde a data**.
Desde a Data	Data a partir da qual os dados devem ser recuperados da Symantec. Este campo pode ser definido como no máximo três meses.



Tradução automática

3. Para salvar a configuração de perfil criada, clique em **Concluir** na janela pop-up.
4. Para ativar o perfil, abra o perfil criado.
5. Habilite a opção **Ativa**.
6. Clique em **Atualizar**.

Resultado

Após a criação e a ativação bem-sucedidas do perfil, os incidentes são recuperados periodicamente de acordo com a configuração definida no perfil e adicionados à tabela de incidentes do DLP.

Mapeamento de Symantec status de incidente DLP com ServiceNow status de incidente

Sincronize o status dos incidentes DLP ingeridos no ServiceNow com os incidentes DLP do Symantec. Mapeie o campo Status do **incidente da ServiceNow com o campo Status** do **incidente da Symantec**.

Antes de Iniciar

Função necessária: sn_dlir.admin

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Por Que e Quando Desempenhar Esta Tarefa

O status do incidente é recuperado dinamicamente da Origem do endpoint Symantec, que é adicionada ao mapeamento. Você precisa executar um mapeamento de status de incidente individual.

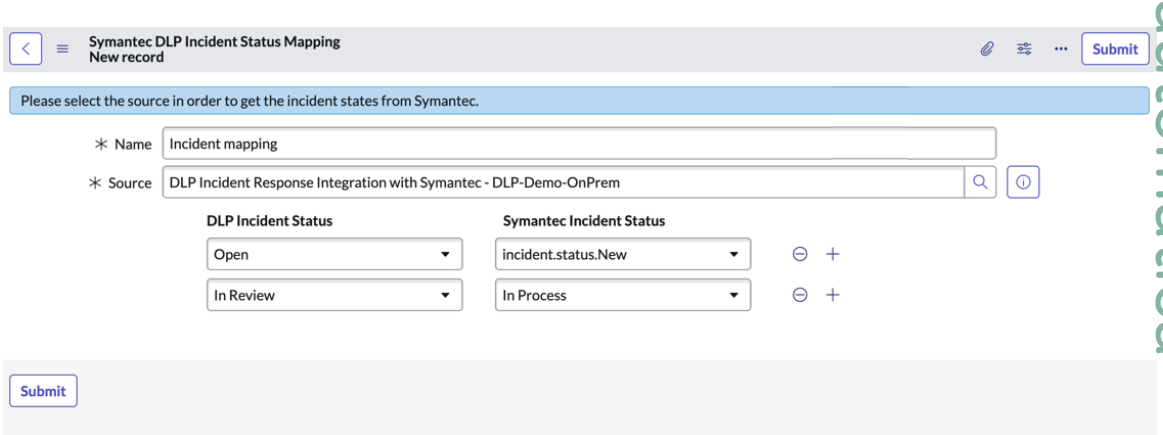
Procedimento

1. Navegar até **Integração do Symantec DLP** > **Mapeamento de status do incidente**.
2. Forneça um **Nome** para identificar o mapeamento.
3. Selecione a Integração de **origem** da qual você deseja buscar o status.
4. Mapeie o status de **incidente do DLP com o status** de **incidente do Symantec**.

Nota:
Não é necessário mapear todos os estados, você pode mapear somente os estados necessários.

Mapeamento de status de incidentes do Symantec DLP

Campo	Descrição
Nome	Nome do registro de mapeamento.
Origem	A origem do Symantec Endpoint configurada de onde você deseja buscar o status do incidente.
Status do incidente da DLP	Lista de status de incidentes do DLP.
Status do incidente da Symantec DLP	Lista de status buscada na origem (endpoint da Symantec).



5. Clique em **Enviar**.

Resultado

Depois de criar com sucesso o registro para mapear status dos ServiceNow incidentes, o status dos incidentes ServiceNow será sincronizado com o status dos incidentes do DLP Symantec.

Se você alterar o status de qualquer incidente do DLP na sua instância ServiceNow, o status dos incidentes do DLP Symantec associados será alterado na plataforma de origem Symantec com base no mapeamento definido no registro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapeamento de severidade entre incidentes do Symantec DLP com incidentes da ServiceNow

Use o recurso de mapeamento de severidade para configurar e sincronizar o mapeamento entre Symantec incidentes e Now Platform® incidentes.

Antes de Iniciar

Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa

O mapeamento de severidade do DLP permite mapear a severidade de origem com a severidade do incidente do DLP. Você pode personalizar e definir o valor de severidade de origem e mapeá-lo para o valor de severidade de incidente DLP desejado.

Procedimento

1. Navegar até **Integração do Symantec DLP** > **Mapeamento do incidente de gravidade**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

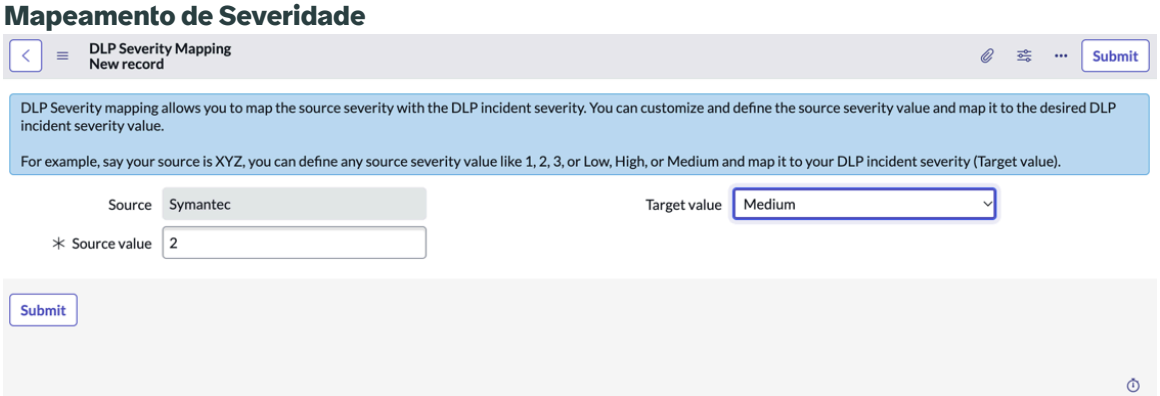
Mapeamento de severidade do DLP

Campo	Descrição
Origem	A origem do Symantec Endpoint configurada de onde você deseja buscar o incidente.
Valor de meta	O valor de meta é o ID de severidade do incidente do DLP. Os valores disponíveis são Crítico, Alto, Médio, Baixo e Informações (usadas como a gravidade das informações no Symantec).
Valor de Origem	O valor de origem é a severidade do incidente da Symantec.

Nota:
No sistema de base, há quatro mapeamentos de severidade que são enviados para os usuários do DLP.

4. Clique em **Enviar**.

Mapeamento de Severidade



Definir as configurações de integração do DLP Symantec

Modifique as propriedades do sistema padrão da Symantec integração DLP.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar

Função necessária: sn_dlir.admin

Procedimento

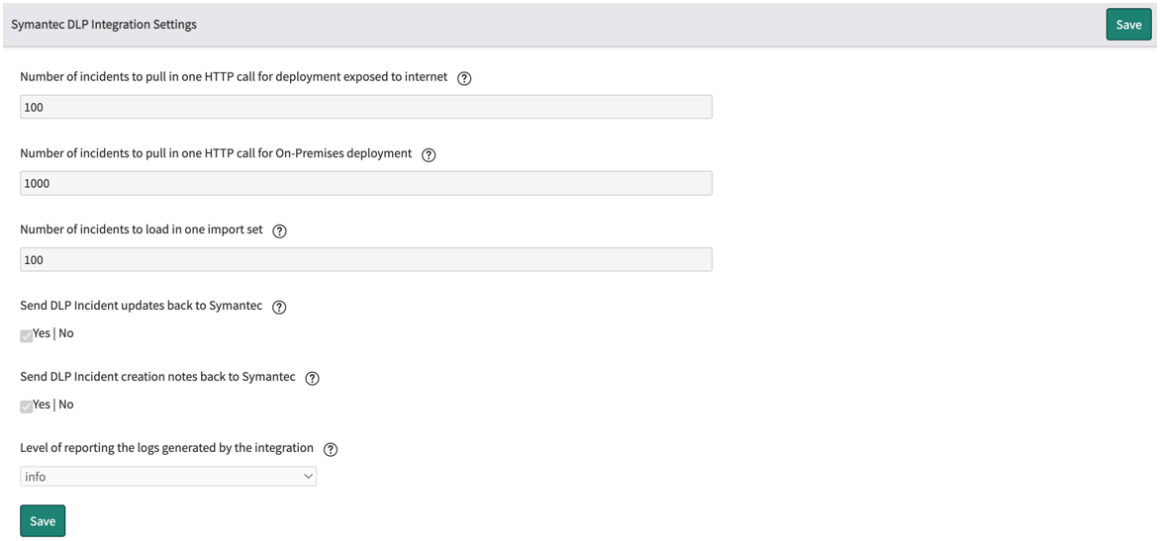
1. Navegar até **Integração da DLP da Symantec** > **Configurações**.
2. Modifique as configurações a seguir conforme necessário.

Configurações

Campo	Descrição
Impor um limite no número de incidentes a serem extraídos em uma chamada HTTP para implantação no local sn_sym_dlp.page_size_on_prem	Número máximo de incidentes a serem obtidos em uma chamada HTTP para implantação no local de Symantec. ○ Tipo: inteiro ○ Valor padrão: 1000
Impor um limite no número de incidentes a serem extraídos em uma chamada HTTP para implantação exposta na internet sn_sym_dlp.page_size_on_internet	Número máximo de incidentes a serem obtidos em uma chamada HTTP para implantação Symantec exposta na Internet. ○ Tipo: inteiro ○ Valor padrão: 100
Número de incidentes a serem carregados em um conjunto de importação sn_sym_dlp.incidents_per_attachment	Número de registros a serem armazenados em um arquivo de anexo para processamento. ○ Tipo: inteiro ○ Valor padrão: 100
Enviar atualizações de incidentes do DLP de volta para o Symantec sn_sym_dlp.incident_update	Esta propriedade permite restringir qualquer sincronização de estado entre ServiceNow e Symantec incidentes do DLP. ○ Tipo: booleano ○ Valor padrão: **verdadeiro**
Enviar anotações de criação de incidentes do DLP de volta para a Symantec sn_sym_dlp.incident_creation_notes	Esta propriedade permite que você envie uma anotação de volta para a Symantec assim que um incidente for criado em ServiceNow. ○ Tipo: booleano ○ Valor padrão: **verdadeiro**
Nível de relatório dos logs gerados pela integração sn_sym_dlp.logging.verbosity	Propriedade que define o relatório dos logs gerados pela integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.



3. Clique em **Salvar**.

Domain Separation na integração DLP Symantec

O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: Básico.

Como a separação de domínio funciona com a integração de DLP Symantec

Siga estas etapas para obter a separação de domínio:

- Crie um usuário com a função necessária no respectivo domínio.
- Execute os procedimentos de integração DLP Symantec no domínio apropriado.

Integração de resposta a incidentes de prevenção de perda de dados com Proofpoint

A integração DLP Proofpoint oferece suporte à ingestão de incidentes de Prevenção de perda de dados criados na implantação Proofpoint de Prevenção de perda de dados. Após a ingestão, você pode usar as funcionalidades de gerenciamento de incidentes para corrigir os incidentes do DLP.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Visão geral e principais recursos

A integração do DLP Proofpoint ajuda as empresas a rastrear o uso e a movimentação de dados confidenciais em várias plataformas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Esta integração inclui os seguintes recursos principais:

- Criação de vários perfis para diferentes endpoints Proofpoint.
- Automatizando a criação de incidentes do DLP.
- Mapeamento do campo de estado de incidente DLP Proofpoint para o campo de estado de incidente DLP.
- Filtragem de Proofpoint incidentes do DLP.
- Ingestão de incidentes em sua instância ServiceNow assim que os incidentes forem criados no Proofpoint locatário DLP.
- Proofpoint A integração do DLP oferece suporte a endpoints e tipos de incidentes de e-mail.
- Atualizações automáticas para o status do incidente DLP Proofpoint e comentários para a criação de incidente DLP e para mudança de estado e fechamento no lado ServiceNow.

Conheça esta integração

Identificador de documento	Título do documento
Proofpoint site da documentação do produto	Documentação do produto Proofpoint
ServiceNow® site da documentação do produto	Site de documentação do produto da ServiceNow

Introdução à integração Proofpoint para Prevenção de perda de dados

A integração de DLP Proofpoint oferece suporte à ingestão de incidentes de Prevenção de perda de dados criados no locatário Proofpoint de Prevenção de perda de dados. Após a ingestão, serão usadas as funcionalidades de gestão de incidentes que corrigem os incidentes do DLP.

Check-list

Revise as informações a seguir antes de começar a configurar sua integração DLP Proofpoint para Prevenção de perda de dados.

Check-list

Campo	Descrição
Verifique se você atribuiu as funções de aplicativo Now Platform e Data Loss Prevention Incident Response necessárias.	As funções a seguir são usadas na integração do DLP Proofpoint no Now Platform: • O administrador (admin) instala as aplicações do ServiceNow® Store e atribui o administrador de prevenção de perda de dados (sn_dlir.admin). • O usuário com a função sn_dlir.admin pode configurar a integração e configurar os perfis de incidente. • Os usuários com a função sn_dlir.analyst têm funções de leitura na integração.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Campo	Descrição
Atribua as funções de usuário DLP Proofpoint necessárias.	Analise as Proofpoint funções e permissões de integração do DLP.
Verifique se você está usando Proofpoint DLP 1.0.1 ou posterior.	A Proofpoint DLP integration for Data Loss Prevention foi testada com o Proofpoint Data Loss Prevention, versão 1.0.1 ou posterior.
Verifique se a aplicação principal do usuário final necessária para oferecer suporte à integração DLP Proofpoint está instalada e ativada.	Verifique se as seguintes aplicações DLP e aplicações comuns de suporte de segurança estão instaladas e ativadas na ServiceNow Store. Se não estiver instalado, instale e ative na aplicação. • Security Support Common • Data Loss Prevention Incident Response

Instalar e configurar a integração Proofpoint para Prevenção de perda de dados

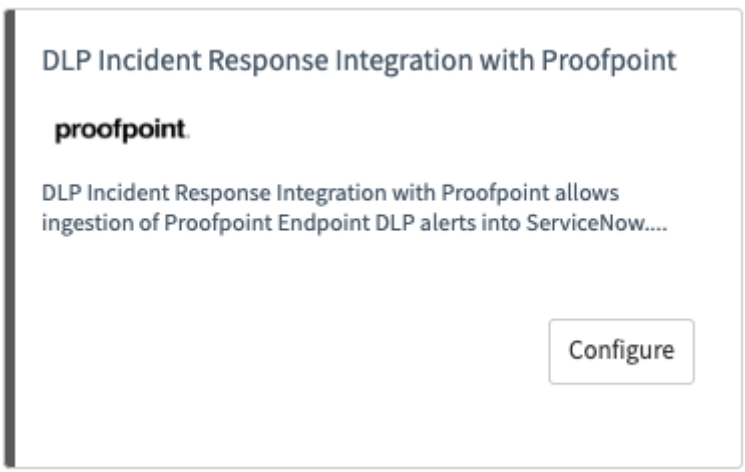
Instale e configure a integração DLP [Proofpoint do ServiceNow® Store na sua instância Now Platform. Comece a investigar incidentes do DLP usando os dados de incidentes do DLP Proofpoint.

Antes de Iniciar

Função necessária: sn_dlir.admin

Procedimento

1. Baixe a integração DLP [Proofpoint do ServiceNow® Store e instale-a.
2. Navegar até **Security Operations** > **Integrações** > **Configurações de Integração**.
3. Pesquise o bloco DLP Incident Response Integration with Proofpoint e clique em **Configurar**.



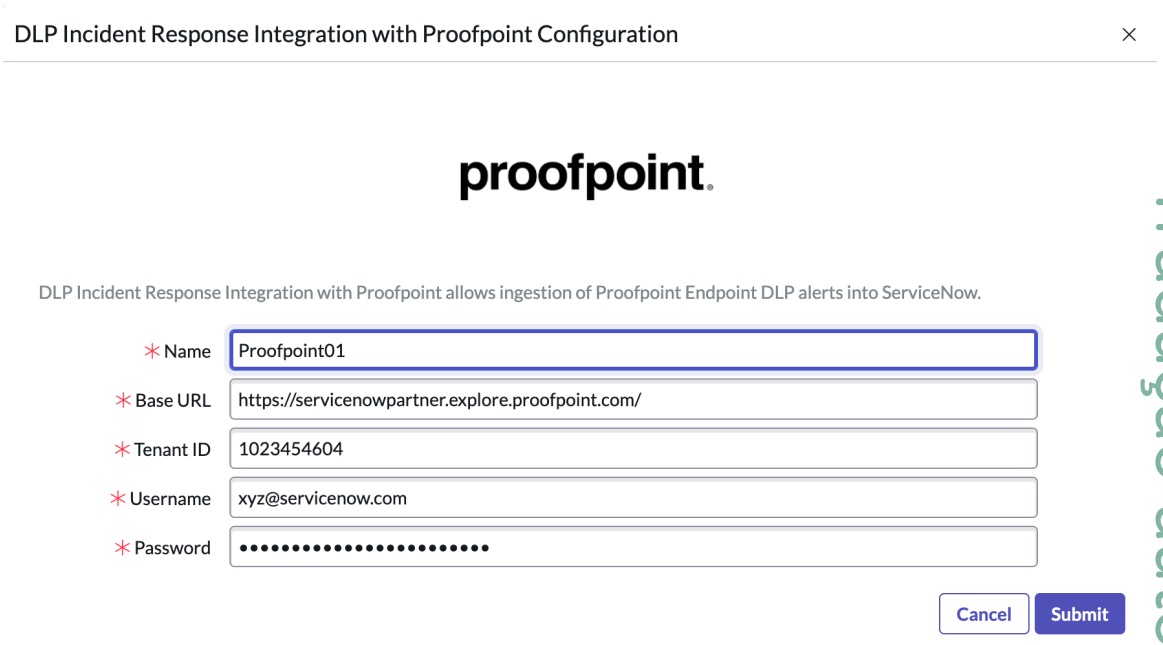
4. No formulário, preencha os campos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Proofpoint Formulário de configuração de integração do DLP

Campo	Descrição
Nome	Nome da configuração de integração do DLP Proofpoint.
URL base	URL do Proofpoint que serve como endpoint REST.
ID de locatário	O ID do locatário Proofpoint a ser usado.
Nome do usuário	Nome de usuário configurado para sua conta de usuário em Proofpoint.
Senha	Senha configurada para sua conta de usuário em Proofpoint.



5. Clique em **Enviar**.

Resultado
Depois de validar e enviar a configuração com sucesso, a Proofpoint Integração DLP é salva na página Integrações de segurança como um bloco.

Configure o Webhook no locatário do DLP Proofpoint para notificações de alerta para ServiceNow

Configure um webhook em Proofpoint usando o endpoint da REST API para começar a receber os alertas do Proofpoint locatário do DLP. Sua instância ServiceNow cria incidentes DLP a partir desses alertas. A integração DLP Proofpoint fornece um endpoint de REST API para que os usuários finais configurem o webhook.

Antes de Iniciar
Função necessária: sn_pp_dlp.api_integration_user

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Faça login no **Proofpoint**.
2. Navegar até **Locatário do Proofpoint** > **Aplicação de administração** > **Integração** > **Políticas de notificação**.
3. Crie uma política de notificação com um nome apropriado.
4. Clique na **política de notificação** e gerencie os webhooks configurados na política de notificação.
5. Crie uma nova configuração de webhook clicando em **Adicionar Webhooks**.
6. Selecione o tipo de webhook como **Genérico**.
7. Em Entrada de URL, insira uma URL usando o formato: `https://`<Instance_Name> .service-now.com/api/sn_pp_dlp/provapointalertapi/getalerts .
8. Mantenha o método como **POST**.
9. Adicione os seguintes cabeçalhos ao webhook:
   - ```
     Name: Authorization
     Value: Basic <Base64Encoded Username and Password of the ServiceNow instance user>
     ```
   - ```
     Name: Content-Type
     Value: application/json
     ```
10. D não mude os outros valores.
11. Clique em **Salvar**.
12. Navegar até **Locatário do Proofpoint** > **Aplicação de administração** > **Políticas** > **Regras**.
13. Na seção Ações, selecione as regras para as quais a notificação do webhook deve ser gerada.
14. Adicione as políticas de notificação recém-criadas que tenham um webhook configurado.
15. Clique em **Salvar**.

Criar um perfil para integração DLP Proofpoint

Crie um perfil de incidente na sua instância Now Platform. Determine os Proofpoint incidentes DLP que são adequados para criar incidentes DLP.

Antes de Iniciar

Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa

Configure o Now Platform para preencher alertas DLP de Proofpoint. Armazene os alertas como incidentes do DLP em sua instância ServiceNow.

Procedimento

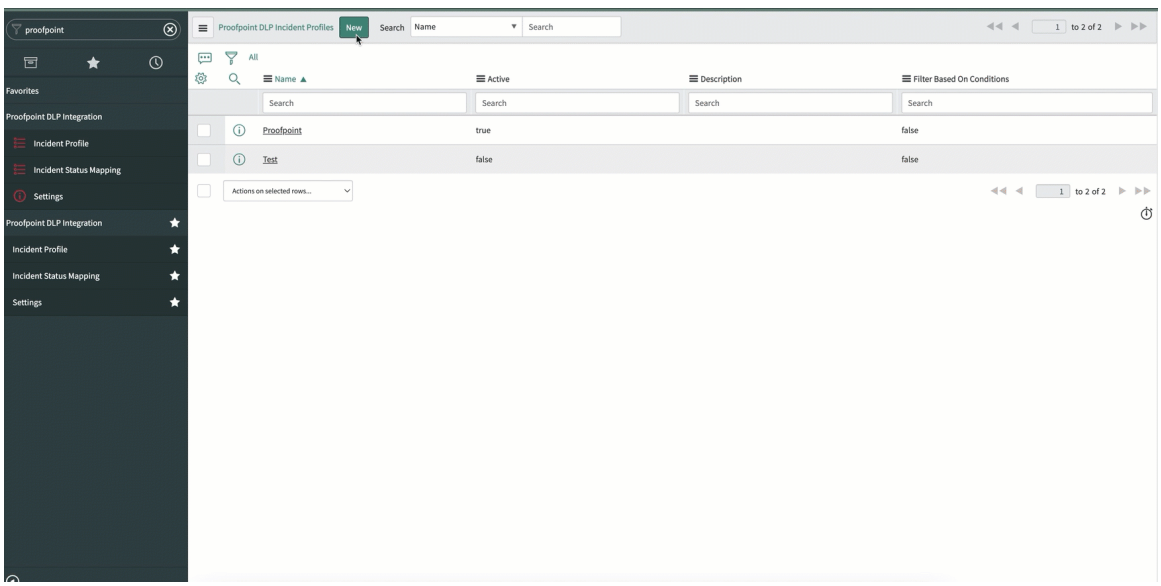
1. Navegar até **Integração com o Proofpoint do DLP** > **Perfil do incidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos na seção **Nome**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criar um perfil para o formulário de integração DLP Proofpoint

Campo	Descrição
Nome	Nome do perfil. Este nome ajuda a identificar o perfil. **Nota:** O nome deve ser exclusivo para cada perfil.
Origem	A instância Proofpoint do DLP que você configurou para ingerir incidentes. Se você tiver várias instâncias configuradas, selecione a instância apropriada para os tipos de incidentes que você planeja ingerir para o perfil.
Ativo	Opção para ativar o perfil. Quando o perfil está ativo, sua instância Now Platform está pronta para receber os incidentes de Proofpoint.
Descrição	Descrição para ajudar a distinguir este perfil de outros perfis.



4. Clique em **Continuar** e vá para a seção Filtragem.

Definir filtros a serem aplicados na criação do Incidente

Defina e defina condições de filtro para filtrar os Proofpoint incidentes DLP de entrada. Controle quais incidentes do DLP devem ser criados em ServiceNow®.

Antes de Iniciar

Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa

Este tipo de filtragem ajuda a isolar incidentes DLP e limitar o número de incidentes DLP que você cria. Se critérios de filtragem adicionais forem definidos, somente os incidentes que corresponderem às condições serão criados.

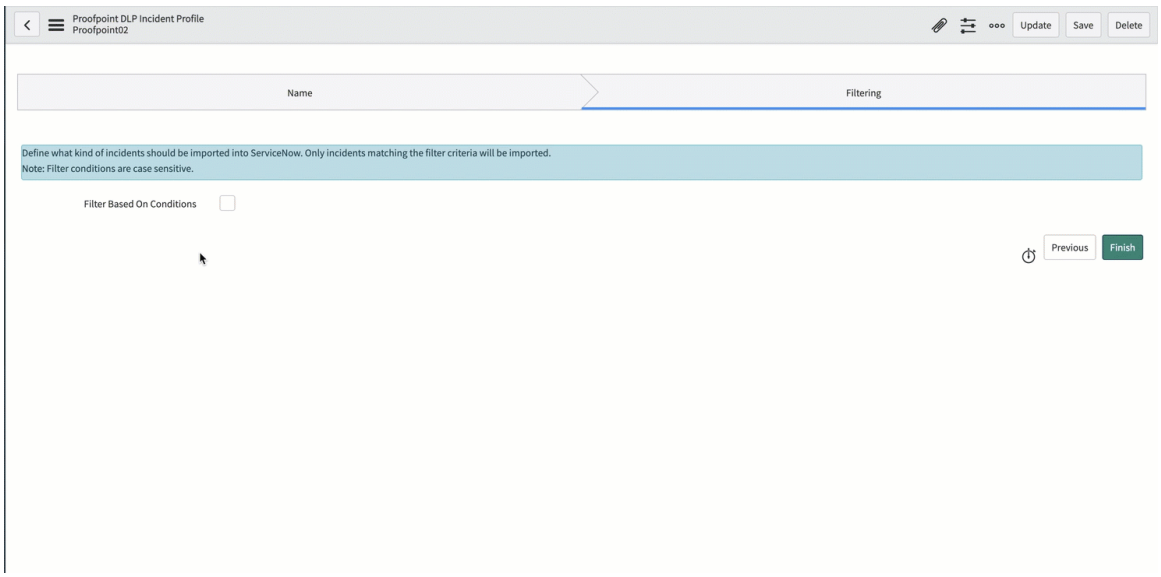
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Procedimento

1. Selecione a opção **Filtrar com base nas condições** e defina os critérios que um incidente DLP de entrada Proofpoint deve satisfazer para que um incidente de segurança seja criado.
2. Usando as listas e os campos do construtor de condição, defina os filtros no campo **Condições do filtro**.

   As opções no primeiro campo nas **Condições do filtro** correspondem aos campos que estão disponíveis no incidente do DLP. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas. Verifique se os critérios definidos correspondem aos valores do incidente.



3. Adicione mais condições clicando em **E**ou **OU**.
   - Se **AND**for selecionado, todas as condições deverão ser correspondidas.
   - Se **OU**for selecionado, qualquer uma das condições poderá ser correspondida.
4. Clique em **Concluir**.

Mapear Proofpoint status de incidentes do DLP com ServiceNow status de incidente

Sincronize o status dos incidentes DLP ingeridos em sua instância ServiceNow e os incidentes DLP de Proofpoint. Mapeie o status do incidente ServiceNow com o status do incidente Proofpoint.

Antes de Iniciar

Função necessária: sn_dlir.admin

Procedimento

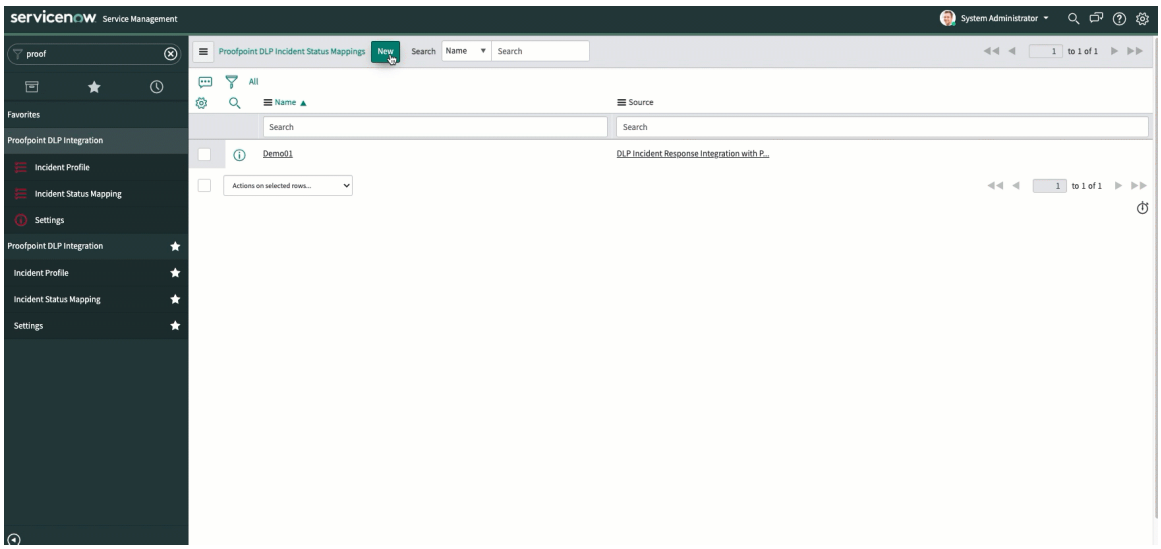
1. Navegar até **Integração com o Proofpoint do DLP** > **Incidente** > **Mapeamento do status do incidente**.
2. Forneça um **Nome** para identificar o mapeamento.
3. Selecione o bloco de **origem** (configuração de integração) para o qual o mapeamento de status deve ser aplicado.
4. Mapeie o status do **incidente do DLP da ServiceNow com o status** do incidente do **Proofpoint**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Mapear status de incidentes do Proofpoint do DLP com o formulário de status de incidente da ServiceNow

Campo	Descrição
Nome	Espaço reservado para o registro de mapeamento.
Origem	Origem de endpoint Proofpoint configurada da qual você deseja buscar o status do incidente.
Status do incidente da ServiceNow	Lista de status de incidentes do DLP.
Status de incidente do Proofpoint	Valores mapeados padrão para estados padrão disponíveis em incidentes do DLP. Para estados personalizados, o status Proofpoint padrão é **Novo**. Você pode modificar e adicionar o status Proofpoint necessário no campo de entrada.



5. Clique em **Enviar**.

Resultado

Um registro para mapeamento foi criado com sucesso. Os status dos ServiceNow incidentes serão sincronizados com Proofpoint incidentes DLP.

Quando você altera o status de qualquer incidente DLP na sua instância ServiceNow, o status do incidente DLP Proofpoint associado será alterado na plataforma de origem Proofpoint de acordo com o mapeamento definido no registro.

Definir Proofpoint configurações de integração DLP

Modifique as propriedades do sistema padrão da Proofpoint integração DLP.

Antes de Iniciar

Função necessária: sn_dlir.admin

Procedimento

1. Navegar até **Integração com o Proofpoint da DLP** > **Configurações**.
2. Modifique as configurações a seguir conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

3. Clique em **Salvar**.

Resultado
Suas configurações de integração modificadas são aplicadas no próximo intervalo de pesquisa, conforme definido no perfil.

Domain Separation em Proofpoint integração DLP

O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: Básico.

Como a separação de domínio funciona com a integração de DLP Proofpoint

Siga estas etapas para obter a separação de domínio:

- Crie um usuário com a função necessária no respectivo domínio.
- Execute os procedimentos de integração DLP Proofpoint no domínio apropriado.

Integração de resposta a incidentes de prevenção de perda de dados com Netskope

A integração DLP Netskope oferece suporte à ingestão de incidentes de Prevenção de perda de dados criados na implantação Netskope de Prevenção de perda de dados. Netskope O DLP ajuda as empresas a rastrear o uso e a movimentação de dados confidenciais em várias plataformas.

Após a ingestão, você pode usar as funcionalidades de gerenciamento de incidentes para corrigir os incidentes do DLP.

Principais recursos

Esta integração inclui os seguintes recursos principais:

- Criação de vários perfis para diferentes endpoints Netskope.
- Automatizando a criação de incidentes DLP de Netskope alertas DLP.
- Filtragem de Netskope alertas do DLP.
- Ingestão programada de incidentes DLP que criam incidentes DLP.
- Notificação por e-mail para o usuário na expiração da credencial Netskope.

Introdução à integração de DLP Netskope para Prevenção de perda de dados

Revise as informações a seguir antes de começar a configurar sua integração DLP Netskope para Prevenção de perda de dados.

Instalar e configurar a integração DLP Netskope para Prevenção de perda de dados

Instale e configure a integração DLP Netskope] da instância [ServiceNowServiceNow StoreNow Platform . Você pode começar a investigar incidentes do DLP usando os dados de incidentes do DLP Netskope.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Antes de Iniciar
Função necessária: sn_dlir.admin

Procedimento

1. Baixe a integração DLP [Netskope do ServiceNow ServiceNow Store e instale-a.
2. Navegue até **Security Operations** > **Integrações** > **Configurações de Integração**
3. Pesquise o bloco DLP Incident Response Integration with Netskope e clique em **Configurar**.
4. No formulário, preencha os campos.

Campo	Descrição
Nome	Nome da configuração de integração do DLP Netskope.
URL de endpoint	URL da instância Netskope que serve como endpoint REST.
Token	Token configurado para REST API v2 em sua conta de usuário em Netskope.

5. Clique em **Enviar**.

Resultado
Depois de validar e enviar a configuração com sucesso, a Netskope Integração DLP é salva na página Integrações de segurança como um bloco.

Criar um perfil para integração DLP Netskope

Crie um perfil de incidente na sua instância Now Platform. Determine os Netskope Alertas do DLP que são adequados para criar incidentes do DLP.

Antes de Iniciar
Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa
Configure a plataforma Now Platform para recuperar os incidentes DLP do endpoint Netskope. Armazene os incidentes em sua instância ServiceNow como incidentes DLP.

Procedimento

1. Navegar até **Netskope DLP integration** > **Perfil do incidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos.

Criar um perfil

Campo	Descrição
Nome	Nome do perfil. O nome deve ser exclusivo para cada perfil. Este nome ajuda a identificar o perfil.
Origem	Netskope Instância do DLP que você configurou para ingerir incidentes. Se você tiver várias instâncias configuradas, selecione a instância

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	apropriada para os tipos de incidentes que você planeja ingerir para o perfil.
Ativo	Indicador de que o perfil está ativo. **Nota:** Este campo está disponível somente depois de clicar em **Concluir** na última seção Programação. Quando o perfil está ativo, sua instância Now Platform está pesquisando ativamente Netskope incidentes do DLP. Os incidentes correspondentes do DLP são criados no DLIR quando as condições de filtragem são correspondidas com base nos parâmetros de programação fornecidos.
Ordem	Ordem de execução do perfil. O perfil com a ordem mais baixa considerada como a prioridade mais alta. Por padrão, o valor é 100.
Descrição	Descrição para ajudar a distinguir este perfil de outros perfis.

4. Clique em **Continuar** e vá para a seção Filtragem.

Definir filtros a serem aplicados na criação do incidente

Defina e defina condições de filtro para filtrar os Netskope incidentes DLP de entrada. Controle quais desses incidentes devem ser criados como incidentes DLP em sua instância ServiceNow.

Antes de Iniciar
Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa
Este tipo de filtragem ajuda a isolar incidentes DLP e limitar o número de incidentes DLP que você cria. Se critérios de filtragem adicionais forem definidos, somente os incidentes que corresponderem às condições serão criados.

Procedimento

1. Selecione a opção **Filtrar com base nas condições** e defina os critérios que um incidente DLP de entrada Netskope deve satisfazer para que um incidente de segurança seja criado.
2. Usando as listas e os campos do construtor de condição, defina os filtros no campo **Condições do filtro**.

   As opções no primeiro campo nas **Condições do filtro** correspondem aos campos disponíveis no incidente do DLP. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas. Verifique se os critérios definidos correspondem aos valores do incidente.
3. Adicione mais condições clicando em **E**ou **OU**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Se **AND**for selecionado, todas as condições deverão ser correspondidas.
- Se **OU**for selecionado, qualquer uma das condições poderá ser correspondida.

4. Clique em **Continuar** e vá para a seção Programação.

Programar a Netskope recuperação de alertas de prevenção de perda de dados

Defina uma programação para recuperar os dados de alertas e ingerir Netskope incidentes DLP que correspondam aos critérios no perfil.

Antes de Iniciar
Função necessária: sn_dlir.admin

Por Que e Quando Desempenhar Esta Tarefa
Você pode planejar a frequência com que pesquisará incidentes futuros que correspondam à configuração do perfil de incidente. Para habilitar a ingestão automatizada de incidentes, você deve configurar a programação e a recuperação de incidentes antes de ativar o perfil. O perfil pode ser configurado para fazer uma recuperação única usando a caixa de seleção **Recuperação única**. A data histórica pode ser de até três meses do passado.

O intervalo de pesquisa é configurado para cada perfil individualmente. Os diferentes intervalos de pesquisa podem afetar o desempenho da integração de incidentes do DLP Netskope. Ao programar, planeje equilibrar a carga do sistema em relação à urgência de um incidente.

Procedimento

1. Configure a programação para definir como e quando você extrai alertas de Netskope.
2. No formulário, preencha os campos.

Programar os Netskope alertas do DLP

Campo	Descrição
Adição de incidentes em andamento	Ingestão de incidentes em andamento que sua instância Now Platform extrai de Netskope para novos incidentes. Se houver alertas acionados encontrados, que correspondam aos critérios de filtragem de incidentes, os incidentes do DLP serão criados.
Incremento de pesquisa (horas)	Frequência de pesquisa definida em horas. Este campo é definido automaticamente como **5**.
Definir horário de adição do incidente inicial	Opção para definir a ingestão de incidente inicial com base na data e hora configuradas. Você pode usar esta opção para definir uma data e hora específicas para a ingestão inicial. As adições subsequentes são baseadas no período de intervalo de pesquisa.
Horário de entrada de adição do incidente inicial	Data e hora que você especifica para a ingestão de incidentes.
Horário de adição do incidente inicial	A primeira vez em que os dados são ingeridos.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	Nota: O valor ficará visível somente se a opção **Definir tempo de ingestão do incidente inicial** estiver selecionada.
Horário de adição do próximo incidente (estimado)	O próximo tempo estimado de adição de incidente.
Recuperação Única	Opção para habilitar a extração única de dados históricos. **Nota:** Se selecionado, os dados históricos serão extraídos do Netskope DLP de acordo com a data adicionada em **Desde a data**.
Desde a Data	Data de quando os dados são obtidos de Netskope. **Nota:** No máximo, os últimos três meses de dados podem ser obtidos de Netskope.

3. Clique em **Concluir**.
4. No pop-up, salve a configuração de perfil criada clicando em **Concluir**.
5. Ative o perfil.
   a. Abra o perfil criado.
   b. Defina **Ativo** como **verdadeiro**.
   c. Clique em **Atualizar**.

Resultado
Após a ativação bem-sucedida da criação do perfil, os alertas serão obtidos periodicamente de acordo com a configuração definida no perfil. Os alertas serão adicionados à tabela de incidentes do DLP.

Definir Netskope configurações de integração DLP

Modifique as propriedades do sistema padrão da Netskope integração DLP.

Antes de Iniciar
Função necessária: sn_dlir.admin

Procedimento
1. Navegar até **Integração do Netskope DLP** > **Configurações**.
2. Modifique as configurações a seguir conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Definir Netskope configurações de integração DLP

Campo	Descrição
Impor um limite no número de incidentes a serem extraídos em uma chamada HTTP do Netskope sn_ns_dlp.page_size	Tempo limite máximo para chamadas HTTP, em segundos. Este campo é definido automaticamente como **30**.
Nível de relatório dos logs gerados pela integração sn_ns_dlp.logging.verbosity	Defina o nível de logs de relatório gerados pela integração. Este campo é definido automaticamente como **info**.

3. Clique em **Salvar**.

Resultado

Suas configurações de integração modificadas são aplicadas no próximo intervalo de pesquisa, conforme definido no perfil.

Notificações para usuários sobre a expiração da credencial

O token Netskope pode ser válido por até 12 meses para REST-API v2. Quando o token usado na instância ServiceNow expira, Netskope envia uma notificação por e-mail para usuários com a função de administrador do DLP (sn_dlir.admin).

Depois que a configuração da integração for concluída, forneça a função de administrador do DLP (sn_dlir.admin) aos usuários que devem ser notificados se o token expirar.

Se o token expirar, a ingestão de dados para os perfis associados ficará em espera até que o tíquete seja atualizado com um token válido.

Você deve criar um token ou renovar o antigo em Netskopee atualizar o token na instância ServiceNow. Se você renovar o token estendendo o tempo de expiração, a aplicação Netskope detectará automaticamente a renovação e continuará com a coleta de dados. Se você criar um token, deverá atualizar o token na configuração.

Domain Separation em Netskope integração DLP

O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: Básico.

Como a separação de domínio funciona com a integração de DLP Netskope

Siga estas etapas para obter a separação de domínio:

- Crie um usuário com a função necessária no respectivo domínio.
- Execute os procedimentos de integração DLP Netskope no domínio apropriado.

Data Loss Prevention Incident Response com Microsoft

O Data Loss Prevention Incident Response com Microsoft fornece uma estrutura principal para importar incidentes de Prevenção de perda de dados (DLP) de várias fontes, como Microsoft aplicações de alcance (Microsoft Teams, Exchange Online, SharePoint Online, OneDrive for Business). Os dispositivos de endpoint permitem um fluxo de trabalho de correção

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

que envolve usuários finais, gerentes e a equipe de operações do DLP com atribuição e escalações de incidentes automatizadas.

Solicitar aplicativos na Store

Acesse o site ServiceNow Store para ver todos os aplicativos disponíveis e obter informações sobre como enviar solicitações para a loja. Para obter informações sobre notas de versão cumulativa para todos os aplicativos liberados, consulte as ServiceNow Store notas de versão do histórico de versão .

Principais recursos

Use os principais recursos desta integração para realizar as seguintes ações:

- Crie vários perfis para contas diferentes.
- Automatize a criação de DLP IR incidentes.
- Mapeie os campos de evento [Microsoft DLP IR para campos de incidente DLP IR.
- Filtrar Microsoft DLP IR eventos.
- Programe a ingestão de DLP IR eventos que criam DLP IR incidentes periodicamente.
- Armazene o conteúdo correspondente de cada evento DLP da Microsoft em armazenamento em nuvem externa.
- Exclua o conteúdo correspondente no armazenamento em nuvem externa após a exclusão do incidente [DLP IR em ServiceNow.
- Baixe arquivos para DLP IR incidentes do tipo Exchange, OneDrive e SharePoint.

Conheça esta integração

Identificador de documento	Título do documento
Microsoft site da documentação do produto	Site de documentação do produto Microsoft
ServiceNow site da documentação do produto	Site de documentação do produto da ServiceNow

Introdução à integração do Microsoft DLP IR para prevenção de perda de dados

Revise as informações a seguir antes de começar a configurar sua integração Microsoft DLP IR para prevenção de perda de dados.

Check-list

Configuração de tarefa	Descrição
Obtenha as credenciais do Microsoft Purview para buscar os dados do evento e as credenciais da conta de armazenamento do AWS/Azure para armazenar o conteúdo de correspondência Registrar uma aplicação com a plataforma de identidade da Microsoft	Registre uma aplicação na plataforma Microsoft Azure aqui para obter o ID do cliente, o segredo do cliente e o ID do locatário. Para obter informações sobre as funções necessárias para criar uma aplicação, consulte Pré -requisitos. Para obter informações sobre as permissões/funções de API necessárias em uma aplicação do Microsoft Azure para configurá-la na ServiceNow integração do Microsoft DLP, consulte a tabela a seguir.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Check-list

Configuração de tarefa	Descrição
Permissões necessárias para que o usuário do Azure obtenha o acesso de leitura/gravação/exclusão do blob no armazenamento do Azure	O usuário do Azure deve ter a função **de colaborador de dados de blob de armazenamento** para ler, gravar e excluir blobs no armazenamento do Azure.
Permissões necessárias para que o usuário da AWS obtenha o acesso de leitura/gravação/exclusão de objeto no armazenamento da AWS	Deve ser criada uma política que forneça acesso de lista, leitura, gravação e exclusão para o objeto no armazenamento AWS S3.
Atribua e verifique se você tem as funções necessárias para Now Platform e as funções de administração de perda de dados.	As funções a seguir são necessárias para configuração e verificação dos resultados esperados: • A função de administrador instala a integração do ServiceNow Store e atribui a função sn_dlir.admin. • A função sn_dlir.admin executa as seguintes tarefas: ◦ Configura a integração. ◦ Configura os perfis de incidentes.
Verifique se as aplicações principais ServiceNow necessárias para oferecer suporte à integração do Microsoft DLP IR estão instaladas e ativadas antes de configurar esta integração.	Verifique se as seguintes DLP IR aplicações e aplicações comuns de suporte de segurança estão instaladas e ativadas na ServiceNow Store. Se não estiver instalado, instale e ative na aplicação. • Security Support Common • Data Loss Prevention Incident Response

Permissões/funções de API necessárias em uma aplicação do Microsoft Azure

Você precisa das seguintes permissões/funções de API em uma aplicação do Microsoft Azure para configurá-la na* ServiceNow *integração do Microsoft DLP.

API	Nome da permissão	Tipo	Descrição	Necessário para qual funcionalidade da ServiceNow?	O consentimento do administrador é necessário?
API de gestão do Office 365	FeedDeAtividade.Ler.Dlp	Aplicação	Ler eventos de política do DLP, incluindo dados confidenciais detectados.	Para ingerir os eventos DLP do escopo da MSFT para ServiceNow. **Nota:** Esta permissão é obrigatória para obter os dados da MSFT em ServiceNow.	Sim

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Permissões/funções de API necessárias em uma aplicação do Microsoft Azure
Você precisa das seguintes permissões/funções de API em uma aplicação do Microsoft Azure para configurá-la na **ServiceNow** *integração do Microsoft DLP.*

API	Nome da permissão	Tipo	Descrição	Necessário para qual funcionalidade da ServiceNow?	O consentimento do administrador é necessário?
API do Microsoft Graph	Arquivos.Leitura.Todos	Aplicação	Leia arquivos em todos os conjuntos de sites que você pode acessar.	Baixar arquivo: para baixar o anexo na instância da ServiceNow que causou o evento DLP do OneDrive ou do SharePoint **Nota:** Isso é opcional. Você pode ignorar esta permissão de API se não quiser permitir que os analistas baixem o anexo que causou o evento DLP.	Sim
	E-mail.Lido	Aplicação	Ler e-mails em todas as caixas de correio.	Baixar arquivo: para baixar o conteúdo do e-mail (corpo e anexo) na instância da ServiceNow que causou o evento DLP do Exchange. **Nota:** Isso é opcional. Você pode ignorar esta permissão de API se não quiser permitir que os analistas baixem o conteúdo de e-mail (corpo, anexo) que causou o evento DLP.	Sim
	User.Read	Delegado	Entre e leia o perfil do usuário.	Esta é a permissão padrão que estará disponível para todas as novas aplicações.	Não

Informações confidenciais detectadas (opcional)

O conteúdo de correspondência é armazenado externamente no armazenamento de blob do Azure ou no bucket do Amazon S3 e será extraído do armazenamento externo quando o usuário exibir um incidente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Qualquer uma das permissões a seguir será necessária se os usuários quiserem exibir a correspondência de conteúdo/informações confidenciais detectadas na aplicação DLP Core:

1. Se você for um usuário Microsoft Azure, deverá ter a função de colaborador de dados de blob de armazenamento para ler, gravar e excluir blobs no armazenamento do Azure.
2. Se você for um usuário do Amazon S3, deverá criar uma política que forneça acesso de lista, leitura, gravação e exclusão para o objeto no armazenamento do Amazon S3.

Instalar e configurar a integração do Microsoft DLP

Instale e configure a integração do DLP Incident Response com Microsoft DLP do ServiceNow® Store na sua instância Now Platform. Comece a investigar incidentes do DLP usando os dados de evento do DLP Microsoft.

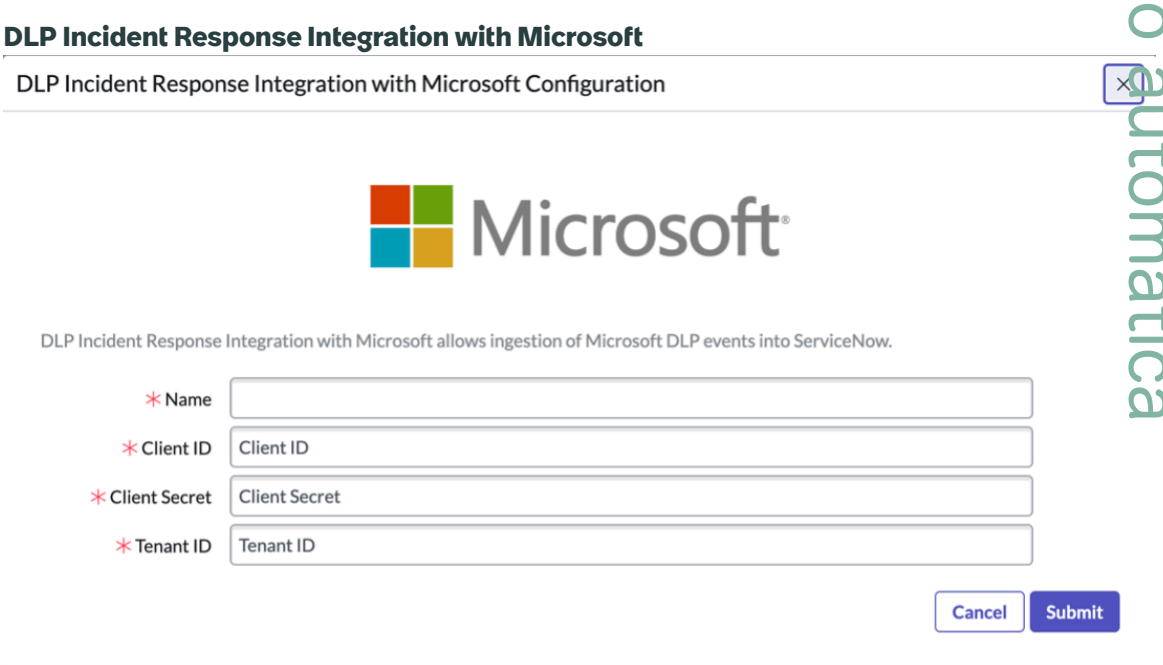
Antes de Iniciar

Função necessária: sn_dlir.admin

Procedimento

1. Baixe a integração DLP [Microsoft do ServiceNow® Store e instale-a.
2. Navegar até **Security Operations** > **Integrações** > **Configurações de Integração**.
3. Configure a integração do DLP Microsoft.

   a. Pesquise o bloco **DLP Incident Response Integration with Microsoft** e clique em **Configurar**.



   b. No formulário, preencha os campos.

Formulário de configuração de integração do Microsoft DLP

Campo	Descrição
Nome	Nome da configuração de integração do DLP Microsoft.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
ID de cliente	ID de cliente do app criado no portal do Microsoft Azure.
Segredo do Cliente	Segredo do cliente do app criado no portal do Microsoft Azure.
ID de locatário	ID de locatário do usuário.

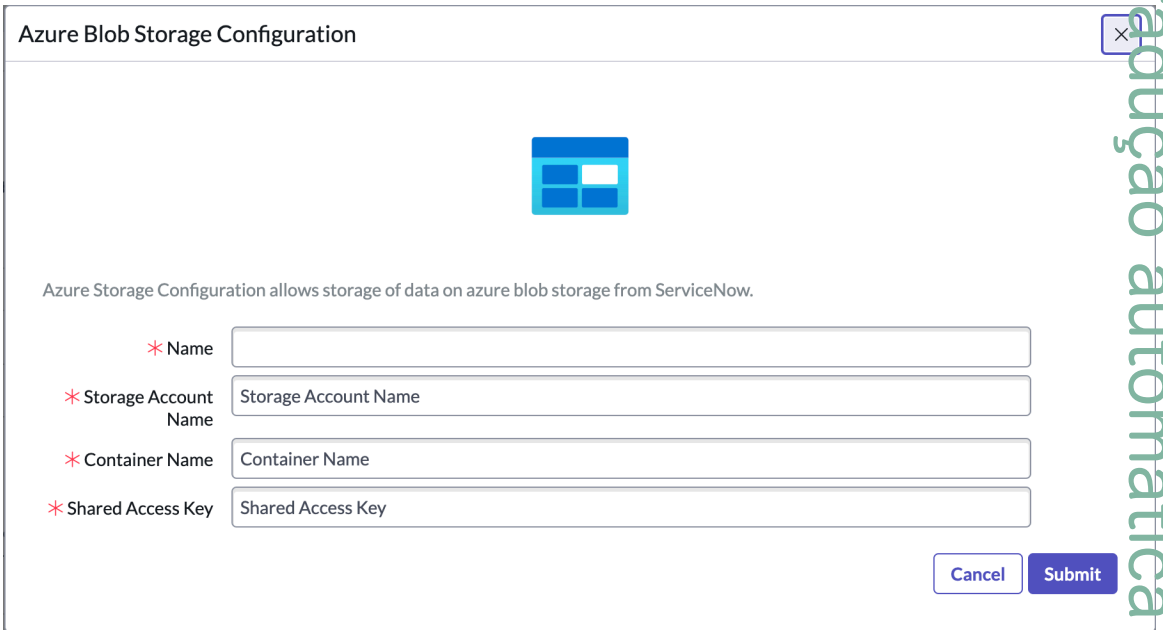
c. Clique em **Enviar**.

Depois de validar e enviar a configuração com sucesso, a Microsoft Integração DLP é salva na página Integrações de segurança como um bloco.

4. Atualize a configuração de armazenamento do Azure.

a. Na página Integrações de segurança, pesquise o bloco **Configuração de armazenamento do Azure**.

b. No bloco Configuração de armazenamento do Azure, clique em **Atualizar**.



Tradução automática

c. No formulário, preencha os campos.

Formulário de configuração de armazenamento do Azure

Campo	Descrição
Nome	Nome da configuração de armazenamento do Azure.
Nome da conta de armazenamento	Nome da conta de armazenamento criada no portal do Azure
Nome do contêiner	Nome do contêiner criado na conta de armazenamento no portal do Azure.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Chave de acesso compartilhada	Chave de acesso compartilhada para a conta de armazenamento.

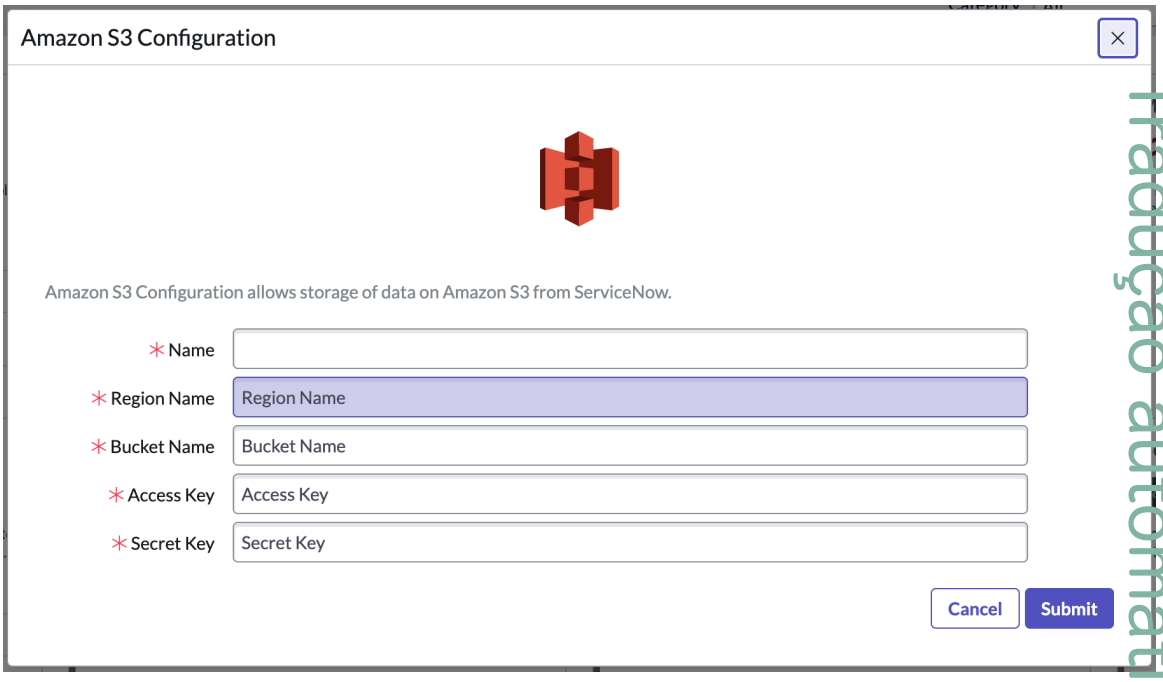
d. Clique em **Enviar**.

Depois de validar e enviar a configuração com sucesso, a configuração de armazenamento do Azure será salva na página Integrações de segurança como um bloco.

5. Atualize a configuração de armazenamento da AWS.

a. Na página Integrações de segurança, pesquise o bloco **Configuração de armazenamento da AWS**.

b. No bloco Configuração de armazenamento da AWS, clique em **Atualizar**.



Tradução automática

c. No formulário, preencha os campos.

Formulário de configuração de armazenamento da AWS

Campo	Descrição
Nome	Nome da configuração de armazenamento da AWS.
Nome da região	Nome da região da conta de armazenamento da AWS.
Nome do Bucket	Nome do bucket criado no portal da AWS.
Chave de acesso	Chave de acesso com acesso de leitura, gravação e exclusão.
Chave Secreta	Chave compartilhada com acesso de leitura, gravação e exclusão

d. Clique em **Enviar**.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Resultado
Depois de validar e enviar a configuração com sucesso, a configuração do AWS S3 será salva na página Integrações de segurança como um bloco.

Criar um novo perfil de incidente para integração DLP Microsoft

Crie um perfil de incidente em sua instância Now Platform para recuperar os dados do Microsoft Purview e adicionar os dados à tabela de incidentes ServiceNow DLP IR.

Antes de Iniciar
Função necessária: sn_dlir.admin (criar, editar e excluir)

sn_dlir.analyst - Exibir (somente leitura)

Por Que e Quando Desempenhar Esta Tarefa
Configure o Now Platform® para recuperar os eventos do campo Microsoft. Armazene esses eventos na tabela Incidente DLP IR em sua instância ServiceNow®.

Procedimento
1. Navegar até **Integração do Microsoft DLP** > **Perfil do incidente**.
2. Clique em **Nova**.
3. No formulário, preencha os campos na seção Nome.

Criar um formulário de perfil

Campo	Descrição
Nome	Nome do perfil. Este campo ajuda a identificar o perfil. **Nota:** O nome deve ser exclusivo para cada perfil.
Origem	A instância Microsoft DLP IR que você configurou para ingerir incidentes. Se você tiver várias configurações de integração, selecione o registro de configuração de integração apropriado para os tipos de incidente que você planeja ingerir para o perfil.
Ativo	Opção para indicar se o perfil está ativo. Este campo só pode ser habilitado depois de clicar no campo **Concluir** na seção Programação. Quando o perfil está ativo, isso implica que o Now Platform está pesquisando ativamente Microsoft DLP IR eventos com base na configuração definida no perfil.
Ordem	Ordem de execução do perfil. O perfil com a ordem mais baixa considerada como a prioridade mais alta. Por padrão, o valor é 100.
Descrição	Descrição exclusiva do perfil.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O que Fazer Depois
Para mover para a seção Filtragem, clique em **Continuar**.

Definir filtros a serem aplicados na criação do Incidente

Defina e defina condições de filtro para filtrar os eventos de entrada do Microsoft DLP. Controle quais desses eventos devem ser criados como DLP IR incidentes em sua instância ServiceNow.

Antes de Iniciar
Função necessária: sn_dlir.admin (criar, editar e excluir)

sn_dlir.analyst - Exibir (somente leitura)

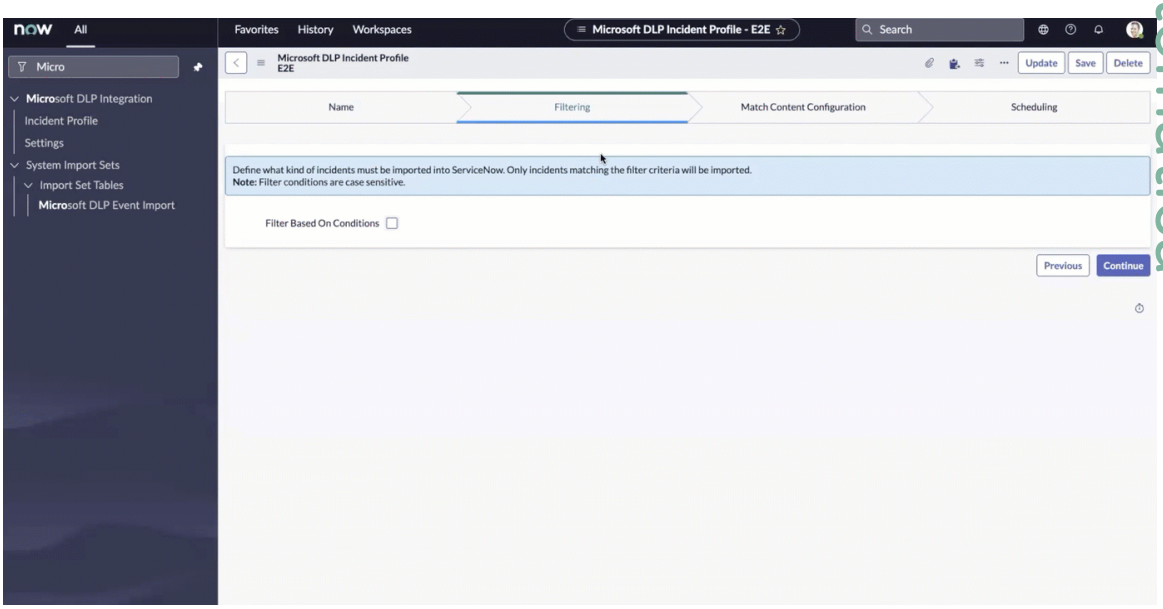
Por Que e Quando Desempenhar Esta Tarefa
Este tipo de filtragem ajuda a isolar os eventos DLP da Microsoft para limitar o número de DLP IR incidentes que você cria. Se o critério de filtragem estiver definido, somente os eventos que corresponderem às condições serão criados como incidentes do DLP.

Procedimento

1. Selecione a opção **Filtrar com base nas condições**.
2. Usando as listas e os campos do construtor de condição, defina os filtros no campo **Condições do filtro**.

   Defina os critérios que um evento DLP de entrada Microsoft deve satisfazer para que um incidente DLP seja criado.

   As opções no primeiro campo nas **Condições do filtro** correspondem aos campos disponíveis no evento Microsoft DLP. Os critérios inseridos fazem distinção entre maiúsculas e minúsculas. Verifique se os critérios definidos correspondem aos valores do evento.



3. Adicione mais condições clicando em **E**ou **OU**.
   - Se **AND**for selecionado, todas as condições deverão ser correspondidas.
   - Se **OU**for selecionado, qualquer uma das condições poderá ser correspondida.
4. Clique em **Continuar** e vá para a seção Corresponder configuração de conteúdo.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurar a correspondência de conteúdo para o incidente

Forneça a configuração para armazenar as informações confidenciais no armazenamento em nuvem externa, como o armazenamento do Azure ou o bucket do AWS S3, para recuperar esse conteúdo em uma carga ao acessar o incidente de IR do DLP.

Antes de Iniciar

Função necessária: sn_dlir.admin (criar, editar e excluir)

sn_dlir.analyst - Exibir (somente leitura)

Procedimento

1. Na barra de andamento, clique na etapa **Corresponder configuração de conteúdo**.
2. No formulário, preencha os campos.

Corresponder configuração de conteúdo

Campo	Descrição
Armazenar conteúdo de correspondência	Opção para armazenar o conteúdo correspondente no armazenamento em nuvem. **Importante:** Se esta opção não for selecionada, o conteúdo de correspondência de política para incidentes do DLP não poderá ser visto no espaço do DLP. Habilitar esta opção garante que o conteúdo correspondente retornado nos incidentes do DLP seja armazenado no armazenamento em nuvem externo (por exemplo, Azure, AWS). Você também pode recuperar e exibir o conteúdo de correspondência sempre que um incidente DLP for aberto no espaço. Para obter informações sobre a configuração do armazenamento em nuvem externo, consulte Instalar e configurar a integração do Microsoft DLP.
Excluir conteúdo de correspondência na exclusão de incidente	Opção para excluir o conteúdo de correspondência de incidente do armazenamento em nuvem externa. Esta opção está visível somente quando o campo **Armazenar conteúdo de correspondência** está selecionado.
Credenciais externas de nuvem	O armazenamento em nuvem externo em que o conteúdo de correspondência é armazenado. Você pode consultar as Credenciais de nuvem externas adicionadas para a configuração de armazenamento. Esta opção está visível somente quando o campo **Armazenar conteúdo de correspondência** está selecionado.

3. Clique em **Continuar** e vá para a seção Programação.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Programar a DLP IR recuperação de incidente da Microsoft

Defina uma programação para recuperar os dados do incidente e ingerir Microsoft DLP IR incidentes que correspondam aos critérios no perfil. Configure a programação para definir como e quando você extrai incidentes de Microsoft.

Antes de Iniciar

Função necessária: sn_dlir.admin (criar, editar e excluir)

sn_dlir.analyst - Exibir (somente leitura)

Por Que e Quando Desempenhar Esta Tarefa

Você pode planejar a frequência com que pesquisará incidentes futuros que correspondam à configuração do perfil de incidente. Para habilitar a ingestão automatizada de incidentes, você deve configurar a programação e a recuperação de incidentes antes de ativar o perfil. O perfil pode ser configurado para fazer uma recuperação única usando a caixa de seleção **Recuperação única**. A data histórica pode ser até os últimos três meses a partir da data atual.

O intervalo de pesquisa é configurado para cada perfil individualmente. Os diferentes intervalos de pesquisa podem afetar o desempenho da integração de incidente Microsoft DLP IR. Ao programar, planeje equilibrar a carga do sistema em relação à urgência de um incidente.

Procedimento

1. Defina uma programação para recuperar dados e incluir incidentes que correspondam aos critérios no perfil.
2. No formulário, preencha os campos.

Programação do formulário de incidente do DLP

Campo	Descrição
Adição de incidentes em andamento	A ingestão de incidentes em andamento que a instância Now Platform extrai da Microsoft para novos incidentes. DLP IR incidentes serão criados se incidentes acionados forem encontrados e os critérios de filtragem de geração de incidentes corresponderem.
Incrementos de pesquisa (minutos)	A frequência de pesquisa da Microsoft. Este campo é definido automaticamente como 300 minutos.
Definir horário de adição do incidente inicial	Opção para definir uma data e hora para a ingestão inicial. As adições subsequentes são baseadas no período de intervalo de pesquisa. Esta opção está visível somente quando o campo **Ingestão de incidente em andamento** está selecionado.
Horário de entrada de adição do incidente inicial	Data e hora que você especifica para a ingestão de incidentes.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
	○ Se o valor for definido, a recuperação de dados da Microsoft começará a partir da data futura adicionada. ○ Este campo fica visível somente quando **Definir tempo de ingestão inicial** é selecionado.
Horário de adição do incidente inicial	Primeira vez em que os dados são ingeridos. Você pode ver que os valores começam a aparecer quando o tempo de ingestão do incidente inicial é definido.
Horário de adição do próximo incidente (estimado)	O próximo período para uma ingestão de incidente estimada.
Recuperação Única	Opção para habilitar extrações de dados históricos únicas. Se este campo for selecionado, os dados históricos serão extraídos da Microsoft DLP IR de acordo com a data adicionada ao campo **Desde a data**.
Desde a Data	Data a partir da qual os dados devem ser recuperados da Microsoft. Este campo pode ser definido para um máximo de 7 dias.

3. Salve a configuração de perfil criada clicando em **Concluir** na janela pop-up.
4. Ative o perfil.
   a. Abra o perfil criado.
   b. Habilite a opção **Ativo**.
   c. Clique em **Atualizar**.

Resultado
Após a criação e a ativação bem-sucedidas do perfil, os incidentes são recuperados periodicamente de acordo com a configuração definida no perfil e adicionados à tabela de incidentes do DLP.

Definir configurações de integração do Microsoft DLP IR

Modifique as propriedades do sistema padrão de integração Microsoft DLP IR.

Antes de Iniciar
Função necessária: sn_dlir.admin

Procedimento
1. Navegar até **Integração Microsoft com DLP** > **Configurações**.
2. Modifique as propriedades a seguir conforme necessário.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Configurações de integração do Microsoft DLP

Campo	Descrição
Tempo limite máximo para chamadas HTTP (sn_pp_dlp.maximum_http_time_out)	Tempo limite máximo para chamadas HTTP (em segundos). ○ Tipo: inteiro ○ Valor padrão: 30
Nível de relatório dos logs gerados pela integração (sn_pp_dlp.logging.verbosity)	O nível de logs de relatório gerados pela integração, ou seja, o nome do tipo de informação. Você também pode atualizar o valor para as seguintes opções: ○ **error** ○ **aviso** ○ **informações** ○ **depurar** ○ **desativado** Por padrão, o valor é **info**.
Destino do relatório dos logs gerados pela integração (sn_pp_dlp.logging.destination)	O destino dos logs gerados pela integração. Você também pode atualizar o valor para as seguintes opções: ○ **banco de dados** ○ **arquivo** ○ **nenhum** Por padrão, o valor é **db**.

3. Clique em **Salvar**.

Resultado

Suas configurações de integração modificadas são aplicadas no próximo intervalo de pesquisa, conforme definido no perfil.

Solicitar e-mail de liberação da quarentena

Use este recurso para liberar o e-mail que está em quarentena no portal de conformidade do Microsoft Purview.

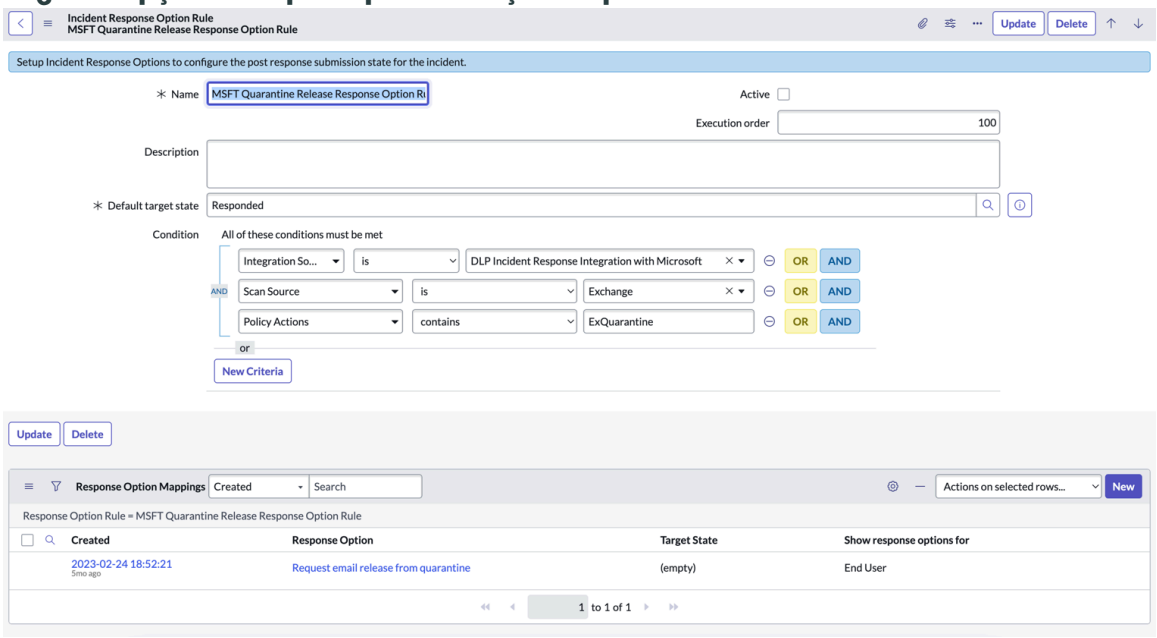
Antes de Iniciar

Por padrão, o sistema de base fornece a opção de resposta **Solicitar liberação de e-mail da quarentena** e a **Regra de opção de resposta de liberação da quarentena da MSFT** para liberar o e-mail da quarentena. Este registro padrão também tem a **Regra de aprovação para liberação da quarentena** configurada com ele para aproveitar a funcionalidade de aprovação para esta ação. Para obter mais informações, consulte Configurar regras de opção de resposta do incidente para seus incidentes do DLP, Configure a opção de resposta para seus incidentes do DLP e Configurar regras de aprovação.

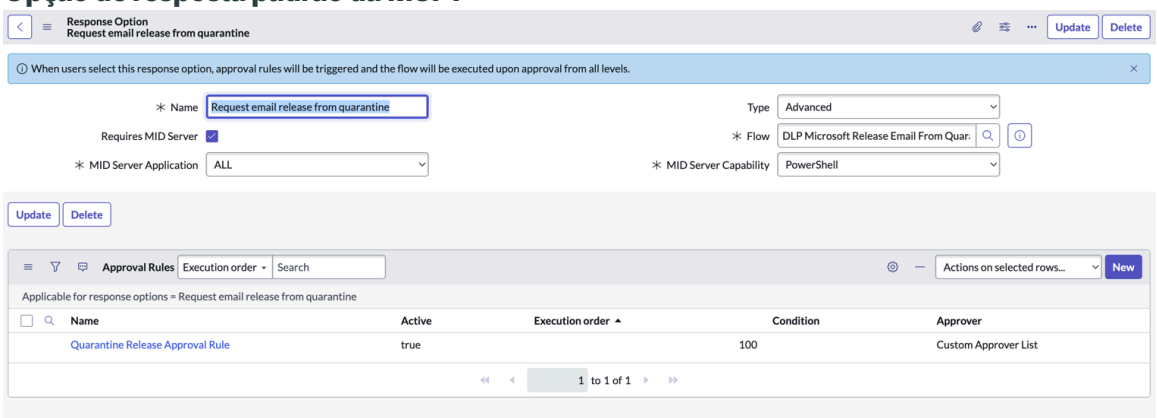
Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Regra de opção de resposta para liberação da quarentena da MSFT



Opção de resposta padrão da MSFT



Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Se você estiver usando esta opção de resposta, verifique se o MID Server está instalado e funcionando com o recurso PowerShell. Se um MID Server não estiver instalado e em execução e não tiver o recurso PowerShell, o usuário final não poderá selecionar **Solicitar liberação de e-mail da ação de quarentena** no espaço Usuários do DLP. Para obter mais informações, consulte Configurar regras de opção de resposta do incidente para seus incidentes do DLP e Configure a opção de resposta para seus incidentes do DLP.

- Se você quiser um MID Server específico da lista, será necessário configurar o app MID e torná-lo visível na lista e, em seguida, pelo menos um MID Server configurado deve estar instalado e funcionando a partir dos aplicativos MID selecionados e deve ter o Capacidade do Power Shell.
- Para usar a opção Liberar da quarentena, você precisa de permissões de API. Na página de permissões de API da Microsoft, verifique **Exchange Online do Office 365** > **Exchange.GerenciarComoApp** está listado e contém os seguintes valores:
  - ▪ **Tipo**: **Aplicação**.
  - ▪ **Consentimento do administrador necessário**: **Sim**.
  - ▪ **Status**: o valor incorreto atual é **Não concedido para** <Organization> para a entrada **Office 365 Exchange Online** > **Exchange.ManageAsApp** e altere o valor do status. Para obter mais etapas sobre as permissões de API, consulte Atribuir permissões de API à aplicação no site de documentação da Microsoft.

    Nota:
    Esta etapa é necessária para se conectar ao Exchange Online usando o princípio de serviço.

- Você também deve precisar da função de **administrador de segurança** no princípio do serviço,
  - Pesquise **as funções do Microsoft Entra ID e os administradores** no portal do Microsoft Azure, adicione a atribuição ao app registrado (princípio do serviço) e siga o procedimento explicado na documentação da Microsoft sobre como atribuir uma função .
- Esta opção é aplicável somente para incidentes do Microsoft Exchange que têm a opção **de ação de política** como **ExQuarantine** na exibição do formulário de incidente.

Função necessária: usuário final

O procedimento a seguir explica como enviar esta ação do espaço do usuário do DLP.

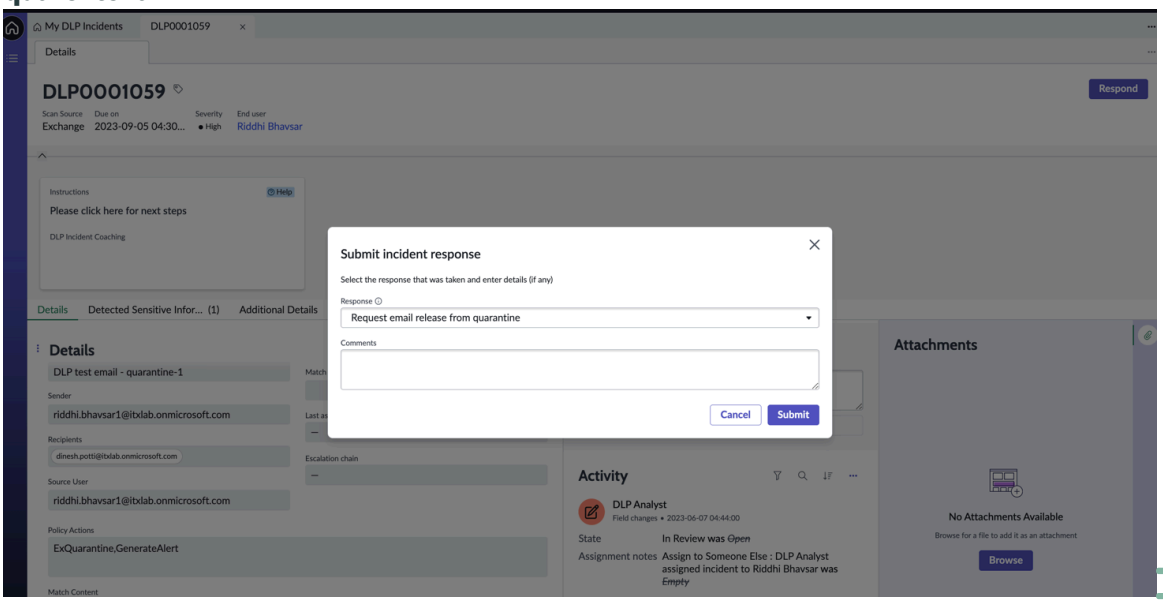
Procedimento

1. Navegar até **DLP** > **Espaço do usuário do DLP**.
2. Abra qualquer incidente do Microsoft Exchange DLP.
   Verifique se a **ação da política de** incidente está definida como ExQuarantine.
3. Clique **em Responder**.
4. Selecione a opção **Solicitar e-mail de liberação da quarentena** na lista suspensa Resposta.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Enviar resposta do incidente - Solicitar liberação de e-mail da opção de quarentena



5. Clique em **Enviar**.

> **Nota:**
> Quando uma regra de aprovação estiver configurada para esta ação, o fluxo de aprovação será acionado primeiro e, depois de receber todas as aprovações, o fluxo Solicitar liberação de e-mail da quarentena será acionado e o e-mail será liberado da quarentena. O estado do incidente DLP será atualizado para **Liberado da quarentena** após a liberação bem-sucedida.

Baixar arquivos para incidentes do DLP do tipo Exchange Online, OneDrive e SharePoint

Baixe arquivos ou e-mail que violem a política DLP no Microsoft Purview. Baixe este arquivo ou envie um e-mail para sua máquina local na exibição DLP IR Incidente. Você pode baixar os arquivos para DLP IR incidentes do tipo Origem de verificação Exchange Online, OneDrive e SharePoint.

Antes de Iniciar

Função necessária:

- sn_dlir.admin, sn_dlir.analyst
- Qualquer aprovador válido

Procedimento

1. Navegar até **Todos** > **Gestão de incidentes do DLP** > **Espaço do analista do DLP**.
2. Abre um registro de incidente DLP do tipo Origem de verificação Exchange Online, OneDrive ou SharePoint que é ingerido da origem da Microsoft.
3. Clique **em Baixar arquivo**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

O arquivo ou e-mail que violou a política DLP no lado do escopo da Microsoft será baixado para a máquina local do usuário.

Nota:
O administrador do DLP pode controlar o acesso da ação **Baixar arquivo** desabilitando a configuração **Deve ser permitido baixar o arquivo violador do incidente relatado** na página Configurações avançadas. Para obter mais informações, consulte Definir configurações avançadas para Data Loss Prevention Incident Response.

Domain Separation na integração de DLP Microsoft

O Domain Separation permite separar dados, processos e tarefas administrativas em agrupamentos lógicos chamados de domínios. Você pode então controlar vários aspectos dessa separação, incluindo quais usuários podem ver e acessar os dados.

Nível de suporte

Suporte: Básico.

Como a separação de domínio funciona com a integração de DLP Microsoft

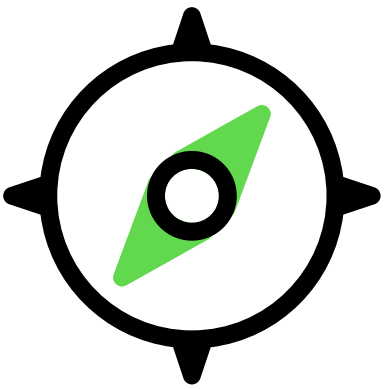
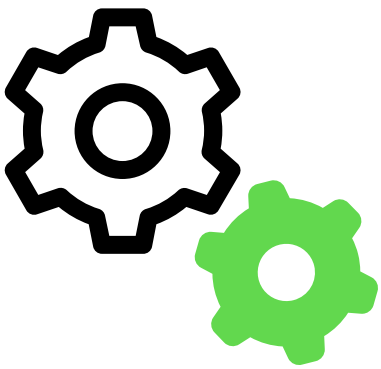
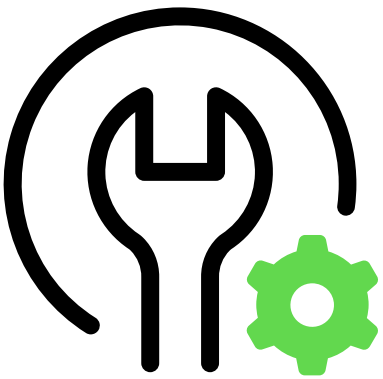
Siga estas etapas para obter a separação de domínio:

- Crie um usuário com a função necessária no respectivo domínio.
- Execute os procedimentos de integração DLP Microsoft no domínio apropriado.

Lista de materiais de software

Exiba uma lista dos componentes de software de código aberto e de terceiros que você está usando no desenvolvimento de aplicações. Obtenha informações sobre licenças de software, informações de versão e vulnerabilidades conhecidas em seus componentes nos arquivos da Lista de materiais de software (SBOM) que você carrega em sua instância.

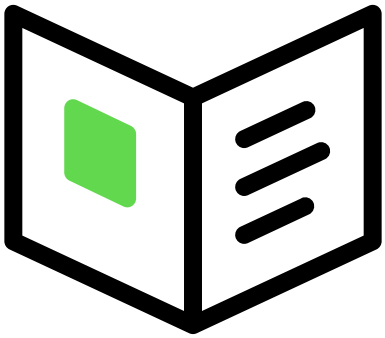
Primeiros passos

Explorar	Configurar	Usar
		
Saiba mais sobre SBOM conceitos e recursos.	Configure aplicações SBOM.	Saiba como importar componentes SBOM e exibir dados no espaço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Referência



Veja os detalhes sobre SBOM formulários, campos, tabelas e propriedades.

Solucionar problemas e obter ajuda

- CycloneDX - Lista de materiais de software (SBOM)
- Pesquise artigos de erros conhecidos no portal de erros conhecidos
- Contato Suporte e atendimento ao cliente

Explorar o Lista de materiais de software

Identifique os componentes usados nas aplicações da sua organização de arquivos Lista de materiais de software (SBOM) que você carrega em sua instância. Entenda todos os riscos associados ao uso de software de código aberto para ajudá-lo a determinar sua possível exposição e corrigir vulnerabilidades.

Disponível Lista de materiais de software versões

Versão de lançamento	Notas de versão
Modelo de dados para SBOM v1.3, v1.1, v1.0	Para obter informações de compatibilidade, consulte KB0856498 Matriz de compatibilidade do Vulnerability Response e Mudanças no esquema de versão Application Vulnerability Response release notes
SBOM Núcleo v2.1, v2.0, v1.0	
SBOM Resposta v3.1, v3.0, v2.0	

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Caso de uso do SBOM

Componentes de terceiros e de código aberto oferecem muitas vantagens para a criação e o lançamento rápidos de seus projetos de software. No entanto, em alguns casos, há riscos associados ao uso de componentes acessíveis publicamente, como o seguinte:

- Falta de visibilidade da integridade do componente
- Vulnerabilidades no software
- Conformidade de licenciamento

Três aplicações Lista de materiais de software permitem que você exiba um inventário preciso dos componentes de software:

- Modelo de dados para SBOM
- SBOM Núcleo
- SBOM Resposta

Você pode carregar sua lista de materiais de software por meio de uma API ou manualmente. Exiba os arquivos importados como entidades, que são inventários das bibliotecas de componentes de terceiros usadas em seu software, incluindo quaisquer dependências transitivas. Para obter mais informações sobre o que está incluído nos inventários de software nos SBOMs do CycloneDX, consulte CycloneDX - Software Bill of Materials (SBOM) .

Modelo de dados para SBOM

Esta aplicação fornece as tabelas usadas para armazenar dados de SBOM.

SBOM Núcleo

Carregue, analise e processe seus arquivos de lista de materiais de software no formato CycloneDXJSON em sua instância Now Platform®. Exiba entidades de lista de materiais (BOM) e um inventário de seus componentes de software. Uma entidade da lista de materiais é o componente de nível raiz em um arquivo SBOM. Por exemplo, para um SBOM do CycloneDX, o componente listado nos metadados é considerado a entidade da lista de materiais.

SBOM Resposta

Exiba seu inventário de componentes e avalie sua exposição ao risco no espaço do SBOM. Você pode identificar se alguma vulnerabilidade conhecida está associada a componentes de software e exibir informações de licenciamento e versão junto com outros detalhes.

Consulte a tabela a seguir para obter mais informações sobre cada aplicação ServiceNow® SBOM.

Aplicações necessárias para SBOM

ServiceNow aplicativo	Descrição
Modelo de dados para SBOM	Esta aplicação é necessária. Ele inclui as tabelas, ACLs e funções que são necessárias para ler dados SBOM.
SBOM **Núcleo**	Esta aplicação é necessária. Inclui a API necessária para carregar SBOM documentos e a lógica de negócios necessária

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicações necessárias para SBOM

ServiceNow aplicativo	Descrição
	para analisar e importar os dados desses documentos para sua instância. A partir da v2.1, você pode exibir um inventário dos componentes de software no espaço do SBOM.
SBOM **Resposta**	A aplicação Vulnerability Response será necessária se você instalar a aplicação SBOM Response. Instale o Vulnerability Response antes de instalar o SBOM Response. Exiba seu inventário de componentes e avalie sua exposição ao risco no espaço do SBOM. Configure regras para criar itens vulneráveis de aplicação (AVITs) automaticamente e corrigi-los com o fluxo de trabalho do Application Vulnerability Response. As integrações OSV.dev e Deps.dev são incluídas ao instalar o SBOM Response. • OSV.dev é uma API de código aberto que fornece informações de inteligência de vulnerabilidade para uma determinada versão de um pacote ou biblioteca. • Deps.dev é uma API de código aberto que fornece uma lista de versões para um determinado pacote ou biblioteca.

A instalação de inteligência de vulnerabilidade de terceiros compatível e outras integrações permite que você exiba as contagens de componentes considerados obsoletos e abandonados, bem como informações sobre se é possível corrigir vulnerabilidades associadas aos componentes. As aplicações ServiceNow® e integrações de terceiros listadas na tabela a seguir são compatíveis com a aplicação SBOM. Essas aplicações fornecem dados de vulnerabilidade aprimorados, inteligência de vulnerabilidade e outras informações importantes que podem ajudá-lo a exibir e priorizar as vulnerabilidades associadas aos arquivos SBOM. Todas essas aplicações e integrações estão disponíveis na ServiceNow Store.

Outras aplicações compatíveis com SBOM

Aplicação	Descrição
Vulnerability Response	Obrigatório se você instalar a aplicação de resposta SBOM. Os recursos do Application Vulnerability Response são instalados com o Vulnerability Response. Esses recursos permitem o acesso ao espaço do Vulnerability Manager na aplicação Vulnerability Response e ao fluxo de trabalho de vulnerabilidade para ajudá-lo a corrigir itens vulneráveis da aplicação (AVITs). Fornece acesso ao banco de dados nacional de vulnerabilidades (NVD), enumeração de pontos fracos comuns (CWE) e dados de vulnerabilidade de aplicações de terceiros.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Outras aplicações compatíveis com SBOM

Aplicação	Descrição
Trabalhos programados do Vulnerability Response Integration with NVD e CWE	Exiba dados aprimorados de vulnerabilidade e severidade do NVD. Se você instalou o SBOM Response, poderá exibir os dados importados das integrações de NVD e CWE para aprimorar todos os dados de vulnerabilidade encontrados em seus dados de SBOM. Para obter mais informações, consulte Importação de dados com as integrações de NVD e CWE e gestão de bibliotecas de terceiros.
Integração de vulnerabilidade da Veracode	Importe listas de materiais de software de arquivos com Veracode Vulnerability Integration. Se você já tem esta integração instalada, também pode carregar dados Veracode SBOM importados no formato CycloneDX JSON.

Instalar as aplicações compatíveis para Lista de materiais de software

Baixe e ative as aplicações necessárias para a aplicação Lista de materiais de software (SBOM) antes de carregar arquivos.

Antes de Iniciar

Funções necessárias: administrador para download, instalação e ativação de todas as aplicações e atribuições de função em sua instância.

Por Que e Quando Desempenhar Esta Tarefa

Procedimento

1. Baixe as aplicações [SBOM necessárias da instância ServiceNow Store para sua instância ServiceNow.

   Essas aplicações permitem que você carregue e importe arquivos SBOM para sua instância. Você pode exibir os dados do componente no espaço do SBOM começando com a v2.1 do SBOM Core.

   - Modelo de dados para SBOM
   - SBOM Núcleo

   Para obter mais informações sobre como baixar e ativar aplicações, consulte o seguinte:

   - Security Operations e a ServiceNow Store
   - Baixe uma aplicação de ServiceNow Store pela primeira vez

2. **Opcional:** Se você quiser exibir seus dados [SBOM no espaço SBOM, exibir informações de vulnerabilidade de terceiros importadas, avaliar sua exposição a riscos e corrigir vulnerabilidades com os fluxos de trabalho do Application Vulnerability Response e Vulnerability Response, baixe os seguintes aplicativos:

   - Vulnerability Response e suas dependências
   - Vulnerability Response Integration with NVD
   - SBOM Resposta

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações sobre essas e outras aplicações SBOM compatíveis, consulte Explorar o Lista de materiais de software.

3. Depois de baixar as aplicações, navegue até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos**.
4. Localize as aplicações SBOM que você baixou e selecione **Instalar** para ativá-las junto com suas dependências.

   Uma mensagem é exibida depois que uma aplicação é ativada com sucesso. Ative as aplicações na seguinte ordem:

   - Vulnerability Response e suas dependências
   - Vulnerability Response Integration with NVD
   - Modelo de dados para SBOM
   - SBOM Núcleo
   - SBOM Resposta, que inclui as integrações OSV.dev e Deps.dev

   Se instalada, a integração Deps.dev é ativada (caixa de seleção Ativa marcada no registro de integração) por padrão e programada para ser executada semanalmente. Você pode editar a programação e iniciar o trabalho programado sob demanda a partir do registro de integração. Navegar até **Todos** > **Vulnerability Response** > **Integrações** > **Integração Deps.dev**. A função sn_vul.app_configure_integrations é necessária para editar a programação desta integração.

   A integração Deps.dev é usada para identificar componentes que estão nos estados **Obsoleto** e **Abandonado**. A versão de um componente obsoleto está mais de duas versões principais atrás da versão mais recente e dois anos atrás da versão mais recente. Um componente abandonado não é atualizado há mais de dois anos. Os limites de dois anos e duas versões podem ser editados com as propriedades do sistema. Para editar esses parâmetros, navegue até **Todos** > **Propriedades do sistema** > **Todas as Propriedades** e localize os seguintes registros:

   - sn_sbom_resp.pkg_abandoned_threshold
   - sn_sbom_resp.pkg_stale_threshold
   - sn_sbom_resp.pkg_stale_version_threshold

   Os valores de limite para abandonados e obsoletos estão em meses. O valor limite da versão é numérico.

   Se instalada, a integração OSV.dev será ativada (caixa de seleção Ativa marcada no registro de integração) por padrão. No entanto, você deve iniciá-la sob demanda a partir do registro de integração. Navegar até **Todos** > **Vulnerability Response** > **Integrações** > **Integração OSV.dev - Abrangente**. A função sn_vul.app_configure_integrations é necessária para editar a programação desta integração.

   Nota:
   Você pode configurar o parâmetro de integração `batchSize` do OSV.dev na integração de vulnerabilidades de código aberto. O padrão é 75 PURLs por chamada de API.

5. **Opcional:** Ative integrações navegando até **Todos** > **Aplicações do sistema** > **Todas as aplicações disponíveis** > **Todos** e selecionando **Instalar**.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

(Optional) Para obter mais informações sobre essas integrações e os recursos que elas fornecem, consulte Explorar o Lista de materiais de software.

- Vulnerability Response Integration with Veracode. Para obter mais informações, consulte Instalar o Vulnerability Response Integration [ServiceNow com Veracode.
- Vulnerability Response Integration with NVD, que é necessário se você quiser exibir os dados aprimorados de vulnerabilidades associadas aos componentes carregados. Para obter mais informações, consulte Noções básicas sobre as integrações do NVD.
- Integração abrangente do CWE 2000. Consulte Configurar e executar o trabalho programado para atualizar registros CWE para obter mais informações sobre como ativar este trabalho programado.
- Integração do Snyk Vulnerability Insights. Consulte a documentação do Snyk para obter mais informações.

Uma mensagem é exibida depois que uma aplicação é ativada com sucesso.

6. Atribua as funções a seguir aos usuários.
   - sn_sbom_dm.app_create
   - sn_sbom_dm.app_read
   - sn_sbom_dm.app_write
   - sn_sbom_core.sbom_ingest
   - sn_sbom_core.admin
   - sn_sbom_resp.sbom_analyst
   - sn_sbom_resp.manage_avi_rule
7. **Opcional:** Atribua usuários ao grupo App-Sec Manager se você estiver criando itens vulneráveis de aplicação para vulnerabilidades em seus dados SBOM importados.

   (Optional) Usuários atribuídos ao grupo do App-Sec Manager priorizam e gerenciam itens vulneráveis da aplicação. Os usuários neste grupo herdam muitas das funções necessárias para ler e editar registros e configurar as aplicações compatíveis com a aplicação Application Vulnerability Response e seus fluxos de trabalho de correção.

O que Fazer Depois

Carregue seus arquivos SBOM. Para obter mais informações, consulte Carregar Lista de materiais de software arquivos manualmente e Carregando Lista de materiais de software arquivos usando uma REST API.

Como usar o espaço da lista de materiais de software

As aplicações SBOM permitem que você carregue arquivos e exiba detalhes de entidades e inventários de componentes no espaço Lista de materiais de software (SBOM).

As aplicações SBOM permitem que você execute as seguintes tarefas:

1. Carregue arquivos com uma API ou manualmente.

   Para obter mais informações, consulte Carregando Lista de materiais de software arquivos usando uma REST API e Carregar Lista de materiais de software arquivos manualmente.

2. Revise os componentes da lista de materiais carregados no espaço. A forma como você revisa os componentes depende dos aplicativos instalados.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Para obter mais informações, consulte Exibição de relatórios e painéis no espaço Lista de materiais de software.

3. Avalie sua exposição a riscos e crie itens vulneráveis da aplicação para componentes que tenham vulnerabilidades associadas.
   - Identifique se alguma vulnerabilidade conhecida está associada a componentes de software.
   - Revise os detalhes aprimorados da inteligência de vulnerabilidade, como informações de versão, disponibilidade de versões fixas e informações de licenciamento para ajudá-lo a resolver itens vulneráveis.

   Para obter mais informações, consulte Exibição de relatórios e painéis no espaço Lista de materiais de software e Criação de regras para itens vulneráveis da aplicação no espaço Lista de materiais de software.

Carregando Lista de materiais de software arquivos usando uma REST API

Revise as informações a seguir antes de carregar arquivos Lista de materiais de software usando uma API.

REST API

Para carregar dados com uma API, use o seguinte endpoint REST de script. A função sn_sbom_core.sbom_ingest é necessária.

<host_name*/api/sbom/core/upload*.

Nota:
<host_name>é o nome da sua instância ServiceNow .

Depois que um SBOM é processado com sucesso, onde você exibe os registros carregados depende dos aplicativos que você está usando.

- Se você estiver usando SBOM Resposta, o registro de entidade da lista de materiais será exibido na lista de status de ingestão SBOM no módulo Fila da lista de materiais no espaço SBOM.
- Se você estiver usando o SBOM Core, navegue até **Núcleo de SBOM** > **Status de ingestão da lista de materiais**.

Usando a REST API

Você pode carregar somente SBOM arquivos no formato CycloneDX JSON.

Se o usuário que chama for autenticado com sucesso e tiver a função sn_sbom_core.sbom_ingest em sua instância ServiceNow, você poderá acessar a API de fora da sua instância para carregar os dados SBOM.

O conteúdoSBOM pode ser enviado para a API como um corpo da solicitação HTTP ou por meio de uma solicitação de linha de comando com um arquivo de dados SBOM. Por exemplo, você pode usar a ferramenta de linha de comando *curl*, desde que os usuários tenham seu próprio processo para gerenciar os arquivos.

Além disso, você pode incluir o sys_id do modelo de produto e a aplicação de negócios em seus parâmetros de consulta. A entidade da lista de materiais será mapeada para esses parâmetros se você os incluir. Os seguintes parâmetros são compatíveis:

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- productModelId
- businessApplicationId

Cada chamada de API é enfileirada e um sys_id do registro enfileirado é retornado como a resposta da API.

Por meio da REST API, os dados SBOM são enviados para sua instância Now Platform.

Depois que os dados são carregados, eles são analisados. Antes que os dados sejam analisados, os seguintes requisitos são verificados:

- Os dados de entrada são verificados se são JSON válidos.
- O formato de lista de materiais é compatível. Para esta integração, somente o formato CycloneDX é compatível.
- Os campos mínimos estão disponíveis para que os dados possam ser analisados.

Depois que essas verificações forem verificadas, uma entrada será feita na tabela Lista de materiais [sn_sbom_doc] com os dados SBOM de entrada como anexo.

A regra de negócios *`Process BOM file`* é acionada automaticamente como resultado da inserção do registro e da análise de dados.

Nota:
Esta regra de negócios é ativada durante a instalação do SBOM Core por padrão.

Todos os componentes listados em um SBOM têm um tipodefinido.

- Componentes para os quais os arquivos SBOM foram carregados são considerados entidades da lista de materiais.
- Os componentes listados como type=library são considerados componentes de terceiros.

Tópicos relacionados

Exibindo o status de upload de Lista de materiais de software arquivos

Exibição de relatórios e painéis no espaço Lista de materiais de software

Carregar Lista de materiais de software arquivos manualmente

Carregar arquivos Lista de materiais de software (SBOM) manualmente.

Antes de Iniciar

Você pode carregar somente SBOM arquivos no formato CycloneDX JSON.

Função necessária: sn_sbom_core.sbom_ingest

Procedimento

1. Carregar arquivos manualmente.

   O método usado para carregar seus arquivos depende se você tem as aplicações SBOM Core ou SBOM Response instaladas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

2. **Opcional:** Carregar arquivos SBOM importados pelo Veracode Vulnerability Integration.

> **Nota:**
> Você pode carregar arquivos Veracode no formato CycloneDX JSON somente se tiver instalado e ativado a integração [Veracode com Application Vulnerability Response. Consulte Veracode Vulnerability Integration para obter mais informações.

Resultado

Depois que um SBOM é processado com sucesso, onde você exibe o status do upload depende dos aplicativos que você está usando.

- Se você estiver usando SBOM Resposta, o registro de entidade da lista de materiais será exibido na lista de status de ingestão SBOM no módulo Fila da lista de materiais no espaço SBOM.
- Se você estiver usando o SBOM Core, navegue até **Núcleo de SBOM** > **Status de ingestão da lista de materiais**.

Tópicos relacionados

Carregando Lista de materiais de software arquivos usando uma REST API

Exibição de relatórios e painéis no espaço Lista de materiais de software

Os analistas de vulnerabilidade exibem arquivos de lista de materiais de software carregados em registros, visualizações de dados, bem como inteligência de vulnerabilidade aprimorada no espaço Lista de materiais de software (SBOM).

Requisitos para exibir dados

Núcleo de SBOM

A partir da v2.1 da aplicação SBOM Core, você pode exibir as entidades da lista de materiais e uma lista de componentes carregados na página inicial (landing) e no módulo Componentes no espaço do SBOM. Antes da v2.1, navegue até **Núcleo de SBOM** > **Status de ingestão da lista de materiais** para exibir os componentes.

Resposta de SBOM

A aplicação SBOM Response fornece visualizações de dados com informações detalhadas sobre entidades da lista de materiais, entidades com vulnerabilidades e itens vulneráveis da aplicação ativos na página inicial do SBOM Workspace. O espaço com SBOM Response inclui os seguintes módulos:

- Página inicial: visualizações de dados e detalhes de vulnerabilidade aprimorados.
- Componentes — Informações de versão e correção dos componentes.
- Regras de criação de AVIT (item vulnerável da aplicação) — Condições para quando os itens vulneráveis da aplicação (AVITs) são criados.
- Fila da lista de materiais — Status e histórico de upload de arquivo.
- Lista — Registros AVIT para seus componentes vulneráveis e bibliotecas (NVD, CWE e vulnerabilidades da aplicação).

Os tópicos a seguir fornecem mais informações sobre como localizar detalhes sobre seus componentes no Lista de materiais de software Espaço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

- Revisando a página inicial no espaço Lista de materiais de software
- Revisando o módulo Componentes no espaço Lista de materiais de software
- Exibindo o status de upload de Lista de materiais de software arquivos
- Verificando uma entidade Lista de materiais de software para vulnerabilidades

Revisando a página inicial no espaço Lista de materiais de software

Os dados carregados são acumulados para as visualizações na página inicial (Inicial) no espaço Lista de materiais de software (SBOM). Os dados são modificados depois de carregar arquivos para que os analistas de vulnerabilidade possam ver as tendências e revisar as informações atuais sobre seus componentes.

Exibição da página inicial

Funções necessárias:

- Iniciando com v2.1 do SBOM Core - sn_sbom_resp.sbom_analyst
- Antes da v2.1 do SBOM Core - sn_sbom_resp.admin

1. Navegar até **Espaços** > **Espaço de SBOM**. Por padrão, a página principal (Página inicial) é exibida.

   O que você pode ver no módulo depende dos aplicativos que você instalou.

Aplicação instalada	Descrição
Se você instalou o SBOM Core	a partir da v2.1, uma lista de entidades da lista de materiais. A lista inclui o Nome, o Classificador (Aplicação, Contêiner, Biblioteca e assim por diante) e a contagem de componentes de cada entidade. Uma entidade de lista de materiais se refere ao componente de nível raiz em um arquivo SBOM para o qual um documento SBOM foi gerado e carregado. Antes da v2.1, navegue até **SBOM Core** > **Status de ingestão** da lista de materiais para exibir a lista de entidades da lista de materiais.
Se você instalou o SBOM Response	, as visualizações de dados a seguir serão exibidas. ○ Todas as entidades da lista de materiais: um detalhamento das entidades da lista de materiais por tipo: aplicação, contêiner, biblioteca e outros. Uma entidade de lista de materiais se refere ao componente de nível raiz em um arquivo SBOM para o qual um documento SBOM foi gerado e carregado.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação instalada	Descrição
	○ Entidades da lista de materiais com vulnerabilidades: entidades que têm uma vulnerabilidade associada a qualquer componente do qual dependem. Se uma dependência de entidade tiver uma vulnerabilidade **crítica**, a severidade da entidade será considerada crítica. ○ AVIs ativos - A tendência do número de itens vulneráveis da aplicação (IVA) criados a cada dia. As visualizações de dados exibem dados dos últimos 30 dias. O intervalo de 30 dias não é editável. Esses dados ficam disponíveis depois que você revisa e configura as regras de criação para itens vulneráveis da aplicação. Para obter mais informações, consulte Criação de regras para itens vulneráveis da aplicação no espaço Lista de materiais de software.

2. Selecione um cartão de visualização de dados para ver sua lista de registros.
3. Selecione a guia **Início** para retornar à página principal.
4. Selecione um registro na **lista Entidades** da lista de materiais.

   O nome e a versão da entidade são exibidos na parte superior do registro, por exemplo, SNC-SECOPS-SIR2.0.

5. Selecione as guias no registro da entidade para revisar os dados.
   a. Se não for selecionado, selecione a guia **Visão geral**.

   Revise os dados. Se um campo não estiver preenchido neste registro, os dados não foram incluídos com os arquivos SBOM que você carregou.

Nome	Descrição
Nome Nome	da entidade.
Classificador	Tipo de entidade, por exemplo, uma aplicação, componente ou biblioteca.
Versão	Número da versão da entidade.
Fornecedor	O produto que forneceu a entidade.
Modelo do produto	Se não houver nenhum modelo de produto existente ou se você não incluir um no momento do carregamento de SBOM por meio da API, um será criado. O nome da entidade é usado para o registro do modelo do produto, por exemplo SNC-SECOPS-SIR2.0.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

b. Selecione a guia **Depende de**.

Todas as dependências desta entidade são listadas, bem como classificadores, por exemplo, Biblioteca. O número da versão, Licençase outras informações são exibidos.

Selecionar um link nesta lista abre um registro. Sua guia é exibida abaixo das guias Página inicial e Registro da entidade. O registro aberto pode incluir as seguintes listas relacionadas que você pode revisar: Visão geral, Hashes, Entidades da lista de materiais, Vulnerabilidades e itens vulneráveis da aplicação (AVITs).

A lista relacionada Entidades da lista de materiais exibe todas as entidades nas quais este item exibido é usado.

c. Selecione a guia **Vulnerabilidades** para ver as vulnerabilidades associadas a uma dependência desta entidade.

Para obter mais informações sobre as vulnerabilidades exibidas para uma entidade, consulte Exibindo o status de upload de Lista de materiais de software arquivos.

d. Selecione a guia **AVIs** para ver se há itens vulneráveis da aplicação para esta entidade.

Revisando o módulo Componentes no espaço Lista de materiais de software

O módulo Componentes no espaço Lista de materiais de software (SBOM) exibe informações atuais sobre combinações vulneráveis, obsoletas, abandonadas e de alto risco para os componentes importados.

Exibição do módulo Componentes

Funções necessárias:

- Iniciando com v2.1 do SBOM Core - sn_sbom_resp.sbom_analyst
- Antes da v2.1 do SBOM Core - sn_sbom_resp.admin

Navegar até **Espaços** > **Espaço de SBOM** > **Componentes**.

O que você pode ver no módulo depende dos aplicativos que você instalou.

Aplicação instalada	Descrição
Se você instalou o SBOM Core	A partir da v2.1, um inventário de todos os componentes carregados que inclui as seguintes informações: • Nome • Descrição • Versão • Contagem de entidades da lista de materiais
Se você instalou o SBOM Response	A partir da v3.1 do SBOM Response, selecione um gráfico ou um número no gráfico para exibir uma lista de registros associados. **Todos os componentes**

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação instalada	Descrição
	A lista de componentes **obsoletos** e **abandonados**, bem como aqueles com pelo menos uma vulnerabilidade na contagem total de componentes. Essas contagens podem ajudar a identificar componentes que requerem sua atenção. Esses subconjuntos de componentes podem não corresponder à contagem total de componentes porque todos os seus componentes podem não se encaixar nessas categorias. • A versão de um componente obsoleto está mais de duas versões principais atrás da versão mais recente e dois anos atrás da versão mais recente. • Um componente abandonado não é atualizado há mais de dois anos. • Componentes vulneráveis são componentes que têm vulnerabilidades com uma severidade **Alta** ou maior. **Combinações de alto risco** Componentes de alto risco podem exigir sua atenção imediata. A integração Deps.dev, que é instalada quando você instala a aplicação de resposta SBOM, fornece a inteligência de pacotes para componentes nos estados **Obsoleto** e **Abandonado**. Se a integração do Snyk Vulnerability Insights estiver instalada, você poderá ver as informações de correção de uma vulnerabilidade em um componente. Observe que as correções podem não estar disponíveis para todos os componentes. As combinações importadas de alto risco são compostas por componentes obsoletos e abandonados com pelo menos uma vulnerabilidade grave (**Crítica** ou **Alta**) que você pode corrigir com atualizações,

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Aplicação instalada	Descrição
	substituições ou outro tipo de reparo. O status **Totalmente corrigível** significa que um componente tem uma versão disponível que pode corrigi-lo. A porcentagem do número total de componentes de alto risco que têm versões corrigíveis é anotada. **Componentes vulneráveis que podem ser corrigidas** Totais e detalhamentos dos componentes com vulnerabilidades **Críticas**, **Altas**, **Médias**e **Baixas** e se algumas ou todas as suas vulnerabilidades podem ser corrigidas. Se um componente tiver mais de uma vulnerabilidade, a vulnerabilidade mais crítica terá precedência. O status de capacidade de correção: • Concluído - Há versões de correção para todas as vulnerabilidades associadas à versão atual do componente. • Parcial - há uma versão de correção para pelo menos uma, mas não todas as vulnerabilidades associadas à versão atual do componente. **Componentes por licença** Totais e detalhamentos de componentes por licenças. A Lista de Componentes nos gráficos permite que você veja o nome, a descrição, a versão e as contagens de entidade. No painel direito, você pode exibir um histórico de versões. A versão atual é realçada no histórico de versões. As colunas Vulnerabilidades e exposição comuns (**CVE**) e **Capacidade** de correção também são exibidas.

Como avaliar o risco com a inteligência de vulnerabilidade

Consulte Verificando uma entidade Lista de materiais de software para vulnerabilidades para obter mais informações sobre como revisar dados de inteligência de vulnerabilidade no espaço.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Criação de regras para itens vulneráveis da aplicação no espaço Lista de materiais de software

Antes de ver os itens vulneráveis da aplicação (AVITs) no espaço da lista de materiais de software (SBOM), você deve configurar as condições sob as quais os AVITs são criados.

AVITs no espaço SBOM

Se você instalou e ativou a aplicação SBOM Response, os AVITs serão criados para arquivos SBOM se algum dos dados importados corresponder às condições das regras de criação de AVIT existentes.

As aplicações SBOM Response e Vulnerability Response são necessárias para configurar regras para criar itens vulneráveis da aplicação (AVITs) automaticamente e corrigi-los com o fluxo de trabalho do Application Vulnerability Response. Para obter mais informações, consulte Explorar o Lista de materiais de software.

Você deve adicionar regras de criação de AVIT no espaço SBOM antes de criar AVITs para as vulnerabilidades encontradas nos dados SBOM ingeridos. Os AVITs permitem que você avalie a integridade dos componentes de terceiros em suas aplicações. Um AVIT é criado em sua instância quando uma aplicação é correspondida a um componente que tem uma vulnerabilidade associada.

No espaço SBOM, você pode exibir somente AVITs de SBOM. No entanto, você pode exibir AVITs de SBOM junto com outros tipos de itens vulneráveis no Vulnerability Manager Workspace no Vulnerability Response. Você pode exibir todos os AVITs que foram criados no espaço do SBOM no módulo de lista. O módulo de lista também inclui todas as entradas de NVD e CWE e as vulnerabilidades da aplicação.

Se você tiver a integração de vulnerabilidade Snyk ou tiver executado a integração OSV.dev, se as informações de correção estiverem disponíveis, elas serão exibidas em uma lista relacionada no registro AVIT.

Você também pode atribuir AVITs para correção com base em recomendações de listas de vulnerabilidades conhecidas, como o National Vulnerability Database (NVD). Um trabalho programado é acionado e, se as condições das regras de criação corresponderem aos dados ingeridos, os AVITs serão criados.

Você pode rastrear e corrigir AVITs configurando regras personalizadas.

Consulte Criar uma regra de item vulnerável da aplicação no espaço Lista de materiais de software para obter informações sobre como criar uma regra.

SBOM AVITs em Vulnerability Manager Workspace em Vulnerability Response

Você pode exibir quaisquer SBOM AVITs criados no espaço SBOM no Vulnerability Manager Workspace se você tiver acesso a ele.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Nota:
Para exibir somente SBOM AVITs da lista de itens vulneráveis da aplicação no Vulnerability Manager Workspace em vez de todos os AVITs, defina a condição **[Source] [is] [SBOM] E [Scan type] [is] [SBOM-SCA]** na aplicação Vulnerable Tabela de itens [sn_vul_app_vulnerable_item]. Para exibir a tabela, navegue em sua instância até **Todos** e insira **sn_vul_app_vulnerable_item.list** no navegador de filtros.

Para obter mais informações sobre o Vulnerability Manager Workspace, como exibir tópicos de observação, esforços de correção de aplicação e regras de tarefa de correção de aplicação para AVITs que são configurados na aplicação Vulnerability Response no Vulnerability Manager Workspace, consulte Usar tópicos de observação no Vulnerability Manager Workspace.

Tarefas de correção (AVULs) são criadas a partir de AVITs e atribuídas automaticamente a grupos para correção com base em suas regras de atribuição. Para obter mais informações sobre como criar essas regras, consulte os seguintes tópicos:

- Criar ou editar Vulnerability Response regras de atribuição
- Criar ou editar Vulnerability Response regras de tarefa de correção e Criar um esforço de correção no Vulnerability Manager Workspace.

Exibindo o status de upload de Lista de materiais de software arquivos

Verifique o status de carregamento dos arquivos da lista de materiais de software (SBOM) que você carrega no módulo Fila da lista de materiais no espaço Lista de materiais de software (SBOM). Rastreie os arquivos que você carregou com sucesso, seu histórico de upload e erros.

Função necessária:

- Iniciando com v2.1 do SBOM Core - sn_sbom_resp.sbom_analyst
- Antes da v2.1 do SBOM Core - sn_sbom_resp.admin

1. Exiba seu status de upload.

   O método usado para exibir o status de carregamento depende dos aplicativos instalados.

   As informações de status na tabela Lista de materiais [sn_sbom_doc_list] e no módulo Fila da lista de materiais incluem formatos da lista de materiais, status de ingestão e tempo de geração da lista de materiais. A coluna Status da ingestão da lista de materiais inclui os seguintes estados:

   - Em fila - SBOM dados foram carregados.
   - Processamento - Os dados do componente estão sendo processados como parte da importação.
   - Processado — A ingestão de dados foi concluída com sucesso.
   - Erro: ocorreu um erro durante o processamento.

   Além do status dos arquivos carregados, você pode exibir listas de componentes que ingeriu selecionando um registro de entidade da lista de materiais.

2. Acesse mais informações sobre erros e status de upload selecionando o ícone de engrenagem e o ícone de e adicionando campos como **Categoria** de **erro e Detalhe**do erro.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Verificando uma entidade Lista de materiais de software para vulnerabilidades

Determine se alguma vulnerabilidade está associada aos componentes em um arquivo Lista de materiais de software (SBOM) carregado.

As seguintes aplicações devem ser instaladas e ativadas antes que você possa exibir as vulnerabilidades e os dados de vulnerabilidade aprimorados:

- SBOM Resposta
- Integração do Vulnerability Response com trabalhos do NVD e CWE
- Vulnerability Response

Para obter mais informações, consulte Explorar o Lista de materiais de software.

Função necessária:

- A partir da v2.1 do SBOM Core - sn_sbom_resp.sbom_analyst
- Antes da v2.1 do SBOM Core - sn_sbom_resp.admin

1. Navegar até **Todos** > **Espaço de SBOM** > **Componentes**.
2. Antes da versão 3.1 do SBOM Response, exiba as informações de vulnerabilidade por meio de uma visualização ou de um registro de componente.

Como avaliar o risco com a inteligência de vulnerabilidade

A partir da versão 3.1 do SBOM Response, exiba mais dados de vulnerabilidade aprimorados com o SBOM Response em registros de componente. Os trabalhos programados da aplicação SBOM Response, Vulnerability Response, integração do National Vulnerability Database (NVD) e Common Weakness Enumeration (CWE) descritos em aplicações compatíveis devem ser instalados e ativados.

1. Selecione o gráfico **Todos os componentes** para exibir a lista de registros associados.
2. Selecione um link na coluna **Nome** para abrir um registro.

   Estados, **Obsoleto**, **Abandonado**e **Vulnerável** são exibidos abaixo do nome do componente. Um componente pode ter qualquer combinação desses estados. Se nenhum estado for exibido, o componente não está obsoleto, abandonado ou vulnerável.

   Revise a versão atual e a versão mais recente publicada. No painel direito, você pode exibir um histórico de versões. A versão atual é realçada no histórico de versões e sua localização na lista pode fornecer informações sobre o motivo pelo qual um componente está **Obsoleto**, **Abandonado**e **Vulnerável**. Por exemplo, você pode estar usando uma versão mais antiga de um componente.

3. Selecione as guias relacionadas **Visão geral**, **Hashes**, **Entidades da lista**de materiais, **Vulnerabilidades**e **AVIs** no registro.
   - Visão geral - Um resumo dos detalhes do componente.
   - Entidades da lista de materiais - Uma lista das entidades associadas a este componente.
   - Hashes — Se importados, os hashes serão exibidos.
   - Vulnerabilidades - Informações sobre vulnerabilidades conhecidas associadas a este componente. Se esta lista estiver vazia, não há vulnerabilidades conhecidas.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Se a lista estiver preenchida, selecione a guia para exibir IDs de vulnerabilidade, resumos e outras informações de vulnerabilidade dos dados de Vulnerabilidades e exposições comuns (CVE) e Enumeração de fraqueza comum (CWE) associados a este registro. Os CVEs são divididos por severidade, os CWEs são divididos pela probabilidade de o componente ser explorado. Você pode exibir os registros de vulnerabilidade aprimorados nas aplicações Vulnerability Response ou Application Vulnerability Response selecionando o link do ID de vulnerabilidade.

- AVIs (AVITs) - Itens vulneráveis da aplicação associados a este componente se você tiver criado regras de criação de AVIT que correspondam o componente a uma vulnerabilidade conhecida. A aplicação Vulnerability Response (AVR) relaciona uma vulnerabilidade a uma aplicação para criar um registro AVI. Para obter mais informações, consulte Criação de regras para itens vulneráveis da aplicação no espaço Lista de materiais de software.

Componentes instalados com aplicações Lista de materiais de software

Vários tipos de componentes são instalados com a ativação das aplicações Lista de materiais de software, incluindo tabelas, funções de usuário e trabalhos programados.

Funções instaladas

Título da função [nome]	Descrição	Contém as funções
SBOM gravar [sn_sbom_dm.app_write], SBOM criar [sn_sbom_dm.app_create], SBOM ler [sbom_dm.app_read]	Essas funções são instaladas com a aplicação Modelo de dados para SBOM. Eles permitem que você leia, crie e edite registros em SBOM tabelas.	Nenhum(a)
SBOM Ingestões de núcleos [sn_sbom_core.sbom_ingest] e SBOM Administrador de núcleo [sn_sbom_core.admin]	Essas funções são instaladas com a aplicação Core SBOM. A função sn_sbom_core.sbom_ingest permite que você carregue SBOMs manualmente e por meio da REST API. A função sn_sbom_core.admin permite criar, ler, editar dados e carregar SBOMs. Esta função também concede acesso aos módulos do Core SBOM em sua instância. Ele herda as funções da aplicação	• sn_sbom_dm.app_write • sn_sbom_dm.app_create • sn_ sbom_dm.app_read

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Título da função [nome]	Descrição	Contém as funções
	Modelo de dados para SBOM.	
Analista de SBOM [sn_sbom_resp.sbom_analyst]	Esta função é instalada com a aplicação de resposta SBOM. Ele herda a função sn_sbom_core.admin e permite que você acesse o espaço SBOM.	• sn_sbom_core.admin • sn_sbom_dm.app_write • sn_sbom_dm.app_create • sn_ sbom_dm.app_read • sn_sbom_resp.manage_avi_rule • Tabela sn_sbom_config_rule

Tabelas instaladas com as aplicações SBOM

As tabelas listadas na tabela a seguir são instaladas com a aplicação Modelo de dados para SBOM.

Modelo de dados para SBOM tabelas

Tabela	Descrição
Documento de SBOM [sn_sbom_doc]	Contém as entidades da lista de materiais que você carregou.
SBOM componente [sn_sbom_component]	Contém componentes importados SBOM, classificadores e versões que estão incluídos no componente primário.
SBOM relacionamento do componente [sn_sbom_comp_relationship]	Contém componentes e suas dependências.
SBOM componente da lista de materiais m2m [sn_sbom_m2m_bom_comp]	Contém os mapeamentos de componente da lista de materiais.
Licença do SBOM [sn_sbom_license]	Contém os IDs de licença de código aberto usados para componentes.
SBOM fornecedor [sn_sbom_supplier]	Contém a organização que forneceu o componente, que pode ser um fabricante, um distribuídor ou um reempacotador.
SBOM ID do componente	Contém os identificadores do componente.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Modelo de dados para SBOM tabelas

Tabela	Descrição
[sn_sbom_comp_id]	
SBOM propriedades do componente [sn_sbom_comp_property]	Contém as propriedades de nome-valor do componente.
SBOM hash [sn_sbom_hash]	Contém algoritmos de hash de componente.
SBOM contato [sn_sbom_contact]	Contém informações de contato do fornecedor.
SBOM referências externas [sn_sbom_comp_external_ref]	Contém componentes, tipos de componente e URLs externos que documentam sistemas, sites e informações que podem ser relevantes, mas não estão incluídos com o SBOM.
SBOM grupo de pacotes [sn_sbom_pkg_group]	Contém as informações do grupo de pacotes para cada componente. Várias versões de bibliotecas podem ser usadas em aplicações. Versões dos mesmos componentes são agrupadas e adicionadas a esta tabela para evitar a extração dos mesmos dados várias vezes.

As tabelas listadas na tabela a seguir são instaladas com a aplicação de resposta SBOM

SBOM Tabelas de resposta

Tabela	Descrição
SBOM configuração de regra de criação [sn_sbom_config_rule]	Contém regras de criação de AVIT usadas no espaço SBOM.
SBOM vulnerabilidades do componente m2m [sn_sbom_m2m_comp_vuln]	Contém os componentes e as vulnerabilidades associadas.
Informações de correção de vulnerabilidade do componente [sn_sbom_comp_vuln_fix_info]	Contém as versões de correção para cada vulnerabilidade de terceiros associada a uma versão do componente.
Informações do relatório do componente [sn_sbom_comp_report_insight]	Contém informações sobre dados obsoletos, abandonados e de capacidade de correção para componentes.
Importações de integrações de Deps	Contém informações da lista de versões importadas de um determinado pacote ou biblioteca.

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

SBOM Tabelas de resposta

Tabela	Descrição
[sn_sbom_deps_integration_import]	
Importações de integrações de OSV [sn_sbom_osv_integration_import]	Contém informações de inteligência de vulnerabilidade para uma determinada versão de um pacote ou biblioteca.
Listas de versão de componentes [sn_sbom_st_version_list]	Contém informações de versão e datas publicadas para componentes.

Trabalhos programados

Trabalho	Descrição
Calcular a Fixabilidade e a Vulnerabilidade do Componente	Calcula informações sobre como corrigir componentes com vulnerabilidades e a probabilidade de você corrigir componentes.
Novos componentes de integração de OSV	Recupera todas as vulnerabilidades conhecidas publicamente associadas a pacotes (bibliotecas) que foram importados após a última execução de integração.
Integração de OSV Abrangente	Recupera todas as vulnerabilidades conhecidas publicamente associadas a todos os pacotes que foram importados.
Integração Deps.dev	Recupera todas as versões conhecidas publicamente dos pacotes e é usado com para identificar componentes nos estados **Obsoleto** e **Abandonado**.
Atualizar vuln_based_criticality em componentes do BOM	Atualiza a criticidade dos componentes com vulnerabilidades.

Tradução automática

Criar uma regra de item vulnerável da aplicação no espaço Lista de materiais de software

Configure as condições sob as quais os itens vulneráveis da aplicação (AVITs) são criados automaticamente no módulo Regras de criação de AVI no espaço Lista de materiais de software (SBOM).

Antes de Iniciar

A aplicação de resposta SBOM será necessária se você quiser criar itens vulneráveis da aplicação. Para obter mais informações, consulte Explorar o Lista de materiais de software.

Função necessária: sn_sbom_resp.manage_avi_rule.

Procedimento

1. Navegar até **Espaço de SBOM** > **Regras de criação de AVI**.
2. Selecione **Novo**.
3. Preencha os campos.

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Campo	Descrição
Nome	Nome da regra.
Ativo	Indica se a regra de criação está ativada.
Ordem de execução	Ordem na qual as regras são avaliadas. A regra com o valor numérico mais baixo é executada primeiro. Por exemplo, você pode criar regras de prioridade mais alta para itens que precisam de tratamento especial ou quando o risco é crítico, portanto, elas são executadas primeiro. Em seguida, crie regras gerais para itens que não requerem tratamento especial. Por fim, crie uma regra padrão para capturar todos os componentes que tenham vulnerabilidades.
Descrição	Descrição da regra para ajudar a diferenciá-la de outras regras.
Condições	Crie as condições sob as quais os itens vulneráveis (IVAs) da aplicação são criados. Por exemplo, você pode selecionar **[Vulnerability > Severity [is] [1-Crítico]** para criar AVITs para componentes que têm vulnerabilidades de alto risco e podem afetar gravemente você. Observe que você pode adicionar mais condições.

4. Selecione **Salvar**.
   Sua regra de criação é executada automaticamente após o próximo carregamento e cria AVIs para componentes que correspondem às suas condições. Você também pode executar a regra sob demanda no módulo Regras de criação de AVI selecionando **Executar agora**.

Resultado

Depois que eles são criados, você pode verificar se um AVIT foi criado especificamente para dados SBOM verificando os valores nos campos **Origem** e **Tipo de verificação** em um registro AVI.

Campo	Valor
Origem	SBOM
Tipo de verificação	SBOM-SCA

Tradução automática

© 2025 ServiceNow, Inc. Todos os direitos reservados.
ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países.
Outros nomes de empresas, nomes de produtos e logotipos podem ser marcas comerciais das respectivas empresas às quais estão associados.